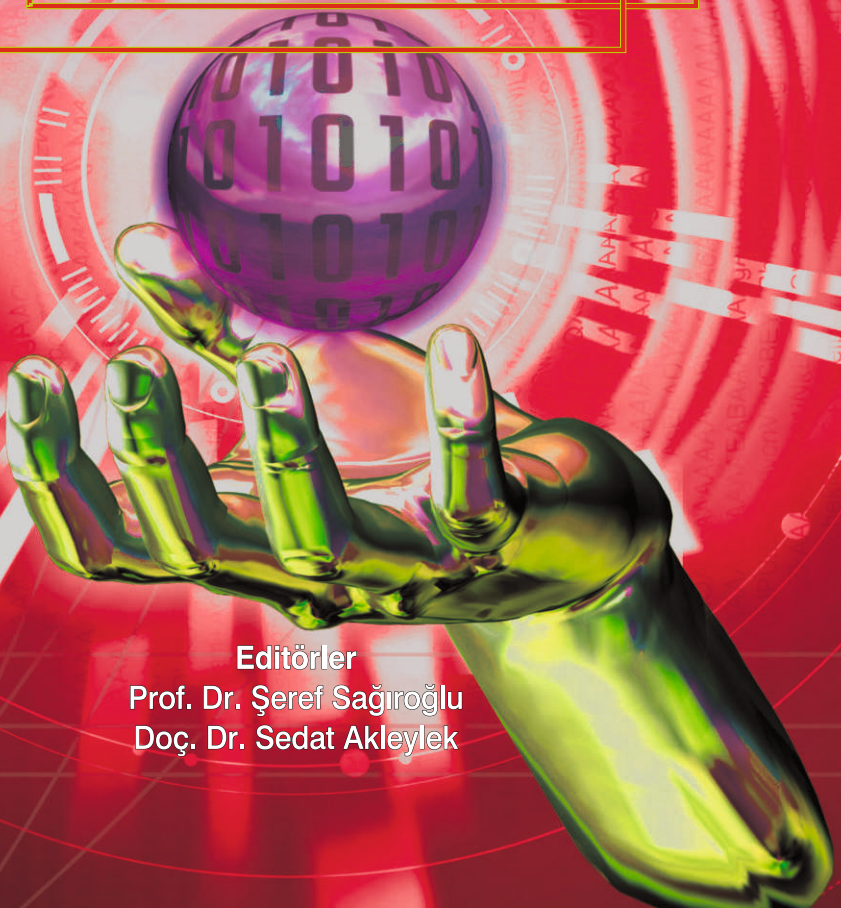
BGD Siber Güvenlik ve Savunma Kitap Serisi 6

Siber Güvenlik ve Savunma

SİBER GÜVENLİK ONTOLOJİSİ, TEHDİTLER VE ÇÖZÜMLER



Editörler
Prof. Dr. Şeref Sağıroğlu
Doç. Dr. Sedat Akleylek

nobel

Siber Güvenlik ve Savunma Kitap Serisi 6:

SİBER GÜVENLİK ONTOLOJİSİ, TEHDİTLER VE ÇÖZÜMLER

Editörler

Prof. Dr. Şeref Sağıroğlu

Doç. Dr. Sedat Akleylek

nobel

Siber Güvenlik ve Savunma Kitap Serisi 6:
SİBER GÜVENLİK ONTOLOJİSİ, TEHDİTLER VE ÇÖZÜMLER
Editör: Prof. Dr. Şeref Sağıroğlu - Doç. Dr. Sedat Akleylek

Yayın No.: 4148
Mühendislik/Teknik No.: 397
ISBN: 978-625-417-877-1
E-ISBN: 978-625-417-876-4
Basım Sayısı: 1. Basım, Haziran 2022

Nobel Yayın Grubu, 1984 yılından itibaren ulusal ve 2011 yılından itibaren ise uluslararası düzeyde düzenli olarak faaliyet yürütmekte ve yayınladığı kitaplar, ulusal ve uluslararası düzeydeki yükseköğretim kurumları kataloglarında yer almaktadır.

Genel Yayın Yönetmeni: Nevzat Argun -nargun@nobelyayin.com-
Genel Yayın Koordinatörü: Gülfem Dursun -gulfem@nobelyayin.com-
Alan Editörü: Sadık Küçükakman -sadik@nobelyayin.com

Sayfa Tasarım: Tarkan Kara -erdal@nobelyayin.com-
Redaksiyon: Sergen Öz -sergen@nobelyayin.com-
Kapak Tasarım: Sezai Özden -sezai@nobelyayin.com-
Görsel Tasarım Uzmanı: Mehtap Yürümez -mehtap@nobelyayin.com-
Baskı Sorumlusu: Yavuz Şahin -yavuz@nobelyayin.com-

Kütüphane Bilgi Kartı

Sağıroğlu, Şeref., Akleylek, Sedat.
Siber Güvenlik ve Savunma Kitap Serisi 6: Siber Güvenlik Ontolojisi, Tehditler ve Çözümler /
Şeref Sağıroğlu, Sedat Akleylek
1. Basım, XVI+ 470 s., 16x23,5 cm. Kaynakça ve dizin var.
ISBN: 978-625-417-877-1
E-ISBN: 978-625-417-876-4

1. Siber Güvenlik Ontolojisi 2. Kişisel Verilerin Korunması İçin Anlamsal WEB Teknolojilerinin Kullanımı 3. Siber Güvenlik Tehdit Bilgisi Paylaşımı 4. Zararlı Yazılımların ve Yayılımlarının Matematiksel Olarak Modellenmesi 5. Kritik Altyapılarda Siber Güvenlik ve Savunma Önerileri 6. Biyometrik Sistemlerde Güvenlik: Saldırı Vektörleri ve Savunma Yolları 7. Dağıtık Hizmet Engelleme / Aksattırma Saldırıları (DDoS) ve Karşı Önlemler 8. Ağ Veri Katmanı Programlama ve Siber Güvenlik 9. Havacılık Sistemlerinde Siber Güvenlik 10. Klavye Deseni ile Kimlik Doğrulama 11. Nesnelerin İnterneti Aygıtlarının Güvenliği İçin Hafif Siklet Kriptografik Algoritmalara Genel Bakış 12. Kuantum Öncesinden Kuantum Sonrasına Eliptik Eğri Kriptografi ve Uygulamaları

Genel Dağıtım

ATLAS AKADEMİK BASIM YAYIN DAĞITIM TİC. LTD. ŞTİ.
Adres: Bahçekapı Mh. 2465 Sk. Oto Sanayi Sitesi No:7 Bodrum Kat, Şaşmaz/ANKARA
Telefon: +90 312 278 50 77 - **Faks:** 0 312 278 21 65 - **Sipariş:** siparis@nobelyayin.com-
E-Satış: www.nobelkitap.com - esatis@nobelkitap.com / www.atlaskitap.com - info@atlaskitap.com

Dağıtım ve Satış Noktaları: Alfa Basım Dağıtım, Arasta, Arkadaş Kitabevi, D&R Mağazaları, Dost Dağıtım, Ekip Dağıtım, Kida Dağıtım, Kitapsan, Nezih Kitabevleri, Pandora, Prefix, Remzi Kitabevleri

Baskı ve Cilt

Meteksan Matbaacılık ve Teknik Sanayi Tic. Anonim Şirketi Sertifika No.: 46519
Beytepe Köy Yolu No.: 3 06800 Bilkent-Çankaya/ANKARA

BÖLÜM YAZARLARI

Bölüm 1
Siber Güvenlik Ontolojisi - I
Şeref Sağıroğlu

Bölüm 2
Kişisel Verilerin Korunması İçin Anlamsal WEB Teknolojilerinin Kullanımı
Özgü Can

Bölüm 3
Siber Güvenlik Tehdit Bilgisi Paylaşımı
Ali Melih Kanca - Şeref Sağıroğlu

Bölüm 4
Zararlı Yazılımların ve Yayılımlarının Matematiksel Olarak Modellenmesi
Yunus Geçer

Bölüm 5
Kritik Altyapılarda Siber Güvenlik ve Savunma Önerileri
Mehmet Yavuz Yağcı - Ebu Yusuf Güven - Sevda Altan - Muhammed Ali Aydın

Bölüm 6
Biyometrik Sistemlerde Güvenlik: Saldırı Vektörleri ve Savunma Yolları
Ceren Güzel Turhan - Eyüp Burak Ceyhan - Şeref Sağıroğlu

Bölüm 7
Dağıtık Hizmet Engelleme / Aksattırma Saldırıları (DDoS) ve Karşı Önlemler
Süreyya Atasever - İlker Özçelik - Şeref Sağıroğlu

Bölüm 8
Ağ Veri Katmanı Programlama ve Siber Güvenlik
Özgür Yürekten

Bölüm 9
Havacılık Sistemlerinde Siber Güvenlik
Nurşah Çevik - Sedat Akleylek

EDİTÖRLERDEN

Siber Güvenlik ve Savunma Kitapları Serisi, ülkemizin **bilgi ve siber** güvenliği **ile savunmasının** gelişimine katkı sağlamak amacıyla hazırlanan açık kaynak bir kitap serisidir.

Tehditlerin, saldırıların veya açıklıkların artması, boyut ve yön değiştirmesi, farklılaşması, siber tehdit ekosisteminin gittikçe güçlenmesi, kritik altyapıların daha çok hedef haline gelmesi, bilgi ve kaynak hırsızlıklarının çoğalması, yeraltı yapıların etkinleşmesi, siber tehditlerin artık savaşa dönüşmesi, siber suç ve suçlularının çoğalması, siber terörün yaygınlaşması vb. olumsuzlukların hızla artması, yapılacak mücadele, alınacak önlem ve karşı koyulacak yaklaşımlara duyulan ihtiyacı artırmıştır. Kapsamlı bir mücadele için; ulusal strateji ve eylem planlarına, araştırma merkezlerine, gelişmiş altyapı ve araçlara, lisans ve lisansüstü programlara, nitelikli insan kaynağına, yerli ve milli ürünlerin geliştirilmesine, siber güvenlik ve savunma ekosisteminin oluşturulmasına, ulusal siber olaylara müdahale ekiplerinin sayısının ve niteliğinin arttırılmasına, savunma sanayinin gelişmesine katkı sağlayacak yeni çalışma ve projelerin hayata geçirilmesine mevcut sistem, yapı ve organizasyonların kapsamının büyütülmesine, yeni yapıların kurulmasına ihtiyaç vardır. Duyulan bu ihtiyacı bir nebze de olsa karşılamak için bu kitap serisi hazırlanmıştır. Bu kitap serisinde, 100'e yakın farklı konu irdelenmektedir. Her bölümde, farklı bir konu siber güvenlik ve savunma kapsamında ele alınmakta, değerlendirilmekte ve alınması gereken önlemlere yer verilmektedir.

Bu kitap serisinde sunulan konu başlıkları, ülkemizde bu alanda çalışan akademisyenler, uzmanlar ve çalışanlar ile paylaşılmış ve bu kitap serisine katkı sağlamaları istenilmiştir. Zamanı uygun olan, katkı vermek isteyen uzman veya akademisyenler belirlenen bir konuda bölüm yazarı olmaları için davet edilmişlerdir. Belirlenen süre içerisinde bölümlerini tamamlayan yazarlarımızın eserleri ise uygun olan ciltlerde basılmaktadır. Siber güvenlik ve savunmaya çok kapsamlı bir bakış sunmayı amaçlayan ve farklı başlıkları bir araya toplayan bu kapsamlı eserin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

Bu kitap serimizin **altıncı cildinde**; "***Siber Güvenlik Ontolojisi, Tehditler ve Çözümler***" konuları ele alınmış ve 12 farklı bölüm altında siber güvenlik ve savunma konuları sunulmuştur. Her bir bölüm; ülkemizde bu alana katkı sağlayan, bu alanda eğitim almış, tez hazırlamış, çalışmalar yapmış değerli akademisyen, kamu çalışanı ve üst düzey yöneticiler tarafından hazırlanmıştır. Editörler olarak bu kitap serisinin özenle hazırlanmasına dikkat edilmiştir. Ayrıca; kitapta konu bütünlüğü ve devamlılığının sağlanmasına özen gösterilmiş, yazarlara konu içeriği ve başlıklarla ilgili olarak bazı önerilerde bulunulmuş, düzeltmeler yapılması istenilmiş, bölümler intihal taramasından geçirilmiş ve sonuçta yapılan değişiklikler dikkate alınarak bu kitap hazırlanmıştır.

Bu kitabın; siber güvenlik ve savunma konusunda yapılacak olan çalışmalara ışık tutması, yeni çalışmaların yapılmasına katkılar sağlaması, bu alanda ihtiyaç duyulan Türkçe akademik kaynağın bir nebze de olsa karşılanması ve en önemlisi ise açık kaynak felsefesinin yaygınlaşması ile bu alanda ihtiyaç duyulan güncel kaynaklara erişimi kolaylaştırıcı **bir başvuru kitap serisi** olması beklenmektedir. Bu eser serisi **açık kaynak** olarak, internette yayımlanmaktadır.

Bu kitapta yazarlarımız; alan uzmanlıklarına göre bölümleri hazırlamışlar, kişisel ve kurumsal bilgi birikimlerini hazırladıkları bölümlerde sunmuşlar, hazırladıkları bölümlerin açık kaynak olarak yayımlanmasını kabul etmişler ve bu kitabın basımı ve dağıtımı ile ilgili olarak herhangi bir telif hakkı talep etmemişlerdir. Yazarlarımıza, bu kitap serisinin editörleri olarak çok özel teşekkürlerimi ve şükranlarımı sunarız.

Kitabın titizlikle hazırlanmasında, kontrolünde ve basılmasında başta yazarlarımız olmak üzere emeği geçen tüm paydaşlarımıza, bu fikrimizin hayata geçirilmesine katkı sağlayan dostlarımıza teşekkürlerimizi sunarız.

Prof. Dr. Şeref SAĞIROĞLU

- EMO Ankara Şube Başkanı
- BGD Kurucu Üyesi, 2008-2012 Dönem BGD YK Başkanı
- Gazi Üniversitesi Yapay Zeka ve Büyük Veri Analitiği Güvenliği Uygulama ve Araştırma Merkezi Müdürü
- IPv6 Forum Turkey Başkanı
- Bilgi Güvenliği Derneği Ulusal Bilim Kurulu Başkanı
- ISCTurkey Eş Başkanı
- Gazi Üniversitesi MF Bilgisayar Mühendisliği Bölümü Öğretim Üyesi
- FutureTech Genel Müdürü

Doç. Dr. Sedat AKLEYLEK

- BGD Ulusal Bilim Kurulu Üyesi,
- ISCTurkey Akademik Program Başkanı
- 19 Mayıs Üniversitesi MF Bilgisayar Mühendisliği Bölümü Öğretim Üyesi
- Uluslararası Bilgi Güvenliği Bilimi Dergisi (IJISS) Editörü

İÇİNDEKİLER

Bölüm 1

SİBER GÜVENLİK ONTOLOJİSİ - I

Şeref Sağıroğlu

Bu bölüm; 2020'de CyberMag Dergisi Editörü olarak kaleme aldığım "Siber Güvenlik Ontolojisi" yazımda belirttiğim hususların kapsamlı hale getirilmiş halidir. Son yıllarda katıldığım siber güvenlik etkinlikleri, toplantıları ve çalışmalarında, bu konuya sistematik bakış açımızın yeterli seviyede olmadığını gördüğümden kaleme alınmıştır. Siber güvenlik ve savunma konulara, epistomolojik, taksonomik veya semantik olarak yeni yeni bakılmaya başlandığı, terminolojiler, bakış açıları, çözümler veya önerilerin sayısının hızla arttığı bir dönemde yaşıyoruz. Genel izlenimlerim bana; terim ve terminolojilerin iyi anlaşılamadığı veya kavranamadığı, tanımların iyi yapılamadığı veya anlaşılamadığını göstermektedir. Bunun haklı gerekçelerinden birisi de belki güncel hayatımızda sıkça kullanılan "siber" kelimesinin bile TDK'da yer almaması da olabilir. Ayrıca, siber güvenlik ekosistemimiz büyümeye başlasa da siber güvenlik ve savunma alanına katkımızın %1 oranında olması, çalışılan veya proje üretilen konuların ise %20'lik bir dilim içerisine sıkışmış olması, pazarı doğru anlayamama, akademik tarafta da bu konuya gereken önemin verilememesi ve dünya siber güvenlik ekonomisinden de yeteri kadar faydalanılamamasıdır. Bu konunun kapsamının daha iyi anlaşılması, konuya sistematik bakılması ve tüm alanları kapsayışı bakış açılarının geliştirilmesi için, yeni çözümler geliştirilmesine veya yapılan çalışmaların "ontolojik" olarak ta ele alınmasına

ihtiyaç olduğu düşünülmektedir. Kısaca, Bilgi Boşluğu Teorisi açısından bakıldığında ise siber güvenlik bakış açımızda hem bilgi boşluğu hem de stratejik boşluk olduğu görülmektedir. Bunu gidermek veya doldurmak için ise yeteri kadar Türkçe kaynak olmadığı da görüldüğünden, bu kitap serimizde "Siber Güvenlik Ontolojisi" ele alınmıştır. Temel bakış açımızı geliştirmeye yönelik olarak hazırlanan bu bölümde, mümkün olduğunca konu kapsamlı olarak açıklanmaya, sunulmaya, anlatılmaya ve örneklendirilmeye çalışılmıştır.

1.1. TERİM VE TERMİNOLOJİLER

Ontoloji kelimesi, TDK'ya göre "varlık bilimi" olarak ifade edilmektedir. Gerçekliğin doğası ve bunların yapılarını açıklayan bir kavramdır. Bazı kaynaklara göre de temeli varlık olan bir felsefe terimi veya felsefenin bir alt bölümüdür. Ansiklopedilerde ise ontoloji; "**varlık felsefesi"** veya "**varlıkbilim"** olarak "varlığın mahiyetinde varlığın bilimi veya varlıkların incelenmesi" olarak ifade edilmekte, "bilgi bilimi" olarak açıklanmakta hem felsefi hem de bilimsel bilgiyi içeren ve "var olan bir şeyin bilgisi" olarak ta tanımlanmaktadır. Bilim dallarına göre de ontoloji, farklı şekilde tanımlanabilmektedir. Fidan ve Erden [1]; "madde, yaşam, insan, dünya ve evrenle ilgili bir bütünlük arayışı", "hayat ve evren hakkında genel bir görüş", "genel bir ilke bulmaya çalışma" ve temel olarak "bilimsel bilgileri alma ve onların ötesinde bilime yol gösterici görüşler ve hipotezler ortaya koyma" olarak tanımlanmaktadır. Bu farklılığı ifade eden diğer tanımlara bakıldığında ise **Wolf** ontolojiyi "temel ilkeler bilimi"; **Hartmann** ontolojinin "var olanı bir bütünlük içinde ele alma ve bütünüyle varlığın varoluş ilkelerini inceleme"; **Husserl** "anlamlı davranışların içeriğini inceleme"; **Gruber** "bir kavramsallaştırmanın açık bir tanımlaması"; ve **Bater** ise "kavramları ve onların ilişkilerini tanımlama ve ayırt etme, içeriği ve ilişkileri tanımlama, kavramlar arasındaki hiyerarşik ilişkileri resmileştirme ve her birine atıfta bulunmada kullanılacak terimleri belirtme, yapıyı ve terminolojiyi belirleme" olarak tanımlanmaktadır. Nutku [2] çalışmasında, ontolojik bakış açısının çeşitliliğin içinden geçen bütünleyici bir bakış olduğunu, "disiplinlerin özgül sorunlarına müdahale etmeden onların varlık

dayanaklarını gösterdiğini", bilgi teorisinde "insanın var olanların çeşitliliğini ve bağıntılarını bilmeye yönelişindeki değişmezlerle yönelinen nesne alanlarının değişmezleri" ve kısaca "bilginin varlık temelini gösterdiğini" belirtmektedir.

Ontolojiler [23], "en basit anlamda, bir alandaki varlıkların ve varlıklar arası ilişkilerin temsillerini belirleyen ve modelleyen sistemlerdir". Varlıklar ve ilişkiler bileşenlerinden oluşan ontolojilerde; "varlıklara ve ilişkilere verilen adların farklı anlamları olabileceğinden, modellemenin mümkün olması için ortak terimlerin belirlenmesiyle işe başlanır. Böylece, ister kuramsal ister pratik amaçlarla ontolojileri kullanacaklar arasında dilsel bir ortaklaşma sağlanır". Ortak terimlerin belirlenmesi bir başlangıç olsa da, bir siber güvenlik ve savunma makalesinde geçen önemli kelimelerin listelenmesinden öte bir çalışma olup, elde edilen liste alandaki tüm bilim insanları ve uzmanlar tarafından aynı semantik amaçlarla kullanılacaktır. Modellemede kullanılacak varlıklar (insan, yazılım, süreç, saldırı, araç, ortam, vb.) belirlendikten sonra, varlığa atfettiğimiz kategorilere (öznitelik, süreç, vb.) göre sınıflandırılırlar. Bir ontolojideki en önemli sınıflandırma, varlıkların kapsam ilişkisi içinde düzenlendiği taksonomilerdir.

Örneğin, "Mobil kötücül yazılımlar, kötücül yazılımlardan sadece birisidir." ifadesinde kötücül yazılım sınıfı mobil kötücül yazılım sınıfını kapsamaktadır. "İlişkiler, taksonomideki iki ya da daha fazla varlık arasındaki etkileşimi tanımlarlar." [23], İlişkilere örnek olarak bir sürece dahil olmak anlamında "katılmak" ilişkisi ile bir siber saldırı ontolojisinde "saldırı" ve "saldırı türü" varlık arasında yönlendirilmiş "katılmak" ilişkisi vardır: bir saldırı, bir saldırı türüne aittir (katılır). "Kapsam ilişkisinin doğasında taksonomilerin ağaç yapısı vardır, ancak diğer ilişkilerin de varlıklar arasında tanımlanmasından sonra bir yönlendirilmiş çizge ortaya çıkar. Ontolojideki hiyerarşik yapılar—kapsam ilişkisi ile kurulan taksonomiler ve parça-bütün ilişkisi ile kurulan ontolojilerin fonksiyonlarına göre farklılık gösterebilirler" [24]'den aktaran [23]. Dolayısıyla; her alana ait farklı ontolojiler oluşturulabilir. Ontolojik model oluşturma, bakış açısı ve uygulama alanlarına göre farklılık gösterebilir, aynı alan farklı biçimlerde de modellenebilir [23]. En temelde oluşturulma amaçları ve yöntemlerine göre ontolojiler, felsefe, bilim ve teknik olarak ay-

rıştırılmıştır [23]. Felsefe olarak "varlığı varlık olması bakımından araştıran, bir şeye var demenin sınırlarını belirleyen disiplin", bilim olarak "bilimsel bulguların ışığında bir bilim alanına ait varlıkların ve ilişkilerin incelendiği bir tetkik" ve teknik olarak ise "makinelerde bilgiyi temsil etmek için oluşturulan teknolojiler" olarak tanımlanmaktadır.

Farklı bilim dalları temel alındığında ise bu tanımlarda değişiklik olabileceği de literatür incelendiğinde görülmektedir. **Sosyal bilimlerde**; "kavramlar, objeler, varlıklar, ilişkiler ve insanlar arasındaki bağlantıları anlama, kavrama ve sorgulama, varlık kategorilerinin temeli bilme ve sosyal dünyayı algılama ve anlamlandırma", **Eğitim biliminde**; "okulun varlık amacını, öğrenmenin katkılarını, uygulanan programların artı ve eksiklerini, etkili öğrenme stratejilerini, öğrenme çıktılarını, kavramlar, objeler, varlıklar ve insanlar arasındaki ilişkiler ile varlık kategorilerinin temeli anlama, kavrama ve sorgulama" ve **Bilgisayar Mühendisliği'nde**; "veriler ve bilgi varlıkları arasındaki kavramlar, ilişkiler ve özelliklerin kendi terminolojisiyle ifade edilmesi ve sunulması" olarak ifade edilebilmektedir.

Sonuç olarak; ontolojilerin her alanda bilinmesi ve anlaşılması, doğru terim ve terminolojilerin kullanılmasıyla mümkündür. Ontolojilerin, ontolojik bakış açılarının ve terminolojilerinin; her alanın gelişmesine, karmaşıklığı gidermeye, alan bilgilerinin oluşturulması, ilişkilendirilmesi ve düzenlenmesine katkılar sağlamanın yanında yeni ontolojilerin geliştirilmesine, karşılaşılabilecek pek çok problemin çözümlenmesine katkılar sağlayacağı açıktır.

1.2. TAKSONOMİ VE ONTOLOJİ

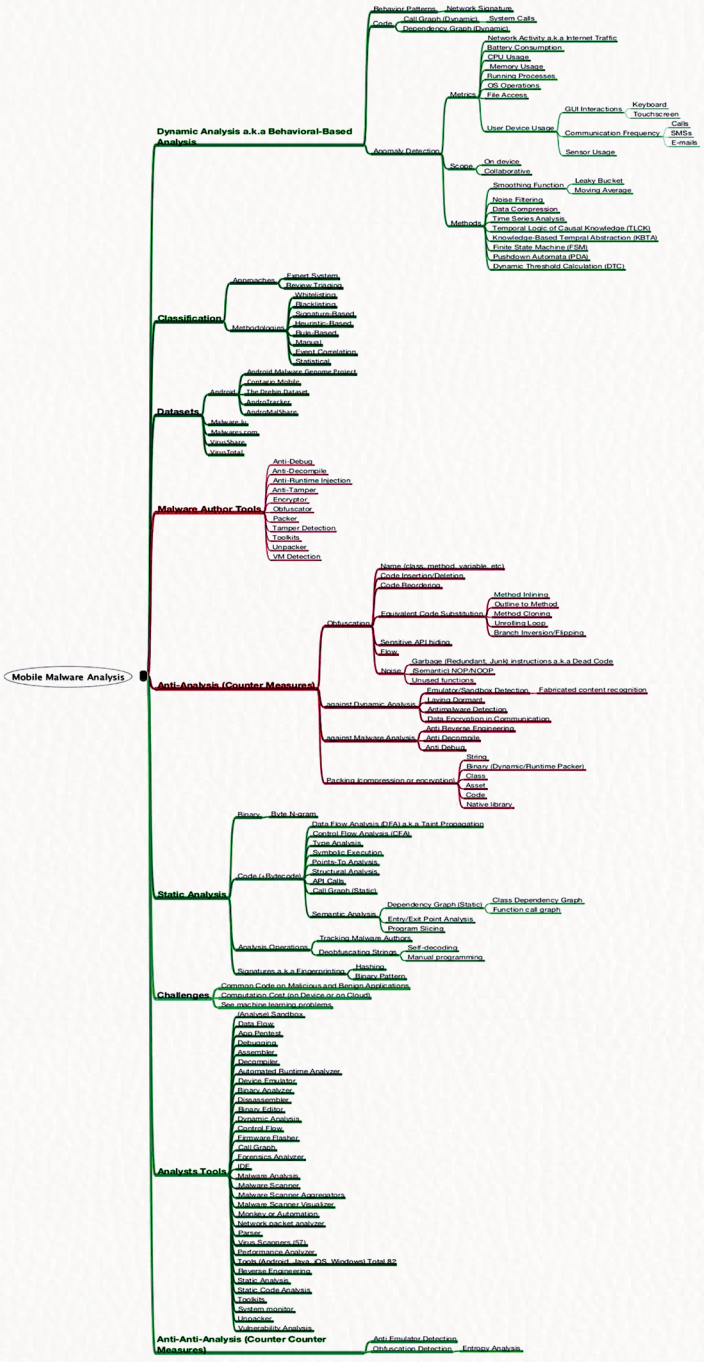
Taksonomi; TDK'da "sınıflandırılma ve bu sınıflandırmada kullanılan kurallar bütünü" olarak tanımlansa da farklı ansiklopedilerde ve literatürde ise "sınıflandırma ilkelerini, yöntemlerini ve amaçlarını inceleyen bilim dalı", "alanına veya konuya ait verilerin sınıflandırma adımları", "bir sınıflandırma şeması biçimi", "anlamsallık içeren bir tür bilgi haritası" olarak ta tanımlanmaktadır. Diğer bir ifadeyle, belirli bir alandaki öğelerin sistematik olarak sınıflandırmasını sağlamakta, kavramları yapısal bir şekilde ifade etme yolu-

nu açmakta ve verimli bir şekilde kullanılmaktadır. Taksonomiler, çok farklı amaçlar için kullanılabilmektedir. Örnek olarak; bir kurumdaki belgeleri, sözleşmeleri, yazışmaları, raporlamaları, bilgilendirmeleri, uyarıları, görevlendirmeleri, atamaları, projeleri, içerikleri kategorilere ayırmak, sınıflandırmak veya ayrıştırmak için kullanılabileceği gibi bir alandaki bilgilerin farklı kriter veya bakış açılarına göre sınıflandırılması için de kullanılabilir. Burada yapılacak her sınıflandırma, öğeleri tek bir boyut altında sınıflara ayırmak için tasarlanır. Sınırlamaları olup farklı alanlardaki veya sınıflardaki ilişkileri temsil edemez, açıklayamaz veya kategorileri tanımlayamazlar.

Ontoloji ise yukarıda verilen terimlerde de açıklandığı gibi varlıklar arasındaki ilişkiler hakkında bilgiler de dahil olmak üzere daha zengin bilgiler sağlayarak daha yüksek bir karmaşıklık açıklama düzeyine ulaşıp, bu ilişkiye ek katmanlar sağlayarak taksonomiyi bir adım öteye taşıyan ve diğer alanlarla ilişkilerin kurulması için yeni bakış açıları sunar [4]. Bunlara ilave olarak; çok boyutlu ilişkilerin tanımlanmasına, tüm bu ilişkileri kapsayacak şekilde yapılar kurulmasına, dinamik bağlantılar oluşturulmasına, kavramlar arasındaki ilişkiler ile kısıtları tanımlayarak bilginin ortak bir terminoloji kullanılarak paylaşılmasını kolaylaştırırlar [4],[11],[16].

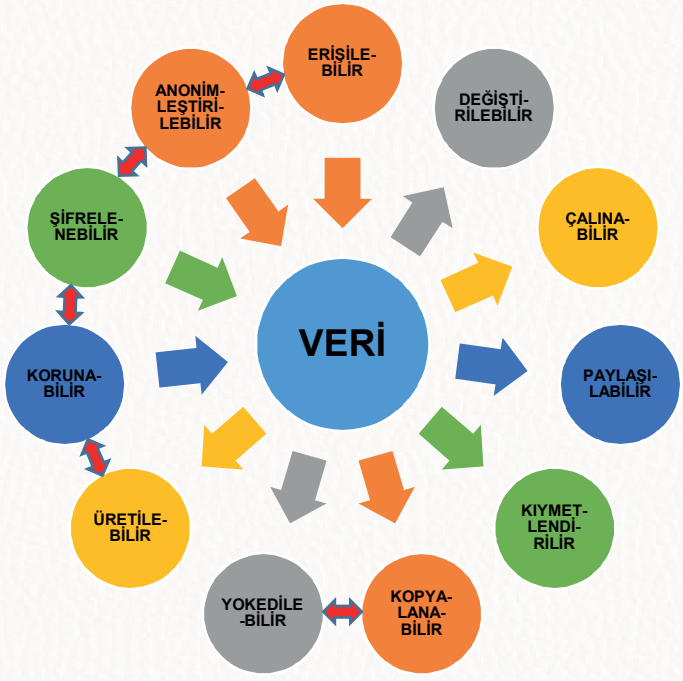
Literatürde ontoloji kelimesi yerine bazen taksonomi kelimesinin kullanıldığı yapılan incelemelerden görülmüştür. Bu iki terminolojinin farkını bilmek, ayrıştırmak ve en önemlisi birbirine olan katkılarının farkında olmak gereklidir. Burada taksonomi tanımının yapılmasının da gerekli olduğu görülmüş, kısaca bu terim tanımlanmış ve aralarındaki farklar da açıklanmıştır. Bu iki tanım arasındaki farkı "**veriler**" özelinde inceleyelim, değerlendirelim ve örneklendirerek açıklayalım.

Taksonomik açısından **veriler** incelendiğinde; temel olarak veriler sınıflandırılır. Kamu yazışmalarında içerisindeki veri durumuna göre dokümanların sınıflandırılması (çok gizli, gizli, özel, özel, kişiye hizmete özel, tasnif dışı) ile bunlara ilave olarak verilebilecek başlıklar; sayısal veri, analog veri, istatistiksel veri, görsel veri, büyük veri, şifreli veri, gürültülü veri, açık veri, kritik veri, anonim veri, zeki (smart) veri vb. buna verilebilecek örnekler olup bakış açısı sınıflandırmalarda kullanılabilir. Şekil 1.1'de sunulan Mobil Casus Yazılım Taksonomisi [10] buna verilebilecek diğer bir örnektir.



Şekil 1.1. Mobil casus yazılım taksonomisi [10]

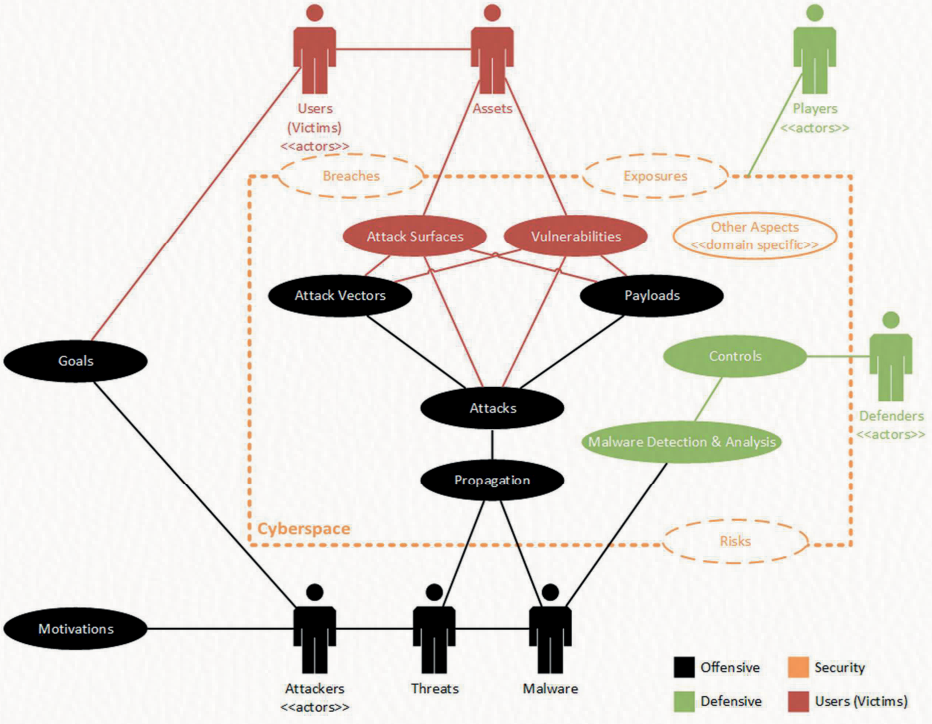
Ontolojik açısından **veriler** incelendiğinde; veriler arasındaki ilişkilere bakılır. Bu çok basit bir örnek olsa da konunun anlaşılmasını kolaylaştıracaktır. Genel olarak verilerin ontolojik olarak değerlendirilmesi Şekil 1.2'de verilmiştir. Şekilden de görülebileceği gibi veriler kendi içerisinde korunabilir iken aynı zamanda erişilebilir, şifrelenebilir veya anonimleştirilebilir. Aynı zamanda erişilen veriler, çalınabilir, kopyalanabilir, değiştirilebilir veya yok edilebilir. Veriler incelendiğinde; veri türleri ve aralarındaki ilişkiler ile kısıtların tanımlanması ontolojik bir bakış akışı için yeterli olacaktır. Tanımlanacak olan ontolojilerde, alana özgü ontolojiler de birbirinden farklı olacaktır. 2016 yılında Canbek ve arkadaşları [10] tarafından geliştirilen mobil güvenlik ontolojisine verilebilecek diğer bir basit örnek, kötü amaçlı mobil yazılımlar için örnek Şekil 1.3'te verilmiştir. 2016 yılında Canbek ve arkadaşları tarafından geliştirilen mobil güvenlik taksonomisi aynı zamanda kendi içerisinde bir ontolojiyi de belirli bir düzen olmasa da barındırabilir. Dolayısıyla taksonomi ve ontoloji kavramlarını doğru anlamak için bu kavramları iyi anlamak ve ayrıştırmak gereklidir.



Şekil 1.2. Veriler için basit bir ontolojisi örneği.

1.3. SİBER GÜVENLİK ONTOLOJİLERİ

Siber Güvenlik Ontolojisi (SGO) veya ontolojik yaklaşımlar bizlere yapılan işin temelini, felsefesini, boyutunu veya kapsamını daha doğru anlama, kavrama veya uygulamada yardımcı olacak bakış açıları sunmaktadır. Bu bakış açısını kazanmak, bunu siber güvenliğe uygulamak, ve hayata geçirmek ise temel amaç ve hedeftir. SGO, yukarıda yapılan tanımlar ile benzer olup daha çok siber güvenlik ve savunma alanına spesifik bir yapı içerisinde kavramlar, fikirler, kategoriler, saldırılar, saldırganlar, uzmanlar, tehditler ve tehdit vektörleri, korsanlar, kullanıcılar, geliştiriciler, açıklıklar, çözümler ve savunma metodolojileri ile bunların ilişkilerinin belirlenmesi ve oluşturulması ile ilgilenmektedir. SGO ile ilgili olarak yapılan çalışmalar ve bu bölümde atıf verilen çalışmalar gözden geçirildiğinde;



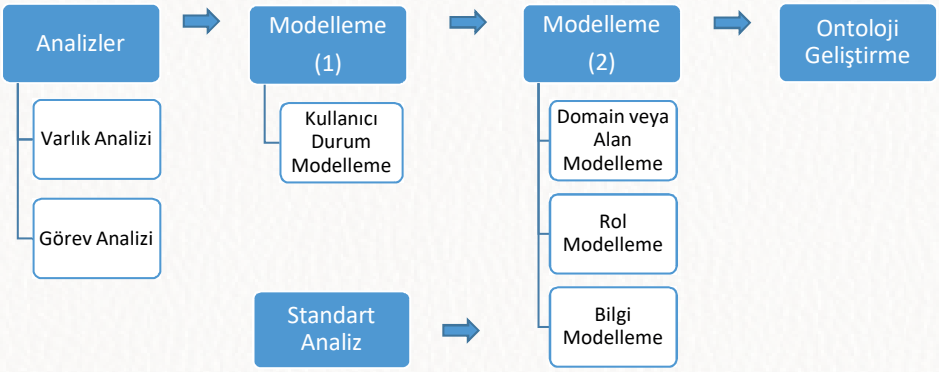
Şekil 1.3. Mobil casus yazılım ontolojisi [10]

1) Siber güvenlik dünyasında yeni yeni popüler olan ve faydalanılan bir bilim dalı olduğu,
2) Konuyu ciddiye alan ülkelerin ontoloji konularında araştırma enstitüleri kurduğu ve yapılan çalışmalarda bu yapılardan faydalandığı,
3) SGO'nun ilk olarak 2012 yılında Carnegie Mellon Üniversitesi CERT programında tanıtıldığı,
4) Akademik olarak farklı alanlarda siber güvenlik ontolojileri ve modelleri geliştirildiği ve paylaşıldığı,
5) Literatürdeki mevcut taksonomi, topoloji, yapı, sınıflandırma ve gruplandırma gibi çözümlerden de faydalanıldığı,
6) Farklı organizasyonlarda, kurumlarda ve yapılarda görev yapan siber güvenlik uzmanlarının veya alan çalışanlarının hızlı, doğru ve sorunsuz iletişim kurmalarına ve sağlıklı kararlar almalarına imkânlar sunduğu,
7) Olaylar, sonuçlar ve kavramlar arasındaki çok değerli ilişkiler kurulmasında önemli bir bakış açısı sağladığı,
8) Özellikle, kritik açıklıkları tanımlama, riskli durumları ortaya koyma, zayıflıkları belirlemede organizasyonlara ve çalışanlara yardımcı olduğu,
9) Geliştirilen ürünlerin iyileştirilmesi veya yeni ürünlerin geliştirilmesinde yeni bakış açıları sunduğu veya kazandırdığı,
10) Kaynakların daha verimli olarak kullanılmasına destek verdiği,
11) Veri boyutunun arttığı bir dönemde hem veri işlemenin hızlanması ve otomatikleştirilmesi hem de verilerin makineler tarafından işlenmesini kolaylaştırdığı,
12) Kurumların/ülkelerin siber güvenlik yapılandırmalarına önemli katkılar sunduğu veya sunabileceği ve
13) Atakların/saldırıların sürekli değişiklik göstermesinden dolayı savunma sistemlerinde ve alınan önlemlerde değişiklik olabileceğinden bu yapıların zaman zaman genişletilmesi gerektiği

görülmektedir.

Örnek olarak; bir arama motorunu seçmek, arama yapmak, sonuçları ifade etmek veya ontolojik bakış açılarından faydalanmak için kullanıcıların öğrenme materyallerini (öğrenme nesneleri) desteklemek, öğrenme nesnelerini anlamlı

bir şekilde tanımlamak önemlidir [16,34]. Bu tür sorunların üstesinden gelmek için, farklı dilsel ifadelerin (terimler) altında yatan siber güvenlik alanı kavramlarının (sınıfların) modelini ve kavramlar arasında var olan ilişkilerin açık modelini sağlayan SGO kullanılır. Bu kavrama dayalı semantik model yaklaşımı, daha iyi arama sonuçları elde etmek için öğrenme materyallerinin anlamsal indekslenmesine ve semantik sorgu yeniden yazılmasına yardımcı olabilir. Bu işlemleri gerçekleştirmenin zahmetli ve zaman alıcı olduğu ise aşikardır. SGO'yu geliştirirken temel olarak iki zorluğun ortadan kaldırılması beklenir. Birincisi, ontoloji geliştirme sürecini olabildiğince nasıl otomatikleştirebileceğidir. İkincisi ise otomatik olarak geliştirilen ontolojik bakış açısının alan uzmanları tarafından doğrulanmasıdır. Bunu sağlamak için ise mevcut temel ontoloji modelini alan terimleri kullanarak otomatikleştirmek, ontolojiyi doğrulamak ve daha da geliştirmek için uzman araçlarla ortaya çıkan ontolojiyi basitleştirmektir [16].



Şekil 1.4. Siber güvenlik ontolojisi geliştirmede kullanılabilecek modeller ve işlem adımları ([16] nolu kaynaktan Türkçeleştirilmiştir).

1.4. SİBER GÜVENLİK ONTOLOJİLERİ KULLANIM ALANLARI

Siber güvenlik ontolojilerinin kullanım alanlarına bakıldığında literatürdeki bazı bilgilere [20],[25]-[34] ile bazı öngörülerimiz aşağıda verilmiştir;

- Ontolojilerin gizli fırsatların veya zayıf alanların belirlenmesine yardımcı olabileceği dikkate alındığında, bir kurum altyapısının fidye

yazılım gibi belirli bir siber tehdide karşı koruma düzeyini analiz edebilir. Bunu yapmak için, olası fidye yazılımı önleme çözümlerinin bir ontolojisi oluşturulup kurumdaki mevcut güvenlik önlemleri arasına eklenebilir.

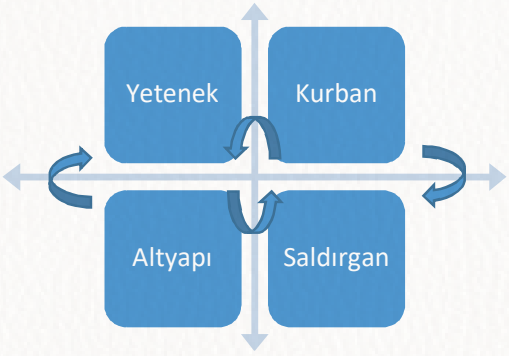
- Ontolojilerden faydalanılarak mevcut altyapının yeterli korumaya sahip olup olmadığını belirleme, herhangi bir çalışmaya ihtiyaç duyulup duyulmayacağı, yapılacak çalışmaların kapsamının kolaylıkla anlaşılmasını sağlayacaktır. Bir BT güvenlik sisteminin IEC, NIST veya diğer standartları karşılayıp karşılamadığını belirlemek için aynı yöntemin kullanıldığı unutulmamalıdır. Bu işlemler son yıllarda otomatikleştirilmeye çalışılsa da manuel olarak yapılan çalışmalar hala var olup, yüksek maliyetlidir.
- Ontolojiler doğru eğitim içeriği üretilmesi, eğitimin kapsamının belirlenmesi, eğitimde ortak dil oluşturulması, ayrıca BT güvenlik uzmanlarının birbirleriyle aynı dilde iletişim kurmalarını sağlayarak hayatlarını kolaylaştırır.
- Siber saldırıların kavramsal modelleri ve taksonomilerine ait Howard and Longstaff Saldırı Modeli ontolojisi [25], Swimmer'in Kötücül Yazılım Sınıflandırma Ontolojisi [26], Saldırı Tespit Sistemi Ontolojisi [27], Ağ Güvenliği Saldırıları Ontolojisi [28], Ağ Güvenliği Saldırıları Ontolojisi [28], Birleştirilmiş Siber Güvenlik Ontolojisi [29], [32], Kritik Altyapılar için Siber Güvenlik Ontolojisi [30], Bulut Güvenliği Hizmetlerinin Ontolojisi [31] ve Akıllı Şebekelerin Ontolojisi [33] gibi modeller vardır.
- Ontolojik bakış açıları ve çözümlerle her geçen gün karşılaşılmaktadır. Günlük hayatımızda ise bunlar kullanılmaktadır. İnternet aramalarında ontolojiler [34], semantik aramaların temelini oluştur ve gerçek sorgulara cevapların aramasına izin verir. Arama sonuçlarının kalitesini büyük ölçüde artırır. Mesela; görsel paylaşımlı bir sosyal ağ olan Pinterest'in benzer teknolojileri kullandığı, kullanıcıların eylemlerini ve tepkilerini analiz etmek için ontolojilerden faydalanıldığı, verilerden öneriler çıkarılmasında, hedefli reklamların optimize edilmesinde kullanıldığı görülmektedir.

Ontolojilerin; ontolojik araçlar kullanılarak yeni çözümlerin geliştirilmesine katkı sağladığı, veri analizinde kullanılabildiği, tahmin yapmada kullanma yerine sağlanan parametrelerden mantıksal olarak ortaya çıkan ilişkilere ve bilgilere odaklandığı, bilgileri analiz etmek için öğrenmediği veya önceki deneyimlerden yararlanmadığı bilinmektedir. Mesela [35,36]; ontolojide **A** e-postasının bir kimlik avı e-postası olduğunu ve tüm kimlik avı e-postalarının kötü niyetli olduğunu belirtirsek ve ardından **B** e-postasının bir kimlik avı e-postası olduğunu belirtirsek, ontoloji şu sonuca varır: e-posta **B** kötü amaçlıdır. Eğer yeni bir **C** e-postası analiz edilirse, herhangi bir özellik olmama durumunda ontolojik herhangi bir sonuç elde edilemeyecektir. Makine öğrenme algoritmaları; kurulan model ile problem sonucunu tahmin edebilmekte, büyük verileri analiz edebilmekte, probleme göre tahminleme modellerini öğrenerek çıkarım yapabildiği bilinmektedir. Sonuçta; bir makine öğrenme algoritmasının öğrendiği model ile 100 kötü amaçlı e-postaya bakabileceği, belirli özellikleri ayrıştırabileceği, gelen yeni bir e-postada bu özelliklerden bazılarını tanırsa, yeni mesajın da kötü amaçlı olduğunu belirleyebileceği ortadadır. Yeni bir bakış açısı olarak; ontolojiler ile makine öğrenme algoritmalarının birbirini tamamlayabileceği, ontolojilerin makine öğrenimi modellerini optimize edebileceğini ve hızlandırabileceğini, mantıksal akıl yürütmeyi simüle ederek bilgileri otomatik olarak sınıflandırabileceği ve bu sayede eğitim adımlarını daha da kolaylaştıracağını, ve sonuçta zaman kazandıran ontolojik aksiyomları (kavramlar arasındaki ilişkiyi tanımlayan kurallar) kullanarak, makine öğrenimi modelinin giriş sayısını düşürerek daha hızlı çözüm bulunmasına katkılar sağlayacağı raporlanmaktadır.

Ontolojiden faydalanma örneklerinde verildiği gibi başkalarının sunduğu farklı ontolojik çözümlerden mutlaka faydalanılması, karşılaşılan sorunlara sunulan modellerin kullanılması, hızlı ve kapsamlı çözümlerin geliştirilmesine yardımcı olmaktadır. Bu tür yaklaşımlar ile; siber güvenlik sıkılaştırılabilir, iyileştirebilir, çözüm odaklı önlem alınmasını kolaylaştırır ve yeni çözümlere erişilmesine katkılar sağlar. Güvenlik açıklarının, saldırılarının ve bunların ilişkilerinin sistematik bir bakış açısıyla ele alınmasını kolaylaştırır, sıfırdan bilgi güvenliği mimarileri ve çözümleri oluşturulmasına katkı sağlar, işleri ve işlemleri de hızlandırabilir.

1.5. SİBER GÜVENLİK ONTOLOJİSİ GELİŞTİRME

Bir siber ontoloji, insanlar, zaman, mekan ve olaylarla ilgili kavramlar gibi siber güvenliği aşan alanlardan da kavramları içerebilir. Kişiler, zaman aralığı, ve yer-uzamsal (geospatial) gibi farklı parametreler kullanılarak farklı ontolojik yaklaşımlar geliştirilebileceği, [19] nolu çalışmada raporlanmıştır. Siber güvenlik ontolojileri geliştirmenin önemli olduğu, konunun iyi anlaşılması için ise farklı şekiller üzerinde katkılarının sunulmaya çalışıldığı görülmektedir. Şekilden de görülebileceği gibi kullanıcılar açısından bakıldığında; Şekil 1.5'teki Saldırgan ve Kurban ilişkisinin kurulması, kişilerin sosyal rolleri ve ilişkileri ile onların nesnelerle ilişkileri, diğer bir ontolojik tanım olarak karşımıza çıkabilir. Arkadaşın arkadaşı, onların sosyal rolleri ve organizasyonlarını içeren mevcut ontolojiler eklemek ve bunun ontolojileri oluşturmak için ihtiyaca cevap verebilecek yeni ontolojileri buna dahil etmek gerekebilir [19].



Şekil 1.5. Siber güvenlik bileşenleri ([19] nolu kaynaktan Türkçeleştirilmiştir.)

ABD Savunma Bakanlığının desteğiyle Carnegie Mellon Üniversitesi CYLAB ekibinin hazırladıkları raporlarında [18], ontoloji ile ilgili önemli bulgulara yer vermişler, siber güvenlik teorisi ve uygulamalarını incelenmişler, bilimsel bir yaklaşım benimsenmesini kolaylaştıracak temel ilkelerin belirlenmesine yardımcı olacak bazı önemli adımlar geliştirip önermişlerdir. Kısaca ontolojik bakış açısının;

- siber güvenliğin bir bilime dönüştürülmesinde etkili olacağı, bilimsel bakış açısıyla doğru ilerlemek için kontrollü kelime dağarcığı ve ontolojiye ihtiyaç duyulduğu,

- siber güvenliğin geliştirilmesinde kritik bir adım olduğu,
- ortak bir dil oluşturulmasına ve aynı zamanda ortak bir anlayış geliştirebilmesinde temel teşkil edeceği,
- sağlıklı bir siber güvenlik ekosisteminin geliştirilmesine katkı sağlayacağı, yapı ve üzerinde mutabık kalınan protokoller ile hipotezlerin test edilmesini ve kavramların doğrulanmasını kolaylaştıracağı,
- siber saldırıların, siber olayların, kötü niyetli ve etkilenen yazılım programlarının daha kolay sınıflandırılmasını sağlayacağı,
- siber güvenlikte insan bileşeninin çok önemli olduğunu ve bakış açısına göre saldırganların, kullanıcıların, savunucuların ve politikaların oynadığı farklı rollere, ekip, ekip lideri ve bunları gerçekleştirmek için gereken bilgi, beceri ve yeteneklerin belirlenmesi ve buna göre bir yönetim ve denetim anlayışı geliştirilmesine katkılar sağlayacağını

belirtmektedir.

Ülkemizde yapılan bir çalışmada [17] ise; Vakıflar Genel Müdürlüğü'ne ait milyonlarca belgenin kolaylıkla aranmasını, mevcut veri kaynaklarından bilgi keşfi kapsamında kullanılabilirliğini anlamsal ağ yaklaşımıyla sunan bir sistem mimarisi önerilmiş, resim formatında arşivlenmiş olan belgeler bilgisayar teknolojilerinin anlayacağı ve ayrıştırabileceği bir yapıya dönüştürülmüş, genel bir arşiv "ontoloji bilgi tabanı" geliştirilmiş, her belgenin, standart bir formatta saklanması ve anlamsal aramada kullanılması amaçlanmış ve sunulan bilgi tabanı ile herhangi bir anlamsal arama motoru ile belge sorgusuna girilen arama kelimelerinin, ontolojideki mevcut kavramsal bağlara (türemiş kelime, eş anlamlılık gibi özellikler, tekil-çoğul vb. anlam ilişkileri) göre arama yapmasına imkan sağlamaktadır. Çalışmada geliştirilen bilgi tabanı temel adımları ise aşağıda verilmiştir. Bunlar;

- klasör, dosya, belge ve sayfa kavramlarına ait etiketlerin belirlenmesi,
- ontolojik kavram ya da sınıf yapılarının belirlenmesi
- belirlenen sınıf yapıları arasındaki özelliklerin önceden belirlenmiş yapılara göre kurgulanması ve yaratılması,
- belirlenen sınıf yapılarına ait veri elemanlarının belirlenmesi,
- Anlamsal Kural Tabanının SWRL dili ile geliştirilmesi, ve
- doğrulama testlerinin tamamlanmasıdır.

1.6. SİBER GÜVENLİK ONTOLOJİLERİ GELİŞTİRMEDE DİKKAT EDİLMESİ GEREKEN HUSUSLAR

SGO'ları geliştirmek için başlangıçta bazı soruların ve cevaplarının bilinmesi veya bazı sorulara cevap bulunması işleri kolaylaştırmaktadır. Burada, ontolojik bakış açısına sahip olmak, adımlarını öğrenmek, temel sorulara cevapları bilmek hem bulana kolay uyum sağlanması hem de sağlayacağı faydayı daha hızlı anlamaya katkı sağlayacaktır. Bunun için, [15] nolu çalışmada sunulan ontolojileri geliştirmek için sunulmuş olan hususlardan faydalanılmış, cevaplanması gereken sorular gözden geçirilmiş, sorulara cevaplar ise aşağıda maddeler halinde kısaca açıklanmıştır.

i. Ontolojinin temsil edeceği alan hangisidir?

Bir ontoloji yanlış olarak yapılandırılamaz ancak hedeflenen alanın bilgisini yeterince kapsayamayabilir. Bu da, kötü oluşturulmuş bir ontoloji geliştirilmesine sebep olur. Bu nedenle ontolojinin temsil edeceği alanın sınırlarını, kavramlarını, ilişkilerini ve terimlerini kesin olarak tanımlamak önemlidir.

ii. Ontolojiye neden ihtiyaç duyulur?

Siber güvenlik ontolojileri ve kazanımlar bölümünde de açıklandığı gibi ontolojilere neden ihtiyaç duyulduğu kapsamlı olarak açıklanmıştır. Ontolojinin ne tür bilgiler, kolaylıklar ve faydalar sağladığını bilmek ve bunları tanımlamak önemlidir. Burada siber güvenlik alanında farklı problemleri çözmek için farklı bakış açılarına ve çözümlere ihtiyaç vardır. Mesela; sistem yöneticilerinin; olaylar, açıklıklar, önlemler, saldırılar, savunma teknikleri gibi konularda neler bilmeleri ve yapmaları gerektiği bilinciyle sahip oldukları güvenlik sorunlarını ontolojik bakış açısıyla nasıl ilişkilendirebileceklerini bilmeleri önemli olduğundan ihtiyaç duyulmaktadır.

iii. Ontolojiler, ne tür sorulara cevap verirler?

Ontoloji geliştirmede mevcut metodolojilerden, çalışmalardan, tanımlardan ve yetkinliklerden faydalanılmaktadır. Ontolojiler, pek çok soruya cevap verebilirler. Literatürde karşılaşılan pek çok yetkinlik soruları da vardır. Mesela, Şekil 1.1'de de verildiği gibi kötücül veya zararlı yazılımlar konusu ele alınmış ve sorulabilecek sorulara verilebilecek örnek sorular aşağıda verilmiştir.

- Kötücül yazılımlar hangi güvenlik açıklıklarından/zafiyetlerden yararlanabilir?

- Kullanılan açıklıklar/zafiyetler arasındaki ilişkiler nelerdir?
- Kötücül yazılımın matematiksel modeli var mıdır?
- Kötücül yazılım diğer yazılım özelliklerini ne kadar içermektedir?
- Kötücül yazılımda kullanılan özellikler nelerdir? Ne kadarı bilinmektedir?
- Kötücül yazılımların oluşturduğu tehditler nelerdir?
- Karşılaşılan güvenlik olayları arasındaki ilişkiler nelerdir?
- Belirli bir güvenlik olayı ne gibi sonuçlar doğurabilir?
- Sistemlerde kurulu olan kötücül yazılımların ne tür açıklıkları/zafiyetleri vardır?
- Karşılaşılan olaylarda hangi güvenlik zafiyetlerinden/açıklarından yararlanılmaktadır?

iv. Ontolojiyi kim/kimler kullanacaktır?

Ontolojilerden faydalanacak olan kullanıcıları, yöneticileri, geliştiricileri, araçları veya sistemleri tanımlamak önemlidir. Farklı çalışmalarda önerilen veya açıklanan ontolojiler, gerek teknolojiler ve diller gerekse alanlar temel alınarak belirlenebilir. Örnek olarak; OWL aracı, sadece kullanıcılara bilgi sunmak yerine bilgi içeriğini işlemesi gereken uygulamalar tarafından kullanılmak üzere tasarlanmış, ücretsiz, açık kaynaklı bir ontoloji editörü ve bilgi tabanı çerçevesidir.

Bu ve buna benzer soruların sayısını artırmak tabii ki mümkündür.

1.7. ONTOLOJİK BAKIŞ AÇILARI VE KAZANIMLAR

Teknolojinin hayatımızın her aşamasına girdiği, toplumun değişim ve dönüşümünü hızlandırdığı, veri boyutunun aylar içerisinde ikiye katlandığı bir zamanda, verilere zamandan, mekandan ve kişilerden bağımsız olarak erişilebildiği bir zamanda dijital dünyayı anlamak, anlamlandırmak, ilişkilendirmek, kavramak, analiz etmek, tehditleri bilmek ve korunmak için yeni bakış açışlarına ihtiyaç vardır. Mesela; veriye erişimde önemli araçlardan olan arama motorları, verilere erişim ve yönetiminde etkili çözümler sunmaktadır. Doğru bilgiye erişim ise en önemli sorunların başında gelmektedir. Özellikle,

anahtar kelimeye dayalı olarak verilere erişim zorlaşmakta, zaman alıcı ve maliyeti yüksek çözümler haline gelmektedir. Bilgiye erişimin sürdürülmesi, verilerin sadece uzmanlar veya araştırmacılar için değil makineler tarafından da anlaşılması, anlamlandırılması veya ayrıştırılması için de yeni çözümlere ve yaklaşımlara ihtiyaç vardır. Semantik, ontolojik, veya epistomolojik bakış açılarıyla yeni çözümler geliştirmek mümkün olabilmektedir.

Ontolojileri kurgulamak, geliştirmek ve kullanmak için farklı gerekçelerimiz olabilir. Daha çok veriler temel alınarak kazanımlar aşağıda alt başlıklarda verilmiş ve kısaca açıklanmıştır [3],[4],[5],[21].

i. Bireyler veya siber güvenlik araçları arasında yapılandırılmış bilgilerin ortak bir anlayışla geliştirilmesi ve paylaşılmasına katkılar sağlar.

Şekil 1.1'de verilen mobil casus yazılım taksonomisinin farklı açılardan bilgi içerdiği varsayımıyla, kullanılan terimler ile bunların ilişkilerinin ortak bir anlayışla geliştirilmesi ve paylaşılması ile farklı bilgiler çıkarabilir, farklı soruları cevaplandırmaya katkı sağlayabilir, çeşitli uygulamalara girdi olarak kullanılabilir, kişiler veya araçlar arasındaki bilgiler toplanabilir, diğer hususlarda alan bilgilerinin geliştirilmesine katkılar sağlayabilir.

ii. Bilgiyi yeniden kullanmaya imkan verir.

Bir grup araştırmacı bir ontoloji geliştirirse, diğerleri onu kendi alanları için yeniden kullanabilir ve böylece çabadan tasarruf edebilirler. Örneğin, bu kitap bölümünde özetlenen ontolojilerden faydalanılarak yeni ontolojiler geliştirilebilir veya literatürde geliştirilen ve açıklanan SecOnto gibi güvenlik olayı ontolojisi [6], güvenlik açığı ontolojisi [7] gibi ontolojilerden faydalanılabilir. Diğer bir ifadeyle güvenlik olayı ontolojisi, güvenlik açığı ontolojisi içine aktarılarak, veri ve bilgilerin yeniden kullanım kapasitesi daha net görülebilir. Mesela; bir virüs ontolojisi veya bir solucan ontolojisi gibi güvenlik etki alanlarıyla ilgili diğer ontolojiler oluşturulabilir ve içe aktarılabilir [21]. SecOnto, olay ontolojisini içe aktardığı için yeniden kullanılabilir.

iii. Birlikte çalışabilirliği kolaylaştırır.

Birlikte çalışabilirlik; ilgili paydaşlar arasında ortak dil birliği ve anlayış kültürü oluşturulması, verimliliğin arttırılması, iletişim ve koordinasyonun kolaylaştırması gibi kazanımların elde edilmesini sağlar. Aynı zamanda; gerek

kurumların gerekse sistemlerin uyum içerisinde çalışması için vazgeçilmezdir. Veriler; "kurumlar arasında ve bilgi sistemlerinde kullanılabilme ve transfer edilebilme yeteneği", örnek alınabilecek "verimli, uyumlu, üretici, başarılı ve odaklı çalışmalar için vazgeçilmez bir yaklaşım", "yasal, organizasyonel, anlamsal ve teknik gibi farklı çalışabilirlik katmanları" oluşturulabilmesine imkan vermektedir [8]. Bu sayede; veri ve bilgilerin biçimi, önemi, değeri ve anlamı, ilişkileri, bağlantıları taraflar arasında çok daha iyi anlaşılabilir ve tanımlanabilir, paylaşım veya diğer bir risk durumunda hassasiyet tam olarak kavranabilir, verilerin korunması ve mahremiyetine saygının gereği daha iyi yerine getirilebilir, hem anlamsal hem de söz dizimsel birlikte çalışılabilirlik sağlanabilir, ve sonuçta hedeflenen başarı elde edilebilir.

Daha spesifik olarak ontolojiler [21]; farklı güvenlik araçları arasında birlikte çalışabilirliği kolaylaştırarak, güvenlik verilerini temsil etmek için benzersiz bir yol sunabilir, oluşturulmasına katkı sağlayabilir, karşılaşılabilecek sorunların minimize edilmesini sağlayabilir, herhangi bir güvenlik sisteminden alınan verilerinin, güvenlik olayı gibi bir ontolojiyle eşleştirebilir, haritalama kolaylığı gibi unsurların kullanılmasıyla da herhangi bir güvenlik aracındaki verilerin tanımlanan ontolojik formatta yapılandırılmasına izin verebilir.

iv. Ortak bir terminoloji oluşturulmasına, kelime dağarcığı geliştirilmesini kolaylaştırır.

Dünyada ontolojinin katkılarını bilen ülkeler bu konuda enstitüler açmış, ortak terminoloji oluşturma, kelime dağarcığını geliştirme gibi çalışmalara önem vermişlerdir. Özellikle, siber güvenlik verilerini ve bilgilerini sınıflandırma ve kataloglama için çaba gösteren organizasyonlara örnekler aşağıda verilmiştir.

- MITRE Enstitüsünde geliştirilen CVE Projesi [9] buna verilebilecek en iyi örneklerden birisidir. Herkes tarafından bilinen bu projede, tüm güvenlik açıkları, bunların standartlaştırılması, farklı güvenlik araçları kullanılarak güvenlik açıklarının sınıflandırılması ve tanımlanmasını kolaylaştırmak için bu proje hayata geçirilmiştir.
- Carnegie Mellon Üniversitesi bünyesinde oluşturulan CERTw/CC, güvenlik açığı uyarıları, güvenlik olayları, virüs uyarıları ve diğerleri dahil olmak üzere hesaplama güvenliği hakkındaki bilgiler gruplandırılmış ve kullanıma sunulmuştur [11].

v. Çok paydaşlı etkileşimlerden kaynaklanan belirsizlik ve iletişim sorunlarının kolaylıkla anlaşılmasına ve çözümlenmesine yardımcı olan ortak bir çözüm sunar.

Büyük çaplı veya ulusal bazda bir konuda ontoloji geliştirmek için çok paydaşlı etkileşimlerden kaynaklanan belirsizlik ve iletişim sorunlarının çözülmesi, karşılaşılan problemlerin kolaylıkla anlaşılması ve ortak çözümlerin geliştirilmesi gereklidir.

Ortak veri sözlüğü oluşturma çalışmaları da bunlara verilebilecek önemli örnekler arasındadır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Sağlık Bakanlığı [12], Orman ve Su İşleri Bakanlığı [13] gibi kurumlarımız, üniversitelerimiz, araştırma enstitülerimiz, verileri ve bilgileri sınıflandırmak ve kataloglamak için çaba göstermektedir. Özellikle; CB DDO Ulusal Veri Sözlüğü Projesi [14], buna bir örnek olarak verilebilir. Bu proje hayata geçirildiğinde; entegrasyon kolaylaşmış, tekrarlı, çelişen ve tutarsız veriler ayıklanmış, taraflara karşı bağımlılık ortadan kaldırılmış, ortak paydada bilgiye erişim kolaylaştırılmış, kamu kurumları için ortak bir dil oluşturulmuş, ulusal veri envanteri hazırlanmış, e-devlet veri sözlüğü hizmete sunulmuş, ve verilerin standartlaştırılarak tekil hale getirilmesi sağlanmıştır.

vi. Alan bilgisinin bir araya getirilmesinde, genişletilmesinde ve yeni ontolojilerin geliştirilmesinde mevcut referans modellerinden faydalanılır.

Mann ve Christey [9] tarafından önerilen Zafiyet Ontolojisi buna örnek verilebilir. CVE Projesi kapsamında Mitre Enstitüsü tarafından geliştirilen bir ontoloji modelinde; güvenlik sınıfları, öznitelikleri ve ilişkileri gösteren kavramsal bir model sunulmuştur. Ayrıca bunlara verilebilecek diğer örnekler; "güvenlik olayı ontolojisi" [6], güvenlik olayları ve güvenlik açıklarıyla ilgili benzersiz kavramlar ve ilişkiler sözlüğünü içeren "güvenlik açığı ontolojisi" [7] ve Mobil Casus Yazılım Ontolojisi [10] olabilir.

vii. Yüksek seviyede koruma yaklaşımı geliştirme, alan bilgilerinden daha sağlıklı analizler yapma, problemlere daha kapsamlı bakma ve bütüncül çözümlere odaklanmayı sağlar.

Buna verilebilecek en önemli örnek siber vatandır. Vatan; bir milletin hâkim olarak üzerinde yaşadığı, barındığı, uğruna canların verildiği ve gerekirse vermeye devam edilecek toprak parçasıdır. Siber vatan kavramını; bu açıdan ele

almak, analojiler yaparak anlamak veya algılamak gerçekten zordur. Bunun haklı gerekçeleri olup, bazıları aşağıda verilmiştir.

- Sanal dünyanın sınırlarını veya sınırsızlığını bilmek özellikle de dijital sınırlarımızın farkında olmak gereklidir. Paylaşım izni bir şekilde verilmeden veya verilerek paylaşılmış, izinsiz olarak ülke için veya dışına aktarılmış her türlü verilerin bulunduğu tüm ortamlar dijital topraklardır.
- Vatandaş verilerinin bulunduğu her türlü ortam siber vatanın dijital topraklarıdır. Sanal ortamlarda sahip olunan kişisel, kurumsal veya ulusal bilgi varlıklarının tamamını (hangi ülkelerde olduğunu) bilmek ve korumak gereklidir.
- Egemenlik alanlarımızın boyutunu iyi anlamak için kara-hava-deniz-uzay-siber ilişkisini iyi kavramak gereklidir. Bunun için ilkelerimizi, politikalarımızı ve stratejilerimizi bu boyutu dikkate alarak kapsamlı hazırlamak, önceliklerimizi belirlemek, hedef olan varlıklarımızı en uçta bile olsa korumalıdır.
- Ulusal değerlerimizi, çıkarlarımızı ve hedeflerimizi bilmek, verilerden değer elde etmek, büyük boyutu görmede verilerden faydalanmak ve sonuçta onları korumak ve savunmak gereklidir.
- Tehdit vektörünü iyi belirlemek, mevcut riskleri doğru tespit etmek, yönetmek ve gidermek, hatta gelecekte oluşabilecek riskleri de öngörüp önlemleri de bugünden geliştirmek gereklidir.
- Siber güvenliği ve savunmayı sağlamak kurumsal veya ulusal bir konu olduğu kadar kişisel de bir konudur. Bu konu başkalarına havale edilecek bir konu değildir. Bundan herkes sorumludur.

Siber vatanımızı korumak için;

- siber ortamlarımızı, varlıklarımızı ve değerlerimizi koruyacak yapılara, araçlara, silahlara, siber askerlere ve savaşçılara kısaca ordulara, nitelikli araştırmacılara ve uzmanlara, eğitim, araştırma ve tatbikat merkezlerine, üstün nitelikli yöneticilere, ileri düzey altyapılara, üst düzey kapasite ve yeteneklere, caydırıcı güç olmak için altyapılara ve savunmanın tüm dünyaya karşı yapıldığının farkında olarak gerekli hazırlıklara ihtiyaç vardır.

- sanal dünyanın doğru anlaşılmasına, boyutunun ve sınırlarının iyi belirlenmesine, tehdidin doğru algılanmasına, karşılaşılan tehditleri, riskleri, saldırıları ve saldırı vektörlerini, açıkları, zafiyetleri, alınan önlemleri, korunma tekniklerini, öncelikleri, varlıkları, teknolojileri, gelişmeleri, yetenekleri, kapasiteleri bilmek belki de en önemlisi bunlar arasındaki ilişkileri tanımlamak ve kurmak, bu terimleri doğru anlamlandırmak ve yeni bakış açıları geliştirmek gereklidir
- verilerimizin siber vatanın toprakları olduğunu bilmek, dijital verilerin büyüklüğünün vatan topraklarının büyüklüğü olduğunun farkında olmak, dijital verilerin bulunduğu her sanal ortamın vatan sınırlarımızı oluşturduğunun bilincinde olmak, tehdidin tüm uluslardan geleceğini bilerek hazırlık yapmak ve bu çerçevede koruma yaklaşımı geliştirmek gereklidir.

Sonuç olarak; vatanı gerçek manada korumak için siber güvenlik ontolojilerinin oluşturulması, mevcut ontolojilerden faydalanılması ve ulusal ontolojilerin geliştirilmesi gereklidir. Bunun için, stratejik düzeyde kurumsal/ulusal bilgi güvenliği yönetimi politikalarına, araçlarına, kurallarına, ilişkilerine, standartlarına, bilgi sistemlerine entegre edilebilir çözümlere, koruma yaklaşımlarına, kurumun kendi alanını daha iyi bilmesine, kurumlar arası işbirliklerini daha iyi anlamasına ve bunlar arası ilişkilerin kurulması ve anlaşılmayı kolaylaştıran kavramsal modellerin geliştirilmesine katkılar sağlamaktadır [21]. Ayrıca, bu özellik, güvenlik açığı ontolojisi tarafından tanımlanan kavramlar ve ilişkiler kullanılarak, farklı uygulamalar ve bunlar arasındaki veri paylaşımına izin veren birlikte çalışabilirlik gibi bazı özellikleri de kolaylaştırılabilir.

viii. Risk yönetiminin planlanması, işlevsel gereksinimlerin formüle edilmesi, risklerin otomatik olarak değerlenmesi ve kolaylıkla yönetilmesine katkı sağlar.

Siber güvenlik riskleri pek çok sebepten ortaya çıkabilmektedir. Bu riskler, yazılımsal olabileceği gibi kullanılan donanım, ağların yanlış yapılandırılması, yazılım güncellemelerinin yapılmaması, insan faktörü, saldırganlar, uygulama eksiklikleri, vb. kaynaklanmaktadır. Tüm hususların dikkate alınması, planlanması, yapılandırılması, ilişkilendirilmesi, yönetilmesini ve sonuçta otomatik olarak değerlendirilmesi gereklidir. Ontolojiler özellikle yöneticilerin [21];

- veri ve bilgi güvenliği yönetimi hakkında alınan kararlardan daha emin olmasına yardımcı olabilir,
- önceki güvenlik sorunlarından bütüncül bir şekilde ders almasına imkan sağlayabilir,
- yeni sorunları görme, çözme ve önlemelerine destek olabilir,
- güvenlik olayları, güvenlik açıkları ve politikalarla ilgili yeni kuralların getirilmesi yoluyla çıkarım sürecinin sürekli iyileştirilmesi, en uygun çözümün geliştirilmesine yardımcı olabilir, ve sonuçta
- risk yönetiminin doğru ve sağlıklı bir şekilde yapılmasını sağlar.

ix. Olaylara, sistemlere ve saldırılara daha kapsamlı bir bakış sağladığı için yüksek seviyede koruma başarıları elde edilmesine katkı sağlar.

Güvenlik dinamik bir süreçtir ve yönetilmesi gereklidir. Bunun için karşılaşılan riskler ve farklı güvenlik uyarılarının çözülmesi için alınabilecek önlemler ile ilgili sürekli olarak yeni kararlara ihtiyaç duyulmaktadır. Bu kararların çoğu, yöneticilerin bilgi birikimleri ile deneyimlerine, olaylara, sistemlere ve saldırılara kısaca tehdit ve tehlikelere bakış açısına dayanılarak verilmektedir. Bu nedenle ontolojik bakış açısı, farklı kaynaklardan gelen farklı güvenlik olayları ve açıklarının otomatik olarak ilişkilendirilmesini, güvenlik bilgisi ile bunun yönetimini kolaylaştıracak çözümler sunarlar.

x. Araştırmacılar ve sistem yöneticileri gibi toplulukların bilgi paylaşması ve bir bilgi alanı hakkında ortak bir anlayışa sahip olması gereken yazılım aracıları için ortak bir yapı oluşturabilir.

Canbek ve arkadaşları tarafından 2016 yılında geliştirilen mobil güvenlik sınıflandırması [10] buna bir örnek olabilir. Çalışmada;

- kötü amaçlı yazılımların belirli bir sistematik içerisinde sınıflandırılması ve analiz edilmesi için bir seviyelendirme şeması ve notasyonlarını içeren genel bir güvenlik yapısı önerilmiş,
- araştırmacılar, güvenlik uzmanları ve son kullanıcılar için 1.300'den fazla düğüme sahip olan bu yapı görselleştirilmiş,
- hiçbir ayrıntı atlanmadan mobil güvenliğin tüm perspektifini görmeye yardımcı olacak ve mobil hesaplama ile siber güvenlik bilim disiplinlerini yakınlaştıracak yeni bir bakış açısı sunulmuştur.

Şekil 1.1'de bir kısmı verilen Mobil Casus Yazılım Taksonomisinin daha kapsamlısına **http://bit.ly/mobilemalwaretaxo** adresinden erişilebilir.

xi. Bilgi keşfini kolaylaştırmakta ve otomatikleştirmektedir.

Bilgi keşfi; adından da anlaşılabileceği gibi veriden bilgi elde edilmesi ve keşfedilmesi için kullanılmaktadır. Odaklanılan alanı ve veriyi anlama, veri sınıfı ve özelliklerine göre konunun ontolojik olarak öğrenilmesi, değerlendirilmesi ve iyileştirilmesi gibi işlem adımlarını içerir. Bilgisayar mühendisliğinde en çok çalışılan konulardan da birisidir.

Verilerin boyutunun ve çeşitliliğinin hızla arattığı bir dönemde; verilerin bilgisayarlar, arama robotları, uygulamalar veya kullanılan yazılım araçları tarafından erişilebilir, anlaşılabilir, yorumlanabilir ve kullanılabilir olması, veriyi kolayca bulması, anlamlandırması, paylaşması, birleştirmesi veya ayrıştırmasına ihtiyaç vardır. Günümüzde verilerin bilgisayarlar tarafından anlaşılabilmesi veya bilgisayarların anlayabileceği şekle dönüştürülmesi kolaylaşmakta ve kavramlar arasında anlamsal ve mantıksal bağlantılar kurabilmesiyle de verilerden daha kolay değer elde edilebilmektedir. Bu sayede veriler, semantik yapılar içinde anlamlı hale getirile sistemler tarafından tanınmakta, ayrıştırılmakta ve yorumlanmaktadır. Ancak, ontolojinin gelişimine büyük katkılar sağlasalar da saklanan ve yayınlanan bilgilere anlamsallık atfetmezler. Diğer bir ifadeyle ontoloji, bilgiyi yapılandırmayı ve anlamını işlemeye yardımcı olmayı mümkün kılsa da bu anlamsal yapı olmadan, yazılım aracıları veya sistem yöneticileri, güvenlik olayları ve güvenlik açıkları arasında otomatik olarak önemli ve örtük ilişkiler kuramazlar [15].

1.8. SONUÇ VE DEĞERLENDİRMELER

Ülkemizde ihmal edildiğini değerlendirdiğim bu konuyu gündeme taşımak, temel bakış açısını tanıtmak, faydalarını açıklamak, katkılarını ortaya koymak, yapılacak yeni çalışmalara ışık tutmak amacıyla bu bölüm hazırlanmıştır. Ontolojiler ve ontolojik yapılar veya sistemler, siber güvenliğe bakış açımızı temelden etkilemekte, bir bilgi alanı hakkında birbirilerimizle iletişim kurma şeklini belirlemekte, kolaylaştırmakta ve en önemlisi konu ile boşlukların doldurulması ve kapsamlı çözümler geliştirilmesine katkılar sağlamaktadır.

Ontolojik yaklaşımların gerek siber güvenlik gerekse diğer alanların hem doğru anlaşılması hem de farklı gelişmelerin veya çözümlerin önünü açacağı unutulmamalıdır.

Ülkemizdeki SGO çalışmalarını incelendiğimizde;

- çok fazla akademik çalışma olmadığı veya yapılmadığı,
- sadece siber güvenlikte değil diğer alanlarda da kullanılabilecek hazır ontolojik yapıların veya modellerin bulunmadığı,
- strateji dokümanlarında ontolojik bakış açısına çok ta yer verilmediği ancak buna katkı sağlayacak ulusal veri sözlükleri hazırlanmasına ağırlık verildiği veya odaklanıldığı,
- yapılan çalışmaların sınıflandırma ve bazı alanlara yönelik geliştirilen taksonomiler olduğu; ve
- siber güvenlikte yeni ve köklü tanımların ve çözümlerin yeni yeni geliştirilmeye çalışıldığı görülmektedir.
- Ontolojilerin son zamanlardaki katkılarına iki güncel örnek aşağıda verilmiştir;
- Moiseev'in ontoloji ile ilgili görüşlerine bakıldığında [20], "şirket ürünlerini geliştirmek için yeni teknolojileri düzenli olarak takip ve analiz ettiğini, yenilikleri siber güvenlik çözümlerinde kullanmanın yollarını aradıklarını ve ontolojinin birçok süreci hızlandırabileceği ve basitleştirebileceğine inanıldığı, siber güvenlik için ontolojiyi kullanmanın sadece bir zaman meselesi" olduğu belirtilmektedir.
- Mayıs 2021'de yayınlanan "Yapay Zekada Ontoloji: Bilgi Paylaşımını Hızlandırmak İçin Ortak Bir Kelime" başlıklı bir yazıda [22] vurgulandığı gibi; ontolojik bakışın kuruluşlar için dijital dönüşümü hızlandıracağı ve bunun için ise YZ projelerinin birbirine entegre edildiği, hızlı ölçeklendirme yeteneğinin önemli olduğu, bunu sağlamak için şirketlerin bir dizi bağlantısız projeye sahip olmak yerine tekrarlanabilir bir çerçevede bunu geliştirdikleri, yerinde ontolojik yaklaşım ve mevcut ilişkisel yapılar ile yayılabilen tek bir konumdaki verilerde değişikliklerin yapılabileceği; kuruluşların YZ projelerini güçlendirmeleri için yeniden kullanılabilir, uyarlanabilir bir

yapıya sahip olmalarının gerekli olduğu; her ne kadar YZ'de net bir ontoloji geliştirmek için çeşitli zorluklar olsa da bunların aşılabileceği raporlanmıştır.

Sonuç olarak;

- bu kitap bölümünde açıklanan 11 farklı durumun iyi anlaşılması pratiğe aktarılması gereklidir.
- Siber güvenlik ve savunmaya her zamankinden daha fazla ihtiyaç duyulduğu bir dönemde, SGO alanının gelişmesi ve karşılaşılan problemlere uygulanması için aşağıdaki hususlara yer verilmesi, yeni çalışmaların yapılması ve en önemlisi de bu konunun sadece SGO değil diğer alanlarda da dikkatlice uygulanmasının faydalı olacağı değerlendirilmektedir.
- SGO yapılarının oluşturulması ve geliştirilmesi için buna yönelik yapılar, enstitüler veya merkezler kurulmalıdır. Farklı siber güvenlik alanları için ontolojiler oluşturulmalı ve uygulanmalıdır.
- Üniversite ve araştırma enstitülerimizde SGO'ların geliştirilmesi, akademik çalışmaların ve yayınların yapılması, yenilerinin geliştirilmesi için akademik çalışmalar teşvik edilmelidir.
- Birlikte çalışabilirlik ile ortak çalışma kültürünün geliştirilmesine önem verilerek hem enerji ve sinerjiyi arttıracak hem de yeni önlemlerin alınmasına katkı sağlayacak çalışmalar yapılmalıdır.
- Türkiye Veri Sözlüğü Projesi gibi önemli projelerin kısa sürede tamamlanması gereklidir. 3. ve son fazının bu yıl sonunda tamamlanacağı planlanmış olsa da bu çalışmaların siber güvenlik ve savunma bakış açısıyla güncellenmesi faydalı olacaktır.
- Siber Vatan tanımının yapıldığı ve çok benimsendiği bir dönemde, siber savunmanın ontolojik bakış açısıyla da ele alınması gereklidir. Mevcut boşlukların daha kolay tespit edilmesi ve kapatılmasına büyük katkı sağlayacaktır.
- Normalleşmeye çalıştığımız küresel salgında insan faktöründen kaynaklanan zafiyetlerin tavan yaptığı bir dönemde özellikle bunun ontolojik olarak ele alınması ve yeni bakış açılarının geliştirilmesine katkı sağlayacağı değerlendirilmektedir.

- Nitelikli ve yetenekli uzmanların yetiştirilmesine, gelecekte ihtiyaç duyulacak alanlara daha kolay odaklanılmasına, mevcut kaynaklardan maksimum faydalanılmasına, oluşan boşlukların giderilmesine ve en önemlisi ise bu alandaki kaynak ve zaman yönetiminde SGO'lardan faydalanılması gerektiği düşünülmektedir.

TEŞEKKÜR

Bu kitap bölümünün yazılması gerektiği konusunda bana ilham veren Sn. Prof. Dr. Hüseyin Kemal Bayazıt'a teşekkür ederim.

KAYNAKLAR

[1]. N. Fidan ve M. Erden (1998). "Eğitime Giriş" Alkım Yayınevi, Ankara.

[2]. U. Nutku, "Felsefenin Temel Disiplini: Ontoloji", FLSF Felsefe ve Sosyal Bilimler Dergisi, sayı. 1, ss. 79-84, Nis. 2006

[3]. T. Gruber, Ontology. Encyclopedia of Database Systems (Springer-Verlag). Liu, Ling; Özsu, M. Tamer, eds. ISBN 978-0-387-49616-0, http://tomgruber.org/writing/ontology- definition-2007.htm, (2008).

[4]. M. Uschold and M. Grüninger (1996), "Ontologies: principles, methods and applications", Knowledge Engineering Review, Vol. 11 No. 2, pp. 93-155.

[5]. N. F. Noy and D. L. McGuinness (2001), "Ontology development 101: a guide to create your first ontology", Knowledge Systems Laboratory Technical Report KSL-01-05, Stanford University, Stanford, CA.

[6]. L. A. F. Martimiano (2006), "On the structuring of information in computer security systems: the use of ontologies", PhD thesis, ICMC-USP, Sao Carlos (in Portuguese).

[7]. A. J. S. Brandao (2004), "Using ontologies to classify vulnerabilities on security systems", Master Thesis, ICMC-USP, Sao Carlos (in Portuguese).

[8]. https://cbs.csb.gov.tr/birlikte-calisabilirlik-usul-ve-esaslari-i-91315

[9]. D. E. Mann and S. M. Christey (1999), Towards a Common Enumeration of Vulnerabilities, The MITRE Corporation, Bedford, MA, available at: http://cve.mitre.org/docs/docs-2000/ cerias.html

[10]. G. Canbek, S. Sagiroglu & N. Baykal (2016). New Comprehensive Taxonomies on Mobile Security and Malware Analysis. International Journal of Information Security Science (IJISS), 5(4), 106–138.

[11]. CMU Software Engineering Institute, Security and Ontology Resources, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485475

[12]. Ulusal Sağlık Veri Sözlüğü, Çevrimiçi: https://e-saglik.gov.tr/TR,7141/usvs.html.

[13]. T.C. Orman Ve Su İşleri Bakanlığı, Strateji Geliştirme Başkanlığı, Veri Yönetimi ve Bilgi Sistemleri Dairesi Başkanlığı, Veri Envanteri Projesi, Veri Sözlüğü Hazırlama El Kitabı, 2015.

[14]. CB DDO Ulusal Veri Sözlüğü, https://cbddo.gov.tr/projeler/ulusalverisozlugu/

[15]. E. S. Moreira, L. A. F. Martimiano, A. J. S. Brandao, M. C. Bernardes (2008), "Ontologies for information security management and governance", Information Management & Computer Security, Vol.16 No.2, pp.150-165, https:// doi.org/10.1108/09685220810879627 Permanent link to this document: https://doi.org/10.1108/09685220810879627

[16]. T. Takahashi and Y. Kadobayashi, Reference Ontology for Cybersecurity Operational Information, Section D: Security in Computer Systems and Networks The Computer Journal, Vol.58, No.10, pp.2297-2312, 2015. DOI:10.1093/comjnl/bxu101

[17]. M. Ertugrul, A. Gunes, Development of Ontology Knowledgebase for Archive Management Systems, Aksaray University Journal of Science and Engineering, Vol.1, No.2, pp.85-109 DOI: 10.29002/asujse.305026

[18]. https://stids.c4i.gmu.edu/papers/STIDSPapers/STIDS2014_T8_OltramariEtAl.pdf

[19]. L. Obrst, P. Chase, R. Markeloff, Developing an Ontology of the Cyber Security Domain, Semantic Technologies for Intelligence, Defense, and Security (STIDS) 2012 October 23-26, 2012.

[20]. A. Moiseev, Ontologies in information security, 28 June 2021 https://www.kaspersky.com/blog/cybersecurity-ontology/40404/

[21]. W. Swartout and A. Tate (1999), "Ontologies", IEEE Intelligent Systems, Vol.14, No.1, pp.18-19.

[22]. Ontology In AI: A Common Vocabulary To Accelerate Information Sharing, 29/05/2021, https://analyticsindiamag.com/ontology-in-ai-a-common-vocabulary-to-accelerate-information-sharing/

[23]. D. Yargan, A. F. Zambak, Medikal Ontolojiler, DOI: 10.26650/B/ET07.2021.003.02, https://cdn.istanbul.edu.tr/file/JTA6CLJ8T5/3AAB247724B348108564B39347450BDC

[24]. A. Gibson ve R. Stevens (2009). Introduction to Ontologies. M. Popescu ve D. Xu (Eds.) *Data mining in bio-medicine using ontologies*, s.1-21, Artech House.

[25]. M. Swimmer, Towards An Ontology of Malware Classes. [Online] January 27, 2008. http://www.scribd.com/doc/24058261/Towards-an-Ontology-of- Malware-Classes.

[26]. J. D. Howard and T. A. Longstaff, Common Language for Computer Security Incidents. [Technical Report]. Sandia National Laboratories, 1998.

[27]. J. Undercoffer; Pinkston, J.; Joshi, A.; and T. Finin, 2004. A target-centric ontology for intrusion detection. In *18th International Joint Conference on Artificial Intelligence*, 9–15.

[28]. A. Simmonds; Sandilands, P.; and van Ekert, L. 2004. An ontology for network security attacks. In *Applied Comput- ing*. Springer. 317–323.

[29]. Z. Syed, Padia, A., Finin, T., Mathews, L., and Joshi, A. (2016). UCO: A unified cybersecurity ontology. In *Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security*. AAAI Press. http: //ebiquity.umbc.edu/get/a/publication/781.pdf.

[30]. M. Valja, Heiding, F., Franke, U., and Lagerstro ¨m, R. (2020). Automating threat modeling using an ontology framework: Validated with data from critical infrastructures. *Cybersecurity*, 3(19). doi:10.1186/s42400-020-00060-8.

[31]. C. Choi and Choi, J. (2019). Ontology-based security context reasoning for power IoT-cloud security service. *IEEE Access*, 7:110510–110517. doi:10.1109/ACCESS.2019.2933859.

[32]. A. Ekelhart, Fenz, S., Klemen, M. D., and Weippl, E. R. (2006). Security ontology: Simulating threats to corporate assets. In *International Conference on Information Systems Security*, pages 249–259. Springer. doi:10.1007/11961635 17.

[33]. S.A. Petrenko and K. A. Makoveichuk (2017), Ontology of cyber security of self-recovering smart grid. In *Secure Information Technologies (BIT 2017)*, pages 98–106. http://ceur-ws.org/Vol-2081/paper21.pdf.

[34]. O. Menemencioğlu ve I. M. Orak, Semantik Web Arama Motoru Üzerine Bir İnceleme, ISITES 2014, s.614-623, Karabük, Türkiye.

[35]. H. Yang, J: Callan, Ontology Generation for Large Email Collections, https://www.cs.cmu.edu/~callan/Papers/dgo08-huiyang.pdf

[36]. M. Beseiso, A. Rahim Ahmad, R. Ismail, A New Architecture for Email Knowledge Extraction, International Journal of Web & Semantic Technology (IJWesT) Vol.3, No.3, pp.1-10, July 2012.

Bölüm 2

KİŞİSEL VERİLERİN KORUNMASI İÇİN ANLAMSAL WEB TEKNOLOJİLERİNİN KULLANIMI

Özgü Can

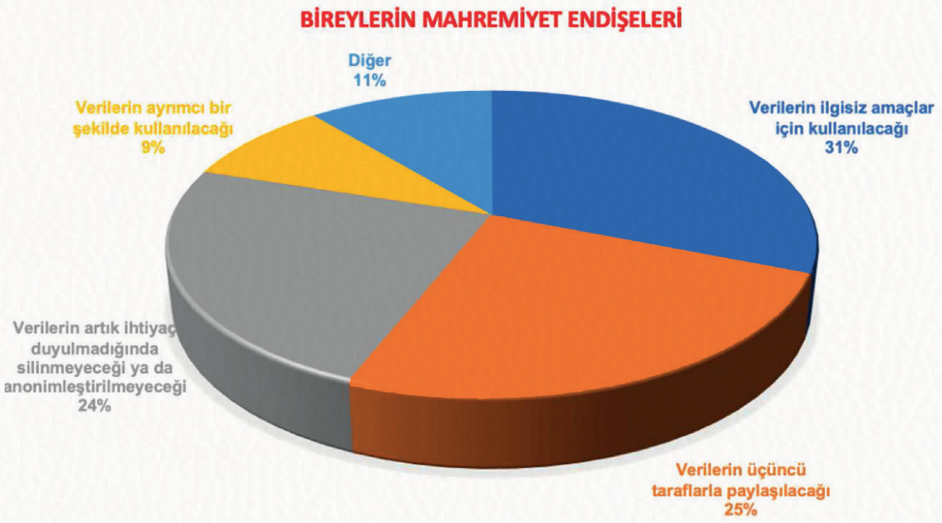
Bilişim teknolojilerindeki gelişmeler bilgi sistemlerinin dijital dönüşüm sürecini hızlandırmıştır. Bu dijitalleşmenin bir sonucu olarak, veriler herhangi bir zamanda ve herhangi bir yerden ulaşılabilir ve kullanılabilir hale gelmiştir. Ancak, veriye erişimin kolaylaşması ile kişilerin mahremiyet kaygıları artmış ve veri mahremiyetine yönelik tehditler ortaya çıkmıştır. Bu nedenle, kişisel verilerin toplanması, saklanması, erişilmesi, paylaşılması ve arşivlenmesi sonucunda ciddi mahremiyet sorunları ortaya çıkmaktadır. Bu amaçla, mahremiyetin korunmasına ve kişisel verilerin gizliliğinin sağlanmasına yönelik önlemler alınmalıdır. Bu kapsamda, kişisel verilerin toplanması, saklanması, yönetilmesi ve paylaşılması için kişisel verilerin korunmasına yönelik KVKK ve GDPR gibi yasal düzenlemeler bulunmaktadır. Bu bölümde, kişisel veri gizliliğinin sağlanması ve mahremiyetin korunması için Anlamsal Web tabanlı çalışmalar ve çözümler sunulmaktadır. Geleceğin Web'i olarak belirtilen Anlamsal Web, bilginin temsilinde ontolojileri kullanarak bilginin makineler tarafından yorumlanabilmesini ve ortak bir bilgi formatı sunarak bilgi sistemlerinin birlikte çalışabilirliğini sağlamaktadır. Bu bölümde, kişisel verilerin korunmasının ve kişisel veri mahremiyetinin önemi, Anlamsal Web'in kişisel veri mahremiyetinin sağlanması ve yasal düzenlemelerin uygulanması kapsamında sunduğu çözümler sunulmaktadır.

2.1. GİRİŞ

Bilginin güç olarak kabul edildiği günümüzde kişisel veriler toplanıp işlenmekte ve karar verme sürecinde kullanılmaktadır. Açık veri yaklaşımı, verilerin uygun şekilde kullanıldığında önemli bir güç sunacağı fikrine dayanmaktadır [1]. İnternet'in bilgiye erişimi kolaylaştırması, bilişim ve iletişim teknolojilerindeki hızlı değişim ve gelişim ile birlikte bu süreçte bilgi güvenliğine ve mahremiyete yönelik birçok tehdit oluşmaktadır. Bireyler, dosya indirme, hizmet/ürün satın alma, oyun oynama, sosyal medya kullanımı ve uzaktan eğitim gibi çeşitli amaçlarla bilerek ya da bilmeyerek kişisel verilerini paylaşmaktadır. Ayrıca, bireylerin belirli servisleri kullanabilmeleri için de bu verileri girmeleri talep edilmektedir. Kullanıcıların demografik bilgileri ile birlikte alışveriş geçmişlerini, tercihlerini, günlük sağlık verilerini ya da üyesi oldukları programları içeren bu kullanıcı verileri kurumlar için oldukça önemli varlıklardır. Veri madenciliği teknikleri kullanılarak kullanıcıların yalnızca ad-soyad ve e-posta adresi bilgileri ile kişisel verileri kolayca çıkarılabilmektedir [2]. Belirli bir kişiyi tanımlamak amacıyla kullanabilecek olan herhangi bir veri, kişisel olarak tanımlanabilir bir bilgidir (*personally identifiable information*, PII). PII'lar, ad, soyad, adres bilgisi, kimlik numarası, ehliyet numarası, banka hesap numarası ya da pasaport numarası gibi bilgiler olabilir. Bu veriler faydalı amaçlar için kullanılabileceği gibi kişisel mahremiyeti ihlal etmeye yönelik bir tehdit de oluşturabilmektedir. Anonim olarak toplansa bile büyük miktardaki kişisel veri, veri sahibinin mahremiyetini ihlal etme potansiyeline sahip üst veri veya kişisel olarak tanımlanabilir veriler şeklinde toplanmaktadır [3].

Bireylerin farklı alanlardan elde edilen verileri tek başına bir anlam ifade etmeyebilirken gerçekleştirilen entegrasyon ve analizler sonucunda farklı veriler ile birlikte kullanıldığında kişilere ait hassas verilerin ortaya çıkmasına neden olmaktadır. Veri ihlali (*data breach*) olarak bilinen bu durumda gizli ya da hassas bilgilere izinsiz olarak erişilmekte, bilgiler çalınmakta ve yetkilendirilmemiş kişiler tarafından kullanılmaktadır. Son yıllarda yaşanan skandallar ile (örneğin, 2018 yılında ortaya çıkan Cambridge Analytica veri skandalı, 2013 yılında 3 milyar kullanıcıyı etkileyen Yahoo veri ihlali, 2021 yılında 700 milyon kullanıcının etkilendiği LinkedIn veri ihlali, vb.) kuruluşların, platform

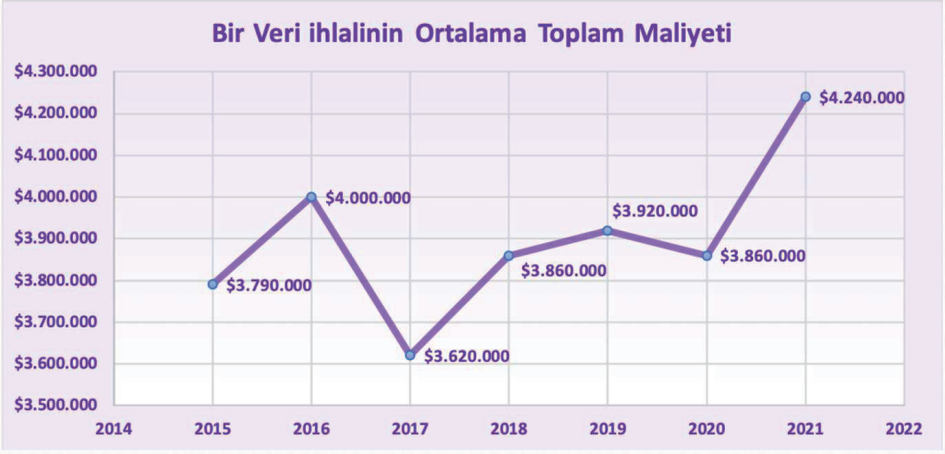
sahiplerinin, araştırmacıların ve diğer üçüncü şahısların bireylerin kişisel bilgilerini kötüye kullandıkları ortaya çıkmıştır. Bu skandallar, bireylerin kişisel veri toplamanın ve analizinin teknik, ticari, politik ve etik yönleri hakkındaki endişelerini arttırmıştır [4]. Pew Araştırma Merkezi'nin ABD'deki yetişkinler üzerinde yapmış olduğu bir araştırmada yetişkinlerin %81'inin şirketler tarafından toplanan verilerinin üzerinde çok az kontrole sahip olduklarını veya hiç kontrollerinin olmadıklarını, %79'unun toplanan veriler ile ilgili endişe duyduklarını, %59'unun toplanan verilerin hangi amaçla kullanıldığı ile ilgili olarak çok az bilgi sahibi olduklarını ya da hiç bilgi sahibi olmadıklarını ve %81'inin risklerin faydalardan ağır bastığını belirttikleri görülmektedir [5]. Cisco tarafından tüketici mahremiyeti kapsamında gerçekleştirilen çalışma sonucunda kişisel verilerinin paylaşımında bireylerin duydukları endişeler Şekil 2.1'de görülmektedir [6]. Bu çalışmaya göre, mahremiyete yönelik en önemli endişeleri şeffaflık ve izlenebilirlik olan bireyler, kişisel verilerinin herhangi bir şekilde kullanılmasının sıkı bir şekilde kontrol edilmesini talep etmektedir. Bireyler özellikle, kişisel verilerinin açıklanmayan, ilgisiz amaçlarla kullanılacağından, pazarlama amacıyla satılacağından ya da üçüncü taraflarla paylaşılacağından ve verilere artık ihtiyaç duyulmadığında verilerin silinmeyeceğinden endişe etmektedir.



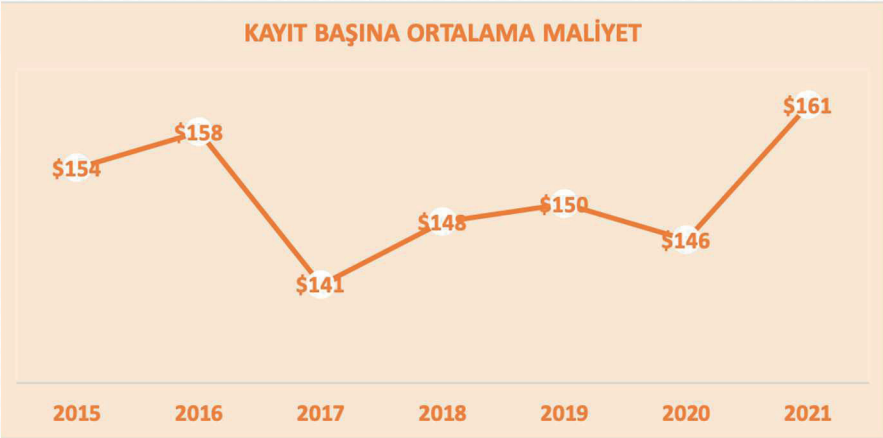
Şekil 2.1. Bireylerin kişisel veri paylaşımındaki mahremiyet endişeleri [6]

IBM'in veri ihlallerinin maliyetine yönelik 2021 yılı raporunda [7], kişisel olarak tanımlanabilir bilgilerin kayıt başına maliyeti en çok ihlalin olduğu müşteri PII'ları için 180 Dolar, tüm veri türleri dikkate alındığında kayıt başına ortalama maliyet 161 Dolar ve bir veri ihlalinin küresel ortalama toplam maliyeti ise 4.24 milyon Dolar olarak belirtilmektedir. Bu rakamların önceki yıllara göre karşılaştırması [7] Şekil 2.2 ve Şekil 2.3'te verilmektedir. İlgili şekillerde de görüleceği üzere veri ihlalinde toplam maliyet hızlı bir şekilde artmaktadır. IBM'in raporunda ayrıca, veri ihlalinde ortalama toplam maliyet için ilk beş sektör (1) sağlık, (2) finans, (3) ilaç endüstrisi, (4) teknoloji ve (5) enerji olarak belirtilmektedir. Şekil 2.4'te veri ihlalinden etkilenen veri türleri [7] görülmektedir. Buna göre, güvenliği en çok ihlal edilen veri türü müşterilerin kişisel olarak tanımlanabilir bilgileridir.

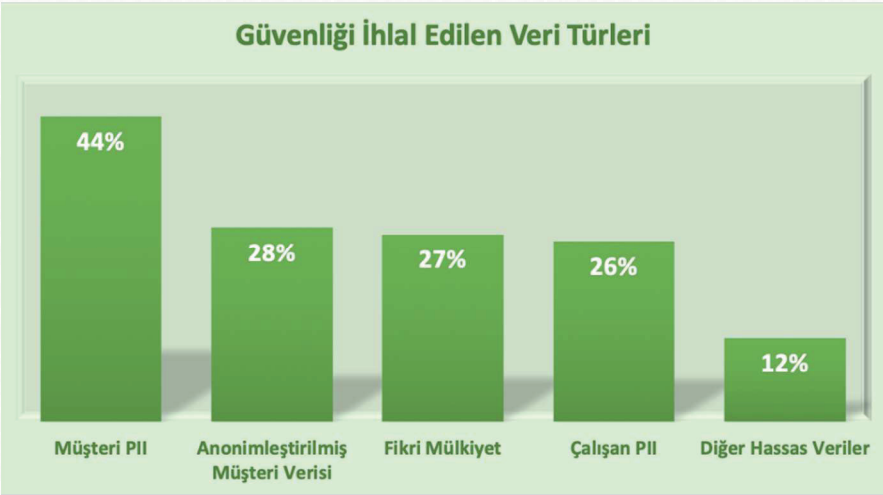
İfşa-kontrolü (*disclosure-control*) olarak adlandırılan süreçte kullanıcıların gizliliğinin korunması hedeflenmektedir [8]. Ayrıca, kullanıcılar da kişisel verilerinin başkaları tarafından kullanımını kontrol etmek istemektedir. Bu amaçla, etkin ve ölçeklenebilir çözümler tasarlanarak mahremiyeti koruyan güçlü modeller geliştirilmelidir. Bu kapsamda, Cisco'nun 2021 yılı veri mahremiyeti çalışmasında da mahremiyetin her zamankinden daha önemli bir önceliğe sahip olduğu ve mahremiyet çağının geldiği raporlanmaktadır [6].



Şekil 2.2. Bir veri ihlalinin ortalama toplam maliyeti.



Şekil 2.3. Bir veri ihlalinin kayıt başına ortalama maliyeti.



Şekil 2.4. Güvenliği en çok ihlal edilen veri türleri.

Günümüzde, kullanıcıların kişisel verilerini korumaya yönelik bilinci artmıştır. Ayrıca, çevrimiçi işlemlere olan güvenin arttırılması amacı ile kullanıcıların kişisel verilerini kontrol edebilmelerine olanak sağlayacak çalışmalar yürütülmektedir. Bu çalışmalarla birlikte her ülkenin kişisel verilerin korunmasına yönelik olarak yürütmekte olduğu regülasyonları ve onam yönetim

süreçleri bulunmaktadır. Regülasyonlar, genel olarak siber güvenlik risklerine odaklanmamakta, temel insan haklarının korunmasıyla ilgilenmektedir. Bu kapsamda, Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK) 2016 yılında [9], Avrupa Birliği'ndeki bireylere ve şirketlere yönelik olan Genel Veri Koruma Yönetmeliği (General Data Protection Regulation, GDPR) ise 2018 yılında [10] yayımlanarak yürürlüğe girmiştir. ABD'nin California eyaletinde 2020 yılında itibaren geçerli olan 2018 Kaliforniya Tüketici Gizliliği Yasası (California Consumer Privacy Act of 2018, CCPA) ve 2023'te yürürlüğe girecek olan Kaliforniya Tüketici Gizliliği Hakları Yasası (California Consumer Privacy Rights Act) gibi çeşitli mahremiyet ve veri gizliliği yasaları bulunmaktadır. Ülkelerin uyguladıkları yönetmelikler konusunda detaylı bir sorgulama ve karşılaştırma DLA Piper'ın Dünya Veri Koruma Kanunları El Kitabı'ndan [11] yapılabilmektedir.

Açık Rıza olarak da bilinen Onam (*consent*) kavramı, mahremiyet yasalarında kullanılmakta ve hassas bilgilerin ifşasını bilginin sahibinin isteklerine göre kısıtlama olarak tanımlanmaktadır [12]. Kişisel verilerin işlenmesinin meşrulaştırılmasında onam önemli bir gerekliliktir ve veri sahiplerinin kişisel verileri üzerindeki kontrolleri için önem arz etmektedir. Bu kapsamda, onam, kanunlar kapsamında kişisel verilerin işlenmesi için bir yasal dayanak olup, yalnızca özgürce verildiğinde, belirli, bilgilendirilmiş ve açık olduğunda geçerli kabul edilmektedir. Elektronik onam yönetim sistemleri, elektronik bilginin sahibinin, belirli durumlarda bu bilgilerin belirli kişilere ifşa edilmesine izin vermesine veya vermemesine olanak sağlar [13]. Böylelikle, hassas verinin ifşasının kontrolü gerçekleştirilebilmektedir.

PII'ları korumaya yönelik olarak çıkarılan kanunlar yürürlüğe girdiğinde kurumlar bu kanunlara uymak zorundadır. Bir kurumun ilgili yasalara, düzenlemelere ve iş kurallarına uymasını sağlamaya yönelik süreç uyumluluk (*compliance*) olarak bilinmektedir. Onam ve uyumluluk ile ilgili bilgilerin temsil edilebilmesi ve farklı taraflar (veri sahibi, veri sorumlusu, veri işleyen ve yetki sahipleri) arasında paylaşılabilmesi için birlikte çalışabilirliğin (*interoperability*) sağlanması gerekmektedir [14]. Ayrıca, veri sahibi ve yetkililerin isteklerine uymak için bilginin sorgulanması gerekmektedir. Anlamsal Web (*Semantic Web*) teknolojileri, kavramları ve kavramlar arasındaki ilişkileri standartları temel alarak açık, birlikte çalışabilir ve sorgulanabilir bir şekilde ifade etmede esneklik sağlamaktadır. Bu nedenle, onam yönetimi sürecindeki

bu bilgilerin temsil edilmesinde Anlamsal Web teknolojilerinin kullanımı ideal bir çözüm sunmaktadır [14].

Anlamsal Web, mevcut Web'in bir uzantısı olup ayrı bir Web değildir. Anlamsal Web'de makine tarafından okunabilir bir Web hedeflenmektedir. Makine tarafından okunabilen bir Web, insan-bilgisayar işbirliğini kolaylaştırmaktadır. Bu amaçla, Anlamsal Web'de bilgisayarların ve insanların işbirliği içinde çalışmasını sağlamak için bilgiye iyi tanımlanmış bir anlam verilmektedir [15]. Böylelikle, bilginin paylaşılması, yeniden kullanılması ve entegrasyonu gerçekleştirilebilmekte, mevcut gerçeklerden ve kurallardan yeni bilgiler çıkarılabilmekte, anlamsal birlikte çalışabilirlik ve makine-makine iletişimi sağlanabilmektedir. Anlamsal Web tarafından sağlanan semantik, makine işlemeyi daha akıllı, uyarlanabilir ve verimli hale getirmek için alan bilgisinin açık bir yorumudur [16]. Anlamsal Web'in sunduğu birlikte çalışabilirlik, farklı tarafların anlamı açık olarak tanımlanmış verilere erişebilmelerini ve bu verileri yorumlayabilmelerini sağlamaktadır [17]. Yorumlanan bu veriler aynı zamanda karar verme sürecine yardımcı olmak amacı ile kullanılmaktadır.

Bu bölümde, veri gizliliği ve kişisel veri mahremiyeti kapsamındaki temel kavramlar açıklanmakta, Anlamsal Web teknolojileri ve önemi anlatılmakta, onam yönetiminin gerçekleştirilmesi ve kişisel verilerin mahremiyetinin korunmasında Anlamsal Web temelli çözümler incelenmektedir.

2.2. TEMEL KAVRAMLAR

Bu bölümde, kişisel veri, veri mahremiyeti ve onam kavramlarının tanımları verilmekte ve ilgili kavramlara yönelik temel bilgiler sunulmaktadır.

2.2.1. Kişisel Veri

Kişisel veri, veri mahremiyetinin sağlanmasındaki temel unsurdur. Hızlı teknolojik gelişmelerin yaşandığı çağımızda, kişisel veri "*internetin yeni yakıtı ve dijital dünyanın yeni para birimi*" [18] olarak belirtilmektedir.

Kişisel veri, veri gizliliğinin ve mahremiyetin korunmasına yönelik yasaların da odak noktasıdır. Kişisel veri kavramı KVKK içerisinde "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmakta-

dır [9]. GDPR'da yer alan 'kişisel veri' tanımı (*Madde 4(1)*) ise "*tanımlanmış veya tanımlanabilir bir gerçek kişiye ('veri sahibi') ilişkin her türlü bilgi*" olarak verilmektedir [19]. Bu tanımda belirtilen 'gerçek kişi'nin tanımı Madde 4(1)'in devamında "*tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir*" olarak yapılmaktadır. İlgili yasalarda da belirtildiği üzere, kişisel veri kişinin uyruğu ve ikametgahı ne olursa olsun korunmalı ve kişilerin kişisel verilerinin korunması haklarına saygı gösterilmelidir.

Bir kişiyi tanımlamanın en yaygın yolu "isim" bilgisidir. Ancak, herhangi bir potansiyel tanımlayıcının (*identifier*) bir bireyi gerçekten tanımlayıp tanımlamadığı bağlama (*context*) bağlıdır [20]. Örneğin, "Ali Yılmaz" her zaman için kişisel veri olmayabilir. Çünkü, bu isme sahip birçok kişi vardır. Ancak, isim bilgisinin başka bilgilerle (doğum yeri, adres, iş yeri veya telefon numarası gibi) birleştirilmesi sonucunda kişiyi açıkça tanımlamak mümkün olabilmektedir. Bu amaçla, bir verinin kişisel veri olup olmadığını belirlemek için çeşitli adımlar bulunmaktadır. Bu adımlar ve bu adımlar ile ilgili kararları vermede kullanılabilecek sorular aşağıdaki gibidir [20]:

- *Tanımlanabilirlik (Identifiability)*: Verilerden veya veri sorumlusunun sahip olduğu veya eline geçmesi muhtemel verilerden ve diğer bilgilerden bireyin kimliği belirlenebilir mi?
- *'İlgili' olma ('relates to')*: Veriler, ister kişisel veya aile hayatı ile ister iş veya meslek ile ilgili olsun, kimliği belirlenebilir bir bireyle 'ilgili' mi?
- *Belirli bir birey hakkında 'açıkça belli' veriler*: Veriler "açıkça" belirli bir birey hakkında mı?
- *Bir bireye bağlı veriler*: Veriler, bir birey hakkında belirli bilgiler sağlayacak şekilde ilgili birey ile 'bağlantılı' mı?
- *İşlemin amacı*: Veriler, tanımlanabilir bir bireyi etkileyen eylemleri veya kararları bilgilendirmek veya etkilemek için mi kullanılıyor ya da kullanılacak?
- *Biyografik önem*: Verilerin bireyle ilgili herhangi bir biyografik önemi var mı?

- *Bilginin bireye odaklanması*: Veri, başka bir kişi, nesne, işlem veya olay yerine temel olarak bireye mi odaklanıyor?
- *Bireyler üzerinde etkisi olan işlem*: Veriler ister kişisel veya aile kapsamında ister iş veya profesyonel kapsamda olsun, bir bireyi etkiliyor mu ya da etkileme potansiyeli var mı?

Verinin kişisel olması onun hassas veri olduğunu belirtmemektedir. Kişisel veri, veri (veri ister hassas ister önemsiz olsun) ile birey arasındaki ilişkiyi ve verinin bir bireye tanımlanabilir olduğunu belirtir [21]. Hassas kişisel veri (*sensitive personal data*) kavramı ise kişisel verinin bir alt kümesidir. Hassas kişisel veri, bireyin ırkını, etnik kökenini, siyasi veya felsefi görüşlerini, dini inançlarını, sendika üyeliğini, sabıka kaydını ya da sağlığı ile ilgili herhangi bir veriyi doğrudan veya dolaylı olarak ortaya çıkaran bilgiler olarak tanımlanmaktadır [22]. Hassas veriler, gizlilik öznitelikleri (*privacy attributes*), açık tanımlayıcılar (*explicit identifiers*) ve yarı-tanımlayıcılar (*quasi-identifiers*) olmak üzere üç kategoriye ayrılmaktadır [23]. Gizlilik öznitelikleri, hastalık ya da engellilik gibi bir birey hakkında herhangi bir özel tanımlanabilir bilgiyi temsil etmektedir. Açık tanımlayıcılar, kimlik numarası, hasta adı ve iletişim bilgileri gibi kişisel olarak tanımlanabilir bilgileri temsil etmektedir. Yarı-tanımlayıcı, doğum tarihi, yaş, cinsiyet ve posta kodu gibi bir bireyin kimliğini yeniden tanımlamak için harici bilgilerle ilişkilendirilebilen bir dizi özelliktir [24]. Yarı tanımlayıcılar, bireyleri kendi başlarına tanımlamak için yeterli olmasa da bireylerin kimliklerini ifşa etmek için kamuya açık verilerle entegre edilebilirler [25]. Örneğin, seçmen kayıt listeleri gibi bazı kamuya açık veritabanları, bireysel kimliğin yanı sıra yaş, cinsiyet ve posta kodu gibi nitelikleri de içerebilir. Yayınlanan veri setleri ile kamuya açık veri setleri entegre edilerek bireyin kimliği ifşa edebilmektedir. Önemli özel bilgilerin sızmasına neden olan bu tür saldırılara bağlama saldırısı (*linking attack*) denir. Bağlama saldırıları verilerin yayınlanmasına yönelik olarak ciddi endişelere neden olmaktadır. Örneğin, 1990 ABD Nüfus Sayımı özet verileri ile gerçekleştirilen çalışma sonucunda Amerika Birleşik Devletleri'ndeki bireylerin %87'si cinsiyetleri, doğum tarihleri ve adreslerinin beş haneli posta kodları ile tanımlanabilmektedir [26].

Kişisel veri olarak kabul edilen verilerin kategorilendirilmiş [27] şekli aşağıda örneklendirilmektedir. Bu veriler tek başına ya da birlikte kullanıldıklarında kişisel veri olarak kabul edilmektedir.

- Biyografik veriler ya da mevcuttaki geçerli bilgileri: Doğum tarihi, kimlik numarası, telefon numarası, e-posta adresi, vb.
- Görünüm ve davranış bilgileri: Göz rengi, boy, kilo, karakter özellikleri, vb.
- Eğitim ve iş yeri bilgileri: Öğrenci numarası, okul adı, maaş, vergi numarası, vb.
- Özel bilgiler: Dini inanç, politik görüş, konum bilgisi, vb.
- Sağlık, genetik ve hastalık bilgileri: Tıbbi geçmiş, hastalık raporları, genetik veri, vb.

2.2.2. Veri Mahremiyeti

Mahremiyet kavramı ülkeler, kültürler ve yargı alanları arasında farklılıklar göstermektedir. Ayrıca, bireylerin mahremiyetlerinin korunmasına yönelik endişeleri ve mahremiyet derecelendirmeleri de kişiden kişiye değişebilmektedir. Kamusal beklentiler ve hukuki yorumlarla şekillenen mahremiyet hakları ve yükümlülükler, kişisel verilerin toplanması, kullanılması, ifşa edilmesi, saklanması ve imhasıyla ilgilidir [28].

Sanayi toplumundan bilgi toplumuna geçiş ile birlikte veri ihlallerinin ortaya çıkması sonucunda bireylerin veri mahremiyetine yönelik endişeleri artmıştır. Bugün devlet kurumları ve özel şirketler, vatandaşlarına ve müşterilerine daha iyi hizmet vermek amacı ile bireylerin kişisel verilerini toplamaktadır. Bireylerin, kuruluşların kendileri hakkında hangi kişisel verileri topladığını, toplanan bu verileri nasıl ve hangi amaçlar için kullandıklarını ve işlediklerini bilmesi gerekmektedir. Kişisel verilerin başkaları tarafından kanuni olmayan yollarla elde edilmesi kişisel veri ihlalidir. GDPR'da 'kişisel veri ihlali'nin tanımı, "*iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlali*" olarak verilmektedir [19].

Kişisel veriler üzerinde otomatikleştirilmiş ya da manuel olarak yürütülen eylemler kişisel verinin işlenmesi kapsamında yer almaktadır. Kişisel verilerin işlenmesi kavramı KVKK tarafından "*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muha-*

faza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" olarak tanımlanmaktadır.

Veri mahremiyetinin korunması, kurumların topladıkları kişisel verileri nasıl işlediklerini ve kullandıklarını kapsaması nedeni ile veri güvenliğinin sağlanmasından çok daha fazlasıdır. Mahremiyet, bireyin temel bir değeridir ve Avrupa İnsan Hakları Sözleşmesi ve İnsan Hakları Evrensel Beyannamesi (*European Convention on Human Rights and the Universal Declaration of Human Rights*) tarafından temel bir hak olarak kabul edilmiştir [29].

ABD Yüksek Mahkemesi'nde Yargıçlık yapmış olan Louis Brandeis'in Samuel D. Warren ile birlikte 1890 yılında yayınladığı ve yasal mahremiyet hakkını savunan ilk çalışma olan Mahremiyet Hakkı (*The Right to Privacy*) makalesinde mahremiyeti "*yalnız kalma hakkı (the right to be left alone)*" olarak tanımlamıştır [30]. Brandeis aynı zamanda mahremiyet hakkının "*hakların en kapsamlısı ve uygar insanların en çok değer verdiği hak*" olduğunu belirtmektedir [31]. Mahremiyet, ahlaki ve yasal bir hak olmasına rağmen, diğer kişi ve kurumların müdahalesinden bağımsız olarak, bireylerin kişisel bir alanı sürdürmeye yönelik çıkarları olarak da algılanmaktadır [32]. Bu kişisel alan, kişinin fiziksel mahremiyetini (bireyin bedeninin ve fiziksel alanının bütünlüğü), kişisel davranışların mahremiyetini, kişisel iletişimlerin mahremiyetini ve kişisel verilerin mahremiyetini içermektedir. Literatürde mahremiyet, (i) kişiye veya kişisel alana erişimin engellenmesi (kişiyi çevreleyen fiziksel alanla ilgili olan bölgesel mahremiyet), (ii) kişisel bilgiler üzerinde kontrol (kişisel verinin nasıl toplanacağı, saklanacağı, işleneceği ve dağıtılacağı ile ilgili kontrol) ve (iii) başkaları tarafından yargılanma ya da denetlenme özgürlüğü (fiziksel arama gibi gereksiz müdahaleler) olmak üzere üç kategoride incelenmektedir [33] [34].

1968 yılında Fried mahremiyetin önemli bir endişe konusu olduğunu belirtmekte ve mahremiyeti "*kişinin kendi hakkındaki bilgisi üzerindeki kontrolü*" olarak tanımlamaktadır [35]. Fried ayrıca, gittikçe karmaşıklaşan bilimsel cihazların daha önce dokunulmamış alanlara gizlice girdiğini, kamu ve özel kurumların kişisel bilgilere yönelik gelişen iddialarının mahremiyetin savunulmasına yönelik bir gereklilik yarattığını ifade etmektedir. Benzer şekilde,

bir diğer mahremiyet tanımlaması ise "*kişi, grup veya kurumların, kendileri hakkındaki bilgilerin ne zaman, nasıl ve ne ölçüde başkalarına iletileceğini kendilerinin belirleme iddiası*" olarak yapılmaktadır [36]. Modern dünyada mahremiyet, "*kişinin kendisi hakkında bilgi edinilmesini veya yayınlanmasını kontrol etme yeteneği*" olarak tanımlanmaktadır [37]. Veri mahremiyeti, bir bireyin kişisel bilgilerinin işlenmesi, ifşa edilmesi ve kullanılması üzerindeki kontrolü ile ilgilidir. Enformasyon Altyapısı Görev Gücü (*Information Infrastructure Task Force*, IITF) veri mahremiyetini "*bir bireyin kişisel bilgilerin – kişiyi tanımlayan bilgilerin – edinildiği, ifşa edildiği ve kullanıldığı koşulları kontrol etme iddiası*" olarak tanımlamaktadır [21].

Veri mahremiyetinin sağlanmasındaki temel prensipler şu şekildedir [22]:

- *Yasallık, adalet ve şeffaflık*: Kişisel veriler her zaman adil, hukuka uygun ve şeffaf bir şekilde işlenmelidir.
- *Amaç sınırlaması*: Kişisel veriler yalnızca belirli ve yasal bir amaç için işlenmelidir.
- *Veri minimizasyonu*: Yalnızca gerçekten ihtiyaç duyulan kişisel veriler işlenmelidir.
- *Doğruluk*: Kişisel verilerin güncel tutulmalı, yanlış verilerin düzeltilmesine ve güncellenmesine yönelik gerekli tedbirler alınmış olmalıdır.
- *Depolama sınırlaması*: Kişisel veriler ihtiyaç olandan daha uzun süre saklanmamalıdır.
- *Bütünlük ve Gizlilik*: Kişisel verilerin kaybolmaya, yok edilmeye veya zarar görmeye karşı korunmasını sağlamak için yeterli güvenlik kontrolleri uygulanmalıdır.
- *İzlenebilirlik*: Veri mahremiyetinin korunduğunu gösterebilmek için uygun önlemlere ve ilgili kayıtlara sahip olunmalıdır.

Veri mahremiyetinin korunması amacı ile Mahremiyet Artırıcı Teknolojiler (*Privacy Enhancing Technologies*, PET) kullanılmaktadır. Şifreleme algoritmaları, kimlik tanıma yöntemleri, veritabanlarında özel arama yöntemleri, anonimleştirme ve veri maskeleme teknikleri gibi PET'ler verileri korumak ve mahremiyet ihlallerini önlemek için kullanılmaktadır. Ayrıca, "Tasarım

yoluyla Mahremiyet (*Privacy by Design*, PbD)" yöntemi ile mahremiyet sağlayan sistemler ve hizmetler geliştirilmesi sağlanmaktadır. GDPR içerisinde de yer alan PbD, bireylerin mahremiyetinin korunmasını amaçlayan bir yaklaşımdır. Bu amaçla, mahremiyet önlemleri ve PET'ler doğrudan bilgi teknolojileri ve sistemlerinin tasarımına entegre edilmektedir.

2.2.3. Onam

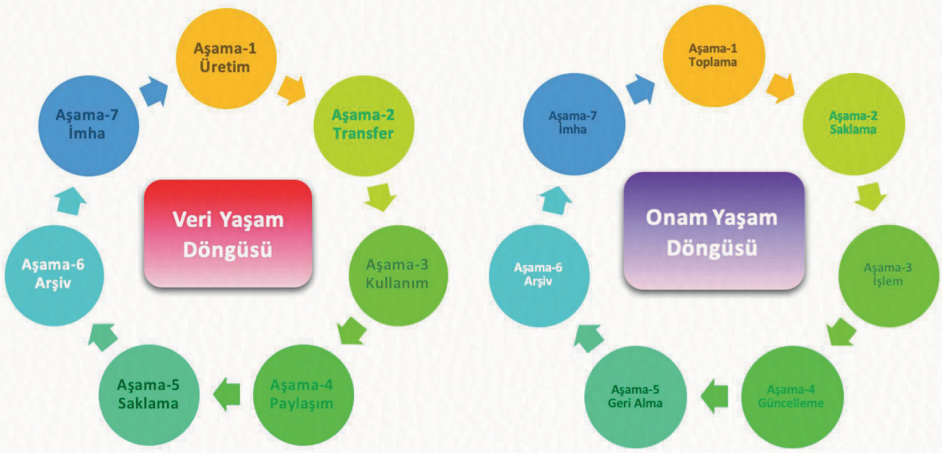
Kuruluşların kişisel verileri etik ve yasal bir şekilde işlemesi, bireylerin onamı olmadan kişisel bilgileri üçüncü taraflarla paylaşmaması gerekmektedir. KVKK ve GDPR gibi hemen hemen her ülkenin özellikle verilerin depolanması ve kullanımı kapsamında veri gizliliğinin sağlanması ve mahremiyetin korunması amacı ile kendi regülasyonu ve bir onam süreci vardır.

Önceki zamanlarda, kişisel veri üzerinde kontrolü sağlamak için en iyi yol verinin ifşasının engellenmesi iken İnternet'in etkin olarak kullanıldığı günümüzde ifşa edilen verinin nasıl kullanıldığını anlamak ve verinin daha fazla kullanımını kontrol etmek için neler yapılabileceği konusu giderek daha çok önem kazanmaktadır [38]. Bu kapsamda, kişisel verilerin işlenmesinde onam kavramı, verilerin nasıl ve ne zaman kullanılabileceğini belirleyen bir mekanizmadır. Onam ayrıca, kişisel verisini kontrol etmek için veri sahibinin elindeki bir önemli araçtır. Kişisel veri, yalnızca veri sahibinin açık onamı ile işlenebilir. Ayrıca, veri sahibi istediği zaman onamını geri çekebilir ve bu durumda da veri işlemenin durdurulması gerekmektedir.

KVKK içerisinde "açık rıza" teriminin kullanıldığı "açık onam" kavramı "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" olarak tanımlanmaktadır [9]. GDPR içerisinde (*Madde 4(11)*) ilgili tanım "*veri sahibinin 'rızası' veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık göstergedir*" olarak verilmektedir [19]. Kişinin onamını özgürce vermesi, kişiye gerçek bir seçim hakkı verilmesini, kişinin onamını reddedebilmesini ve istediği zaman da kolayca geri alabilmesini belirtmektedir. Ayrıca, kişinin farklı veri işleme türleri için farklı onamlar verebilmesi de bu kapsamdadır. Tanımda yer alan spesifik kavramı, onamın açık ve anlaşılır bir dil ile ifade

edilmesini belirtmektedir. Bilinçli onam (*informed consent*) kavramı ise, işlemin niteliği, işlenme amacı ve veri sorumlusunun kimliği ve onamın geri alınmasına ilişkin bilgiler verilerek veri sahibinden onam alınması gerektiğini belirtmektedir [39]. Böylece, onam veren kişinin neye rıza gösterdiğini anlaması gerekmektedir. Bilinçli onamda, onamın hangi eylem(ler)e izin verdiği, yetkilendirmenin kime verildiği, yetkilendirmenin hangi amaç(lar) için geçerli olduğu ve hangi zaman diliminde uygulanacağı açık olarak ifade edilmelidir [13]. Tanımda belirtilen açık gösterge ise veri sahibinin kişisel verilerinin işlenmesini kabul ettiğinin bir göstergesi olarak açık ve olumlu bir eylemde (örneğin, onam verdiğini belirten işaretlenmiş bir onay kutusu) bulunmasını ifade etmektedir [39].

Kişisel veriler Şekil 2.5'te yer alan veri yaşam döngüsünde belirtilen aşamalardan geçmektedir [40]. Kişisel veri yaşam döngüsü veri toplamayı içeren üretim aşaması ile başlamakta, verinin transferi ve kullanımından sonra üçüncü partilerle paylaşılması gerçekleştirilmektedir. Bu aşamada, kullanıcının onamı dikkate alınmaktadır. Ayrıca, verinin paylaşımından önce anonimleştirme ve veri maskeleme gibi verinin başka veriler ile bağlantısını kurulmasını önlemeye yönelik tedbirler de bu aşamada alınmalıdır. Veri daha sonra kurum içerisinde saklanmakta ve bazı durumlarda arşivlenebilmektedir. Son aşamada ise onamın geri alınması durumunda verinin imhası gerçekleşmektedir. Şekil 2.5'te veri yaşam döngüsü ile birlikte onam yaşam döngüsü [39] de sunulmaktadır. Onam yaşam döngüsünün aşamaları farklıdır. Buna göre, ilk aşamada onam toplanmakta, daha sonra veri işlemeye uygunluğun kontrol edilmesi için saklanmakta ve işlenmektedir. Bireyin onamı süreç içerisinde değişebileceğinden, onamın güncellenmesi gerekmektedir. Onamın geri alınması da söz konusu olacağından, imha işleminden önce onam belirli bir süre arşivlenmelidir. Veri ve onam yaşam döngüleri birlikte değerlendirildiğinde, verilerin toplanmasının veri toplamanın onama uygunluğunu sağlamak için onam işlendikten sonra başlaması nedeni ile veri yaşam döngüsünün birinci aşamasının onam yaşam döngüsünün üçüncü aşamasından sonra başladığı görülmektedir [39]. Ayrıca, onamın köken bilgisini (*provenance*) tutmak için onam yaşam döngüsü veri yaşam döngüsü sona erdikten sonra devam etmektedir.



Şekil 2.5. Veri ve onam yaşam döngüleri [39, 40]

Hem kişisel veri yaşam döngüsünde hem de onam yaşam döngüsünde güvenliğin önemli olduğu unutmamalıdır. Verinin toplanması, transferi, saklanması ve işlenmesi gibi aşamalarda güvenliğin sağlanması için kapsamlı bir güvenlik stratejisi uygulanmalıdır. Kapsamlı bir güvenlik stratejisi, mevcut altyapı ile uyumlu olarak tehdit yönetimini, güvenlik açığı yönetimini ve uygulamaya özel güvenliği sağlayan güvenlik önlemlerinden oluşmaktadır [13]. Bir sonraki bölümde, onam yönetiminin gerçekleştirimi, kişisel verilerin gizliliğinin sağlanması ve mahremiyetin korunmasına yönelik mevcut çözümler incelenmektedir.

2.3. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK ÇÖZÜMLER

Onam yönetimi, veri mahremiyeti ve kişisel verilerin korunması kapsamlarındaki çalışmalar hukuk, bilgi güvenliği ve bilgi yönetişimi bağlamlarında değerlendirilmektedir. Veri mahremiyetine yönelik mevzuatların, kişisel veri toplama ve işleme teknolojilerinin gelişmesi ile birlikte yürürlüğe girmesi alandaki çalışmalar için bir temel oluşturmaktadır.

Elektronik onam yönetim sistemi, elektronik bilgilerin sahibinin bu bilgilerin belirli kişilere belirli durumlarda açıklanmasına izin vermesini ya da reddetmesini sağlamaktadır [13]. Elektronik onam yönetim sistemleri, dijital hak yönetim sistemlerine (*Digital Rights Management*) benzerlik göstermektedir

[12]. Fikri mülkiyetin korunması ve telif hakkı yasalarının ihlalleriyle mücadele etmek amacıyla dijital bilgilerin kontrollü dağıtımını kolaylaştırmak için kullanılan dijital haklar yönetimi, ayrıca mahremiyet haklarının yönetimine (*privacy rights management*) yönelik olarak da uygulanabilmektedir [41].

Onam kavramının sağlık sektöründe 'hasta onamı' olarak sıkça yer alması nedeni ile onam yönetimi ile ilgili çalışmalar daha çok sağlık alanı özelinde yoğunlaşmaktadır. Ek olarak, GDPR'da sağlık ile ilgili kişisel verilerin işlenmesinin yasak olduğu belirtilmiştir [19] (*Madde 9 (1): "Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır."*). Bu nedenle, sağlık alanında onam yönetiminin etkin ve doğru bir şekilde gerçekleştirilmesi önem kazanmaktadır. Hasta onamı, tıbbi bir prosedür veya tedavi, bir klinik araştırması veya genetik test hakkında olası riskler ve faydalar ile ilgili önemli bilgileri içeren bir belgedir. Sağlık alanında onam yönetimi sistemi, hastaların sağlık hizmet sağlayıcılarının erişimi ve paylaşımı için hangi verilerine izin vereceklerini belirlemelerini sağlayan bir sistem, süreç veya politikalar kümesidir [12]. Böylelikle, hastalar onam yönetim sistemini sağlık kayıtlarının ve diğer kişisel bilgilerinin açıklanmasını ve paylaşımını kontrol etme yöntemi olarak kullanmaktadır. Sağlık bilgi sistemlerinde onam yönetim sistemlerinin kullanım amacı, hastanın onam sürecini otomatikleştirmek, erişim denetim mekanizmalarını ve politika uygulama süreçlerini kullanan bir bilgi teknolojisi mimarisinden yararlanmaktır [42]. Ayrıca, onamın kişisel verilerin ifşa edilmesine izin verilmesi ya da verilmemesine yönelik genel bir model sunması nedeni ile mahremiyetin sağlanmasını hedefleyen çalışmalarda onam tabanlı mahremiyet modellerinin kullanıldığı çözümler sunulmaktadır [43]. Örneğin, [44]'de sunulan çalışmada IoT (*Nesnelerin İnterneti*, *Internet of Things*) cihazlarında kullanıcıların kişisel verilerinin toplanması ve kullanımı doğrultusunda ortaya çıkan mahremiyet problemlerine yönelik olarak onam tabanlı bir mahremiyet çerçevesi önerilmektedir. Benzer şekilde, IoT-tabanlı akıllı binalardaki mahremiyet endişelerini gidermek için verilerinin nasıl toplandığı ve kullanıldığı konusunda kullanıcıların farkındalıklarını artırmak ve bilgilendirmek amacı ile onam tabanlı bir model [45]'de sunulmaktadır. [46] çalışmasında, sağlık araştırması verilerinin paylaşılmasın-

da onam sürecinin yönetimi için blokzincir tabanlı bir sistem önerilmektedir. Blokzincir tabanlı onam yönetim sistemlerinin sunulduğu diğer çalışmalarda da [47] [48] [49] hastaların sağlık verilerinin işlenmesinde onam yönetim sisteminin gereksinimlerinin karşılanması hedeflenmektedir. Hastaların sağlık verilerine kimlerin ne sıklıkla eriştiğini görerek veri erişimiyle ilişkili riskleri ve faydaları karşılaştırarak bilinçli bir karar önerecek bir hasta onam yönetim sistemi [50] çalışmasında sunulmaktadır. İlgili çalışmalara ek olarak literatürde, sağlık alanı özelinde elektronik sağlık kayıtlarının onam tabanlı mahremiyet-farkında olarak paylaşılması amacı ile çeşitli çözüm yaklaşımları [51] [52] [53] önerilmektedir. Ayrıca, sağlık verilerinin kişisel veri kapsamında mahremiyetinin korunması amacı ile ulusal ve uluslararası yönetmeliklerde yer alan düzenlemeler [54] çalışmasında incelenmektedir.

Son yıllarda kişisel verilerin korunması amacı ile her ülkenin kendi regülasyonunu ve onam sürecini yürürlüğe sokması ile kişisel verilerin korunması ve mahremiyetin sağlanması amacı ile regülasyonları temel alan çözüm yaklaşımları artmıştır. Bu kapsamdaki çalışmalar, GDPR ile uyumlu olarak veri sahiplerinin mahremiyet ayarlarını kontrol etmelerini, değiştirmelerini ve haklarında saklanan tüm kişisel verilerden haberdar olmaları amacı ile onam yönetiminin sağlanması [55], GDPR'da yer alan izlenebilirlik (*accountability*) kavramını desteklemek amacı ile kriptografik bir onam yönetimi sağlanması [56], GDPR'ın gereksinimleri doğrultusunda kişisel verilerin korunmasında blokzincir teknolojisinin kullanımı [57] [58] [59] [60] [61] [62], "Tasarım yoluyla Mahremiyet" kavramının yasal gereksinimler doğrultusunda teknik çözümlerinin uygulanması [63], kişisel verilerin GDPR uyumlu olarak veri mahremiyetini koruyacak şekilde paylaşılması [64] gibi çözüm önerilerini içermektedir. [65] çalışmasında ise KVKK kapsamında bir onam yönetim sistemi önerisi sunulmaktadır.

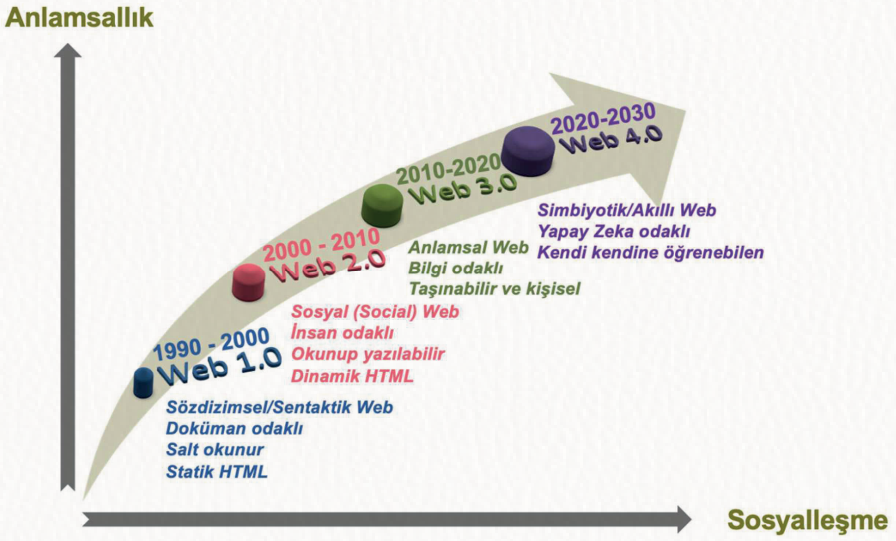
Mahremiyete yönelik çalışmaların odaklandıkları problemlerden biri mahremiyeti arttırırken sistemlerin doğru bir şekilde çalışmasını engellemeyecek çözümlerin geliştirilmesidir. Bir öneri sisteminin kullanıcı hakkında toplanan verileri kullanarak daha doğru öneriler üretmesi sağlanırken, kullanıcıların da kendi verilerini yönetmesine ve kontrol etmesine olanak tanınması [66] ilgili kapsamdaki çözümlere örnek olarak verilebilecek yaklaşımlardan biridir. Literatürde ayrıca, kişisel verilerin korunmasında makine öğrenmesi ve derin öğrenme yöntemleri kullanılarak güvenlik ihlallerinin tespit edilmesine ve mahremiyeti koruyan veri analizi gerçekleştirilmesine yönelik çalışmalar

da mevcuttur [67] [68]. Tüm bu çözüm yaklaşımlarının dışında, kullanıcıların mahremiyet endişelerinin kişisel verilerinin toplanması, kullanılması, işlenmesi ve iletimi ile ilgili endişeleri ile birlikte değerlendirildiği çalışmalarda da kişisel verilerin korunmasının önemi tartışılmaktadır [69] [70].

Mevcut çalışmalar dikkate alındığında, onam yönetimi, kişisel verilerin korunması ve mahremiyetin sağlanmasına yönelik olarak farklı alanlarda güncel teknolojilerin kullanıldığı çözüm yaklaşımları önerilmektedir. Kişisel verilerin korunmasına yönelik regülasyonlarında da etkisi dikkate alındığında elektronik bilgi sistemlerinin artık "Tasarım yoluyla Mahremiyet" kavramı dikkate alınarak tasarlanması gerekmektedir.

2.4. ANLAMSAL WEB TEKNOLOJİLERİ

Başarılı bir mühendislik eseri olan Web milyarlarca web sayfasına ve kullanıcıya sahiptir. Haziran 2021 itibarı ile çevrimiçi olarak 1,86 milyardan fazla web sitesi vardır [71]. Web'in yıllar içerisindeki gelişimi Şekil 2.6'da görülmektedir. 1980'li yıllarda kişisel bilgisayarların hayatımıza girmesi ve 1990'lı yıllarda internetin yaygın olarak kullanılmaya başlanması ile web teknolojilerinde de birçok gelişme meydana gelmiştir.



Şekil 2.6. Web'in gelişimi

Kullanıcılarına değerli bilgiler ve faydalı hizmetler sunan geleneksel Web teknolojileri web sayfalarını tanımlamakta ve web sayfalarını birbirine bağlamaktadır. Geleneksel Web, belgelerin yayınlanmasını, belgeler erişilmesini ve belgeler arasında bağlantılar kurulmasını sağladığı için küresel bir belge deposu sağlamaktadır. Bu nedenle, geleneksek Web'in içeriği makinelerden çok insanlar için biçimlendirilmiştir. Bilgi yönetimi kapsamında geleneksel Web aşağıda belirtilen konularda sınırlı kalmaktadır [72]:

- *Bilginin aranması:* Bilginin aranmasında anahtar kelime tabanlı arama motorlarına bağımlıdır.
- *Bilgi çıkarımı:* Bilginin getirimi (*retrieval*) için kişilerin zamanı ve çabası gerekmektedir. Mevcut akıllı etmenler bu görevi yeterli bir şekilde yerine getirememektedir.
- *Bilginin yönetimi:* Terminolojideki tutarsızlıklar ve güncel olmayan bilgilerin kaldırılamaması nedeni ile problemler yaşanmaktadır.
- *Bilginin keşfi:* Veritabanlarında örtük olarak var olan yeni bilgi, veri madenciliği yöntemleri kullanılarak ortaya çıkarılmaktadır. Ancak bu işlem, dağıtık ve zayıf yapılandırılmış dokümanlar için zordur.
- *Bilginin görüntülenmesi:* Bazı durumlarda, bilgiye erişimin belirli kişilerle sınırlandırılması gerekmektedir. Belirli bilgileri gizleyen "görünümler", veritabanı alanından bilinmektedir. Ancak, bu işlemin Web üzerinden gerçekleştirilmesi zordur.

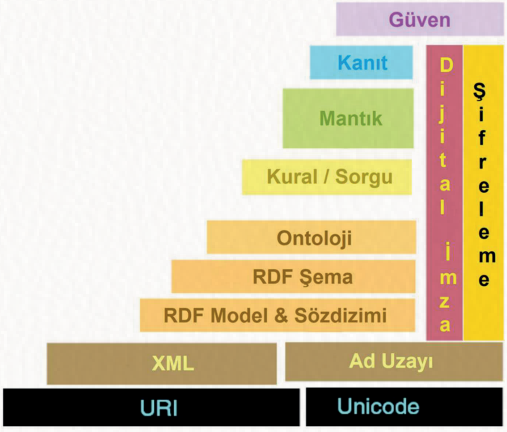
World Wide Web'in (WWW) yaratıcısı olan Tim Berners-Lee, bilginin yönetimini ve paylaşımını sağlayamayan geleneksel web teknolojilerinin yetersizliklerini [73] fark ederek Web'i daha zeki bir duruma getirmek amacı ile bir öneri yapmıştır. Bu kapsamda, makineler tarafından da anlaşılabilecek web sayfalarına ve bilginin bütünleştirilmesi için ontolojilerin kullanımına gereksinim olduğu sonucuna ulaşmış ve Semantik Web olarak da bilinen Anlamsal Web (*Semantic Web*) kavramını ortaya koymuştur.

Anlamsal Web, bilginin paylaşılmasını ve yeniden kullanımını sağlamak için, biçimsel anlambilimini kullanarak makinelerin diğer makineler ile iletişimine izin vermektedir. Böylece, geleneksel Web'de kullanıcılar Web sayfalarını okuyup kararlarını vermekteyken, Anlamsal Web'de ortak ontolojiler ve betimleme dilleri kullanılarak kullanıcıları temsil eden etmenler Web sayfalarını okuyup anlayabilir ve karar verebilirler [74].

Gelişmiş bilgi yönetim sistemlerinin geliştirilmesini amaçlayan Anlamsal Web, geleneksel Web'in sınırlı kaldığı konulara yönelik aşağıdaki çözümleri sunmaktadır [72]:

- Bilgi, anlamına göre kavramsal bir kapsamda düzenlenmektedir.
- Otomatik araçlar, tutarsızlıkları kontrol ederek ve yeni bilgiler çıkararak verinin yönetimini desteklemektedir.
- Anahtar kelimeye dayalı arama, sorgu yanıtlama ile değiştirilmektedir. Böylelikle, istenen bilginin getirimi, çıkarımı ve kişilerin anlayabileceği bir şekilde sunulması gerçekleştirilmektedir.
- Birçok belge üzerinden sorgu yanıtlama desteklenmektedir.
- Kimlerin bilginin/belgelerin belirli kısımlarını görebileceği belirlenebilmektedir.

Anlamsal Web'in vizyonu, Web'in prensiplerini belgelerden verilere genişletmektir. Buna göre, verilere genel Web mimarisi kullanılarak erişilmelidir. Örneğin, URI'lerin kullanımı ile veriler belgeler gibi birbiriyle ilişkili olmalıdır. Böylelikle, verilerin uygulamalar arasında paylaşılması ve yeniden kullanılması, otomatik olarak işlenmesi ve ayrıca veri parçaları arasındaki olası yeni ilişkilerin ortaya çıkarılması sağlanmaktadır [75]. Anlamsal Web'in Tim Berners-Lee tarafından önerilen ve "*Anlamsal Katmanlı Kek (Semantic Layer Cake)*" olarak bilinen katmanlı yapısı Şekil 2.7'de yer almaktadır [76]. Bu katmanlı yapıda yer alan bileşenlerin rolleri Tablo 2.1'de açıklanmaktadır.



Şekil 2.7. Anlamsal web'in katmanlı yapısı.

Tablo 2.1. Anlamsal web bileşenleri.

Bileşen	Rol
Güven	Güven, içeriğin kalitesini, kökenini ve güvenilirliğini belirtir. Sayısal imzaları, güvenilir etmenleri, sertifika kuruluşları ve tüketicilerin önerilerini temel alan diğer bilgi türlerinin kullanımı ile ortaya çıkmaktadır [74]. Güven, Anlamsal Web katmanlı yapısının en üstünde yer alması nedeniyle çok önemli bir kavramdır.
Dijital İmza Şifreleme	Şifreleme, Anlamsal Web ifadelerinin güvenilir bir kaynaktan geldiğinden emin olmak ve doğrulamak için önemlidir. Bunun gerçekleştirilmesi de RDF ifadelerinin dijital imzası ile sağlanmaktadır.
Kanıt	Kanıt katmanı hem tümdengelimli işlemleri hem de Web dillerinde kanıtların temsil edilmesini ve kanıt onaylanmasını içermektedir [74].
Mantık	Mantık, ontoloji dilini güçlendirmek ve uygulamaya özel bildirim deyimi bilgisinin yazımına izin vermek için kullanılmaktadır [74].
Kural Sorgu	Çıkarsama işleminin gerçekleştirilmesi OWL ile sınırlıdır. Bu nedenle, makinelerin anlayabilmesi ve çıkarsama yapabilmesi için kurallar ve kurallar için biçimleme dili tanımlanmalıdır [77]. Kurallar, uyulması gereken kısıtları tanımlamaktadır. Verilerde bulunan sözdizimsel, anlamsal ve yapısal bilgilere dayalı olarak hem açık hem de dolaylı olarak türetilmiş bilgilerin elde edilmesi anlamlı sorgular ile gerçekleştirilmektedir. SPARQL [78], RDF verileri üzerinde sorgu gerçekleştirmek için kullanılan ve W3C tarafından önerilen bir sorgu dilidir. Bu nedenle, RDF depoları için SQL olarak kabul edilir.
Ontoloji	Ontoloji, bir etki alanının (*domain*) kavramlar (*concepts*) ve bu kavramlar arasındaki ilişkiler (*relationships*) açısından tanımını ifade etmektedir. Ontoloji katmanı, Web Ontoloji Dili'nden (*Web Ontology Language*, OWL) [79] oluşur. OWL, sınıflar arasında ilişkilerin tanımlanması, eleman sayısı, eşitlik, özelliklerin zengin bir biçimde sınıflandırılması, özelliklerin nitelikleri ve listelenmiş sınıflar gibi özelliklerin ve sınıfların tanımlanması için zengin bir söz varlığı tanımlama dilidir [74]. OWL, RDFS'den daha anlamlı ontolojiler tanımlanmasını sağlar. W3C tarafından Anlamsal Web için benimsenmiş standart bir ontoloji dilidir.
RDF Şema	RDF Şema (*RDF Schema*, RDFS) [80], RDF (*Resource Description Framework*) [81] tabanlıdır ve RDF kaynaklarının özelliklerini ve sınıflarını anlamsallıkla tanımlayan söz varlığı tanımlama dilidir. RDF, meta verileri işlemek için bir temeldir ve Web üzerinde makineler tarafından anlaşılabilir bilgi alışverişi yapan uygulamalar arasında birlikte çalışabilirliği sağlar. Temel olarak RDF, verilerin makine tarafından işlenebilir anlamsallığını tanımlamak için bir veri modeli tanımlar. RDF hem XML hem URI katmanına dayanır. Bu nedenle bu katmanların üstünde yer almaktadır. RDF Şema, Web nesnelerini sıradüzen içerisine düzenleyen modelleme ilkelleri sağlamaktadır [74]. Sınıflar ve özellikler, alt sınıf ve alt özellik ilişkileri, etki alanı (*domain*) ve sınır (*range*) kısıtlamaları temel ilkellerdir. RDF ve RDF Şema"nın betimleme gücü sınırlıdır. Daha fazla anlamsallığa sahip söz varlıklarının tanımlanmasını ontoloji katmanına bırakır.

RDF Model ve Sözdizimi	RDF veri modelini tanımlar. RDF, kaynaklar (*resources*), özellikler (*properties*) ve ifadeler (*statements)* olmak üzere üç nesne türünden oluşur [82]. URI ile adlandırılan kaynak, bir web sayfası ya da web sayfasının parçası olabilir. Özellikler, kaynağı tanımlamak için kullanılan niteliklerdir. Bir RDF ifadesi ise adlandırılmış bir özellik ile birlikte belirli bir kaynak ve o kaynak için o özelliğin değeridir.
XML Ad Uzayı	XML (*eXtensible Markup Language*), kullanıcı tarafından tanımlanmış söz varlığı kullanılarak yapısal Web belgeleri yazılmasını sağlayan bir dildir. Paylaşılabilir bir içerik oluşturulmasını sağlar. XML çakışan etiket problemini gidermek için ad uzayını kullanır.
URI Unicode	Bir şeyleri tanımlayabilmek ya da onlara başvurabilmek için URI'ler (*Uniform Resource Identifier*) kullanılmaktadır. Benzersiz/özgün bir şekilde tanımlanan bir URI, bilgi temsil yapılarını tanımlayarak, bir kaynağı tek tip bir şekilde temsil edecek bir tanımlayıcıyı açık bir şekilde belirtmektir. Kaynakların bu şekilde etiketlenmesi sonucunda veri kaynaklarının entegrasyonu kolaylaşır.

2.4.1. Ontoloji

Anlamsal Web'te bilgiye iyi tanımlanmış bir anlam verilerek, bilgisayarların ve insanların işbirliği içinde çalışması hedeflenmektedir. Mevcut Web'in bir uzantısı olan Anlamsal Web, makine tarafından okunabilir bir Web'tir. Makine tarafından okunabilen bir Web, insan-bilgisayar işbirliğini kolaylaştırmaktadır [83]. Böylelikle, belirli görevler makinelere devredilebilmekte ve otomatik olarak işlenebilmektedir. Web'in ilkelerini ve teknolojilerini kullanmakta olan Anlamsal Web, Web'in paylaşılan bir kaynak olduğu ve bu nedenle, makine tarafından okunabilen bir Web içinde, anlamın da paylaşılması gerektiği gerçeğiyle ilgilenmektedir [83]. Bu amaçla Anlamsal Web, makine tarafından okunabilen bir temsil olan ontoloji kavramını içermektedir. Ontolojiler aracılığıyla, kavramların anlamı ve kavramlar arasındaki ilişkiler tanımlanmakta ve böylelikle kavramlar yazılım tabanlı akıl yürütücüler (*reasoner*) tarafından işlenebilmekte ve anlaşılabilmektedir.

Bölüm 1'de de kapsamlı açıklandığı gibi Yunan dilindeki özgün biçimi Οντολογια olan ontoloji terimi felsefeden gelmektedir ve felsefenin bir alt alanı olan varlık biliminin adıdır [72]. Genel olarak, var olan şeylerin türlerini ve onların nasıl tanımlanacağından söz eder [74]. Bilgisayar bilimleri alanında da kullanılmaya başlanmış olan ontoloji terimi özgün anlamından farklı olarak teknik bir anlam kazanmıştır.

Thomas R. Gruber tarafından yapılmış olan, daha sonra da Rudi Studer tarafından yenilenmiş olan tanımda "*bir ontoloji paylaşılan bir kavramsallaştırmanın açık ve biçimsel bir belirtimi"*dir [84]. Bu tanımda yer alan kavramların her biri aşağıdaki gibi ifade edilmektedir [83]:

- *Biçimsel:* Belirtim, makine tarafından işlenebilir olan biçimsel bir dilde temsil edilmektedir. Anlamsal Web için bu, RDF ya da OWL gibi standart gösterim dillerinden biridir.
- *Açık:* Bir belirtimde, bir etki alanının ne kadarının içerilmesi gerektiğine dair bir tasarım dengesi vardır: ayrıntı düzeyi ve soyutlama ya da genellik düzeyi. Bu tasarım alanının boyutları kullanılabilirliği ve yeniden kullanılabilirliği içermektedir:
  - *Kullanılabilirlik (Usability):* Hem geliştiriciler ya da hedeflenen bir topluluk tarafından anlaşılabilir olmayı hem de ontolojinin içinde kullanıldığı görevler ve yazılım uygulamaları ile ilgili kavramsallaştırma ve gereksinimler arasındaki eşleşmeyi içermektedir.
  - *Yeniden Kullanılabilirlik (Reusability):* Herhangi bir göreve, yazılım bileşenine ya da başka bir ontolojiye bağımlılığı en aza indirmektedir.
- *Belirtim:* Bir ontoloji, bir artifaktın bir açıklamasıdır ve tanımlanan varlıktan bağımsızdır.
- *Paylaşılan:* Bir ontoloji yalnızca bir kullanım topluluğu tarafından paylaşılırsa anlamlıdır. Anlamsal Web bağlamında ontolojilerin amacı ve faydası, bir kaynağın yaratıcısı ile kullanıcısı arasındaki birlikte çalışabilirliği desteklemesidir. Tek bir makinede gizlenmiş bir dizi biçimsel ifade, bir ontolojinin tanımını ve amacını yerine getirmemektedir.
- *Kavramsallaştırma:* Bir görev veya amaç için gerekli olan bir etki alanının basitleştirilmiş soyut bir görünümüdür. Bu kapsamda, ontolojilerin belirli bir etki alanına göre bir tutarlılık ve tamlık düzeyine sahip olması beklenmektedir.

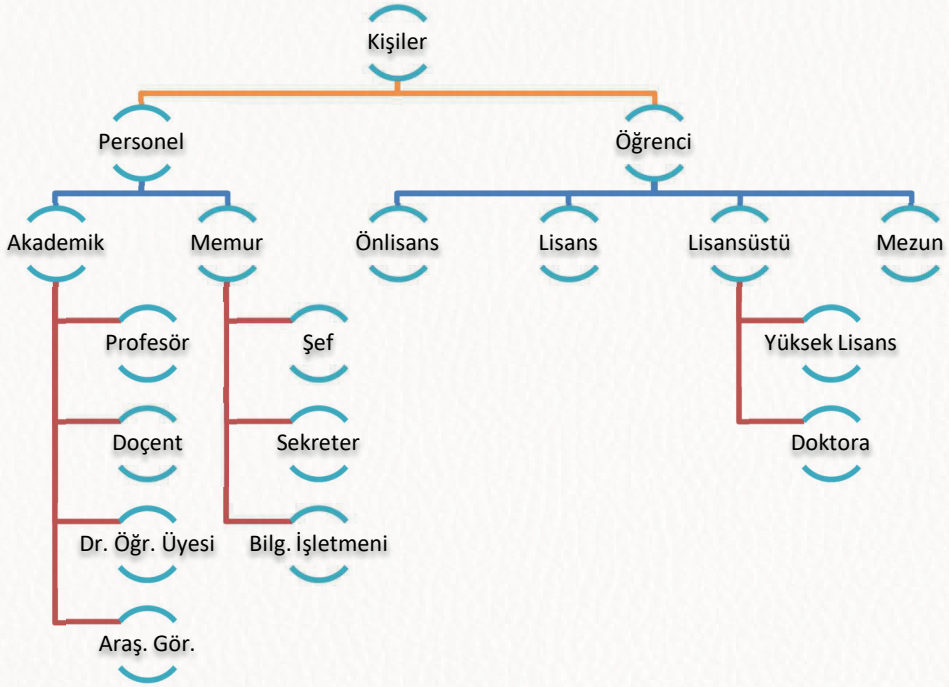
Ontolojiler, birlikte çalışabilirliği ve ortak anlayışı desteklemek için kullanılmaktadır. Böylece, herhangi bir kaynaktan gelen herhangi bir veri, ontolojiler kullanılarak bilgi tabanına entegre edilebilmektedir [85]. Genel olarak, bir ontoloji bir etki alanının biçimsel bir anlatımını tanımlamakta ve etki alanı

hakkında ortak bir anlayış sağlamaktadır. Bu ortak anlayış, terminolojideki farklılıkların üstesinden gelmek için gereklidir. Örneğin, bir uygulamada yer alan "posta kodu" başka bir uygulamadaki "alan kodu" ile aynı olabilir. Benzer şekilde, iki uygulama aynı terimi farklı anlamlar için de kullanabilmektedir. Örneğin, bir uygulama "alan kodu"nu adres bilgisinin posta kodu olarak kullanırken diğer uygulamada "alan kodu" ev telefonu için alan kodu anlamında kullanabilir. Bu nedenle, belirli bir terminolojiyi paylaşılan bir ontolojiye eşleyerek (*mapping*) ya da ontolojiler arasında doğrudan eşlemeler tanımlayarak ilgili problem çözülmektedir [72]. Her iki durumda da ontolojiler anlamsal birlikte çalışabilirliği desteklemektedir.

Bir ontoloji, sonlu bir terimler listesinden ve bu terimler arasındaki ilişkilerden oluşmaktadır. Terimler, etki alanının önemli kavramlarını (nesne sınıflarını) belirtmektedir [72]. Örneğin, bir üniversite ortamında personel, öğrenciler, kurslar, amfiler ve disiplinler temel kavramlardandır. İlişkiler tipik olarak sınıf hiyerarşilerini içermektedir. Eğer bir A sınıfındaki her nesne aynı zamanda A'' sınıfında da yer alıyorsa, bir hiyerarşi A sınıfının A'' sınıfının bir alt sınıfı olduğunu belirtir. Örnek bir hiyerarşi Şekil 2.8'de görülmektedir. Bir ontoloji aynı zamanda aşağıda belirtilen tanımlamaların gerçekleştirilmesini de sağlamaktadır [72]:

- Özelliklerin tanımlanması (*Prof. Dr. Cem Deniz, Siber Güvenlik dersini verir.*)
- Değer kısıtlamalarının yapılması (*Sadece öğretim üyeleri ders verebilir.*)
- Ayrıklık ifadelerinin belirtilmesi (*Fakülte personeli ve sözleşmeli personel ayrıktır.*)
- Nesneler arasındaki mantıksal ilişkilerin belirtilmesi (*Her bölüm en az on öğretim üyesi içermelidir.*)

Ontolojiler; nesneler, kavramlar ve ilişkiler tanımlayarak belirli bir etki alanına ilişkin bilginin modellenmesini sağlamaktadırlar. Böylece sistemler arasında verilerin değiş tokuşu için standart kavramsal söz varlıkları belirtilmekte, bilgi yeniden kullanılabilmekte, sorgulamaların yanıtlanması için gösterim sağlanmakta ve çok çeşitli dizgeler arasında birlikte işlerliği kolaylaştıran gösterimler yapılmaktadır [74].



Şekil 2.8. Üniversite etki alanındaki kişiler için hiyerarşi örneği.

2.5. KİŞİSEL VERİLERİN KORUNMASINDA ANLAMSAL WEB UYGULAMALARI

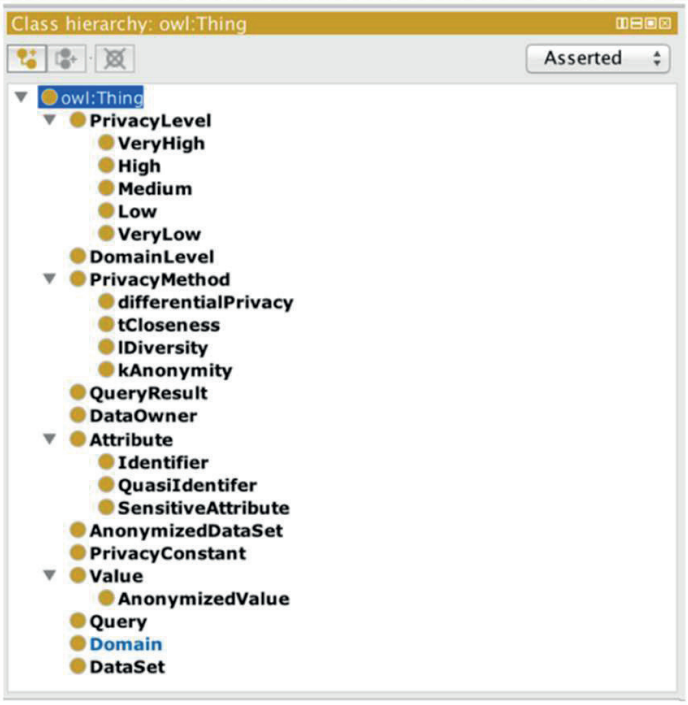
Günümüzde birçok alanda devam eden dijitalleşme süreci ve herşeyin herşeye bağlanması ile artan bağlantılılık durumu çeşitli tehditleri de beraberinde getirmektedir. Güvenilir veriye zamanında erişmek ve bu veriyi kullanabilmek bilgi sistemlerinin her seviyesindeki karar vericiler için kritik bir öneme sahiptir. Ayrıca, istatistiksel ve akademik araştırma gibi amaçlarla yayınlanan verilerin veri analizi sürecinde fayda sağlaması ile bu verilerin sahibinin mahremiyetinin korunması arasında bir denge olmalıdır. Bu dengenin sağlanabilmesi için veriler gizliliği korunarak yayınlanmalıdır. Ancak, kullanıcıların kişisel verilerinin güvenliğini sağlamak ve kullanıcıların mahremiyetini korumak, mevcut teknolojik gelişmeler nedeniyle zorlu bir görev haline gelmiştir. Bu nedenle, bireylerin mahremiyetini korumak ve verilerinin güvenliğini sağ-

lamak için düşük seviyeli güvenlik ve mahremiyet önlemleri kabul edilemez. Etkili bir bilgi sistemi, temel güvenlik öğelerinden ve gizlilik gereksinimlerinden ödün vermemeli, kişisel verilere yeterli düzeyde koruma sağlamalı ve kullanıcıların mahremiyet endişelerini giderecek çözümlere sahip olmalıdır.

Anlamsal Web, belirli bir etki alanı için ilgili alan modelinin oluşturulmasını sağlamaktadır. Bu amaçla, Anlamsal Web teknolojisinin temelini oluşturan ontolojiler kullanılmaktadır. Ontolojiler ile bilgi yönetim sistemleri için anlamsal olarak zengin bir bilgi tabanı tanımlanabilmekte ve farklı kaynaklardan gelen bilgileri bütünleştirilebilmektedir. Böylelikle Anlamsal Web, bilginin paylaşılmasını, yeniden kullanılmasını, bütünleştirilmesini, mevcut gerçeklerden ve kurallardan yeni bilgiler çıkarılmasını ve ayrıca bilgi sistemleri arasında birlikte çalışabilirliği sağlamaktadır. Anlamsal birlikte çalışabilirlik farklı tarafların veriye erişmesine ve verileri yorumlamasına olanak vermektedir [86]. Yorumlanan veriler aynı zamanda karar verme süreci için de kullanılmaktadır.

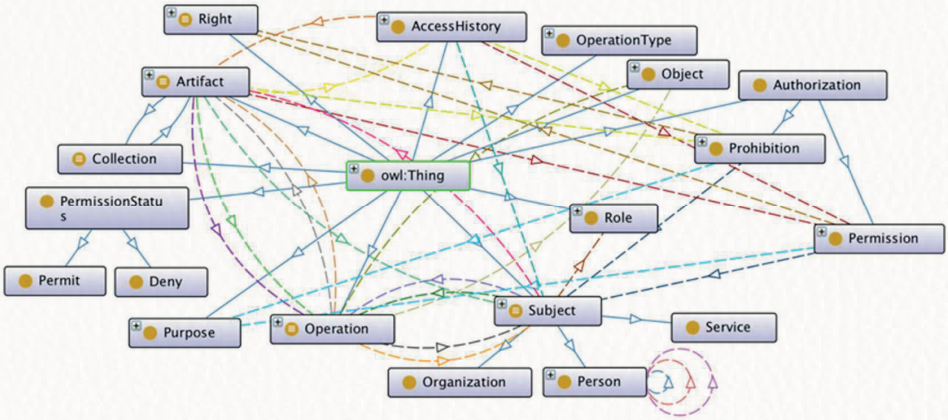
Birlikte çalışabilirlikte önemli bir rol oynayan ontolojiler, açık ve akıl yürütme bilgilerine dayalı güvenlik metriklerinin otomatik olarak oluşturulmasını desteklemekte, güvenlik operasyonlarında verimliliği ve etkinliği artırmakta, analistlerin güvenlik açıklarını ve tehditleri karakterize etmek için ilgili bilgi parçalarını çıkarmasına yardımcı olmaktadır [87]. Bu nedenle, Anlamsal Web teknolojileri kişisel verilerin güvenliğinin sağlanması ve mahremiyetin korunmasında daha etkili mahremiyet-farkında sistemlerin geliştirilmesi amacı ile kullanılmaktadır.

Kişisel verilerin gizliliğinin sağlanması ve mahremiyetin korunmasına yönelik artan endişeler sonucunda kişisel verilerin paylaşımı ve sorgulanması kapsamında literatürde çeşitli yöntemler önerilmektedir. Bu yöntemlerden biri ontoloji tabanlı kişiselleştirilmiş mahremiyet yaklaşımıdır [88]. Kişiselleştirilmiş mahremiyet, her kullanıcının farklı mahremiyet derecelendirmesini dikkate alan bir yaklaşımdır. Bu amaç doğrultusunda önerilen ontoloji tabanlı kişiselleştirilmiş mahremiyet yaklaşımında mevcut anonimleştirme yöntemleri kavramlarının birlikte entegre edildiği ve veri mahremiyetinde farklı seviyelerin bulunduğu kavramsal bir model sunulmaktadır [89]. Önerilen kişiselleştirilmiş mahremiyet-farkında modelin ontoloji sınıf hiyerarşisi Şekil 2.9'da verilmiştir. Benzer bir diğer yaklaşımda da [90] kullanıcıların kendi onam politikalarını yaratmalarını hedefleyen bir Anlamsal Web tabanlı bir kişisel onam yönetimi modeli sunulmaktadır.



Şekil 2.9. Kişiselleştirilmiş mahremiyet-farkında ontoloji için sınıf hiyerarşisi.

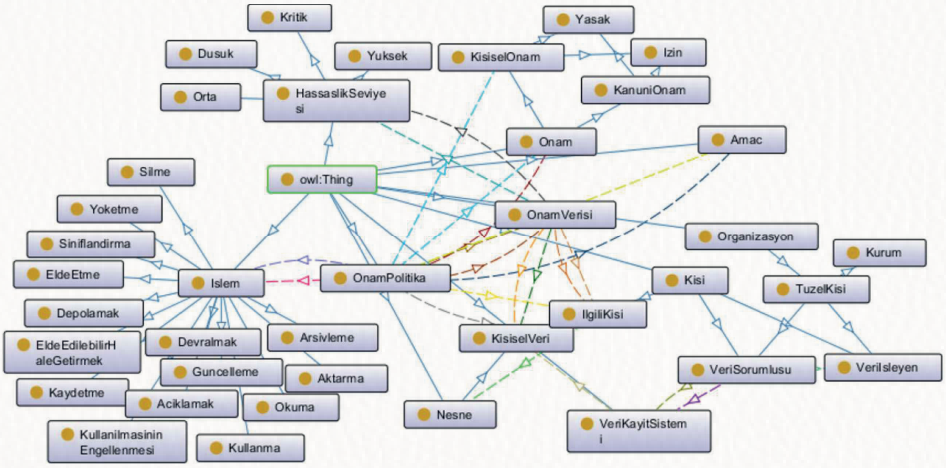
Kişisel verilerin korunması amacı ile Anlamsal Web tabanlı mahremiyet-farkında çözüm yaklaşımlarından bir diğeri de köken yönetimidir. Köken (*provenance*) bilgisi, varlıkların kaynak bilgisini, sahiplik bilgisini ve varlıklar üzerinde gerçekleştirilen eylemleri belirtmektedir. Verilerin yetkilendirilmemiş erişimlerden ve değişikliklerden korunmasının sağlanması ve veriler üzerindeki gizlilik ihlallerinin tespit edilmesi için köken yönetimi yaklaşımı güvenlik kavramlarıyla bütünleştirilerek gerçekleştirilmektedir [91]. Açık Köken Modeli (*Open Provenance Model*, OPM) (*http://openprovenance.org*) köken için genel bir modeldir. OPM, köken bilgisinin dijital olarak temsil edilmesini ve sistemler arasında köken bilgilerinin değiş-tokuş edilmesini sağlamaktadır [92]. Köken bilgisinin temsilinde Anlamsal Web'in kullanımı en uygun yaklaşımdır [93]. Bireylerin mahremiyetini korumak için köken bilgisinin kullanıldığı Anlamsal Web tabanlı köken modeli [94] [95] kapsamında geliştirilen ontolojinin yapısı Şekil 2.10'da görülmektedir.



Şekil 2.10. Mahremiyet-farkında köken ontolojisinin yapısı.

Regülasyonları temel alan mahremiyet-farkında Anlamsal Web tabanlı yaklaşımlarda da kullanıcıların kişisel verileri üzerinde kontrol haklarını uygulayabilmeleri hedeflenmektedir. Bu kapsamda, [96] çalışmasında GDPR uyumlu Blokzincir tabanlı bir kişisel veri yönetim sistemi önerilmektedir. İlgili çalışmada onam bilgisi ontoloji tabanlı olarak temsil edilmektedir. Onamın kapsamlı bir anlamsal temsili, onamın uygulanmasına yönelik mekanizmaların birlikte çalışabilirliği, doğruluğu ve eksiksizliği için temel oluşturmaktadır [96]. Verinin işlenmesi sırasında verinin korunması için GDPR regülasyonu ile uyumlu bir veri koruma ontolojisi [97] çalışmasında sunulmaktadır. İlgili ontoloji, üniversitelerde veri işlenmesi süreci doğrultusunda bir durum çalışması sunmaktadır. [98] çalışmasında ise GDPR kavramlarının ontolojik olarak modellenmesini hedefleyen bir yasal ontoloji sunulmaktadır. GDPR uyumlu onam ontolojilerinin geliştirildiği [14] ve [39] çalışmalarında, onamı GDPR'ın gerektirdiği şekilde spesifik ve açık hale getirmek için anlamsal onam modelleri önerilmektedir. Türkiye'de uygulanmakta olan KVKK regülasyonunu temel alan bir Onam Ontolojisi ve Anlamsal Web teknolojileri tabanlı bir onam çatısı [99] [100] çalışmalarında sunulmaktadır. Şekil 2.11'de KVKK kanun metninden onam ontolojisinin oluşturulması için uygulanan adımlar belirtilmekte, Şekil 2.12'de de Onam Ontolojisi'nin genel görünümü yer almaktadır [99]. İlgili Onam Ontolojisi, kişi bilgilerini tutmak için FOAF Ontolojisi'ni, kişiler arası ilişkileri belirtmek için de İlişki (*Relationship*) Ontolojisi'ni kullanmaktadır [101]. Böylelikle, onam yönetiminde tamamen anlamsal (*fully semantic*) bir yapı oluşturulmaktadır.

Şekil 2.11. KVKK'dan Onam Ontolojisi'nin oluşturulma adımları.



Şekil 2.12. KVKK kapsamında oluşturulan Onam Ontolojisi'nin genel görünümü.

Onamın en sık çalışıldığı sağlık alanında standardizasyonun sağlanması ve farklı sistemler arasında veri entegrasyonun sağlanması amacı ile bilinçli onamın ontoloji tabanlı olarak temsil edildiği çeşitli yaklaşımlar [102] [103] literatürde sunulmaktadır. [104]'te sunulan bir inceleme çalışmasında, literatürde onamın Anlamsal Web teknolojileri kullanılarak uygulandığı çalışmalar ve bu çalışmaların karşılaştırması yer almaktadır.

2.6. SONUÇ VE DEĞERLENDİRMELER

Bilgi ve iletişim teknolojilerindeki gelişmeler ve İnternetin yaygın olarak kullanılması, bilgi üretiminin ve dağıtımının hızlandığı dijital ve bağlantılı bir dünya yaratmıştır. Artan bağlantılılık ve dijitalleşme süreci çeşitli tehditleri de beraberinde getirmektedir. Bilgi paylaşımında, özellikle hassas bilgilerin işlendiği alanlarda veri gizliliğinin sağlanması ve mahremiyetin korunması büyük önem taşımaktadır. Bu hassas bilgilerden çıkarılabilecek bilgiler, bi-

reylerin kişisel bilgilerini açığa çıkarabilmektedir. Bireyler, kişisel verilerine erişme, kişisel verilerine erişim geçmişini takip etme, kişisel verileri üzerinde gerçekleştirilen işlemlerden ve hangi amaçla bu işlemlerin gerçekleştirildiğinden haberdar olma hakkına sahiptir. Bu amaçla, bireylerin mahremiyet endişelerini dikkate alan ve bireylerin kişisel verilerine yönelik olarak yeterli seviyede koruma sağlayan etkili mahremiyet-duyarlı sistemleri geliştirilmelidir.

Anlamsal Web bilgiye iyi tanımlanmış bir anlam verilmesini sağlamakta ve karar verme sürecine yardımcı olmaktadır. Bu amaçla, Anlamsal Web'de ontolojiler kullanılmaktadır. Anlamsal Web'in çekirdeği olan ontolojiler, bir etki alanındaki kavramları ve bu kavramların birbirleriyle ilişkisini temsil eden terimleri ve ilişkileri tanımlamaktadır. Böylelikle, farklı sistemler arasında veri entegrasyonu, bilgi yönetimi, bilginin paylaşılması, yeniden kullanılması, farklı sistemler arasında birlikte çalışabilirlik, mevcut bilgilerden yeni bilginin keşfedilmesi ve bilginin makineler tarafından yorumlanabilmesi sağlanmaktadır.

Kişisel verilerin güvenliğinin sağlanması ve mahremiyetin korunmasında daha etkili mahremiyet-duyarlı sistemlerin geliştirilmesi amacı ile Anlamsal Web kullanılmakta ve Anlamsal Web teknolojileri tabanlı mahremiyet çözümleri geliştirilmektedir. Kişisel verilerin korunmasına yönelik literatürde yer alan Anlamsal Web tabanlı çalışmalar, regülasyonlar ile uyumlu onam yönetim sistemleri ve mahremiyet-duyarlı sistemlerin geliştirilmesine odaklanmaktadır. Bireylerin mahremiyetlerine yönelik endişelerinin artması sonucunda kişisel verilerin kötüye kullanımlarının önlenmesi ve istismarlara karşı korunması ihtiyacı ortaya çıkmıştır. Bu kapsamda, mahremiyete yönelik potansiyel tehditler anlaşılmalı ve veri mahremiyetinin sağlanmasına yönelik etkin çözümler geliştirilmelidir. Bu bağlamda, bilgi sistemlerindeki gizlilik ve mahremiyet sorunlarına yönelik Anlamsal Web tabanlı yaklaşımlar gelecekteki araştırmalara açık bir potansiyeldedir.

KAYNAKLAR

[1] S. Park, "Information is Power", in Digital Capital, London, United Kingdom: Palgrave Macmillan, 2017, Chapter 8, pp. 161-183.

[2] T. M. Jai and N. J. King, "Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and databrokers?", Journal of Retailing and Consumer Services, 28, 296–303, 2016.

[3] S. Mittal and P. Sharma, "The Role of Consent in Legitimising the Processing of Personal Data under the Current EU Data Protection Framework", Asian Journal of Computer Science and Information Technology, 7: 4 August (2017), 76 – 78.

[4] A. Hussain, L. A. Lasrado, R. R. Mukkamala, U. Tanveer, "Sharing Is Caring – Design and Demonstration of a Data Privacy Tool for Interorganizational Transfer of Data", Procedia Computer Science 181, 394–402, 2021.

[5] Pew Research Center, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information", November 2019.

[6] Cisco 2021 Data Privacy Benchmark Study, "Forged by the Pandemic: The Age of Privacy", 2021.

[7] IBM Security, "Cost of a Data Breach Report", 2021.

[8] L. H. Cox, "Suppression Methodology and Statistical Disclosure Control", Journal of the American Statistical Association, Vol. 75, No. 370, pp. 377-385, Jun. 1980.

[9] KVKK, "Kişisel Verilerin Korunması Kanunu", Resmî Gazete, Resmî Gazete Sayısı: 29677, Resmî Gazete Tarihi: 07.04.2016.

[10] GDPR, "General Data Protection Regulation (GDPR)". 25 May 2018. [Online] Available: https://gdpr.eu/tag/gdpr/. Accessed on: September 01, 2021.

[11] DAL Piper's Data Protection Laws of The World. [Online] Available: https://www.dlapiperdataprotection.com. Accessed on: September 01, 2021.

[12] N. P. Sheppard, R. Safavi-Naini and M. Jafari, "A Digital Rights Management Model for Healthcare," 2009 IEEE International Symposium on Policies for Distributed Systems and Networks, 2009.

[13] R. Clarke, "e-consent: A critical element of trust in e-business" in Bled Electronic Commerce Conference 2002 Proceedings, 12, 2002.

[14] H. J. Pandit, C. Debruyne, D. O'Sullivan, D. Lewis, "GConsent - A Consent Ontology Based on the GDPR", in Hitzler P. et al. (eds) The Semantic Web, European Semantic Web Conference 2019. Lecture Notes in Computer Science, Vol 11503, Springer, Cham, 2019.

[15] T. Berners-Lee, J. Hendler, O. Lassila, "The Semantic Web", Scientific American Magazine, pp. 29–37, May 2001.

[16] S. Alam, M. M. R. Chowdhury, J. Noll, "Interoperability of Security-Enabled Internet of Things", Wireless Personal Communications, 61:567–586, 2011.

[17] A. Rhayem, M. B. A. Mhiri, M.B.A., F. Gargouri, "Semantic Web Technologies for the Internet of Things: Systematic Literature Review", Internet of Things 11, 100206, 2020.

[18] M. Kuneva, "Roundtable on Online Data Collection, Targeting and Profiling", Keynote Speech at The European Commission, Brussels, Belgium, 31 March 2009.

[19] Avrupa Birliği Resmi Gazetesi, "Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)", Avrupa Birliği Bakanlığı Çevirisi, Türkçe Versiyon, 2018.

[20] Data Protection Act (DPA), "Determining what is personal data", v1.1, Information Commissioner's Office (ICO), 20121212, 2012.

[21] J. Kang, "Information Privacy in Cyberspace Transactions", Stanford Law Review, Vol. 50, pp. 1193-1294, 1998.

[22] PwC, "Data Privacy Handbook", A starter guide to data privacy compliance, 2020.

[23] S. M., Karunarathne, N. Saxena, M. K. Khan, "Security and Privacy in IoT Smart Healthcare", IEEE Internet Computing, Vol. 25, No. 4, pp. 37-48, 2021.

[24] P. Samarati, "Protecting respondents' identities in microdata release", IEEE Transactions on Knowledge and Data Engineering, 13, (6), pp. 1010–1027, 2001.

[25] O. Can, "Personalised anonymity for microdata release", IET Information Security, 12(4): 341-347, 2018.

[26] L. Sweeney, "Uniqueness of simple demographics in the U.S. Population", Technical Report, Carnegie Mellon University, 2000.

[27] Boxcryptor, "What is Personal Data? Simple Examples from Everyday Life", 26 March 2021. [Online] Available: https://www.boxcryptor.com/en/blog/post/what-is-personal-data-simple-examples/. Accessed on: September 01, 2021.

[28] T. Mather, S. Kumaraswamy, S. Latif, "Cloud security and privacy: an enterprise perspective on risks and compliance", O'Reilly Media, 1st Edition, September 2009.

[29] Enisa (European Union Agency for Network and Information Security). Privacy and Data Protection by Design – from policy to engineering, December 2014.

[30] S.D. Warren and L. D. Brandeis, "The Right to Privacy", Harvard Law Review, Vol. 4, No. 5, pp. 193-220, Dec. 15, 1890.

[31] Olmstead v. United States, 277 U.S. 438, 1928.

[32] R. Clarke, "Internet privacy concerns confirm the case for intervention", Communications of the ACM, 42(2):60–7, 1999.

[33] L. D. Introna, "Privacy and the computer: why we need privacy in the information society", Metaphilosophy, 28(3):259-275, July 1997.

[34] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", Computers & Security, 64, pp. 122–134, 2017.

[35] C. Fried, "Privacy", Yale Law Journal, 77, 1968.

[36] A. Westin, "Privacy and Freedom", New York: Atheneum, 1967.

[37] A. M. Froomkin, "The Death of Privacy?", Stanford Law Review, Vol. 52, No. 5, pp. 1461-1543, 2000.

[38] E. A. Whitley, "Informational privacy, consent and the ''control'' of personal data", Information Security Technical Report, 14, pp. 154-159, 2009.

[39] K. Fatema, E. Hadziselimovic, H. Pandit, C. Debruyne, D. Lewis, D. O'Sullivan "Compliance through Informed Consent: Semantic Based Consent Permission and Data Management Model", CEUR Workshop Proceedings, Vol. 1951, 2017.

[40] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 International Conference on Computer Science and Electronics Engineering, pp. 647-651, 2012.

[41] S. Kenny and L. Korba, "Applying digital rights management systems to privacy rights," Computers & Security, Vol. 21, No 7, pp. 648–664, 2002.

[42] MITRE, "Electronic Consent Management: Landscape Assessment, Challenges, and Technology", Version 1.0, October 2014.

[43] T. Virtanen, "A Consent-patienship Based Privacy Model for Healthcare", 2012 Second International Conference on Cloud and Green Computing, pp. 650-654, 2012.

[44] S. Cha, M. Chuang, K. Yeh, Z. Huang and C. Su, "A User-Friendly Privacy Framework for Users to Achieve Consents With Nearby BLE Devices", IEEE Access, Vol. 6, pp. 20779-20787, 2018.

[45] C. Pathmabandu, J. Grundy, M. B. Chhetri and Z. Baig, "An Informed Consent Model for Managing the Privacy Paradox in Smart Buildings", 35th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW 2020), pp. 19-26, 2020.

[46] D. Hofman et al., "Building Trust & Protecting Privacy: Analyzing Evidentiary Quality in a Blockchain Proof-of-Concept for Health Research Data Consent Management", 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1650-1656, 2018.

[47] C. C. Agbo and Q. H. Mahmoud, "Design and Implementation of a Blockchain-Based E-Health Consent Management Framework", 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 812-817, 2020.

[48] M. M. Madine et al., "Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records", IEEE Access, Vol. 8, pp. 225777-225791, 2020.

[49] P. V. Kakarlapudi, Q. H. Mahmoud, "A Systematic Review of Blockchain for Consent Management", Healthcare (Basel), Feb 1;9(2):137, 2021.

[50] Q. Wang and H. Jin, "Decision Support for Patient Consent Management", 2011 IEEE First International Conference on Healthcare Informatics, Imaging and Systems Biology, pp. 142-149, 2011.

[51] C. Yang, C. Liu and T. Tseng, "Design and Implementation of a Privacy Aware Framework for Sharing Electronic Health Records", 2015 International Conference on Healthcare Informatics, pp. 504-508, 2015.

[52] C. Pruski, "e-CRL: A Rule-Based Language for Expressing Patient Electronic Consent", 2010 Second International Conference on eHealth, Telemedicine, and Social Medicine, pp. 141-146, 2010.

[53] E. Olca, Ö. Can, "Providing Patient Rights with Consent Management", 2nd International Symposium on Digital Forensics and Security (ISDFS'14), pp. 101-104, 2014.

[54] E. Olca, Ö. Can, "Ulusal ve Uluslararası Yönetmeliklerde Kişisel Sağlık Verisi Mahremiyetinin Korunması", 7th International Conference on Information Security and Cryptology (ISCTURKEY 2014), 2014.

[55] S. Tokas O. Owe O., "A Formal Framework for Consent Management", In: Gotsman A., Sokolova A. (eds) Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2020), Lecture Notes in Computer Science, Vol 12136, Springer, Cham., 2020.

[56] M. Laurent, J. Leneutre, S. Chabridon, I. Laaouane, "Authenticated and Privacy-Preserving Consent Management in the Internet of Things", Procedia Computer Science, 151, pp. 256–263, 2019.

[57] W. L. Sim, H. N. Chua and M. Tahir, "Blockchain for Identity Management: The Implications to Personal Data Protection", 2019 IEEE Conference on Application, Information and Network Security (AINS), pp. 30-35, 2019.

[58] A. B. Haque, A. K. M. N. Islam, S. Hyrynsalmi, B. Naqvi and K. Smolander, "GDPR Compliant Blockchains–A Systematic Literature Review", IEEE Access, Vol. 9, pp. 50593-50606, 2021.

[59] J. Ahmed, S. Yildirim, M. Nowostaki, R. Ramachandra, O. Elezaj and M. Abomohara, "GDPR Compliant Consent Driven Data Protection in Online Social Networks: A Blockchain-Based Approach", 2020 3rd International Conference on Information and Computer Technologies (ICICT), pp. 307-312, 2020.

[60] N. B. Truong, K. Sun, G. M. Lee and Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution", IEEE Transactions on Information Forensics and Security, Vol. 15, pp. 1746-1761, 2020.

[61] N. Al-Zaben, M. M. Hassan Onik, J. Yang, N. Lee and C. Kim, "General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management", 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), pp. 77-82, 2018.

[62] C. Daudén-Esmel, J. Castellà-Roca, A. Viejo and J. Domingo-Ferrer, "Lightweight Blockchain-based Platform for GDPR-Compliant Personal Data Management", 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), pp. 68-73, 2021.

[63] F. Blix, S. A. Elshekeil and S. Laoyookhong, "Data protection by design in systems development: From legal requirements to technical solutions", 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 98-103, 2017.

[64] Y. Nam, E. Shin, S. Lee, S. Jung, Y. Bae and J. Kim, "Global-scale GDPR Compliant Data Sharing System", 2020 International Conference on Electronics, Information, and Communication (ICEIC), pp. 1-3, 2020.

[65] E. Olca, Ö. Can, "Kişisel Verilerin Korunması İçin Bir Onam Yönetim Sistemi Önerisi", 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISCTURKEY 2016), 2016.

[66] I. Mazeh, E.Shmueli, "A personal data store approach for recommender systems: enhancing privacy without sacrificing accuracy", Expert Systems With Applications, 139, 112858, 2020.

[67] C. Lin, P. Yang and Y. Lin, "Detecting Security Breaches in Personal Data Protection with Machine Learning", 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM), pp. 1-7, 2020.

[68] R. M. Alguliyev, R. M. Aliguliyev, F. J. Abdullayeva "Privacy-preserving deep learning algorithm for big personal data analysis", Journal of Industrial Information Integration, 15, pp. 1–14, 2019.

[69] E. Cherif, N. Bezaz, M. Mzoughi, "Do personal health concerns and trust in healthcare providers mitigate privacy concerns? Effects on patients' intention to share personal health data on electronic health records", Social Science & Medicine, 283, 114146, 2021.

[70] N. Baloyi and P. Kotzé, "Do users know or care about what is done with their personal data: A South African study", 2017 IST-Africa Week Conference (IST-Africa), pp. 1-11, 2017.

[71] O. Djuraskovic, "How Many Websites Are There? – The Growth of The Web (1990 – 2021)", Updated on: July 5th, 2021. Available: https://firstsiteguide.com/how-many-websites. Accessed on: September 01, 2021.

[72] G. Antoniou and F. van Harmelen, "A Semantic Web Primer", The MIT Press, 2004.

[73] T. Berners-Lee, "Information management: a proposal", March 1989-May1990, Available: http://www.w3.org/History/1989/proposal.html. Accessed on: September 01, 2021.

[74] Ö. Can, "Anlamsal web için kişiselleştirilebilir ontoloji tabanlı erişim denetimi ve politika yönetimi", Ege Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Bölümü Doktora Tezi, 2009.

[75] W3C Semantic Web, "What is Semantic Web?", Available: https://www.w3.org/RDF/FAQ. Accessed on: September 01, 2021.

[76] T. Berners-Lee, "Enabling Standards & Technologies - Layer Cake", Available: https://www.w3.org/2002/Talks/04-sweb/slide12-0.html. Accessed on: September 01, 2021.

[77] B. Thuraisingham, B., "Building Trustworthy Semantic Webs", Auerbach Publications, 2007.

[78] W3C, "SPARQL Query Language for RDF", 2008, Available: https://www.w3.org/TR/rdf-sparql-query. Accessed on: September 01, 2021.

[79] W3C, "Web Ontology Language (OWL)", 2012, Available: https://www.w3.org/OWL. Accessed on: September 01, 2021.

[80] W3C, "RDF Schema 1.1", 2014, Available: https://www.w3.org/TR/rdf-schema. Accessed on: September 01, 2021.

[81] W3C, "Resource Description Framework (RDF)", 2014, Available: https://www.w3.org/RDF. Accessed on: September 01, 2021.

[82] P. F. Patel-Schneider, D. Fensel, "Layering the Semantic Web: Problems and Directions", 2002 International Semantic Web Conference (ISWC), pp. 16-29, 2002.

[83] J. Domingue, D. Fensel, J. A. Hendler, "Introduction to the Semantic Web Technologies", Handbook of Semantic Web Technologies, J. Domingue, D. Fensel, J. A. Hendler (Eds.), Springer, pp. 3-41, 2011.

[84] T. R. Gruber, "A translation approach to portable ontologies", Knowledge Acquisition, 5(2): 199–220, 1993.

[85] Ö. Can and D. Yilmazer, "A novel approach to provenance management for privacy preservation", Journal of Information Science, 46(2):147–160, 2020.

[86] A. Rhayem, M. B. A. Mhiri, F. Gargouri, "Semantic Web Technologies for the Internet of Things: Systematic Literature Review", Internet of Things 11, 100206, 2020.

[87] B. A. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins, R. Jardim-Goncalves, "An Ontology-Based Cybersecurity Framework for the Internet of Things", Sensors, 18(9):3053, 2018.

[88] B. Usenmez, O. Can, "Conceptualization of Personalized Privacy Preserving Algorithms", 9th Metadata and Semantics Research Conference (MTSR 2015), Communications in Computer and Information Science, Vol. 544, 195-200, 2015.

[89] O. Can, B. Usenmez, "An Ontology Based Personalized Privacy Preservation", 11th International Conference on Knowledge Engineering and Ontology Development (KEOD 2019), 500-507, 2019.

[90] O. Can, "A Semantic Model for Personal Consent Management", 7th Metadata and Semantics Research Conference (MTSR 2013), Vol. 390, 146-151, 2013.

[91] O. Can, D. Yilmazer, "A Privacy Aware Semantic Model for Provenance Management", 8th Metadata and Semantics Research Conference (MTSR2014), Communications in Computer and Information Science, Vol. 478, 162-169, 2014.

[92] L. Moreau, B. Clifford, B., et al., "The Open Provenance Model Core Specification (v1.1)", Future Generation Computer Systems ,27(6), 743–756, 2011.

[93] J. Golbeck and J. Hendler, A semantic web approach to the provenance challenge. Concurr Comp Pract E 2008; 20(5): 431–439.

[94] O. Can, D. Yilmazer, "A novel approach to provenance management for privacy preservation", Journal of Information Science, 46(2), 147-160, 2020.

[95] O. Can, D. Yilmazer, "Improving privacy in health care with an ontology-based provenance management system", Expert Systems, 37(1), 1-18, 2020.

[96] M. Davari and E. Bertino, "Access Control Model Extensions to Support Data Privacy Protection based on GDPR", 2019 IEEE International Conference on Big Data (Big Data), pp. 4017-4024, 2019.

[97] B. Di Martino, P. Cantiello, L. C. Cante, A. Diana, A. Esposito, M. Graziano, M. Mastroianni, "An application of Semantic Web Technologies to GDPR compliance of University Processes and Personal Data processing", Available: http://www.semantic-web-journal.net/system/files/swj2652.pdf. Accessed on: September 01, 2021.

[98] M. Palmirani, M. Martoni, A. Rossi, C. Bartolini, L. Robaldo, "Legal Ontology for Modelling GDPR Concepts and Norms", Legal Knowledge and Information Systems, Vol. 313, pp. 91-100, 2018.

[99] Ö. Can, E. Olca, "Kişisel Verilerin Korunması Kanunu için Onam Ontolojisi Geliştirimi", Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi, 21(62), 559-575, 2019.

[100] E. Olca, "Anlamsal onam yönetimi için bir çerçeve geliştirilmesi", Doktora Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Bölümü, 2019.

[101] E. Olca, Ö. Can, "Extending FOAF and Relationship Ontologies with Consent Ontology", International Conference on Computer Science and Engineering (UBMK 2018), 2018.

[102] Y. Lin, J. Zheng & Y. He, "VICO: Ontology-based representation and integrative analysis of Vaccination Informed Consent forms", Journal of Biomedical Semantics, 7:20, 2016.

[103] B. Yu, D. Wijesekera, P. Costa, "An Ontology for Medical Treatment Consent", STIDS 2014, pp. 72-79, 2014.

[104] A. Kurteva, T. R. Chhetri, H. J. Pandit, and A. Fensel, "Consent through the Lens of Semantics: State of the Art Survey and Best Practices", 1 – 27, 2021.

Bölüm 3

SİBER GÜVENLİK TEHDİT BİLGİSİ PAYLAŞIMI

Ali Melih Kanca - Şeref Sağıroğlu

Bu bölümde; siber tehdit bilgi paylaşımı çalışmaları incelenmiş, bilgi paylaşımına ilişkin olarak önemli çalışmalar yapan ülkelerin çalışmaları değerlendirilmiş, ülkemizde siber tehditlere dair güncel bilgilerin gerçek zamanlı olarak dinamik bir ortamda paylaşılması amacıyla kurumlar, birimler veya şirketler arasında siber tehdit bilgisinin paylaşılmasına yönelik değerlendirmeler yapılmış ve ülkemizde kuruluşlar arasında tehdit bilgisinin paylaşıldığı paylaşım modeli oluşturulması önerilmiştir. İncelenen ve sonuçta ülkemizde oluşturulması önerilen işbirliği yaklaşım modeli ile paydaşlar arasında deneyimlerin paylaşılabileceği bir ekosistem oluşturulabilecek, siber tehdit bilgileri gerçek zamanlı olarak paylaşılabilecek ve siber tehditlerle topyekûn mücadele edilmesi kolaylaşacak ve en önemlisi bu alanda yapılacak olan Ar-Ge çalışmalarının kapsamının geliştirilmesi ile daha kapsamlı ürünler geliştirilebilecektir.

3.1. GİRİŞ

Teknolojideki gelişmeler ve internet kullanımı arttıkça, siber alandaki güvenlik riskleri artmakta ve bu riskler giderek küreselleşmektedir. Dijital sistemlere yönelik artan bağımlılık ve bu sistemlerin siber saldırganlar tarafından hedef alınması nedeniyle siber güvenlik kavramı giderek önem kazanmaktadır. Bilişim altyapılarını ve sistemlerini hedef alan siber tehditler, kuruluşlar için

en büyük zorluklardan biri haline gelmiştir. Siber güvenliğin sağlanması ve kritik bilişim altyapılarının korunması, ülkelerin güvenliğinin ve ekonomik refahının sağlanmasında, organizasyonların itibarının korunması ve iş süreçlerinin devamlılığının sağlanmasında çok önemli bir role sahiptir.

Bununla birlikte, siber uzaydaki tehdit yelpazesi giderek genişlemekte, yeni saldırı aktörleri ve yöntemleri ortaya çıkmaktadır. Siber uzaydaki varlıkların, altyapıların, sistemlerin ve verilerin gizliliğinin ve güvenliğinin sağlanması amacıyla gerekli tedbirlerin alınabilmesi ve doğru becerilerin uygulanabilmesi için siber tehditler hakkında bilgi sahibi olunması gerekmektedir. Olası saldırıların gerçekleşmeden önlenebilmesi amacıyla siber tehditlerin tanınması, etkilediği sistemlerin belirlenmesi ve bu tehditlerin olası etkileri hakkında bilgi edinilmesi gerekmektedir. Bu kapsamda, olası tehditlerin önceden tespit edilebilmesi, alınması gerekli tedbirlerin planlanabilmesi ve siber tehditlerle etkin bir şekilde mücadele edilebilmesi için tehdit ve tehdit aktörleri hakkındaki siber tehdit bilgilerine ihtiyaç duyulmaktadır.

Ayrıca sofistike siber tehditlerle mücadelede ihtiyaç duyulan bilgilerin tek bir kaynaktan elde edilebilmesi mümkün olamamaktadır. Siber tehditlere dair en güncel bilgilerin hızlı bir şekilde elde edilmesi, bu bilgiler doğrultusunda gerekli güvenlik tedbirlerinin alınabilmesi ve tehditlere yönelik en güncel bilgilerin hızlı bir şekilde elde edilmesi için bilgi paylaşımı ve işbirliği yapılması gerekmektedir. Bu kapsamda, Siber Vatanımızın topyekûn savunulabilmesi ve siber tehditlerle daha etkin mücadele edilebilmesi amacıyla kuruluşlardaki siber tehdit bilgisi kapasitesi ile yeteneklerinin geliştirilebilmesi ve beslenen kaynakların zenginleştirilmesi için siber güvenlik ekosisteminin oluşturulması, siber tehditlere karşı elde edilen bilgi, deneyim ve tecrübenin diğer paydaşlarla belirli bir model ile paylaşılması gerekmektedir.

3.2. SİBER GÜVENLİK VE SİBER SALDIRILAR

Siber güvenlik; “siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi” şeklinde ifade edilmektedir [1]. Bir diğer

tanımlamada ise "kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü" şeklinde tanımlamaktadır [2]. Bilişim sistemlerinin ve bilginin korunması, sistemlerin devamlılığının sağlanması ve siber tehditlerin bertaraf edilmesi siber güvenliğin amaç ve hedefleri arasında yer almaktadır.

Siber saldırı ise; "bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler" olarak tanımlanmaktadır [1]. Siber saldırganlar siber saldırılarla siber ortamdaki fiziksel veya sanal yapıyı, yazılım, donanım ve altyapı sistemlerini hedef almaktadır. Saldırlar ile bilişim sistemleri ve kritik altyapı bilişim sistemleri çalışamaz hale gelebilmekte ve bilişim sistemleri üzerinden sunulan hizmetlerin aksamasına neden olunabilmektedir. Nitekim dünyada yaşanan bazı siber saldırıların boyutunu ve önemini anlamak ve anlatmak için aşağıda verilen örneklerin kapsamlı olarak değerlendirilmesi gereklidir.

- 2007 yılında Estonya'daki kamu kuruluşlarına ait internet sitelerine ve bankacılık sistemine yönelik Dağıtılmış Hizmet Reddi Saldırıları (DDoS) gerçekleştirilmiş ve bu sitelerin sunucuları hizmet veremez hale gelmiştir.
- 2008 yılında ise Gürcistan kamu internet siteleri DDoS saldırıları ile hedef alınmış ve bu siteler de belirli bir süre hizmet verememiştir.
- 2011 yılında İran'ın Natanz şehrindeki nükleer yakıt zenginleştirme tesisini hedef alan siber saldırıda ise "Stuxnet" adı verilen zararlı yazılım kullanılmıştır. Zararlı yazılımın hedefi enerji üretim ve dağıtımının kontrolü, su, doğal gaz, kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesinde kullanılan denetleme kontrol ve veri toplama sistemi (Supervisory Control and Data Acquisition, SCADA) olup, saldırı sonucunda nükleer çalışmalar sekteye uğratılmıştır.
- 2015 yılında ise Ukrayna'nın Ivano-Frankivsk bölgesinde elektrik tesislerinin hedef alındığı ve 700 bin kişinin saatlerce elektriksiz kalmasına neden olan siber saldırı yaşanmıştır.

- 2017 yılında meydana gelen "WannaCry" siber saldırısında ise 99 ülkedeki 230 bin bilgisayar, WannaCry fidye yazılımı hedef alınmıştır. Hedef alınan bilgisayardaki dosyalar şifrelenerek kullanıcılardan şifrenin çözülmesi karşılığında para talep edilmiştir. Saldırıdan İspanya'daki telekom şirketi Telefónica, enerji şirketi Iberdrola, İngiltere Ulusal Sağlık Servisi, Rusya İçişleri Bakanlığı, Rusya Acil Durum Bakanlığı gibi kuruluşlar etkilenmiş ve buradaki sistemler üzerinden sunulan hizmetlerde aksamalar yaşanmıştır.
- 2017 yılında "NotPedya" adı verilen bir fidye yazılımı ile Ukrayna başta olmak üzere dünya genelindeki pek çok bilgisayar hedef alınmıştır.

Öte yandan, siber saldırganlar tarafından kullanılan siber saldırı türleri incelendiğinde, Gelişmiş Kalıcı Tehditler (APT), DDoS saldırıları, botnet saldırıları, fidye yazılımları, oltalama saldırıları, MITM (Man in The Middle) saldırıları, casus yazılım saldırıları, yaygın kullanılan siber saldırı türleri olarak karşımıza çıkmaktadır.

APT, yüksek düzeydeki sistemlerden bilgi elde edilmesi amacıyla gerçekleştirilen ve yaygın bilinen tekniklerin kombinasyonundan oluşan sofistike siber saldırı türleridir. APT saldırıları, belirli bir hedefe yönelik kalıcı saldırılar olup, birkaç adımda gerçekleştirilmektedir. APT saldırıları temel olarak casusluk ve veri hırsızlığı amacıyla gerçekleştirilmektedir. APT'lerin gelişmiş teknikler kullanması ve bilinmeyen güvenlik açıklıklarından yararlanması sebebiyle mevcut algılama yöntemleri için zorluk teşkil etmektedir. APT saldırılarının tespiti edilmesi zor olabilmekte ve uzun sürebilmektedir. Bu saldırı türleri çok zor tespit edilebilmesi sebebiyle önemli hasarlara ve mali kayıplara neden olabilmektedir [3].

Banka veya çevrimiçi alışveriş sitesi gibi güvenilir bir aracıdan gelen iletilere benzeyecek şekilde tasarlanmış olan elektronik posta iletilerinin kullanımı ile kurbanların hedef alındığı saldırılar ise oltalama saldırıları olarak tanımlanmaktadır. Bu mesajlar ile genellikle kullanıcılardan hesap bilgilerini doğrulaması istenmekte ve kullanıcıyı tuzağa düşürebilmek amacıyla genellikle bir acelecilik duygusu barındıran ifadeler kullanılmaktadır. Hedef alınan kişiler bu mesajları güvenilir bir kaynaktan gelmiş şekilde algılamaktadır. Oltalama saldırıları, insanların kullandığı sistemleri doğrudan hedeflemek yerine, sistemleri kullanan kişileri hedef almaktadır. Siber saldırganlar oltalama yön-

temleri ile bilinçsiz kullanıcıları hedefleyerek büyük zararlara sebep olabilen oltalama saldırıları siber saldırganlar tarafından yaygın bir şekilde kullanılmaktadır.

DDoS, bir bilgi işlem veya bellek kaynağının çalışmasının engellenmesi amacıyla gerçekleştirilen ve bant genişliğinin tamamını kullanarak sistemin cevap vermesini engellemeyi hedefleyen siber saldırı türü olarak tanımlanabilmektedir. DDoS saldırısı ilk olarak Khan C. Smith tarafından 1998 yılında gerçekleştirilmiştir. Bu saldırı türünde hedef alınan sistemin çökertilmesi veya yavaşlatılması ile kullanılamaz hale getirilmesi amaçlanmaktadır. DDoS saldırıları, hedef sistemi kapasitesinden fazla dış iletişim isteklerine maruz bırakmakta ve sistem istek trafiğine cevap veremeyecek konuma gelmektedir. Bu saldırıların, servisin çökmesine sebep olanlar ve servisin aşırı yavaşlamasına neden olanlar şeklinde olmak üzere iki genel formu bulunmaktadır. Siber saldırganlar, ağ bağlantılı bir sistemin güvenlik açıklarını kullanmamakta, ancak kullanılabilirliğine karşı saldırılar gerçekleştirmektedir. 2007 yılında Estonya'da, 2008 yılında Gürcistan'da gerçekleştirilen siber saldırılar, DDoS saldırılarına örnek gösterilebilmektedir.

Kötü amaçlı botnetler, bir operatörün uzaktan yönetilmesi ile "Bot" adı verilen güvenliği ihlal edilmiş bilgisayarlardan oluşan bir ağdır. "Bot" terimi "Robot" kelimesinden türetilmiş olup, botlar önceden tanımlanmış bazı işlevleri otomatik bir şekilde gerçekleştirmek için tasarlanmıştır. Botnet'ler, DDoS saldırıları, oltalama saldırıları ve kötü amaçlı yazılım yayma gibi birçok saldırıya imkân sağladığı için önemli ve büyüyen bir tehdit oluşturmaktadır.

Fidye yazılımı (Ransomware) saldırısı, hedef alınan bilgisayardaki verilerin şifrelenmesi veya bilgisayarın kilitlenmesi amacıyla kötü amaçlı kod kullanan bir kötü amaçlı yazılım türüdür. Siber saldırganlar, fidye yazılımı ile verileri kullanıcılar için erişilemez hale getirmekte ve dosyaların şifrelerinin çözülmesi için kullanıcıdan para talep etmektedir. 2017 yılında gerçekleştirilen "WannaCry" ve "NotPetya" saldırıları, bu saldırı türünde gerçekleştirilen saldırılar olarak gösterilebilmektedir. Fidye yazılımı ile kullanıcı ödeme yapmadığı sürece kullanıcının bilgisayarının devre dışı bırakılması amaçlanmıştır.

Casus yazılımlar, hedef alınan kişilerin bilgisayarlarına gizlice yüklenen kötü amaçlı kod sınıfı şeklinde tanımlanabilmektedir. Bu yazılımlar ile kullanıcıların davranışların sessizce izlenebilmekte, webde gezinme alışkanlıkları kaydedilebilmekte ve hedefin kullanıcı şifreleri elde edilebilmektedir.

MITM saldırısı ise ağda iki bağlantı arasındaki iletişimin dinlenmesi ile çeşitli verilerin ele geçirilmesi veya veriler üzerinde değişikliğin yapılmasına imkân tanıyan bir saldırı yöntemi olarak tanımlanmaktadır. MITM saldırısı, taraflar arasında akan gerçek verileri ve verilerin kendisinin gizliliğini ve bütünlüğünü hedeflemektedir. MITM saldırılarında taraflar arasındaki iletişim kesilebilmekte veya yanıltıcı bir iletişim oluşturulabilmektedir.

3.3. SİBER TEHDİT BİLGİSİ

Siber tehditlerin çeşitliliği, sayıları ve niteliği arttıkça bu tehditlerin tespit edilmesi ve engellenmesi daha zor hale gelmektedir. Siber ortamın tehlikelerinin farkında olan ülkeler ve organizasyonlar kurumsal siber güvenliğini korumaya yönelik çaba göstermekte, başta kritik altyapı sistemleri olmak üzere varlıklarını ve verilerini siber risklere, tehditlere ve saldırılara karşı korumak için çözümler üreterek uygulamaya koymaktadır. Ülkeler son yıllarda siber güvenliğin önemini dikkate alarak gerek maddi olarak gerekse insan gücü, altyapı ve yeteneklerini artırıcı tedbirler almaya başlamıştır [4]. Ayrıca gelişen tehditlere karşı güvenlik stratejilerini sürekli olarak yenilemektedir.

Siber tehditler, bir veya daha fazla açıklığın sömürülmesi ile güvenlik önlemlerini aşabilecek, sistemlere yetkisiz erişimde bulunulabilecek, sistem yapısını bozarak kullanılamaz hale getirebilecek tehditler olarak tanımlanmaktadır [5]. Bir başka tanımda ise; “birbirine bağlı ağlara yönelik tehditler veya yetkisiz erişim sağlanması, tahribat oluşturulması, bilginin değiştirilmesi veya ifşa edilmesi faaliyetleri ile bilgi sistemleri üzerinden organizasyonel süreçlerini, varlıklarını, kişileri veya bir ulusu etkileyen potansiyel olaylar veya durumlar” olarak tanımlanmaktadır [6], [7]. Söz konusu siber tehditlerin tespit edilmesi, sınıflandırılması ve gerekli tedbirlerin alınması, siber saldırıların önlenmesinde önemli bir rol oynamaktadır. Bir organizasyonda zafiyetleri belirleyen, güvenliği destekleyen, korsanların (hackerların) sistemlere nasıl girdiği, ne istediği, nasıl elde ettiğini ortaya koyan bilgilerin olması, siber tehditlerle mücadeleyi kolaylaştırabilmektedir. Bilgiye sahip olan organizasyonların daha bilinçli karar verebileceği değerlendirilmektedir [8].

Siber uzaydaki tehditlerle etkin bir şekilde mücadele edebilmesi için saldırı teknik ve yöntemlerinin anlaşılması gerekmekte, doğru becerilere ih-

tiyaç duyulmakta ve tehditler hakkında kapsamlı tehdit analizi gerçekleştirilmesi gerektirmektedir [9]. Tehditler hakkında kapsamlı tehdit analizi gerçekleştirilebilmesi, saldırın özelliklerinin derinlemesine incelenmesi ve etkin savunma eylemlerinin gerçekleştirilebilmesi için siber tehdit bilgisine ihtiyaç duyulmaktadır. Siber tehdit bilgisi (STB), siber uzaydaki zararlı olayların azaltılmasına yardımcı olan tehditler ve tehdit aktörleri hakkında bilgiler olarak tanımlanmaktadır. Siber tehditlerin tanımlanabilmesi ve bu tehditlerin tespit edilebilmesi için gerekli olan siber tehdit bilgisi ile siber saldırganların amaçları, motivasyonları, yöntem ve metotları hakkında bilgi sahibi olunabilmekte ve bu bilgiler organizasyonların tehdit risklerini belirlenmesine yardımcı olmaktadır. Günümüzde siber suç davranışları ve prosedürleri analizleri paylaşılarak, güvenlik ekiplerinin yeni riskleri algılama, öngörme ve siber saldırılarla birlikte mücadele etme yeteneklerini pekiştirilebilmektedir.

Siber tehdit bilgisi, toplanan verilerin analiz edilerek saldırganların düşüncelerini, amaçlarını, motivasyonlarını, yöntem ve metotlarını tespit etme amacı taşımaktadır. Siber saldırganlar tarafından kullanılan komuta kontrol sunucusuna ait IP adresi, oltalama saldırısında kullanılan e-posta veya bir zararlı aktivitede bulunan saldırgan ve saldırı tekniği hakkında bilgi siber tehdit bilgisine örnek olarak verilebilmektedir. Siber tehdit bilgisi; indikatörler, taktikler, teknikler ve prosedürler (TTPs), güvenlik uyarıları, tehdit bilgisi raporları ve araç konfigürasyonları bileşenlerinden oluşmaktadır [10]. Siber tehdit bilgisinin başlıca amacı, organizasyonların tehdit risklerini tespit etmelerine yardımcı olmaktır.

Siber tehdit bilgisinin kullanımı, bir organizasyonun güvenlik açıklarına odaklanarak değerli bilişim varlıklarını korumasını sağlamakta, aynı zamanda kötü niyetli siber aktörlerin her zaman bir adım önünde olunmasına imkân tanımaktadır. Ayrıca bir organizasyonun sofistike saldırganların yapısını anlamasına ve sistemlerini daha iyi savunabilmek amacıyla bilinçli kararlar almasına olanak tanımaktadır. Hızlı hareket eden bir siber saldırıya karşı saldırı hakkında zaman kaybetmeksizin bilgi elde edilmesi saldırıların önlenmesinde önemli bir paya sahip olmaktadır.

Siber tehdit bilgisi, siber saldırganların teknik, taktik ve prosedürleri hakkında bilgi sunabilmekte, saldırganların oluşturdukları/oluşturabilecekleri tehditlere karşı ek bilgiler verebilmekte, alınması gerekli savunma mekanizmaları

ve alınabilecek önlemler hakkında fikir verebilmektedir. Bu kapsamda, tehdit oluşturabilecek noktalara doğru çözüm önerilerinin sunulması, benzer ihlallerin gerçekleşmemesi adına alınacak önlemlerin daha bilinçli yapılandırılabilmesi mümkün olabilmektedir.

Ayrıca siber aktörler hedef aldıkları kurbanları aldatmak için yaygın yöntemlere ilave olarak son yıllarda daha akıllı ve aşina olunmayan yöntemleri tercih etmektedir [4]. Siber tehdit bilgisi ile olası siber saldırıların tespit edilebilmesi, sistemlere yönelik zararlı girişimlerin izlenebilmesi, olası bir veri ihlalinin erken tespit edilmesi, ek ihlallerin tespit edilerek oluşabilecek zararların en aza indirgenmesi kolaylaşabilmektedir. Organizasyonlarda siber tehdit bilgisinin etkin kullanımı ile yetenekli tehdit aktörleri belirlenebilmekte, siber tehdit ortamı hakkında güncel bilgiye sahip olunabilmektedir. Siber güvenlik ekosistemi için çok önemli olan siber tehdit bilgisi ile olası veri kayıpları önlenebilmekte, güvenlik önlemleri yönlendirilebilmekte (Korsanlar tarafından kullanılan örüntüler (pattern) tespit edilmekte ve gerekli önlemlerin alınmasına yardımcı olmakta), bu bilgiler iç ve dış paydaşlarla paylaşılabilmekte ve diğer paydaşlar bilgilendirilerek siber tehditlerle topyekûn mücadele edilebilmektedir [11].

Siber tehdit bilgisi sayesinde; zararlı IP adresleri ve domainler ile zararlı girişimlerin izlenebilmesi, olası oltalama saldırılarının tespitinin kolaylaşması, verilerin toplanıp analiz edilmesi ve olası benzer durumlar için önlem alınması ve kurum üzerindeki zararının en aza indirgenmesi, veri kaybı veya sızıntısının hangi cihazlar üzerinde gerçekleştiği/gerçekleşmekte olduğu bilgisinin elde edilmesi, benzer ihlallerin gerçekleşmemesi adına alınacak önlemlerin daha bilinçli yapılandırılabilmesi, gerekli savunma mekanizmaları ve alınabilecek önlemler hakkında fikir vermesi, saldırganların teknik, taktik ve prosedürlerinin anlaşılması, tehdit oluşturabilecek noktalara doğru çözüm önerilerinin sunulması, toplanan verilerin analiz edilmesi, saldırganların oluşturdukları/oluşturabilecekleri tehditlere karşı ek bilgiler elde edilmesine yardımcı olması, hedeflenen saldırılara karşı kullanılan önlemlerin geliştirilmesine yardımcı olması mümkün olabilmektedir.

Bununla birlikte, gelişmiş siber saldırıların tespit edilebilmesi için yeni savunma yaklaşımlarının geliştirilmesi gerekmektedir. Saldırılar başlamadan önce tespit edilemese de tehditler önceden analiz edilebilmektedir. Siber tehdit bilgisi derin tehdit analizine yardımcı olabilmekte, aktif tehdit analizi yak-

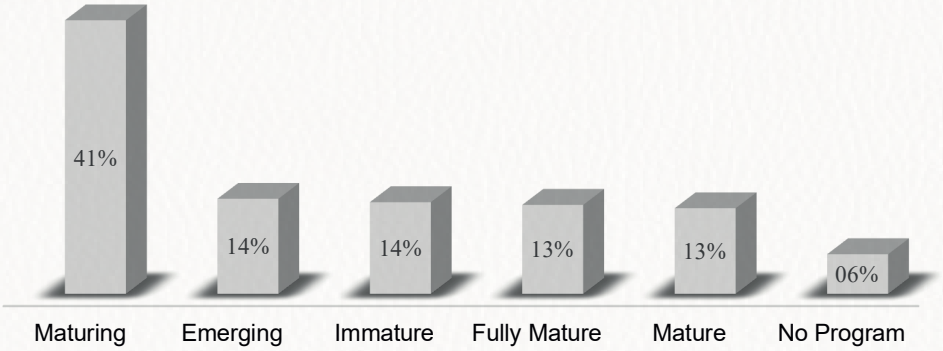
laşımları ise gelişmiş saldırı yöntemleri hakkında bilgi edinmeye yardımcı olmaktadır. Saldırganların davranışları siber tehdit bilgileri ile belirlenebilmekte ve siber güvenlik sistemleri özelleştirebilmektedir [12]. Tablo 6.1'de siber tehdit bilgisinin avantajları listelenmiştir.

Tablo 3.1. Siber tehdit bilgisinin üstünlükleri

Siber Tehdit Bilgisinin Üstünlükleri
▪ Siber tehditlere ilişkin güncel bilgiye sahip olunabilmekte ▪ Siber tehditler ve tehdit aktörleri (Motivasyonlarını, yöntem ve metotları vb.) hakkında bilgi edinilmekte ▪ Tehdit riskleri belirlenebilmekte ▪ Hangi varlıkların risk barındırdığı belirlenebilmekte (Zafiyetler, güvenlik açıklıkları) ▪ Güvenlik önlemleri yönlendirilebilmekte ▪ Sistemlere yönelik zararlı girişimler izlenebilmekte ▪ Olası veri ihlallerinin erken tespit edilmesi sağlanabilmekte ▪ Proaktif yaklaşım benimsenebilmekte ▪ Yeni savunma yaklaşımları geliştirilebilmekte ▪ Personel ve bütçe, teknoloji harcamaları ve emek ve zaman kaybı azaltabilmekte

Bunun yanı sıra, gelecekteki ve mevcut siber saldırılar ile mücadele edebilmek ve bu saldırılara organizasyonları hazır hale getirebilmek amacıyla reaktif koruma yerine proaktif yaklaşım benimsenmesi bir zorunluluk haline gelmiştir. Mevcut siber güvenlik mekanizmaları genellikle reaktif niteliktedir. Etkin bir savunma sağlanabilmesi için siber güvenlikte reaktif yaklaşım yerine proaktif bir yaklaşım benimsenmesi gerekmektedir. Proaktif yaklaşım, potansiyel tehditlerin araştırılmasını ve bir güvenlik açığının istismar edilmeden önce bir çözüm uygulanmasını gerektirmektedir. Bu kapsamda ele alındığında, siber tehdit bilgisi ile beslenmiş bir proaktif yaklaşım güvenlik ekiplerine karar vermede yardımcı olabilecektir [13].

Diğer taraftan, organizasyonların tehditlerle mücadelede tehdit bilgisinin önemli rol oynadığını değerlendirmekte ve bu kapsamda bünyelerindeki tehdit bilgilerini zenginleştirmektedir. Nitekim yapılan bir araştırmaya göre organizasyonların %5,9'nun siber tehdit bilgisine sahip olmadığı, bununla birlikte birçok işletmenin kendi sistemlerini yetersiz bulduğu, yine işletmelerin %40,5'inin ise kendi siber tehdit bilgisi programlarını olgunlaştırdığı sonucu ortaya çıkmıştır.



Şekil 3.1. Organizasyonların siber tehdit bilgisi kapasitesi [8]

Yapılan bir diğer çalışmada ise veri ihlallerin %80'inin siber tehdit bilgisi ile engellenebileceği ya da hasarının en aza indirebileceği sonucu ortaya çıkmıştır. Siber tehdit bilgisi çözümleri eyleme geçirilebilir çözümler olup, gerçek zamanlı önlemler alınabilmekte ve olası saldırılara karşı hazırlıklı olunabilmektedir.

Ayrıca organizasyonlarda güvenlik ekipleri tarafından bilginin işlenmesi amacıyla taktiksel, operasyonel ve stratejik bilgi olmak üzere farklı ürünler kullanılmaktadır. Taktiksel bilgi, olay müdahale prosedürleri için öneriler üzerine kurulmuş olup, kuruluşların güvenlik pozisyonlarını artırmada önemli bir rol oynamaktadır. Taktiksel bilgi, tehdit aktörleri tarafından kullanılan teknikler, taktikler ve prosedürlerle ilgili materyallerden oluşmaktadır. Stratejik bilgi ise siber saldırı gruplarının ve saldırganların ortak belirli özelliklerine ilişkin bilgiler şeklinde tanımlanmaktadır. Stratejik bilgi, taktiksel bilgiden oluşturulan bilgi tabanı üzerine inşa edilmiş olup, güvenlik ekiplerinin önemli kararlar almalarına yardımcı olmak için kullanılabilmektedir. Stratejik bilgi, saldırının kaynağına yönelik aksiyon alınmasını sağlamaktadır. Stratejik bilgi, üst düzey karar vericilerin tehdit ortamı hakkında bilgilendirmek amacıyla kullanılmakta olup, stratejik bilgi ürünleri teknik terminoloji yerine iş riski konularına odaklanmaktadır. Operasyonel bilgi ise siber saldırı belirtilerini hızlı, verimli ve zamanında tespit etmeyi amaçlamaktadır. Operasyonel tehdit istihbaratı genellikle bir kuruluşa karşı yapılması muhtemel operasyonların ayrıntılarıyla ilgili olup, bilinen saldırıların ayrıntılarının incelenmesiyle elde edilen bilgidir.

Öte yandan, siber tehdit bilgisi çözümünün benimsenmesi ve sürdürülmesi için minimum bazı gerekliliklerin bulunması gerekmektedir. Bu gereklilikler ve özellikler aşağıda sıralanmıştır.

- Siber tehdit bilgisi çözümlerinin kurulumu ve bakımı için plan, insan ve teknoloji kaynağı gerekmektedir. SANS Enstitüsü tarafından yapılan ve şirketlerin tehdit bilgisini nasıl benimsediğini ve kullandığını inceleyen yeni bir ankette, ankete katılan şirketlerin %57'sinin siber tehdit bilgisinin entegrasyonu ve kullanımı için iyi tanımlanmış bir planın, şirketler için en iyi uygulamayı temsil ettiğine inandıklarını bildirmiştir.
- Tehdit bilgisi çözümünün, mevcut güvenlik altyapısıyla sorunsuz bir şekilde bütünleşmesi ve tehdit bilgisi çözümünün, tehdit bilgisinin alınması, analizi ve uygulanması ile ilişkili süreçlerin çoğunun otomatikleştirmesi gerekmektedir. SANS Enstitüsü'nün bir raporunda, algılama ve olay müdahale süreçlerini kolaylaştırmak için otomasyonun önemi vurgulanmaktadır. Raporda, otomasyonun güvenlik analistlerine önemli görevlere daha fazla zaman ayırmalarına imkân verdiği ve tehdit bilgisini operasyonelleştirmeyle ilgili idari yönlere daha az zaman ayırmalarına olanak tanıdığı belirtilmektedir. Raporda ayrıca otomasyonun tutarlılık sağlanmasına yardımcı olduğu ve aynı zamanda kalan süreç verimsizliklerinin ortadan kaldırılmasında yenilikçiliğin teşvik edildiği belirtilmektedir.
- Siber tehdit bilgilerinin uygulanabilir olması için; güven, itibar, ilgi düzeyi, anonimlik, zamanlılık ve verilerin birlikte çalışabilirlik özelliklerini taşıması gerekmektedir. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA); uygunluk, zamanlılık, doğruluk, bütünlük ve analiz edilebilirlik olmak üzere beş kriteri karşılayan uygulanabilir/eyleme geçirilebilir siber tehdit bilgisi tanımlamaktadır [14].
- Uygunluk, bilginin içeriğinin ilgi düzeyini göstermektedir. Elde edilen tehdidin sistem için bir risk olduğu anlamına gelmektedir. Bununla birlikte, uygunluk eksiksizlik ve güven ile bir bütün olarak değerlendirilebilmektedir. Zira bilginin temin edildiği paydaş güvenilir değilse veya bilgi eksikse, söz konusu bilgi ilgili kabul edilmeyebilmektedir. Zamanlılık, güncel bilgileri zamanında paydaşlarla paylaşmak ve temin etmeyi ifade etmektedir. Bazı siber saldırılar saniyeler içinde gerçekleştirilebilmektedir. Hızlı bir bilgi paylaşım süreci, siber tehdit

bilgisi paylaşımının önemli bir özelliğidir. Tehdit ortamı hızla değişmekte ve bu nedenle siber tehdit bilgisi hızlı bir şekilde değerlendirilmelidir. Bilgi paylaşımının hızlı bir şekilde gerçekleştirilmesinin önemi, bilginin değerinin çok kısa sürede yok olması halinde anlaşılabilmektedir. Bir paydaş, e-postanın içerisinde yer alan bir kötü amaçlı bir bağlantı hakkında bir gösterge tespit etmesi halinde ve bu bilginin güvenilir bir platform içerisinde birkaç saniye içinde paylaşılması halinde paydaşlar tarafından tehdidin engellenerek riskin azaltılabilmesi mümkün olabilecektir.

- Siber tehdit bilgisi paylaşım işbirliği oluşturmak, paydaşlar arasında kapsamlı bir güven ilişkisi gerektirmektedir. Güven, siber tehdit bilgisi paylaşım ekosisteminde temel bir özelliktir. Siber tehdit bilgisi paylaşım ekosistemindeki en zor özellik olarak kabul edilmektedir [13]. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından, gizli verilere yetkisiz paydaşlarca erişim sağlanmaması, bilginin doğru kullanılması ve paylaşılan bilgilerin inandırıcı ve güvenilir olması olmak üzere üç güven ilişkisi belirlenmiştir.
- Paydaşların, bir tehdit paylaşım topluluğunun güvenilir birer üyeleri olabilmesi için itibarlarını korumaları gerekmektedir. İtibar, yüksek kaliteli ve eyleme geçirilebilir siber tehdit bilgileri paylaşılarak ve siber tehdit paylaşım politikalarına uyarak zaman içinde oluşturulmaktadır. Güvenilirliği artırmak için, paydaşların sürekli olarak siber tehdit bilgisi paylaşması, çeşitli kaynakları ilişkilendirmesi ve paylaşılan bilgi ile ilgili olarak topluluğun sorularını yanıtlaması gerekmektedir [15].
- Uygulanabilir olmayan tehdit göstergeleri nedeniyle, bir analistin tüm verileri değerlendirmesi gerekebilecektir. Bu nedenle, paydaşlar tarafından ölçeklenebilir bir uygunluk düzeyi filtresi kullanılmalıdır. Ayrıca "Veri uygunluğu, veri kalitesinin önemli bir faktörüdür" [16]. Paydaşlar, envanterlerini bilerek sistemleri ile hangi siber tehdit bilgisinin ilgili olduğunu değerlendirmeli ve tanımlamalıdır.
- Organizasyonlar, siber tehdit bilgisini yalnızca güvenilir paydaşlarla paylaşarak ve/veya içeriği anonimleştirerek paydaşların gizliliğine öncelik vermelidir. Paydaşlar, korunması için önemli bir varlık olan itibarlarına zarar verebileceği korkusuyla ihlallerle ilgili bilgileri paylaşma konusunda hala isteksizdir [17]. Anonimliğin bir başka yönü ise, paydaşlar arasında paylaşıldığında siber tehdit bilgisinin şifrelenmesidir.

Böylece Ortadaki Adam (Man in the Middle) saldırılarına karşı söz konusu bilgiler korunabilmektedir. Anonim paylaşım, bir paydaşın henüz kendi sisteminin ihlal edildiğini açıklamak istemediği, ancak bilgiyi diğer paydaşlarla paylaşmak istediği durumlarda kullanılabilmektedir. Ayrıca paydaşlar arasında henüz güven oluşturulamamışsa anonim bilgi paylaşımı tercih edilmektedir. Siber tehdit bilgisinin anonimliği içerik, meta veriler ve veri aktarımı dâhilinde oluşturulmalıdır.

- Siber tehdit bilgisinin şifrelenmesi, güvenlik zafiyeti kapatılmadan önce kritik bilgilerin ortaya çıkmasını ve paydaşlara karşı kullanılmasını önleyebilmektedir. Anonimlik olmaması halinde, kötü niyetli paydaşlar tarafından kapatılmamış güvenlik zafiyetleri, zafiyet barındıran paydaşlara yönelik kullanılabilir. Ayrıca siber tehdit bilgilerinin anonimleştirilmesi halinde kötü niyetli kişiler tarafından ele geçirilen verilerin çözümlenmesi zaman alacak ve bu zaman dilimi içerisinde paydaşların söz konusu zafiyetlere yönelik gerekli tedbirleri alabilecektir.
- Organizasyonlar siber tehdit bilgilerini paylaşmak isteseler bile siber tehdit bilgisi paylaşımı için küresel olarak yaygın bir format bulunmamaktadır. Veri formatları, paydaşların sistemleriyle uyumlu olmalıdır. Bu nedenle, tüm paydaşlar tarafından ortak bir format üzerinde anlaşmaya varılmalıdır. 2014 yılında yapılan bir ENISA çalışmasına göre, topluluk tarafından benimsenen 53 farklı bilgi paylaşım standardı bulunmaktadır [13].

3.4. SİBER TEHDİT BİLGİSİ PAYLAŞIMININ ÖNEMİ

Günümüzde bilgi teknolojileri ve internet kullanımının yaygınlaşması ile geleneksel iletişim yöntemleri yerini elektronik cihazlara, fiziksel nesneler ise yerini siber alandaki cihazlara bırakmaktadır. Siber uzayda birbirine bağlı cihaz sayısı, kullanıcı sayısı ve üretilen veri miktarı her geçen gün artmaktadır. Buna bağlı olarak siber uzayda ortaya çıkan tehditler de aynı oranda artmakta olup, bu tehditlerle topyekûn mücadele edilmesine ihtiyaç duyulmaktadır. Bu nedenlerden dolayı, tehdit bilgisi paylaşımının önemi aşağıda maddeler halinde verilmektedir.

- Gelişen teknoloji ile birlikte siber uzayda ortaya çıkan tehditler de artmaktadır. Siber uzaydaki varlıkların korunabilmesi ve siber teh-

ditlerle etkin bir şekilde mücadele edilebilmesi için siber tehditler hakkında daha detaylı bilgilere ihtiyaç duyulmakta olup, tehditler hakkında daha fazla bilgiye sahip olunabilmesi için diğer paydaşlarla işbirliği yapılması ve paydaşların bilgi birikiminden faydalanılması gerekmektedir. Sonuç olarak, siber tehdit bilgisi tehditlerle topyekûn mücadele edilmesine ihtiyaç duyulduğundan dolayı önemlidir.

- Siber tehditlerle kapsamlı bir şekilde ve tam anlamıyla mücadele edebilmek amacıyla tehdit aktörleri tarafından kullanılan taktiklerin/araçların belirlenmesi ve bunlara yönelik aksiyon alınması gerektiğinden önemlidir.
- Organizasyonlar arasında siber tehdit verilerinin paylaşılması, daha önce karşılaşılmayan siber saldırıların engellenmesine yardımcı olabileceği, analiz edilen bilgiler sayesinde organizasyonların karşılaşabileceği siber tehditlerin öngörülebileceği ve bu sayede gerekli savunma mekanizmalarının geliştirilebileceği, oluşturulabileceği veya kurulabileceği için önemlidir. Organizasyonları hedef alabilecek tehditlerin zamanında bertaraf edilebilmesi için paydaşlar arasında veri, bilgi, deneyim paylaşımına imkân tanıyacak işbirliği altyapısının oluşturulması gerekmektedir. Paydaşlar arasında siber tehdit bilgilerinin paylaşılması ile her paydaşın tehditleri önlemeye yönelik kurumsal yetenek ve kapasitesinin artırılmasına katkı sağlaması açısından önemlidir.
- Sonuç itibarıyla, ülkemizde kurumlar, sektörler veya organizasyonlar arasından siber tehdit bilgilerinin paylaşılması, kolay paylaşım platformlarının oluşturulması, işbirliği mekanizmalarının geliştirilmesinin; siber güvenlik direncinin artmasına, tehdit vektörlerinin daraltılmasına, kaynakların daha verimli kullanılmasına, siber vatanın korunmasına daha stratejik bakılmasına, dolayısıyla daha üst seviyede güvenliğin ve savunmanın sağlanmasına katkı sağlaması açısından önemlidir.

3.5. SİBER TEHDİT BİLGİ PAYLAŞIM ÇALIŞMALARI

Siber tehditlerin hızla arttığı ve tehdit boyutunun büyüdüğü siber uzayda oluşan tehditlerin ise daha iyi anlaşılması ve tespit edilebilmesi için her zamankinden daha çok çabaya, insan gücüne, yeni yöntemler geliştirilmesine, güncel teknolojik altyapılara, bilgilerin otomatik olarak işlenmesine, mevcut

bilgi birikiminin ve kapasitesinin artırılmasına ihtiyaç duyulmaktadır. Bu çalışmaları yapabilmek, gerçekleştirmek, önlemek veya karşılaşılabilecek riskleri mümkün olduğunca engellemek için, siber tehdit bilgi paylaşımına ilişkin literatürde pek çok çalışma vardır [13]-[27]. Bu çalışmalar incelendiğinde;

- Thomas ve arkadaşları tarafından yapılan çalışmada, siber tehdit bilgisi paylaşımında insan rolü, kültürel ve dilsel zorluklar, eyleme geçirilebilir siber tehdit bilgisi için tehdit bilgisinin barındırması gereken özellikler ve tehdit bilgisi paylaşımında 2 yaygın model (direkt bilgi paylaşımına imkân sunan noktadan noktaya iletim ve yayımlanan olayların uçtan ortak havuza iletim) incelenmiş ve bu modellerin birleşiminden oluşan yeni bir hibrid model önerilmiştir [13].
- Jasper tarafından hazırlanan çalışmada [18] ise Amerika Birleşik Devletleri Siber Tehdit Bilgisi Paylaşım Çerçeveleri kapsamında federal hükümet yapıları, gönüllü programlar incelenmiştir. Ayrıca siber tehdit bilgisi paylaşımında karşılaşılan zorluklar ele alınmıştır. Bu kapsamda;
  - Siber güvenlik bilgilerinin analiz edildiği, zamanında ve eyleme geçirilebilir tehdit bilgilerinin paylaşıldığı, müdahale, azaltma ve kurtarma çabalarının koordine edildiği çeşitli gönüllü bilgi paylaşım programlarının yürütüldüğü,
  - Siber Bilgi Paylaşımı ve İşbirliği Programı oluşturularak federal hükümet ve kritik altyapı sektörlerinden kuruluşlar arasında siber tehdit, olay ve güvenlik açığı bilgilerinin gerçek zamanlı olarak paylaşıldığı,
  - Gelişmiş Siber Güvenlik Hizmetleri altında bilgi paylaşım programı oluşturulduğu ve ABD merkezli kamu ve özel kuruluşlara yönelik gelişmiş bir yaklaşımla koruma ve savunma mekanizmaları ile yüksek seviyede koruma sağlandığı vurgulanmıştır.

Siber tehdit bilgi paylaşımı üzerine yapılan bir literatür incelemesinde [19];

- Siber güvenlik ekiplerinin aralarında bilgi paylaşımı gerçekleştirdiği paylaşım araçlarının mevcut olduğu,
- Hâlihazırda bilgi paylaşımında yaygın olarak benimsenen tek bir standardın bulunmadığı,

- Tehdit bilgisi paylaşım standartlarının uyumlu bir şekilde benimsenmesi ile siber güvenlik çabaları için büyük fayda sağlanacağı,
- Ortak standartların benimsenmemesinin kuruluşlar ile sektör, ulusal ve uluslararası Bilgisayar Olaylarına Müdahale Ekipleri arasındaki siber tehditlerle ilgili etkili iletişimi zayıflattığı raporlanmıştır.

Siber tehdit bilgisinin temel zorlukları ve sunduğu fırsatları ele alan bir diğer çalışmada [20];

- Saldırganların daha inovatif ve daha çok zekâ içeren yöntemler kullandığı,
- Yöntemlerin birleştirilerek daha karmaşık saldırıların planlandığı,
- İleri yöntemleri içeren saldırıların, saldırganın ve saldırının varış noktasının tanınmasını zor bir konu haline getirdiği,
- Siber suçluların analizini zorlaştırdığı,
- Kötü niyetli ve zarar verici kodların sayısının hızla artmasından dolayı gelişmiş adli bilişim ve gizlenme yöntemleri kullanmasının genel güvenlik değerlendirme tekniklerini verimsiz hale getirdiği,
- Gelişmiş siber saldırılara yönelik algılama, akıl yürütme, öğrenme ve hareket etme için yapay zekâ ve makine öğrenimi tekniklerinin uygulanması gerektiği,
- Güvenlik uygulayıcıları ve analistleri için güncel bilgileri öğrenmenin yanında bu yöntemlerin bir kombinasyonu hem bilmek hem de bunları birleştirmek zorunda oldukları belirtilmiştir.

Bir başka çalışmada [21];

- Hangi bilgilerin siber tehdit bilgisi olarak kabul edildiğine dair tam bir anlayışa sahip olmadığı ve siber tehdit bilgisini tanımlamak için daha fazla araştırmaya ihtiyaç duyulduğu,
- Tehdit bilgisi veri paylaşımı veya geri bildirimi, tehdit bilgisi standartları ve siber tehdit bilgisi paylaşımında kullanılan araçları içeren mevcut siber tehdit bilgisi ürün ve hizmetlerinin tanımlandığı,
- Siber tehdit bilgisi paylaşımında karşılaşılan sorunlar ve zorlukların ele alındığı,

- Siber tehdit bilgisi potansiyelini tam olarak kullanmak için araştırma ve geliştirmeye ihtiyaç duyulduğu,
- Tehdit verilerini doğrulamak ve üyeler arasında paylaşılan tehdit verilerinin yeterli kalitede olmasını sağlamak için topluluk üyeleri arasında bir ortak girişim çalışması bulunduğu,
- MITRE gibi bir araştırma ve geliştirme merkezinin, tehdit paylaşan paydaşlar arasındaki birlikte çalışabilirlik sorununu çözmek için tehdit bilgisi paylaşımı için standartlar formatını (örneğin; STIX, TAXII, CybOX) geliştirme çabası içerisinde olduğu vurgulanmıştır.

Diğer bir çalışmada ise İngiltere'deki şirketler ve devlet kurumlarının güvenli bir topluluk aracılığıyla yeni riskler ve güvenlik açıklıkları hakkındaki bilgileri paylaştığı Siber Güvenlik Bilgi Paylaşım Ortaklığı (CISP) işbirliği platformu incelenmiş [22] ayrıca;

- Güven ve anonimlik ihtiyacını karşılamanın zorlukları ele alınmış,
- Bir siber güvenlik paylaşım girişimine katılmanın motive edici unsurları incelenmiş,
- CISP işbirliği platformunun; finans, enerji, akademi ve kamu kurumları dâhil olmak üzere çeşitli sektörlere dâhil olan kuruluşlardan oluştuğu açıklanmış,
- Yaklaşık 700'ün üzerinde kuruluşun ve 2 binin üstünde kişinin topluluğa katıldığı belirtilmiş,
- Ağ güvenliğini sağlamak için siber güvenlik bilgilerini paylaşmaya motive eden üç ana faktörün olduğu (tehditlerin engellenmesine yönelik diğer paydaşlara yardımcı olma, paydaşlar tarafından saygınlığın kabul edilmesi ve aynı sektörde faaliyet gösterenlerin ortak bir tehdide karşı savunmalarına yardımcı olma) şeklinde tanımlanmıştır.

Bilgi paylaşımını iyileştirmeye yönelik yaklaşımları belirlemek için siber savunma yönünün incelendiği çalışmada [23];

- İşbirliğinin dört yönünün olduğu ve bunların ise; bilgi paylaşımına yönelik teşvikler ve engeller, işbirliğine dayalı risk yönetimi ve bilgi değeri algısı, veri alışverişinin geliştirilmesine yönelik prosedürel

modellerin araştırılması ve siber savunma verileri için paylaşım mekanizmalarının otomatize edilmesi şeklinde sıralandığı,

- Siber savunma verilerinin paylaşımı için işbirliğine dayalı ilişkiler ve güvenilir ilişkiler kurma becerisinin gerektiği,
- Siber savunma işbirliğinin belirli zorlukları içerdiği,
- İşbirliği platformları ile ilgili olarak net bir ortak anlayışa ulaşıldığında veri paylaşımını iyileştirmeye yönelik prosedür modellerinin, bir kuruluşun risk modellerini bilgi paylaşım modelleriyle entegre etmesine yardımcı olacağı,
- Tehdit seviyesi, öngörülen etki, risk metodolojisi ve risk yönetimi açısından karşılıklı yardımlaşmanın, işbirliği ağının etkinliğini arttıracağı belirtilmiştir.

Siber tehdit bilgisinin paylaşıldığı ekosistem, bilgi paylaşımı için kullanılan standartlar ve protokoller ve bilgi paylaşım modelleri ise [12] nolu kaynakta incelenmiş olup;

- Siber tehdit bilgisinin ilk olarak 2013 yılında Gartner tarafından tanımlandığı,
- Endüstrilerin bugün karşı karşıya olduğu büyük miktardaki tehdit bilgilerinin işlenmesini kolaylaştırabildiği,
- Tehdit bilgisinin, tehditlerin savunulmasında pratik ve eyleme geçirilebilir, araştırılan ve yorumlanan bilgi olduğu ve saldırganın kimliği, saldırı yaklaşımları, önceden başlatılan saldırılar, saldırı hedefleri, hedeflenen sistemlerin güvenlik açıkları ve olası çözümler gibi birçok faktörü içerebileceği,
- Tehdit bilgisi paylaşımı sürecinin üç modelle tanımlanabildiği, bunların ise; Eşler Arası, Kaynak–Paydaş (Kaynaktan diğer paydaşlara bilgi akışı ve Merkez–Paydaş (paydaşlardan sağlanan tehdit bilgilerinin tüm paydaşlarla paylaşılması) şeklinde sıralandığı,
- Geleneksel tehdit bilgi paylaşım yöntemlerinin çoğunlukla eşler arası ve kaynak abone modellerine dayanırken, Merkez–Paydaş modelinin, gelecek nesil tehdit bilgi paylaşım sistemlerinin geliştirilmesi için geniş çapta kabul gördüğü belirtilmiştir.

Risk düzeyine göre kuruluşlar arasında durumsal farkındalık bilgisinin paylaşılmasına yönelik olarak geliştirilen modelde [24];

- Daha yüksek risk seviyelerine sahip doğrudan bağlantıların azaltılabildiği,
- Daha güvenli bilgi paylaşım topluluklarının oluşturulabildiği,
- Durumsal farkındalık bilgilerinin paylaşımının kuruluşlar için son derece önemli olduğu,
- Tehditlere karşı erken uyarı için durumsal farkındalık bilgilerinin gerekli olduğu,
- Paylaşılan bilgilerin kötüye kullanılma ihtimalinin bulunduğu ve bu tür bilgilerin paylaşılmasının riskli olabileceği belirtilmiştir.

Siber tehdit bilgisi sağlayan bazı özel kuruluşlar ve siber tehdit bilgisi kullanımındaki bazı zorlukların incelendiği bir diğer çalışmada [25];

- Operasyonel, taktiksel ve stratejik olmak üzere 3 farklı düzeyde siber tehdit bilgisi türünün bulunduğu,
- Siber tehdit bilgisi kullanımında karşılaşılan zorlukların; tehdit verisinin aşırı yüklemesi, tehdit verisi kalitesi ile özel ve yasal sorunlar olduğu raporlanmıştır.

Farklı paydaşların bağlamsal ve eyleme geçirilebilir siber tehdit bilgisini sorunsuz ve işbirliği içinde toplamaları, bir araya getirmeleri, analiz etmeleri ve zamanında paylaşmalarını teşvik edebilecek ve etkinleştirebilecek kavramsal bir siber tehdit bilgisi paylaşım modeli ve platformunun önerildiği bir diğer çalışmada [26] ise;

- AlienVault, ThreatQ ve ThreatView tehdit bilgisi paylaşım platformları incelenmiş,
- Tehdit bilgisinin paylaşımının stratejik, taktiksel ve operasyonel seviyelerde de gerçekleşebileceğinden, uygun bir paylaşım modelinin formüle edilmesi ve bunlar tarafından kabul edilmesinin önemli olduğu raporlanmış,
- Paydaşlar arasında paylaşılması gereken bilginin, çoğunlukla reaktif operasyonlarda yararlı olan bilgiden daha yüksek düzeyde olması gerektiği, ilgili siber tehdit bilgisinin bağlamsal ve eyleme geçirilebilir

olması gerektiği ve siber saldırılara ve siber suçlara proaktif ve öngörücü yanıtlar sağlaması gerektiği belirtilmiştir.

Paydaşların siber güvenlikle ilgili bilgi paylaşım faydaları ve risklerine yönelik tutumlarını keşfetmek için üçgenleştirilmiş karma yöntem önerisinde [27] ise;

- Bilgi paylaşımın siber güvenlik analistlerinin üretkenliği ve performansı üzerindeki etkisi araştırılmış ve siber güvenlik bilgi paylaşımı ile performans arasında bir bağlantı kuran deneysel verilerin eksik olduğu belirlenmiş,
- Tüm süreçler gibi siber güvenlik bilgi paylaşımında da insan ve finansal kaynaklara ihtiyaç duyulduğu vurgulanmış,
- Siber güvenlik bilgi paylaşımına yönelik deneysel desteğin yetersizliğinin iki önemli konuyu vurguladığı; birincisinin özel sektör kuruluşlarının rekabet, sorumluluk ve yatırım getirisi gibi çeşitli nedenlerden dolayı bilgi paylaşımına bazen ihtiyatlı davrandığı veya bilgi paylaşım çabalarına katılmaya isteksiz olduğu, ikincisinin ise siber güvenlik bilgi paylaşım çabaları ve teknolojisi için değerlendirme yöntemlerinin olmamasının, eksikliklerinin tespit edilmesini ve giderilmesini engellediği belirtilmiştir.

Ülkemizde ise siber tehdit bilgilerinin paylaşımına yönelik olarak Ulusal Siber Olaylara Müdahale Merkezi (USOM) üzerinden bilgi paylaşımı gerçekleştirilmekte olup, kuruluşlarda oluşturulan Siber Olaylara Müdahale Ekibi (SOME)'ler aracılığıyla ise yaşanan siber olaylar USOM'a bildirilmektedir.

Sonuç olarak; literatürde farklı açılardan ele alınan ve özetlenen çalışmalardan da görülebileceği gibi genel itibarıyla siber tehdit bilgisi paylaşımının çok farklı kazanımları olsa da üzerinde detaylı olarak düşünülmesi ve karar verilmesi gereken pek çok husus olduğu, siber tehditlerin engellenmesinde tehdit bilgisi paylaşımının organizasyonlara büyük katkı sağladığı, dünya genelinde siber tehdit bilgi paylaşımı için paylaşım ekosistemleri geliştirildiği görülmektedir. Ülkemizde ise; siber tehdit bilgilerini üreten ve bu bilgileri raporlayan siber güvenlik firmaları arasında bilgi paylaşımına yönelik bir işbirliği platformu bulunmadığı literatür araştırmasından görülmektedir.

3.6. SİBER TEHDİT BİLGİSİ PAYLAŞIMINDA KULLANILAN STANDARTLAR VE PLATFORMLAR

Her alanda olduğu gibi standartlaşma bu alanda da önemli konular içerisindedir. Standartlaştırılmış veri formatları ve taşıma protokolleri, otomasyonu etkinleştirdikleri ve kuruluşlar arasında makine hızında bilgi paylaşımına izin verdikleri için birlikte çalışabilirlik için önemli yapı taşlarıdır [19]. Organizasyonların ve güvenlik uzmanlarının tehdit bilgisi verilerini toplama ve bu verilerin nasıl işleneceğini belirleme konusunda artan bir ilgisi bulunmaktadır. Tehdit bilgisi araçlarının yardımı olmadan bu tehdit verileri yönetilemez veri akışı haline gelebilmektedir. Bu nedenle, bu alt bölümde açıklanan araçlar; tehdit bilgisi paylaşımını yönetilmesine yardımcı olmak için geliştirilmiş araçlardan en önemlileridir. Bununla birlikte, belirli formatların ve protokollerin benimsenmesi, önemli zaman ve kaynaklar gerektirebilmekte ve paydaşlar tarafından farklı yapıların veya protokollerin gerekmesi halinde bu yatırımların değeri önemli ölçüde azaltılabilmekte, yeni imkân ve kabiliyetlerin kazandırılmasına gerek duyulabilmektedir.

Siber tehdit bilgilerinin paylaşılması amacıyla birçok standart kullanılmaktadır. Bu standartların kullanılması ile tüm paydaşlar arasında aynı dilin konuşulması sağlanmakta, siber tehdit bilgisinin herkes tarafından anlaşılabilir ve kullanılabilir olması mümkün olmaktadır. Bu standartlara;

- Structured Threat Intelligence eXpression (STIX),
- Trusted Automated Exchange of Indicator Information (TAXII),
- Incident Object Description Exchange Format (IODEF),
- Collective Intelligence Framework (CIF)

örnek verilebilir [26].

STIX ve TAXII protokolleri; siber tehdit bilgilerinin paylaşılabilmesi, saklanabilmesi ve analiz edilebilmesi için geliştirilmiş protokoller olup, siber tehdit bilgisi paylaşımında yetenekli ve geniş kullanıma sahiptir.

STIX standardı [28];

- Yapılandırılmış siber tehdit bilgilerinin tanımlanması, genişletilebilir, otomatikleştirilebilir ve güvenlik ekipleri tarafından okunabilir bir formatta temsil edilmesi için yapılandırılmış bir dildir.

- Siber tehdit bilgisinin tanımlanması, elde edilmesi, karakterize edilmesi ve standardize edilmesi amacıyla geliştirilmiştir.
- Siber tehdit bilgisi konseptinin anlaşılabilmesi ve yönetebilmesi amacıyla oluşturulmuş bir standart olup, bilgisayar tabanlı saldırıların daha iyi anlaşılabilmesi, daha hızlı ve efektif bir şekilde yanıt üretilebilmesi adına kolaylık sağlamaktadır.
- Yapılandırılmış tehdit bilgisine yönelik ortak bir mekanizma sağlamakta olup, siber gözlenebilir etkenler, indikatörler, siber olaylar, siber aktörlerin taktikleri, teknikleri ve prosedürleri (pattern, malware, exploitler, siber ölüm zincirleri, araçlar, altyapılar ve hedefler vb.), istismar edilen hedefler (zafiyetler ve zayıflıklar vb.), eylem pratikleri (siber olaya yanıt verme veya zafiyet giderme), siber saldırı kampanyaları ve siber tehdit aktörleri bilgilerini içermektedir.
- Bugün itibariyle, tehdit bilgisi paylaşımı (örneğin; CybOX, STIX ve TAXII) ve otomatik bilgi paylaşımını (örneğin; MISP, OTX) desteklemek için tehdit bilgisi paylaşım platformunun geliştirilmesi için standartlara yönelik bir geliştirme artışı olsa da tehdit bilgisi verilerini tanımlamak için fiili standart olarak STIX kabul edilmekte ve tehdit bilgisi paylaşım platformu tarafından yaygın olarak kullanılmaktadır.

TAXII (Trusted Automated eXchange of Indicator Information) standardı [29], [30]**;**

- Siber tehdit bilgilerinin platformlar arasında otomatik olarak paylaşılması için kullanılabilen,
- Temelde, kuruluşların yapılandırılmış siber tehdit bilgilerini güvenli ve otomatik bir şekilde paylaşmasına olanak tanımakta olan,
- Organizasyonların/kuruluşların ortaklarıyla bilgi paylaşmalarına yardımcı olmak amacıyla siber tehdit bilgisi alışverişi için bir dizi özellik olarak tanımlanabilen,
- Bilgi üreticileri, tüketiciler ve geliştiriciler tarafından kullanılmasını amaçlayan,
- Siber tehdit bilgilerinin birden çok paylaşım ortağı ve toplulukla otomatik olarak geniş bir şekilde paylaşma kabiliyetine sahip olan,

- Otomatik bir paylaşım altyapısının parçası olabilecek hizmetleri ve mesaj alışverişlerini tanımlamakta ve aynı zamanda birden fazla paydaşla etkileşim kurmak amacıyla kullanılabilecek tek bir hizmet ve müşteri kümesini mümkün kılan,
- Altyapı ve prosedürlere yeterli sayıda yatırım yapılmasına imkan sağlayan,
- Siber savunma toplulukları içinde ve arasında tehdit bilgilerinin zamanında ve güvenli bir şekilde paylaşılmasının sağlanması ve etkin siber tehdit bilgisi kümelerinin sağlam, güvenli ve yüksek hacimli bir şekilde alışverişinin sağlanması hususlarını mümkün kılan,
- Daha fazla kuruluşun tehdit bilgilerinin daha hızlı ve güvenli bir şekilde paylaşmasını mümkün hale getiren,
- Güvenli ve otomatik bir şekilde sistemler arasında şifreleme, kimlik doğrulama, adresleme, uyarı ve sorgulama gibi yeteneklerle birlikte siber tehdit bilgisi mesajlarının taşınması için ortak, açık spesifikasyonlar sağlayarak tehdit verilerinin hassasiyetini ele alan,
- Organizasyonda eyleme geçirilebilir siber tehdit bilgilerinin paylaşılmasını sağlayan açık kaynaklı bir protokol ve hizmet belirtimine sahip olan,
- Siber tehdit bilgi paylaşımını hızlandıran, tanımlı hizmetler ve mesaj alışverişleri gibi büyük ölçüde manuel olarak yürütülen işleri otomatize hale getirilmesine katkı sağlayan, siber güvenlik alanında çalışanların tehdit verilerini gerçek zamanlı olarak alabilmelerine imkan sunan ve
- Tehdit paylaşım topluluklarına katılmanın önündeki teknik engellerin azaltılarak daha fazla kuruluşun bu paylaşıma katılmasını sağlayan

yapıları barındırmaktadır.

Siber Tehdit Bilgisi Platformu (STBP) ise [31], [32];

- Organizasyonların savunma eylemlerini desteklemek için gerçek zamanlı olarak birden fazla kaynaktan gelen tehdit verilerini bir araya getirmesine, ilişkilendirmesine ve analiz etmesine yardımcı olan yeni bir teknoloji disiplini olarak tanımlanmakta,

- Çeşitli dâhili ve harici kaynaklar (sistem günlükleri ve tehdit bilgisi beslemeleri gibi) tarafından üretilen artan veri miktarını ele almak ve güvenlik ekiplerinin kuruluşlarıyla ilgili tehditleri tanımlamasına yardımcı olmak için geliştirilmekte,
- Birden çok kaynaktan ve formattan içe veri aktararak, bu verileri ilişkilendirerek ve ardından bir kuruluşun mevcut güvenlik sistemlerine aktararak, proaktif tehdit yönetimini otomatik hale getirmekte,
- Tehdit aktörlerinin varlığını tespit ederek, saldırılarını engelleyip mücadele ederek veya altyapılarını bozarak kuruluşların saldırganlara karşı avantaj elde etmesini mümkün kılmakta,
- Tehdit bilgisi kullanarak işletmeler ve kamu kurumları, kendi çevreleriyle en yararlı ve ilgili tehdit kaynaklarını ve verilerini de belirleyerek gereksiz ticari tehdit beslemeleriyle ilişkili maliyetleri düşürebilmekte,
- Güvenlik ekiplerinin tehdit bilgilerini kendi güvenilir çevreleri arasında paylaşmalarını, güvenlik uzmanlarıyla arayüz oluşturmalarını ve eşgüdümlü karşı önlemlerin uygulanması konusunda rehberlik almalarını mümkün kılan ortak bir yaşam alanı sağlamakta,
- Tam özellikli olanları ile güvenlik analistlerinin bu taktik ve stratejik faaliyetleri olay yanıtı, güvenlik operasyonları ve risk yönetimi ekipleriyle eşzamanlı olarak koordine etmesini desteklemekte ve
- Güvenilir topluluklardan veri toplanması için kullanılmaktadır. Bunlara ilave olarak, organizasyonların STBP'yi kullanırken veya bundan faydalanırken [33];
- Çözümler geliştirilirken ve iletirken spesifik gerekliliklerine ve ihtiyaçlara odaklanılması,
- Organizasyonların gerekliliklerini kaydetmeleri ve teknoloji platformları tarafından farklı siber aktivitelerin nasıl sağlanacağı üzerinde çalışılması,
- Geliştiricilerinin, ürünlerin son kullanıcılara daha etkili, tehdit sıralaması yapabilme ve alaka düzeyi belirleme konusunda yardımcı olabilecek analiz yeteneklerinin geliştirilmesine odaklanılması,
- Ürünler için esnek ve kullanılabilir güven modelleme işlevlerinin sağlanması,

- Çok sayıda tehdit bilgisine erişim sağlama, tehdit bilgisi paylaşılması, tehditlerin hızlı bir şekilde durdurulması için entegre çözüm sunulması, sonuçların düzenlenmesi ve açıklanması için kullanımı kolay arayüz imkanı, izleme listelerinin kullanılarak geçerli göstergelerin kontrol edilmesi konularında imkan sunulması,
- Etkili bir tehdit bilgisi çözümü ve birden fazla veri akışından faydalanması ve tam özellikli bir tehdit bilgisi çözümünün, verilerini kısıtlı bir kaynak kümesinden üretilmemesi,
- Sağlayıcının tüm bu verileri topladıktan sonra, işlem yapılabilir hale getirmek için gereken bağlamı sağlamak amacıyla bilgileri iyileştirmesi ve doğrulaması,
- Potansiyel tehdit bilgisinin birçok kaynağı karmaşık olduğundan, gelen tüm ham verilerin iletilmeden önce yeniden doğrulanmasına dikkat edilmesi gerekmektedir.

Siber Tehdit Bilgisinin paylaşımı için kullanılan platformlara;

- Malware Information Sharing Platform (MISP),
- IBM X-Force Exchange,
- AbuseHelper,
- Cyber Threat XChange (CTX),
- Open Threat Exchange (OTX) ve
- Collaborative Research into Threats (CRITs)

örnek gösterilmektedir. Bunlardan önemli olanları aşağıda kısaca tanıtılmıştır.

Malware Information Sharing Platform (MISP) [34]**;**

- Hedefli saldırıların, tehdit bilgisinin, finansal dolandırıcılık bilgilerinin ve güvenlik açığı bilgilerine ilişkin tehdit göstergelerinin paylaşılması, depolanması ve ilişkilendirmesi amacıyla kullanılan bir tehdit bilgisi platformu olarak tanımlanmaktadır.
- Siber güvenlik göstergelerinin depolanması, paylaşılması, işbirliği yapılması, kötü amaçlı yazılım analizi işlemleri ile birlikte aynı zamanda kritik altyapılara, kuruluşlarına veya insanlara yönelik saldırıların, dolandırıcılık faaliyetlerinin veya tehditlerin tespit edilmesi ve önlenmesi amacıyla tehdit bilgileri kullanılmaktadır.

- Farklı tiplere sahip olup aralarında olayları otomatik olarak senkronize edilebilmekte, her kuruluş paylaşım politikasını karşılamak amacıyla gelişmiş filtreleme işlevlerini kullanabilmektedir.
- Olaylar ve olayların korelasyonları arasında inceleme yapılması amacıyla grafiksel bir arayüz imkânı sunulmakta, analistlerin olaylara katkıda bulunmalarına yardımcı olmak amacıyla gelişmiş filtreleme işlevleri ve uyarı listesi sunulmaktadır.

IBM X-Force Research platformu [34]**;**

- Tehdit bilgisi içeriği sağlanarak çeşitli kaynaklardan gelen güvenlik sorunları izlenmekte ve analiz edilmektedir.
- Güvenlik ekiplerine ve araştırmacılara en son güvenlik risklerini daha iyi anlamalarına ve ortaya çıkan tehditlerden daha önde olmalarına yardımcı olmaktadır.
- Tehdit bilgisi kullanılması, paylaşılması ve bunlara yanıt verilmesi amacıyla kullanılmakta olup, en son küresel güvenlik tehditlerinin hızlı bir şekilde belirlenmesi, işlem yapılabilir zekânın bir araya getirilmesi ve sektördeki paydaşlarla işbirliği yapılmasına olanak tanımaktadır.

AbuseHelper;

- Olay bildirimlerini otomatik olarak işlemek amacıyla CERT.FI ve CERT.EE tarafından ClarifiedNetworks ile başlatılan açık kaynaklı bir proje olarak tanımlanmaktadır. Söz konusu araç, CERT'ler için çok çeşitli yüksek hacimli bilgi kaynaklarını takip etme ve iyileştirme konusunda günlük işlerine yardımcı olmak için geliştirilmektedir.

Open Threat Exchange platformu;

- 2012 yılında kurulan, siber saldırıları yönetmek için ticari ve açık kaynak çözümleri geliştiricisi olan AlienVault tarafından oluşturulmuş ve yürütülmektedir. İşbirliğine dayalı tehdit paylaşımı, virüsler, kötü amaçlı yazılımlar ve diğer siber saldırılar hakkında bilgi paylaşan bilgisayar korsanlarına karşı mücadele edilebilmesi amacıyla oluşturulmuştur. 140 ülkede günde 19 milyondan fazla potansiyel tehdidi paylaşan 80.000'den fazla katılımcısı bulunmaktadır.

Open Threat Exchange (OTX) platformu;

- Bulut tabanlı bir platform olup, bilgi paylaşımı, virüsler, kötü amaçlı yazılımlar, izinsiz giriş tespiti ve güvenlik duvarları gibi güvenlikle ilgili çok çeşitli sorunları kapsamaktadır.
- Otomatik araçlar sayesinde, katılımcılar tarafından paylaşılan veriler toplanmakta, doğrulanmakta ve yayınlanmaktadır.

Collaborative Research Into Threats (CRITs);

- Tehdit savunması yapan analistler ve güvenlik uzmanları için birleşik bir araç oluşturmak üzere diğer açık kaynaklı yazılımlardan yararlanan açık kaynaklı bir kötü amaçlı yazılım ve tehdit deposu olarak tanımlanmaktadır.
- 2010 yılından bu yana geliştirilmekte olup, güvenlik topluluğuna tehdit verilerini analiz etmek ve üzerinde çalışmak için esnek ve açık bir platform sunmayı hedeflemektedir.

MITRE;

- Siber tehdit bilgisi yönetim sisteminde farklı ihtiyaçlar için birlikte çalışmak üzere tasarlanmış bir paket olarak üç standart (CybOX, STIX, TAXII) geliştirmiştir. CybOX, kronolojiyi ve olaylar arasındaki zaman aralığını karakterize etmektedir. STIX, siber tehdit bilgilerini açıklamak için CybOX sözlüğünden yararlanan Yapılandırılmış Tehdit Bilgisi İfadesidir ve böylece veriler tutarlı bir şekilde paylaşılabilmekte, depolanabilmekte ve analiz edilebilmektedir. STIX'i temsil eden mimari, gözlemlenebilirler, göstergeler, olaylar, taktikler, teknik ve prosedür, istismar hedefi, eylem planları, kampanyalar, tehdit aktörleri ve raporlar gibi yapılardan oluşmaktadır.

3.7. SİBER TEHDİT BİLGİ PAYLAŞIMINA DUYULAN İHTİYAÇ VE ELDE EDİLEN FAYDALAR

Yeni siber saldırı modellerinin belirlenebilmesi ve gelişmiş siber saldırganların hızına ayak uydurabilmek için yeni savunma yaklaşımlarının geliştirilmesine ihtiyaç duyulmaktadır. Siber tehditlerle etkili bir şekilde müdahale edebilmek amacıyla siber ortamdaki tehditlere ilişkin gerekli bilgilerin zama-

nında elde edilmesi ve işlenmesi gerekmektedir. Ancak organizasyonlar sahip oldukları siber tehdit bilgisi ile belirli nicelik ve nitelikteki tehditleri tespit edebilmektedir. Organizasyonlar siber ortamda diğer paydaşların bilgi birikimine, deneyimlerine ihtiyaç duymakta, işbirliği çabalarını genişletmektedir. Zira siber tehdit bilgisinin işlevselliği, tehdit bilgilerinin paydaşlar arasında paylaşılması ile maksimize edilebilmektedir [12].

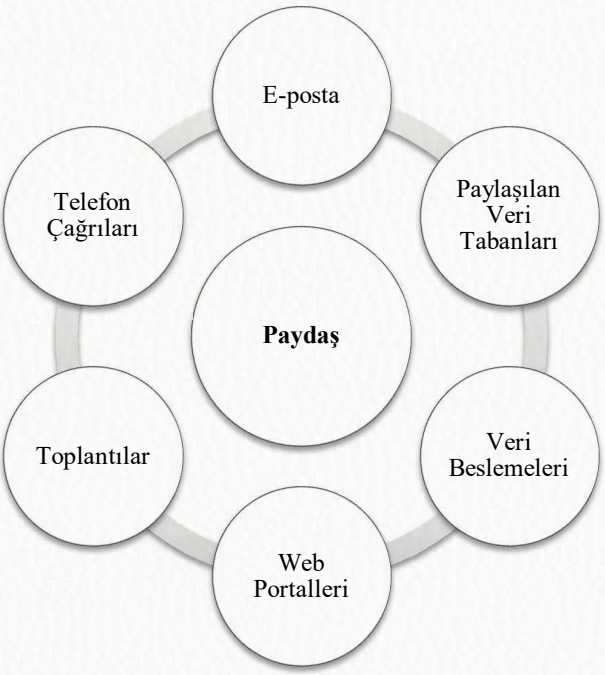
Siber tehdit bilgisi paylaşımında, yeni tehditler ve zafiyetlere yönelik paydaşlar arasında durumsal farkındalığın oluşturulması, artırılması ve hızlı bir şekilde yeni tedbirlerin alınmasının sağlanması amaçlanmaktadır [13].

Tablo 3.2. STB paylaşımına duyulan ihtiyaçlar ve faydalar

STB Paylaşımının Faydaları	STB Paylaşımına Duyulan İhtiyaç
1. Bilgi, deneyim ve tecrübe paylaşımı sağlanabilmekte 2. Siber tehditlere karşı topyekûn mücadele edilebilmekte 3. Siber tehditler hakkında en güncel bilgiye sahip olunabilmekte 4. Tehditleri algılama, öngörme ve saldırılarla birlikte mücadele etme yetenekleri geliştirilebilmekte 5. Gerçek zamanlı önlemler alınabilmekte 6. Tehditlere karşı hız ve zaman kazanılabilmekte 7. Kaynaklar zenginleştirilebilmekte 8. Durumsal farkındalık artırılabilmekte 9. Etkileşim ve fikir paylaşımı sağlanabilmekte 10. Erken uyarı ve müdahale yeteneği kazanılabilmekte 11. Dijital ekosistemin direnci artırılabilmekte 12. Paydaşlarla güvenilir bağlantılar kurulabilmekte 13. Paydaşlar arasında güven duygusu artırılabilmekte 14. İtibar kayıpları ve marka hasarları engellenebilmekte	1. Siber tehdit bilgilerinin elde edilmesinin zor olması, uzman bilgisine ihtiyaç duyulması, uzun ve zahmetli çalışma sürecine ihtiyaç duyulması 2. Tehditler hakkında yeterli bilgiye sahip olunamaması 3. Tehditler hakkında en güncel bilgilerin elde edilememesi 4. Siber tehdit bilgilerinin çok hacimli ve/veya karmaşık olması 5. Fazla iş yükü gerektirdiğinden zaman ayrılamaması 6. Farklı raporlar üzerinden siber tehdit bilgisi oluşturmanın güç olması 7. Yamaları önceliklendirmenin zor olması 8. İncelenmesi gereken çok fazla uyarının bulunması 9. Zararın ve ek ihlallerin tespit edilmesinin zor olması 10. Yanlış değerlendirilmiş bilgiler elde edilebilmesi 11. Doğrulanmamış bulguların hatalı alarmlara neden olması 12. Elde edilen bilgilerin güvenilir olduğundan emin olunamaması

Tablo 3.2'de organizasyonlarda kurumsal siber güvenliğin sağlanması için siber tehdit bilgi paylaşımına duyulan ihtiyaçlar ve siber tehdit bilgi paylaşımının organizasyonların kurumsal siber güvenliğine sağlayacağı üstünlükler aşağıda listelenmiştir.

- Organizasyonlar sahip oldukları siber tehdit bilgilerini paylaştıkça siber tehditler hakkında en güncel bilgiye sahip olunabilecek ve siber tehditlere yönelik gerçek zamanlı önlemler alınabilecektir.
- Kapsamlı ve standartlaştırılmış bilgi paylaşımı, organizasyonlara siber tehditlerle daha etkin mücadele edilmesine olanak sağlamakta ve siber saldırılar henüz gerçekleşmeden engellenebilmektedir.
- Siber tehdit bilgisi, gelişen tehdit örüntülerinin belirlenmesi ve saldırıların önlenebilmesi bakımından önemli bir araç olarak ortaya çıkmaktadır. Bu sayede organizasyonlar elde edecekleri siber tehdit bilgisi ile siber tehditlere yönelik gerekli önlemleri alabilecektir.



Şekil 3.2. Otomatize olmayan STB paylaşımı [13]

- Doğrulanmamış bulgulardan oluşan çok sayıda alarmın olması, incelenmesi gereken çok fazla alarmın oluşması organizasyonların çok fazla emek ve zaman harcamasına neden olabilmektedir. Siber tehdit bilgisinin paylaşımı ile organizasyonlar daha az zaman ve emek harcayarak gerekli tedbirleri alabilecektir.
- Otomatikleştirilmemiş paylaşım yöntemleri, güvenlik açıkları hakkında bilgi alışverişinde yaygın olarak kullanılan yaklaşımlardır. Mevcut siber tehdit bilgisi paylaşım metotları genellikle otomatize olmayan besleme temelli olup, yoğun emek gerektirmektedir. Şekil 3.2'de görüldüğü gibi siber tehdit bilgisi paylaşımı e-postalar, telefon çağrıları, web portalleri, paylaşılan veritabanları ve veri beslemeleri üzerinden gerçekleştirilmektedir.

Ayrıca yeni tehditlerin işlenmesi esnasında hata oranın artması veya ilgi düzeyine göre filtreleme yapılabilmesi nedenleriyle otomatize olmayan sistemler siber tehdit bilgisi paylaşımının etkinliğini azaltabilmektedir. Bunlar aşağıda kısaca özetlenmiştir.

- Siber tehdit bilgisi ilgili ve eyleme geçirilebilir olmalı, tehdit paylaşım modeli ise hızlı, ölçeklenebilir ve otomatize olmalıdır [35].
- Siber tehdit bilgisi verilerinin otomatize bir şekilde değerlendirilmesi, organizasyon içinde üretilen alarmlarla ve organizasyon dışından temin edilen bilgilerin etkin bir şekilde kullanılabilmesi amacıyla önem teşkil etmektedir. Otomasyon, siber tehdit bilgisi paylaşımında kilit rol oynamaktadır [36].
- Otomatik olmayan veri işleme süreçleri yoğun emek ve zaman kaybına neden olmakta ve bilgilerin önemini yitirmesine sebep olmaktadır. Otomatize veri analizi, işbirliği ve siber tehdit bilgisi paylaşımı, siber saldırılarla mücadele edebilmek için zorunludur. Ponemon Enstitüsü tarafından yapılan araştırmada; katılımcıların %39'u otomatize ve hızlı olmayan paylaşım işlemlerinin katılımcıların tam paylaşımını engellediğini, %24'ü ise hızlı olmayan ve otomatize olmayan paylaşım işlemlerinin tümüyle paylaşımı engellediğini belirtmiştir [37].
- Otomatize siber tehdit bilgisi paylaşımının amacı, paylaşımı sürecini basitleştirmek ve hızlandırmak, dokümante etmek, değerlendirmek ve güvenlik bilgilerinin düzeltilmesini sağlamaktır [13].

Sonuç olarak;

- Siber tehdit bilgisi paylaşımının temel bileşenleri; güvenli olması, sürdürülebilir olması ve hızlı bir şekilde özelleştirilebilir olması şeklinde sıralanmış olup efektif bir siber tehdit bilgisi paylaşımı güvenilir olmalı, sürdürülebilir olmalı ve hızlı bir şekilde özelleştirilebilmeli, doğru etiketleme yapılmalı, anonim olmalı, güven sağlamalı ve gizli olmalıdır [13].
- Siber tehdit bilgisi çoğunlukla ulusal düzeyde paylaşılmakta, ancak uluslararası bilgi alışverişleri özellikle dünya çapında faaliyet gösteren daha büyük kuruluşlar arasında ivme kazanmaktadır. Nitekim aralarında ABD, AB, Japonya ve Güney Kore'nin de bulunduğu bazı hükümetler bilgi paylaşımını artırmak ve genişletmek amacıyla çeşitli çalışmalar gerçekleştirmektedir [38].
- Özellikle devlet destekli siber saldırganlar tarafından hedef alınan organizasyonlar kamuyla yakın bir işbirliği ve paylaşıma ihtiyaç duymaktadır [39].
- ENISA'ya göre AB'deki 80 kuruluş ve organizasyon ve 50'den fazla ulusal ve kamu CSIRT (Computer Security Incident Response Teams) siber tehdit bilgisi paylaşımına dâhil olmaktadır [13].
- İngiltere'deki CISP girişimi ise güvenlik olayları hakkında bilgi paylaşımı sağlamak amacıyla [22], siber tehditlere yönelik organizasyonlar arası bilgi paylaşımı, sayısı günden güne artan ve sürekli kendini yenileyen siber tehditlerle mücadele çalışmalarına katkı sağlayacağı değerlendirilmektedir.
- Bauer ve Eeten'e göre bir organizasyon bir siber saldırının kurbanı olduğunda, itibar kaybı ve bunun sonucunda ortaya çıkan marka hasarı nedeniyle, paydaşları siber güvenliğe ve siber tehdit bilgisi paylaşmaya daha fazla yatırım yapmaya teşvik edebilmektedir [40]. Başarıyla savunulan bir ağ, hizmetin çalışma süresine ve sürekliliğine katkıda bulunabilmektedir.
- Murdoch ve Leaver'a göre paylaşıma katılma, paydaş itibarı ve ortak amaç olmak üzere siber güvenlik ekiplerini siber güvenlik bilgilerini paylaşmaya motive eden üç ana faktör bulunmaktadır. Ayrıca paydaşların gelecekteki bir siber tehdidi önlemeye yardımcı olması amacıyla

paydaşlarla ilgili bilgileri paylaşmak isteyebileceği, sektörde diğer paydaşlar tarafından saygınlığı kabul edilen bir paydaş olmak isteyebileceği ve aynı sektörde çalışan paydaşların kendilerini ortak bir tehdide karşı savunmalarına yardımcı olmak için bilgi paylaşabileceği belirtilmektedir [22].

- Paydaşlar arasında saygınlığın artması paydaşları daha fazla katkıda bulunmaya ve itibarlarını inşa etmeye teşvik etmektedir. Ancak bir paydaşın saygınlığın artması ile birlikte anonim kalması da olanaksız hale gelmektedir.
- Anonim paylaşımlar, paydaşlarla ilişkilendirilememesi sebebiyle itibara katkıda bulunamamakta ve paylaşılan bilgi kaynağının saygın olup olmadığına dair karar vermeyi zorlaştırmaktadır. Bu nedenle, bu sorunun üstesinden paylaşılan bilginin değer ve diğer alıcı paydaşlar tarafından puanlanması ile gelinebilmektedir. Bu kapsamda, bilgi paylaşımına açık, güvenli ve standartlara dayalı bir yaklaşım sağlanması, organizasyonların paylaşım modellerine katılım sağlamasına ve kritik ağların güvenliğinin siber tehditlere yönelik korunmasına imkân tanımaktadır [22].
- Organizasyonlar, işletmeler ve uzmanlar arasında etkin bilgi paylaşımının olması gerektiği kadar verimli olmadığı vurgulanmakta, kamu kurumları, özel işletmeler ve hatta endüstri uzmanları tarafından yönetilen çok iyi girişimlerin olduğu doğru olsa da, ortak bir bilgi paylaşım standardı olmadığından bu bilgileri paylaşmak çok zor olabildiği vurgulanmaktadır [41]. Ayrıca özel sektör kuruluşları rekabet, sorumluluk ve yatırım getirisi gibi çeşitli nedenlerden dolayı işbirliği çalışmalarına katılım sağlama konusunda bazen ihtiyatlı davranmakta veya bilgi paylaşım çabalarına katılmaya isteksiz olmaktadır. Bu sebeple siber güvenlik bilgi paylaşımına katılımı teşvik etmek zor olabilmektedir.
- Siber tehdit paylaşımı konusunda çeşitli zorluklar bulunmaktadır. İhtiyaç duyulan siber tehdit bilgisinin elde edilmesinin zor olması, yanlış değerlendirilmiş bilgiler elde edilebilmesi, uzman bilgisine ihtiyaç duyulması, uzun ve zahmetli çalışma sürecine ihtiyaç duyulması, fazla iş yükü gerektirdiğinden şirketlerin ve/veya kurumların siber tehdit

bilgisini üretmek için zaman ayırmaması veya ayıramaması, saldırı tespit sistemleri tarafından üretilen raporlar arasında genel bir benzerlik olmayışı ve her bir saldırı tespit sisteminin çıktısının farklı veri modeli barındırması, farklı raporlar üzerinden siber tehdit bilgisi oluşturmanın güçlüğü, doğrulanmamış bulguların hatalı alarmlara neden olması, yamaları önceliklendirmenin zor olması, incelenmesi gereken çok fazla uyarının bulunması, zararı ve ek ihlalleri tespit etmenin zor olması ve yöneticilerin teknik problemler hakkında bilgisinin bulunmaması belirlenen zorluklar arasında yer almaktadır.

- Ayrıca paydaşlar arasında dilsel ve kültürel farklılıklar bulunabilmektedir. Siber tehdit bilgisi paylaşımı küresel olarak gerçekleştirilmekte ve kültürel ve paydaşlar arasında kültürel ve dilsel engellere sebep olabilmektedir. Paydaşlar farklı çalışma alanlarında faaliyet gösterebilmekte ve farklı dilleri konuşabilmektedir. Bu da bilginin kalitesi üzerinde olumsuz etki oluşturmaktadır [42].
- Paylaşım modellerinde ortak bir paylaşım dili tanımlanmalı ve kültürel yönleri anlaşılmalıdır. Ayrıca aynı dilin konuşulması, paydaşları bilgi paylaşımına teşvik edebilmekte ve bilgi paylaşım sürecini hızlandırabilmektedir [43].
- Bu çerçevede, siber tehdit bilgisi oluşturmada kullanılan manuel adımların otomatize edilmesi ve standartlaştırılması, ayrıca uzman bilgisine gereksinim duyulmaksızın kolaylıkla siber tehdit bilgisi üretebilme yeteneğinin kullanıcılara kazandırılmasına yönelik mekanizmanın oluşturulmasına ihtiyaç duyulmaktadır.
- Ayrıca siber tehdit bilgisi işbirliği bazı güvenlik risklerini barındırmaktadır. Haustein ve arkadaşları, bir olayla ilgili organizasyon içi bilgilerin ifşasının bir paydaşın itibarına zarar verebileceği endişelerini dile getirmektedir [44].
- Pek çok organizasyon, itibarlarını olumsuz etkileyebilecek bilgileri paylaşmaktan kaçınmakta, bazı şirketler ise saldırı bilgilerinin ifşa edilmesinden kaynaklanabilecek itibar zedelenmesi korkusu nedeniyle bilgi paylaşmakta tereddüt edebilmektedir. Bunun yanı sıra, bir rakip tarafından elde edilen siber tehdit bilgisinin sistemlerine henüz yama uygulamamış paydaşlara saldırmak için kullanılabileceği vurgulanmaktadır [45].

- Siber tehdit bilgisinin rakiplerle paylaşılması, ücretsiz bilgi edinmeyi teşvik edebilmekte ve paydaşlarla veya topluluklarla bilgi paylaşılmamasına yol açabilmekte, güven ihlal edilebilmekte ve olumsuz tanıtım marka itibarını etkileyebilmektedir [44].
- Çok sayıda siber tehdit bilgisi kaynağının olması sebebiyle çok sayıda veri akışı olabilmekte, siber saldırıya karşı savunma yapılabilmesi amacıyla paydaşların ilgili, eyleme geçirilebilir tehdit bilgisine zamanında erişmesi ve bu doğrultuda hareket etmesi önem teşkil etmektedir. Ponemon Enstitüsü tarafından 2016 yılında yapılan ve 1000 katılımcının katılım sağladığı bir ankete göre, katılımcıların %70'i tehdit bilgisinin eyleme geçirilebilir bilgi sağlamak için çok hacimli veya karmaşık olduğunu belirtmiştir. Katılımcıların %80'inin tehdit bilgisi platformunun kurulmasının organizasyonun tehdit bilgisini otomatikleştirmesine yardımcı olabileceğini düşündüğü, %54'ünün ise tehdit bilgisi potansiyelini tam olarak kullanmak için nitelikli bir tehdit analisti kadrosuna sahip olmasının gerektiğini ifade etmiştir [21].
- Siber tehdit bilgisi paylaşımında karşılaşılan diğer bir sorun ise tehdit verisinin kalitesidir. Ponemon Enstitüsü tarafından yapılan çalışmada, katılımcılar tarafından tehdit bilgisi beslemelerinin %70'inin işlenmemiş olduğu ve kalite açısından güvenilir olmadığını belirtilmiştir. Siber tehdit bilgisi sağlayıcısının, tehdit bilgisinin değerinin artırmasına ve eyleme geçirilebilir hale getirilmesine yardımcı olmak amacıyla verileri zenginleştirmesi gerekmektedir.

3.8. ÜLKEMİZDE SİBER TEHDİT BİLGİ PAYLAŞIMINA GENEL BAKIŞ

Ülkemizde siber güvenlik çalışmaları Ulaştırma ve Altyapı Bakanlığı koordinasyonunda yürütülmektedir. Ulaştırma ve Altyapı Bakanlığınca Ulusal Siber Güvenlik Stratejisi ve Eylem Planları hazırlanmakta, çalışmalar yürütülmekte ve takip edilmekte, ve koordine edilmektedir. Bu eylem maddelerinde, siber güvenlik ekosisteminin geliştirilmesine yönelik kamu-özel sektör-akademi arasında işbirliğinin artırılmasına yönelik eylem maddeleri bulunmaktadır.

BTK bünyesindeki USOM aracılığıyla siber tehditlere ilişkin bilgi paylaşımı bu merkez bünyesinde belirli bir sistematik ile yapılmakta ve siber tehdit bilgilerinin paylaşımına yönelik USOM aracılığıyla bilgi paylaşım faaliyetleri gerçekleştirilmektedir. Siber tehdit bilgilerinin paylaşımı konusunda sektör, kamu veya enstitülerin net bir yöntemi bulunmamakta, özellikle siber güvenlik firmaları arasında siber tehdit bilgilerinin paylaşıldığı bir işbirliği mekanizması bulunmamaktadır. Ulusal Eylem Planları kapsamında; siber güvenlik ekosisteminin geliştirilmesi amacıyla 2017 yılında Savunma Sanayii Başkanlığı koordinatörlüğünde Siber Güvenlik Kümelenmesi oluşturulmuş olsa da bu tür bilgilerin paylaşıldığına dair herhangi bir bilgi bulunmamaktadır. Ülkemizde siber tehdit bilgisi paylaşımı konusu, ulusal stratejiler ve gerçekleştirilen diğer çalışmalar gözden geçirilerek incelenmiş ve bu konudaki değerlendirmeler Tablo 3.3'te listelenmiştir.

Tablo 3.3. Ulusal stratejilerde STB paylaşım çalışmaları incelemesi

Siber Güvenlik Çalışmaları	STB Paylaşımına Yakın veya Yönelik Eylemler
1. 2013-2014, 2016-2019 ve 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planları 2. USOM ve SOME'lerin kurulması 3. USOM'un siber tehditlere ilişkin bildirim, duyuru ve ikaz faaliyetleri **4.** Siber Güvenlik Kümelenmesinin oluşturulması 5. Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberinin yayımlanması	1. Siber güvenlik ekosisteminin geliştirilmesi 2. Siber tehdit bilgilerinin paylaşıldığı işbirliği mekanizmalarının oluşturulması 3. İşbirliğine yönelik farkındalığın artırılması ve işbirliği kültürünün geliştirilmesi 4. Paydaşların işbirliğine teşvik edilmesi ve desteklenmesi

Sonuç olarak; ülke stratejilerinde ve çalışmalarında bu konu doğrudan ele alınmamış olsa da genel olarak değerlendirildiğinde;

- USOM'un ülkemizde siber tehdit bilgisi paylaşımı konusundaki eksikliği gidermeye yönelik çalışmalar gerçekleştirdiği,
- Sektörel SOME'lerin kendi aralarında bir bilgi paylaşımının olmadığı, bununla ilgili olarak birimler arasında tehdit bilgisi paylaşımı yapılması konusunda bir düzenleme yapılmasının faydalı olabileceği,

- Ağların, verilerin ve uygulamaların, kurumsal ve ulusal bilgi varlıklarının artık tek başına korunamayacağının yeteri kadar anlaşılamadığı,
- Kuruluşların birlikte çalışabilirlik kültürünün henüz beklenilen düzeyde olmadığı,
- Kuruluşların siber tehdit bilgisi paylaşımı konusunda ihtiyatlı davranabildikleri

görülmektedir.

Zaman içerisinde iyi örneklerin sayıları artıkça, gelişen aktörlere karşı etkili bir şekilde mücadele etmenin etkili yollarından birisinin de işbirliği yapılması ve deneyimlerin ve tehdit bilgilerinin paydaşlarla paylaşımdan geçtiği anlaşıldıkça ve en önemlisi de bunun kuralları da net olarak belirlenirse sadece tehdit bilgisi değil pek çok konunun daha hızlı çözüleceği, sistemlerin ve verilerin daha yüksek seviyede korunulacağı aşikardır.

3.9. SİBER UZAY, SİBER VATAN VE TEHDİT BİLGİSİ PAYLAŞIMI

Vatanları korumada kara ve deniz savaşları önemli iken, 20. yüzyılın başından itibaren hava, ortasından itibaren ise uzay yeni alanlar olarak ortaya çıkmıştır. Teknolojinin gelişmesi ve kara, deniz, hava ve uzayda bilişim sistemlerinin kullanımının artması ile birlikte siber uzayın önemi daha da artmış, siber uzay, kara, hava, deniz ve uzaydan sonra savaşın beşinci boyutu olmuştur.

3.9.1. Siber Uzay ve Siber Vatan

Siber uzay; internet, haberleşme ve bilgisayar ağları, bilgisayar sistemleri ve gömülü işlemciler ile denetleyicileri içeren ve birbirine bağlı iletişim ve ağ sistemlerinden oluşan, küresel alan olarak tanımlanmaktadır [46]. Siber uzay günümüzde, dijital çağda harbin ayrılmaz bir parçası haline gelmiştir. Artık, geleneksel harbin yerini siber savaşlar almaya başlamıştır. Değişen tehdit ortamı, ulusal ve uluslararası güvenlik organizasyonlarının da gündemine girmiş, bu savaşları kazanma yönünde stratejiler geliştirilmeye başlanılmıştır. Bunlardan önemlileri aşağıda özetlenmiştir.

- Siber güvenlik NATO'nun da güvenlik stratejileri kapsamına alınmış, 2016 Varşova Zirvesinde siber uzay; kara, deniz, hava ve uzay gibi bir

harekât alanı olarak tanımlamıştır [47]. Siber güvenlik konusu yeni güvenlik konseptinde mücadele edilmesi gereken öncelikli alanlar içerisinde yer almakta olup, ayrıca "siber güvenlik alanında üye ülkelerin daha fazla işbirliği içerisinde olması gerektiğine ve diğer uluslararası kuruluşlar ve ortak ülkelerle olduğu kadar endüstri ve akademi ile işbirliğinin geliştirileceğine" vurgu yapılmıştır [48].

- Siber uzay internet ve internete bağlı bilgi sistemlerini kapsamakta olup, son dönemde ortaya çıkan Nesnelerin İnterneti (IoT) gibi teknolojiler ile birlikte siber uzayın sınırları bilgisayarlarla sınırlı kalmayarak daha da genişlemiştir [49].
- Siber ortam bilişim sistemlerinin kullanımı arttıkça büyümekte ve büyük bir dijital dönüşüm yaşanmaktadır. Mevcut teknolojilerin yanı sıra yapay zekâ, IoT, blokzincir ve 5G teknolojilerin hayatımıza girmesi ile dijital dönüşüm sürecinde büyük ilerlemeler kaydedilmiştir. Pek çok ülke ve organizasyon, bu dönüşüme cevap vermeye, gelişen yeni yetenekleri etkinleştirmeye, bu yeteneklerle organizasyonların ihtiyaçlarını desteklemeye ve gelişmelerin gerisinde kalmamaya, teknolojinin imkânlarından en üst düzeyde yararlanmaya gayret göstermektedir.
- Büyüdükçe tehdit ve tehlikeler de artmaktadır. Dijitalleşmenin ve siber alanın boyutlarının genişlemesi ile birlikte günümüzde egemenliklerin dijital dünyada siber saldırılara maruz kaldığı görülmektedir. Güvenlik kavramı geleneksel yapısından farklı olarak sanal dünyada etkisini göstermeye başlamış, siber uzayda kullanılan siber silahlar da konvansiyonel silahlar gibi yeni bir unsur olarak kullanılmaya başlanmıştır.
- Siber uzayda bilişim sistemlerindeki verilere erişim sağlanması, kişisel veya kurumsal bilgilerin çalınması, yayılması veya bilgi sistemlerinin çalışamaz hale gelmesi ile neticelenebilecek saldırılara maruz kalınmaktadır. Ayrıca kritik altyapı sektörlerinin hedef alındığı saldırılar ile elektrik şebekelerinin, su dağıtım/arıtma tesislerinin, elektronik haberleşme ve finans altyapısının çalışamaz hale gelmesine neden olabilecek ve toplumuzun tüm kesimlerini etkileyebilecek sonuçlar ile karşılaşabilmektedir. Bu sebeple, kritik altyapı sektörleri başta olmak üzere siber alandaki varlıklarının korunması, önemli bir güvenlik unsuru haline gelmiştir.

– Siber uzay, diğer unsurlar gibi savunulması gereken önemli bir vatan parçasıdır. Bunu korumaya yönelik pek çok çaba gösterilmekte, bu çabalar ortaya konulan stratejiler, politikalar ve doktrinler ile desteklenmekte, ayrıca öne sürülen yeni kavramlar ile siber uzayın önemi vurgulanmaktadır.

Bunun yanı sıra, son zamanlarda ortaya çıkan "**Siber Vatan**" kavramı ise siber tehditlerden korunması açısından büyük önem teşkil etmektedir. "Vatan" veya "Yurt" kelimesi sözlükte "bir halkın üzerinde yaşadığı, kültürünü oluşturduğu toprak parçası" şeklinde ifade edilmektedir. Vatan kelimesi ayrıca "yerleşmek, bir yeri yurt edinmek, kendini bir şeye alıştırmak" anlamındaki "vatn" kökünden türemekte, aynı zamanda "kişinin doğduğu, yerleştiği, barındığı ve yaşadığı yer" anlamına gelmektedir. Bununla birlikte, literatürde "Siber Vatan" kavramına ilişkin yapılmış henüz bir tanım bulunmamaktadır. Siber alanda yaşanan gelişmeler ve gelişen siber tehdit ortamı göz önüne alındığında "Siber Vatan" kavramının doğru yapılması, doğru anlaşılması ve kapsamının veya boyutunun doğru bir şekilde belirlenmesi, içinin doldurulması ve iyi tanımlanması ve sonuçta da herkesin bundan aynı şeyi anlaması gereken bir tanımlama yapılması gereklidir.

Cumhurbaşkanımız Sn. Recep Tayyip Erdoğan'ın telaffuz etmesiyle gündeme gelen bir kavram olan siber vatan, "vatan savunmamızı, denizde mavi vatanı olduğu gibi, dijital dünyada siber vatanı da içine alacak şekilde genişletme" şeklinde tanımlanmıştır.

Siber dünya ortamı ve bileşenlerine bakıldığında, "siber vatan" kavramını anlamak veya algılamak zordur. Tabii ki bunun haklı sebepleri bulunmakta olup, bu hususlar aşağıda maddeler halinde verilmiştir [50].

– Sanal dünyanın sınırlarını veya sınırsızlığını bilmek ve buna göre dijital sınırları belirlemek gereklidir.
– Sanal ortamlardaki vatana ve vatandaşlara ait kişisel, kurumsal veya ulusal bilgi varlıklarımızı, yerlerini ve değerlerini bilmek, değişimleri anlık takip etmek ve korumak şarttır.
– Sanal ortam boyutunun kara-hava-deniz-uzay-siber ilişkisini iyi anlamalıdır.
– Sanal dünya ilkelerimizi, politikalarımızı, hedeflerimizi, zenginliklerimizi öne çıkarmak ve ulusal çıkarlarımızı bilmek, savunmak ve korumak gereklidir.

- Sanal dünyanın değişen ve gelişen tehdit vektörünü, risklerini ve büyüklüklerini bilmek, korumak ve korunmak için yetenek ve kapasiteye sahip olmak ve siber saldırılara karşı her zaman hazır olmak gereklidir.
- Sanal dünya risklerini ve tehditlerini yakın olarak takip etmek ve korunmak için; ileri düzey altyapılara, araçlara, gereçlere, uygulamalara ve nitelikli uzmanlara gerek vardır.

Siber vatan algımızın gelişmesi ve gerçek manada siber vatana sahip çıkmak ve kısaca da bu kavramın içini de doldurmak için aşağıdaki hususlara dikkat edilmesinde fayda vardır [50]:

- Siber vatanın ana vatan kavramında olduğu gibi algılanması,
- Sınır komşularımızın tüm sanal dünya olduğunun farkında olunması,
- Siber tehditlere karşı koyma konusunda her kullanıcının sorumlu olduğunun bilinmesi ve buna göre hareket edilmesi,
- Siber ortamların yani siber vatanın, ana vatanın bir parçası olduğu bilinciyle hareket edilmesi,
- Verilerimizin siber vatanın toprakları olduğunun, dijital verilerin büyüklüğünün vatan topraklarının büyüklüğünü gösterdiğinin ve sınırların sahip olunan verilerin barındırıldığı yerlere kadar uzandığının iyi anlaşılması,
- Yüzeysel, derin ve karanlık web ortamlarını, bu ortamlardaki tehdit ve tehlikelerin boyutunu anlamadan, tehditlerin arkasında gelişmiş ülkelerin olduğunun farkında olmadan, bu ortamlardaki tehdit ve tehlikeleri ortadan kaldırmak için kapsamlı tedbirler alınmadan gereken başarı sağlanamayacağının iyi bilinmesi,
- Gerçek ar-ge çalışmalarına önem vermeden, odak alanlar ve ortak hedefler belirleyip çalışmalar yapmadan, üniversite-sanayi-kurum işbirliklerini tam anlamıyla gerçekleştirmeden, makale ve bildiri üretmeye verdiğimiz önemi patent ve faydalı model üretmeye ve bunları teknolojiye dönüştürmeden istenilen yetenek seviyesine erişilemeyeceğinin iyi bilinmesi ve gereğinin yapılması,
- Ülke gelişmesinin bilim ve bilimsel çalışma ve çıktılar üretmekten geçtiğini iyi anlamadan, verilerinden değer elde etmenin yolunun

bilimsel çalışmalardan geçtiğini kavramadan, açık bilim felsefesini yaygınlaştırmadan, teknoloji geliştirmeden, karşılaşılan problemlere veri temelli çözümler geliştirmeden siber vatanın korunamayacağının iyi bilinmesi,

- Ulusal çıkarlarını ön plana alıp, akıl ve bilim ışığında ortak çözüm geliştirilmesi, ortak bir noktada buluşma kültürünün yaygınlaştırılması, birlik ve beraberliğe her zamankinden daha fazla ihtiyaç olduğunun farkında olunması,
- Bu kitap bölümünde odaklanılan siber tehdit istihbarat/bilgisini siber vatan korumasında kullanmadan, verilerden değer elde etmeden, elde edilen değerleri teknolojiye, inovasyona, üretime ve faydaya dönüştürmeden "Siber Vatan" teriminin iyi anlaşılamayacağını değerlendiriyoruz. Siber vatan tanımlarımız ise aşağıda verilmiştir.

Siber Vatan;

- "Bir ülkeye ait bilgi, iletişim altyapısı ve sistemlerinin bulunduğu, kamu kurumlarına, şirketlerine ve vatandaşlarına ait verilerinin üretildiği, depolandığı, işlendiği veya iletildiği siber ortam",
- "Vatandaşlarının dijital verilerinin ve verilerin tutulduğu sistemlerin bulunduğu sanal dünyada her türlü ortam, yer ve lokasyon veya dijital ortam"

şeklinde bir tanım yapılabileceği değerlendirilmektedir.

3.9.2. Siber Vatan ve Siber Tehdit Bilgi Paylaşımı

Siber tehditlerin gelişmesi ve tüm dünyada çok hızlı bir şekilde yayılması, siber uzayda bilgi paylaşımını zorunlu kılmıştır. Zira benzer sektörleri hedef alan tehdit aktörleri genellikle benzer saldırı metotlarını kullanmakta, aynı sektörde faaliyet gösteren paydaşların kendilerini ortak bir tehdide karşı savunmaları, birden fazla kaynaktan gelen siber tehdit bilgisinin analiz edilerek mevcut bilginin artırılması ve tehditlerin yayılmasının önlenmesi amacıyla;

- Siber vatanımızda tehdit göstergeleri hakkında bilgi paylaşımının gerçekleştirilmesine ve bilgi paylaşım ağlarının genişletilmesine,
- Siber vatanda bilgi paylaşımını artıracak işbirliği mekanizmalarının ve siber güvenlik ekosisteminin oluşturulmasına,

- Siber vatan kapsamında olmazsa olmazlardan olan araç, yazılım, donanım, envanter vb. gibi temel gereksinimler karşılandıktan sonra güvenliğe odaklanılmasına, siber vatanımızdaki varlıkların ve sınırların belirlenmesine ve siber vatanın topyekun korunmasına,
- Bu kapsamda, politika ve stratejilerin geliştirilmesine, gerekli teknoloji ve altyapılara yatırım yapılmasına ve bu alanda insan kaynağının yetiştirilmesine,
- Siber vatanımızı korurken, siber güvenliğin en önemli unsurlarından biri olan işbirliği çalışmalarına odaklanılmasına, işbirliğini teşvik edecek siber güvenlik ekosisteminin oluşturulmasına ve kamu-özel-akademi arasında işbirliği çalışmalarının artırılmasına,
- Siber savunma sistemlerine, koruma kalkanlarına, siber güvenlik araçlarına ihtiyaç vardır.

Öte yandan, ülkemizin 2020-2023 döneminde başta kritik altyapılarımız olmak üzere siber uzaydaki varlıklarımızın siber tehditlerden korunmasına yönelik gerçekleştirilmesi hedeflenen çalışmalar, Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanan 2020–2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında belirlenmiştir. Ülkemizin 2020-2023 dönemi ulusal strateji ve eylem planı kapsamında [51];

- "Siber güvenliğin, ulusal güvenliğin ayrılmaz bir parçası olduğu ve siber güvenlik alanında belirlenen hedeflere ulaşılabilmesi gerektiği ve kritik altyapılar aracılığıyla verilen hizmetlerin kesintisiz ve etkin olarak sunulmasının esas olduğu" maddeleri temel alınarak belirlenmiş,
- "Kritik altyapıların siber güvenliğinin sağlanması, yerli ve milli teknolojik kabiliyetlerin geliştirilmesi, proaktif siber savunma anlayışının geliştirilmesi, yeni nesil teknolojilerin güvenliğinin sağlanması, toplumumuzun tüm kesimleri tarafından siber uzayın güvenle kullanılması, siber güvenlik farkındalığının artırılması, paydaşlarla bilgi paylaşımı ve işbirliğinin geliştirilmesi, siber suçların en aza indirgenmesi, internet ve sosyal medyada doğru ve güncel bilgi paylaşımının sağlanmasına yönelik mekanizmaların geliştirilmesi" kapsamında stratejiler oluşturulmuştur.

Ulusal stratejide siber tehdit paylaşımı konusunda USOM'un çalışmaları dışında bir husus veya eylem planı (kamuoyuna açılmadığı için olmadığı değerlendirilmiştir.) yer almamaktadır. Bunlara ilave olarak;

- Siber güvenliğin sağlanması için yapılması gereken önemli çalışmalardan biri olan işbirliği ve paydaşlarla bilgi paylaşımı konusuna net olarak dokümanda değinilmemiştir
- Siber tehditlerin dinamik yapısına uyum sağlayabilmek ve tehditlerin gerisinde kalmamak amacıyla yeni savunma yaklaşımlarının geliştirilmesi hususuna yer verilmemiştir.
- Siber güvenlik ekosistemi oluşturma konusunda özellikle 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında detaylı eylem maddeleri yer alsa da USOM ve Siber Kümelenme dışında aktif bir ekosistemin kurulduğuna dair bir bilgiye erişilememiştir.
- Tüm paydaşlar kendi siber güvenliğini sağlamak adına çeşitli çalışmalar gerçekleştirmekte, bünyelerinde SOME'ler kurmakta, USOM ile bilgi paylaşımı sağlasalar da sadece sahip oldukları bilgiler ile belirli kapasitedeki tehditlere yönelik önlem alabilmiştir.
- Her ne kadar tehdit bilgisi paylaşımı için pek çok gerekçe olsa da bu bilgilerin ulusal mahremiyeti olabileceği bilinmektedir. Bu hususların uluslararası paylaşımlarda dikkate alınması gerekmektedir.

Bu konu uluslararası açıdan değerlendirildiğinde ise;

- Siber uzayda gerçekleştirilen saldırılar ve sunulan istatistiklerden, yapılan saldırıların çok yaygın ölçekte yayılım gösterdiği, pek çok bilişim sistemini veya altyapılarını hedef aldığı ve bu tür saldırılara da karşı konulamadığı,
- Sınır kavramının bulunmadığı siber dünyada, herhangi bir iletişim ağına bağlanabilen bir cihaz ile küresel ölçekte iletişim kurulabildiğinden dolayı tehdidin boyutunun da küresel ölçeğe kayabildiği,
- Yaygın olarak kullanılan cihazlar, uygulamalar, sosyal medya platformlarında zaman zaman karşılaşılan açıklıklar, sosyal medya platformların heklenmesi, uygulama seviyesinde görülen zafiyetler, haberleşme protokollerinde kod seviyesinde açıklıklar, sadece ulusal değil tüm dünya vatandaşlarını ve ülkelerini de tehdit edebildiği,
- Siber uzaydaki paydaşlar arasında işbirliğinin ve koordinasyonun sadece ulusal değil uluslararası boyutlar dikkate alınarak da yapılması gerektiği, tehdit bilgisi paylaşımını uluslararası boyutta da zorunlu kıldığı,

- Uluslararası bilgi paylaşımının, siber aktörlere ve siber saldırılara ilişkin ihtiyaç duyulan tehdit bilgilerin elde edilmesi, bilişim varlıklarının korunmasına yönelik hızlı aksiyon alınması, tehdit örüntülerinin belirlenmesi, bilgi birikiminin ve deneyimlerin paylaşılmasıyla küresel boyutta çözüm geliştirilmesinin önünün açıldığı,
- Ülkeler arası işbirliklerini ve bilgi paylaşımını artırdığı da bilinmektedir.

Siber tehdit bilgisi paylaşımı, siber vatanın yüksek seviyede korunması bakımından büyük öneme sahiptir. Bu yaklaşımların kullanılması, politikaların belirlenmesi ve altyapıların oluşturulmasıyla;

- Gelişmiş tehditlere yönelik savunma mekanizmalarının geliştirilmesine,
- Siber tehditlerle daha etkin mücadele edilmesinin kolaylaşmasına,
- APT türü gelişmiş tehditlerin önlenmesine yönelik bilgi paylaşım mekanizmalarının geliştirilmesine,
- Olası veya kaçırılan siber tehditlerin hızlıca tespiti ve giderilmesine,
- Sonuçta topyekûn mücadele için işbirliği çalışmalarının genişletilmesine

katkı sağlayacaktır.

3.10. SONUÇ VE DEĞERLENDİRMELER

Siber ortamda kötü niyetli siber aktörlerin ve kötü amaçlı yazılımların yetenekleri sürekli olarak değişmekte ve siber suçlular, siber savunma çalışmalarına karşı koymak amacıyla kendilerini güncellemektedir. Böylesine gelişen aktörlere karşı etkili bir şekilde mücadele etmenin en etkili yolu ise işbirliği yapılması ve deneyimlerin paylaşılmasıdır. [52] nolu tezden yola çıkarak hazırlanan ve bu tezin bir bölümü olan bu bölümde, paydaşlar arasındaki işbirliği, siber tehditleri engellemenin en önemli kısmı olup, ağlarını, verilerini ve uygulamalarını kendi başına koruyabileceğine inanan herhangi bir organizasyon ise yanılmaktadır. Siber tehditlerle kapsamlı bir şekilde ve tam anlamıyla mücadele edebilmek amacıyla tehdit aktörleri tarafından kullanılan taktiklerin/araçların belirlenmesi ve bunlara yönelik aksiyon alınması gerek-

mektedir. Organizasyonlar arasında siber tehdit verilerinin paylaşılması, daha önce karşılaşılmayan siber saldırıların engellenmesine yardımcı olabilmektedir. Analiz edilen bilgiler sayesinde organizasyonların karşılaşabileceği siber tehditler öngörülebilmekte ve bu çerçevede gerekli savunma mekanizmaları oluşturulabilmektedir.

Ayrıca teknoloji geliştikçe ve kullanımı arttıkça, bilinen siber saldırıları yöntemlerinin yanı sıra gelişmiş siber saldırıların meydana geldiği görülmektedir. Özellikle gelişmiş saldırıların engellenebilmesi için kuruluşların ve organizasyonların siber güvenlik kapasitelerini artırması, mevcut tehdit bilgilerini geliştirmesi ve artırması ise zorunluluk haline gelmiştir. Bu kapsamda, siber tehdit bilgilerinin elde edilebilmesi için siber vatanda işbirliğinin artırılması gerekmektedir. Siber vatanımızdaki organizasyonları hedef alabilecek tehditlerin zamanında bertaraf edilebilmesi için paydaşlar arasında veri, bilgi, deneyim paylaşımına imkân tanıyacak işbirliği altyapısının oluşturulması gerekmektedir. Paydaşlar arasında siber tehdit bilgilerinin paylaşılması ile her paydaşın tehditleri önlemeye yönelik kapasitesinin artacağı değerlendirilmektedir.

Sonuç olarak;

- Ülkemizde siber tehdit bilgilerinin paylaşıldığı paylaşım mekanizmalarının oluşturulmasının faydalı olacağı önerilmekte olup, siber vatandaki varlıkların korunmasına ve siber güvenlik direncinin artmasına katkı sağlayacağı değerlendirilmektedir. Bu sayede ülkemizde siber tehdit bilgisinin paylaşıldığı işbirliği mekanizması noktasındaki eksikliğin giderilebileceği değerlendirilmektedir.
- Ülkemizde oluşturulması önerilen bilgi paylaşım modeli ile siber vatandaki eksikliklerin giderilmesi, eylem planındaki tehdit bilgisi paylaşımı konusundaki işbirliği hedeflerinin hayata geçirilmesi ve desteklenmesi ve Genelge ve Rehberdeki işbirliği çalışmalarının genişletilmesine katkı sağlanacağı değerlendirilmektedir.
- Ayrıca organizasyonların bilgi paylaşım çalışmalarının genişletilebileceği, bu sayede organizasyonlar tarafından siber güvenlik olaylarının analizi ve kötü amaçlı yazılım analizleri hakkında bilgi toplanması, depolanması, dağıtılması ve paylaşılması, siber saldırganlara ve tehditlere yönelik etkin mücadele edilmesi ve güvenlik uyarılarının takip edilmesinin kolaylaşması mümkün olabilecektir.

- Siber tehditlere yönelik alınacak önlemlerin daha bilinçli yapılandırılabilmesi, saldırılara karşı kullanılan önlemlerin geliştirilebilmesi, gerçek zamanlı önlemlerin alınabilmesi, proaktif bir yaklaşımın benimsenmesi, potansiyel tehditlerin araştırılabilmesi, gerçek problemlerin tespit edilebilmesi ve bu problemlere yönelik çözümlerin oluşturulabilmesi, siber ekosistemde siber tehditlere yönelik direnç sağlamaya yardımcı olunması, paydaşlar arasındaki güvenin artması, farklı paydaşlarla tanışmaya olanak tanınması ve bu sayede kriz anında daha iyi bilgi ve proaktif tutum elde edilmesinin sağlanması, durumsal farkındalığın artırılması, gelecekteki gelişmiş tehditler için tehdit analizinde ileri görüş kazanılması, yeni savunma stratejilerinin geliştirilebilmesi ve potansiyel saldırı vektörlerini ele alan belirli teknolojilere, personele ve programlara ilişkin yatırımların planlanabilmesi mümkün olabilecektir.
- Bu konuda daha fazla detay için [52] nolu kaynağa müracaat edilmeli ve önerilen modeller hakkında bilgi alınmalıdır.

Ayrıca, siber tehdit bilgisi paylaşımında aşağıdaki hususlara da dikkat edilmesi yerinde olacaktır.

- Tehdit bilgisi paylaşımının çok yönlü olmasından dolayı karşılaşılabilecek güvenlik risklerinin öncelikle belirlenmesi, paylaşılacak verilerin değerlendirilmesi ve daha sonra paylaşıma karar verilmesi faydalı olacaktır.
- Paylaşılacak tehdit verileri için paylaşım kurallarının belirlenmesi ve kapsamlı bir bilgi paylaşım platformu oluşturulması önem teşkil etmektedir.
- Siber tehdit istihbaratı veya bilgisi toplama, siber tehditlere yönelik alınacak önlemler açısından çok önemlidir. Siber tehdit bilgilerinin toplanması, değerlendirilmesi ve paylaşılması için yapay zekâ ve makine öğrenmesi gibi yeni teknolojilerin geliştirilmesi ve kullanılmasının faydalı olacağı düşünülmektedir.
- Ulusal strateji ve eylem planlarının yayımlanmadan önce Hizmet Kalitesi-Boşluk Modeli, karar verme modeli ve bilgi boşluğu karar teorisi gibi farklı analiz araçlarıyla test edilmesi, oluşabilecek stratejik, taktiksel veya operasyonel bilgi boşlukları veya stratejik boşluklar var ise bunların önceden tespit edilip giderilmesinde fayda vardır.

- Bilgi paylaşımında bulunurken, kişisel bilgilerinin hassasiyetine uygun paylaşımlarda bulunulması, kimlik bilgileri açıklanmadan paylaşım yapılması, paylaşılan bilgilerin, paylaşılan amaç için gerekli olduğundan, yalnızca ilgili kişilerle paylaşıldığından, doğru ve açık olduğundan emin olunması gibi kurallar belirlenmelidir.

Siber tehdit bilgi paylaşımında karşılaşılan güçlükler genel olarak değerlendirildiğinde ise siber tehdit bilgi paylaşımında karşılaşılan problemlerin pek çoğu;

- İç dinamikler ve karar alma süreçleri,
- Veri boyutunun sürekli artması,
- Verilerin analizinde yeni bakış açılarına duyulan ihtiyaç,
- Sürekli artan uzman ihtiyacı,
- Yüksek bilgi birikimi gereksinimi,
- Siber saldırıları değerlendirmede uzman ihtiyacı yetersizliği,
- Önceliklendirmelerden kaynaklı oluşan atlamalar,
- Verilerin kötü amaçlı kullanılabilme şüphesi,
- Sürekli yeni tehditlerin geliştirilmesi veya oluşması,
- Veri değerlendirme sürelerindeki belirsizlikler,
- Saldırıların hızlıca tespit edilememesi,
- Yeni ekipman, araç, gereç ve altyapılara duyulan ihtiyaçlar,
- Sıkı denetim gerektiren konular olması,
- Paylaşımların tehdide dönüşme riski,
- Bilgi paylaşım kurallarının olmaması,
- Kurumsal ve ulusal risk oluşturma durumu,
- Güven duygusunu zedelemeye açık bir konu olması,
- Kişisel veri mahremiyetinin ihlal edilebilme olasılığı,
- Kanuni yaptırımlara ve cezalara maruz kalma durumu,
- Mevcut standartların tam oturtulamaması

gibi riskleri veya olumsuzlukları barındırmaktadır.

KAYNAKLAR

[1] İnternet: 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. (2016). Ulaştırma ve Altyapı Bakanlığı. URL: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, Son Erişim Tarihi: 10.01.2021.

[2] İnternet: Definition of Cybersecurity. International Telecommunication Union. URL: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, Son Erişim Tarihi: 10.01.2021.

[3] Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., and Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems*, 89, 349-359.

[4] Yılmaz, S., ve Sağıroğlu, Ş. (2013). Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, Ankara, 323-331.

[5] İnternet: Muscat, I. (2019). Cyber Threats, Vulnerabilities and Risks. Acunetix. URL: https://www.acunetix.com/blog/articles/cyber-threats-vulnerabilities-risks/, Son Erişim Tarihi: 16.12.2020.

[6] İnternet: Robinson, N., Gribbon, L., Horvath V. and Robertson, K. (2013) Cybersecurity Threat Characterisation. Rand Cooperation. URL: https://www.rand.org/pubs/research_reports/RR235.html, Son Erişim Tarihi: 10.01.2021.

[7] İnternet: Ross, R. S. (2019). Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf, Son Erişim Tarihi: 10.01.2021.

[8] İnternet: Threat Intelligence Definition. Why Threat Intelligence is Important for Your Business and How to Evaluate a Threat Intelligence Program. Kaspersky. URL: https://www.kaspersky.com/resource-center/definitions/threat-intelligence, Son Erişim Tarihi: 10.01.2021.

[9] Mavroeidis, V. and Bromander, S. (2017). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *IEEE In 2017 European Intelligence and Security Informatics Conference (EISIC)*, Athens, Greece, 91-98.

[10] İnternet: Understanding Cyber Threat Intelligence Operations - CBEST Intelligence-Led Testing. (2016). Bank of England. URL: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf, Son Erişim Tarihi: 10.01.2021.

[11] İnternet: Cyber Threat Intelligence In Government: A Guide For Decision Makers & Analysts. (2019). UK Digital, Data & Technology. URL: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf, Son Erişim Tarihi: 10.01.2021.

[12] Liu, M., Xue, Z., He, X., and Chen, J. (2019). Cyberthreat-intelligence information sharing: Enhancing collaborative security. *IEEE Consumer Electronics Magazine*, 8(3), 17-22.

[13] Wagner, T. D., Mahbub, K., Palomar, E., and Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, 87, 1-13.

[14] İnternet: Actionable Information for Security Incident Response. (2014). European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu/publications/actionable-information-for-security, Son Erişim Tarihi: 10.01.2021.

[15] Feledi, D., Fenz, S., and Lechner, L. (2013). Toward web-based information security knowledge sharing. *Information Security Technical Report*, 17(4), 199-209.

[16] Brown, S., Gommers, J., and Serrano, O. (2015). From cyber security information sharing to threat management. *In Proceedings of the 2nd ACM workshop on information sharing and collaborative security*, Colorado, USA, 43-49.

[17] Garrido-Pelaz, R., González-Manzano, L., and Pastrana, S. (2016). Shall we collaborate? A model to analyse the benefits of information sharing. *In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, Vienna, Austria, 15-24.

[18] Jasper, S. E. (2017). US cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence*, 30(1), 53-65.

[19] Mkuzangwe, N. N., and Khan, Z. C. (2020). Cyber-threat information-sharing standards: a review of evaluation literature. *The African Journal of Information and Communication*, 25, 1-12.

[20] Conti, M., Dargahi, T., and Dehghantanha, A. (2018). Cyber threat intelligence: challenges and opportunities. *In Cyber Threat Intelligence,*1-6.

[21] Abu, M. S., Selamat, S. R., Ariffin, A., and Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), 371-379.

[22] Murdoch, S., and Leaver, N. (2015). Anonymity vs. trust in cyber-security collaboration. *In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, Colorado USA, 27-29.

[23] Vázquez, D. F., Acosta, O. P., Spirito, C., Brown, S., and Reid, E. (2012). Conceptual framework for cyber defense information sharing within trust relationships. *IEEE In 2012 4th International Conference on Cyber Conflict (CYCON 2012*), Tallinn, Estonia, 1-17.

[24] Kokkonen, T., Hautamäki, J., Siltanen, J., and Hämäläinen, T. (2016). Model for sharing the information of cyber security situation awareness between organizations. *IEEE In 2016 23rd International Conference on Telecommunications (ICT)*, Thessaloniki, Greece, 1-5.

[25] Win, K. M. N., and Thaw, Y. M. K. K. (2019). Information Sharing of Cyber Threat Intelligence with their Issue and Challenges. *International Journal of Trend in Scientific Research and Development (IJTSRD)*, 3(5), 878-880.

[26] Mutemwa, M., Mtsweni, J., and Mkhonto, N. (2017). Developing a cyber threat intelligence sharing platform for South African organisations. *IEEE In 2017 Conference on Information Communication Technology and Society (ICTAS),* Durban, South Africa, 1-6.

[27] Zibak, A., and Simpson, A. (2018). Can We Evaluate the Impact of Cyber Security Information Sharing? *IEEE In 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Glasgow, Scotland, 1-2.

[28] İnternet: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™). (2012). MITRE Corporation. URL: https://www.mitre.org/publications/technical-papers/standardizing-cyber-threat-intelligence-information-with-the, Son Erişim Tarihi: 10.01.2021.

[29] İnternet: Impe, K. V. (2015). How STIX, TAXII and CybOX Can Help With Standardizing Threat Information. Security Intelligence. URL: https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information, Son Erişim Tarihi: 16.12.2020.

[30] İnternet: Connolly, J., Davidson, M. and Schmidt, C. (2014). The Trusted Automated eXchange of Indicator Information (TAXII™). URL: https://taxiiproject.github.io/getting-started/whitepaper, Son Erişim Tarihi: 16.12.2020

[31] İnternet: Threat Intelligence Platform. Wikipedia. URL: https://en.wikipedia.org/wiki/Threat_Intelligence_Platform, Son Erişim Tarihi: 10.01.2021.

[32] İnternet: Clean, P. P. (2015). Automated Defense - Using Threat Intelligence to Augment. URL: https://www.sans.org/reading-room/whitepapers/threats/paper/35692, Son Erişim Tarihi: 10.01.2021.

[33] İnternet: IBM X-Force Threat Intelligence. International Business Machines (IBM). URL: https://www.ibm.com/security/xforce, Son Erişim Tarihi: 16.12.2020.

[34] İnternet: Features of MISP, The Open Source Threat Sharing Platform. Malware Information Sharing Platform Project. URL: https://www.misp-project.org/features.html, Son Erişim Tarihi: 16.12.2020.

[35] İnternet: Moriarty, K. M. (2013). Transforming Expectations For Threat-Intelligence Sharing. RSA Security Inc. URL: http://docplayer.net/13281555-Transforming-expectations-for-threat-intelligence-sharing.html, Son Erişim Tarihi: 10.01.2021.

[36] Dandurand, L., and Serrano, O. S. (2013). Towards improved cyber security information sharing. *IEEE In 2013 5th International Conference on Cyber Conflict (CYCON 2013),* Tallinn, Estonia, 1-16.

[37] İnternet: Third Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way Sponsored by Infoblox. (2018). Ponemon Institute. URL: https://www.infoblox.com/wp-content/uploads/infoblox-white-paper-ponemon-infoblox-2018-final-report.pdf, Son Erişim Tarihi: 10.01.2021.

[38] İnternet: Goodwin, C. and Nicholas, J. P. (2015). A framework for cybersecurity information sharing and risk reduction. Microsoft. URL: https://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf, Son Erişim Tarihi: 10.01.2021.

[39] İnternet: Zheng D. E. and Lewis, J. A. (2015). Cyber Threat Information Sharing. Center for Strategic and International Studies (CSIS). URL: http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf, Son Erişim Tarihi: 15.03.2021.

[40] Bauer, J. M., and Van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10-11), 706-719.

[41] İnternet: Threat Intelligence. (2018). Sothis Tech. URL: https://www.sothis.tech/en/threat-intelligence-i/, Son Erişim Tarihi: 10.01.2021.

[42] Abouzahra, M., and Tan, J. (2014). The effect of community type on knowledge sharing incentives in online communities: A meta-analysis. *IEEE In 2014 47th Hawaii International Conference on System*, Waikoloa, USA, 1765-1773.

[43] Tamjidyamcholo, A., Baba, M. S. B., Tamjid, H., and Gholipour, R. (2013). Information security–Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education*, 68, 223-232.

[44] Haustein, M., Sighart, H., Titze, D., and Schoo, P. (2013). Collaboratively Exchanging Warning Messages between Peers While under Attack. *IEEE In 2013 International Conference on Availability, Reliability and Security,* Regensburg, Germany, 726-731.

[45] Al-Ibrahim, O., Mohaisen, A., Kamhoua, C., Kwiat, K., and Njilla, L. (2017). Beyond free riding: quality of indicators for assessing participation in information sharing for threat intelligence, *Cryptography and Security,* 1-12.

[46] İnternet: Glossary of Key Information Security Terms. (2019). National Institute of Standards and Technology (NIST). URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, Son Erişim Tarihi: 10.01.2021.

[47] İnternet: Warsaw Summit Key Decisions. (2017) North Atlantic Treaty Organization (NATO). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf, Son Erişim Tarihi: 10.01.2021.

[48] İnternet: Warsaw Summit Communiqué. (2016). North Atlantic Treaty Organization (NATO). URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm, Son Erişim Tarihi: 15.01.2021.

[49] Polat, D. Ş. (2020). NATO'nun Yeni Operasyon Alanı: Siber Uzay. *Güvenlik Bilimleri Dergisi, (International Security Congress Special Issue),* 135-158.

[50] Ş. Sağıroğlu, "Gündem Siber Vatan," *CyberMag Aylık Siber Güvenlik Dergisi,* 2020.

[51] İnternet: Ulusal Siber Güvenlik Stratejisi ve 2020 – 2023 Eylem Planı. (2021). Ulaştırma ve Altyapı Bakanlığı. URL: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, Son Erişim Tarihi: 10.01.2021.

[52] A. M. Kanca, Organizasyonlar Arası Siber Tehdit Bilgi Paylaşımı Değerlendirmeler Ve Öneriler, Yüksek Lisans Tezi, Bilgi Güvenliği Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 2021.

Bölüm 4

ZARARLI YAZILIMLARIN VE YAYILIMLARININ MATEMATİKSEL OLARAK MODELLENMESİ

Yunus Geçer

Bu bölümde; karmaşık yapılara sahip olan zararlı yazılımların yapıları ve yayılımlarının matematiksel modellenme süreçleri incelenmiş; zararlı yazılım yayılım modellemelerinin gelişimi, etkileri ve gelecek perspektifleri değerlendirilmiş; konunun önem ve farkındalığına katkı sağlanmış; literatür çalışmaları ve güncel çalışmalar ile kapsam geliştirilerek değerlendirmeler sunulmuştur.

4.1. GİRİŞ

Günümüzde zararlı yazılımlar oldukça karmaşık yapılara sahip olup kendi mutasyonlarını üretebilen ayrıca anti virüs programları ile saptanması ve kaldırılması daha zor bir hale gelmiş durumdadır. Giderek gelişen ve karmaşıklaşan bu yapıları araştırmak için diğer alanlarda olduğu gibi bu alanda da matematiksel modellere başvurulduğu görülmektedir. Matematiksel modellemeye başvurulmasında önemli etkenlerden biri olarak ise saldırıların temel özelliklerinin ekonomik karakterize edilmesine ve üzerinde hızla çalışılabilmesine imkân sağlaması olarak belirtilmektedir [1].

Bu zararlı yazılımların yayılmasını araştırmak için geliştirilen matematiksel modellerin, bulaşıcı hastalıkların yayılmasını incelemek için tasarlanmış mo-

dellere dayandığı görülmektedir [1-5]. Bunun nedeni olarak ise yine aynı çalışmaların tümünde, biyolojik virüslerin davranışları ile zararlı yazılımların (bilgisayar virüsleri, bilgisayar solucanları vb.) davranışı arasındaki yüksek benzerlik olduğu vurgulanmaktadır.

Zararlı yazılım yayılım modellenmesinin, bulaşıcı hastalıkların yayılma davranışı için geliştirilen modellere dayanması sonucunda, temel özellikler ve bazı terimlerin (duyarlı, bulaştırıcı, iyileşmiş, maruz kalan, karantinaya alınmış, aşılanmış vb.) zararlı yazılım alanındaki çalışmalara aktarıldığı görülmektedir [5]. Bu özellik ve terimlere zararlı yazılımlar alanı bakımından karşılık gelen ifadeler, ilgili modellemelerin başlıkları altında detaylı olarak sunulmaya çalışılmıştır.

Bu bölümde başlıca literatür çalışmaları [3], [5], [6] ve bu çalışmalardan sonra günümüze kadar yapılan diğer çalışmalar da değerlendirilerek güncel özellikte geniş kapsamlı bir çalışma sunulmaya çalışılmıştır.

4.2. MATEMATİKSEL MODELLERİN ANALİZİ VE GENEL ÖZELLİKLERİ

Matematiksel modelleme tanımını temel anlamda özetlemek gerekirse; belirli bir bilimsel alanda çeşitli nedenlerle (karmaşık yapı, yüksek maliyet, tehlike içermesi, uzun zaman alması vb.) üzerinde doğrudan çalışılamayan problemlerin, matematik terimleriyle temsil edilerek sayısal analizlerle olgu ve mekanizmalar üzerinde çalışılması olarak ifade edilmektedir [1], [5].

Matematiksel modeller ile ilgili olarak bir diğer önemli husus ise temelde üç unsurla karakterize edilmeleridir ki bunlar [5]:

- **İncelenen değişkenler:**

  Zararlı yazılımın yayılmasının modellemesinde, dikkate alınan bazı türlerde bulunan cihazların sayısı kullanılan değişkenlerdendir.

- **Kullanılan parametreler:**

  Genel parametrelerden bazıları, enfeksiyon veya bulaşma oranı, iyileşme oranıdır. Bu parametrelerin kullanımı, uygulanan modele ve dikkate alınan zararlı yazılımın türüne bağlı olarak değişmektedir.

– **Dinamiği yöneten fonksiyonel ilişkiler:**

  Modelde sunulan parametreleri hesaba katan fonksiyonel ilişkiler farklı matematiksel araçlarla düzenlenebilmekle birlikte çoğunlukla sıradan (adi) diferansiyel denklem kullanılmaktadır.

Diferansiyel denklemlerin dışında, fark denklemleri, Markov zincirleri de kullanılmakla birlikte çoğunlukla diferansiyel denklemlerin kullanılmasının temel nedeni olarak, diferansiyel denklemlerin, söz konusu modelin ayrıntılı bir analizinin yapılmasına izin vermesi gösterilmektedir [5].

Ayrıca bu hususta matematiksel modeller yapılarına göre, deterministik modeller ve stokastik modeller olarak da sınıflandırılmaktadır. Deterministik modeller genellikle diferansiyel denklemlere veya fark denklemlerine dayanmaktadır. Stokastik modellerin ise durum değişkeninin ayrık olduğu Markov zincirlerine dayalı olanlar ve hem zaman hem de durum değişkenleri sürekli stokastik diferansiyel denklemlere dayalı olanlar olarak iki temel sınıfa ayrıldığı belirtilmektedir [5].

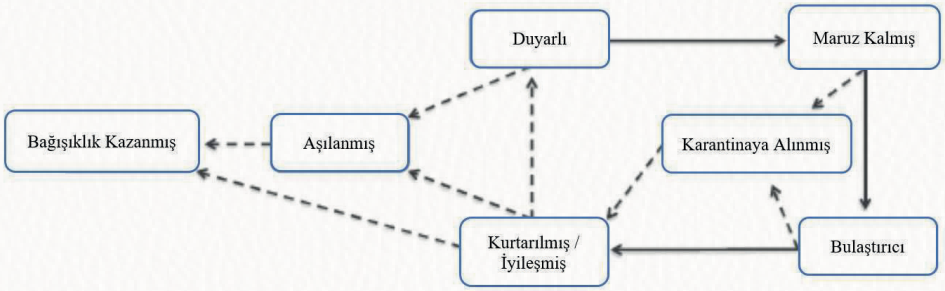
Modellerin yapısından sonra zararlı yazılım yayılımı alanında bilinen modellemelerin bazılarının isim ve açılımları aşağıda sunulmuştur:

– SIR (duyarlı - bulaştırıcı - iyileşmiş) modeller,
– SIS (duyarlı - bulaştırıcı – duyarlı) modeller,
– SEIR (duyarlı - maruz kalmış - bulaştırıcı - iyileşmiş) modeller,
– SEIQR (duyarlı - maruz kalmış - bulaştırıcı - karantinaya alınmış - iyileşmiş) modeller,
– SEIRS - V modelleri (aşılanan sınıf dâhil olarak varyantları bunlar: SIRS, SEIRS, SEIQRS,
– SEIQV (duyarlı - maruz kalan - bulaştırıcı - karantinaya alınmış - aşılanmış)

Geliştirilen modellerden yukarıda yer verilmeyen diğer başlıca modeller SIRS, SEIS, MSIR, MSEIR ve MSEIRS'dir [8].

Burada ele alınan matematiksel modellerin SIR ve SIS olmak üzere iki temel modellemenin modifikasyonları şeklinde olduğu görülmektedir. Bu iki ana modelin temel sınırlandırmaları kaldırmaya yönelik birçok model hazırlanmıştır [8]. Başka bir husus olarak modellerin büyük çoğunluğunda, bilgisayar solucanları ve virüslerinin yayılmasının çalışıldığı görülmekte ve bilgisayar

virüsleri özelinde ise en çok SIS ve SIR modellerinin kullanıldığı da gözlemlenmektedir [5], [8]. SIR modeli bir sonraki başlık altında incelenmiştir. Temel modellerden bir diğeri SIS modeli ise, bireylerin bağışıklık kazanmadığı ve iyileşmesi ile birlikte tekrar hastalığa duyarlı birey olduğu bir modeldir [8].

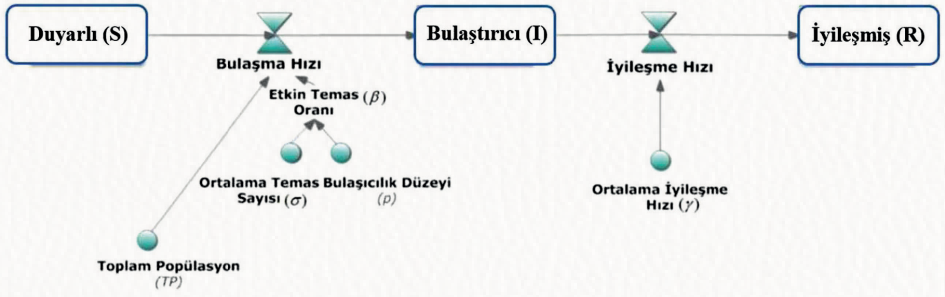


Şekil 4.1. Modellerin davranış türleri diyagramı [5].

Çalışmalarda bulunan yaygın modellerin davranış türlerinin diyagramı ve aralarındaki temel dinamikler Şekil 4.1'de gösterilmektedir.

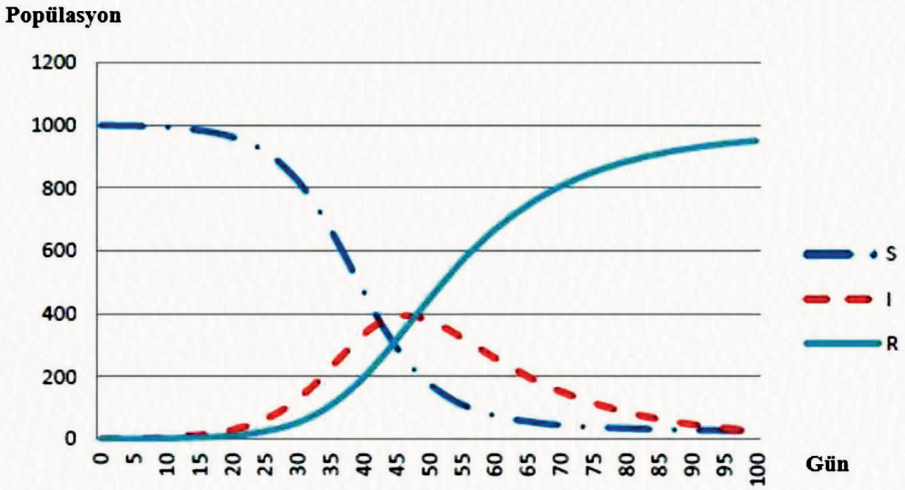
4.2.1. SIR Modellemesi ve Alanda Uygulanması

Kermack ve McKendrick tarafından 1927 yılında [7] önerilen ve bulaşıcı hastalıkların yayılımının tahmininde ilk örnek olarak gösterilen, SIR modelinin ortaya çıkışı diferansiyel denklemlere dayalı tüm epidemiyolojik modeller alanındaki en önemli kilometre taşı olarak değerlendirilmektedir [8],[9]. SIR modelinin aynı zamanda zararlı yazılım yayılma modellerine de temel oluşturduğu ifade edilmektedir [5].



Şekil 4.2. SIR model diyagramı [8].

Şekil 4.2 ile gösterilen SIR modelinin amacı, nüfusun sabit kaldığı başka bir ifadeyle kapalı bir popülasyonda bulaşıcı hastalık yayılımını zaman içinde hesaplamasını sağlamaktadır. İsmini S=Susceptible (Duyarlı), I=Infected (Enfekte olmuş, Bulaşmış veya Bulaşıcı) ve R=Recovered (İyileşmiş) terimlerinden almaktadır. Aynı zamanda bu üç kategori, kompartıman veya bölüm olarak adlandırılmaktadır. Bu durum modelin genel ismine de eklenebilmekte ve kompartımanlı SIR modellemesi olarak da adlandırılabilmektedir.



Şekil 4.3. SIR modelde örnek bir yayılım seyri [8].

Şekil 4.3 ile SIR modelinin yayılma davranışı zaman grafiği verilmiştir. Burada da görüldüğü üzere SIR modelinde, zamana bağlı üç değişken dikkate alınmakta olup, bunlar:

$S(t)$: duyarlı bireylerin sayısı,
$I(t)$: bulaştırıcı bireylerin sayısı ve
$R(t)$: iyileşmiş bireylerin sayısıdır.

Nüfusun sabit kaldığı varsayıldığından, herhangi bir t zamanında bireylerin toplam sayısı popülasyona eşit olacaktır. N, popülasyonu temsil etmek üzere bu ifadenin matematiksel gösterimi;

$$N = S(t) + I(t) + R(t) \tag{4.1}$$

Ayrıca, iki parametre daha dikkate alınır ki bunlar:

- a : bulaşma hızı ve
- b : iyileşme hızı veya oranıdır.

Bu bilgiler ışığında SIR modelinin matematiksel modeli, aşağıdaki Denklem (4.2) adi diferansiyel denklem sisteminde gösterilmiştir.

$$\begin{cases} S'(t) = -aI(t)S(t) \\ I'(t) = aI(t)S(t) - bI(t) \\ R'(t) = bI(t) \end{cases} \quad (4.2)$$

Denklem (15.1); $S'(t)$, $I'(t)$ ve $R'(t)$ birinci türevleri gösterir.

- Sisteminin ilk denklemi, $S'(t) = -aS(t)I(t)$, duyarlı bireylerin sayısındaki zaman içindeki değişimin, bulaştırıcı bireyler ile temas sayısına ve bulaşma hızına bağlı olduğunu,
- Sistemin ikinci denklemi, $I'(t) = aNS(t)I(t) - bI(t)$, bulaştırıcı bireylerin sayısındaki farklılığın tespitini ve
- Son olarak, üçüncü denklem, $R'(t) = bI(t)$, iyileşen bireylerdeki artışın, bulaştırıcı bireylerin sayısı ile orantılı olduğunu göstermektedir.

SIR modelinde yer alan terimler, zararlı yazılımların yayılımı kapsamından bakıldığı zaman, aşağıdaki gibi karşılık bulmaktadırlar:

– S: Duyarlı (Hassas) cihazlar:

Zararlı yazılım bulaşmamış ancak bu zararlı yazılıma karşı duyarlı yani bulaşmasına elverişli olan cihazlardır.

– I: Bulaştırıcı (Enfekte, Virüslü) cihazlar:

Zararlı yazılım bulaşmış ve duyarlı cihazlara da bulaştırma kapasitesine sahip olan cihazlardır.

– R: İyileşmiş (Bağışıklık kazanmış,

Geri kazanılan, Kurtarılmış) cihazlar: Zararlı yazılım bulaşmış olup iyileşen cihazlardır. Zararlı yazılımın tekrar bulaşma olasılığı olmayan veya zararlı yazılımı yayma olasılığı olmayan kalıcı bağışıklık kazanan cihazlardır.

SIR modeli, zararlı yazılım yayılma modeli olarak, diferansiyel denklem sistemi Denklem (4.3) şeklinde formüle edilmiştir [3], [6].

$$\begin{cases} \frac{dS}{dt} = b - \lambda S(t)I(t) - dS(t) \\ \frac{dI}{dt} = \lambda S(t)I(t) - \varepsilon I(t) - dI(t) \\ \qquad\quad \varepsilon I(t) - dR(t) \end{cases} \tag{4.3}$$

Burada, söz konusu ağa bağlı tüm cihazların üç kategoriye ayrıldığı varsayılmaktadır: duyarlı, bulaştırıcı, iyileşmiş cihazlar ve bunlar dışında t zaman ile birlikte dört pozitif parametre içermektedir [3]. Ayrıca daha önce ifade edilmemiş parametreler ve açıklamaları aşağıda sunulmuştur:

t : Zaman,

b : Harici cihazların ağa bağlanma hızı,

ε : Ağın anti virüs sayesinde zararlı yazılım bulaşmış cihazların kurtarılma oranı,

d : Bir cihazın ağdan kaldırılma hızı,

λ : Bulaştırıcı bir cihazla bağlantı kurulduğunda, duyarlı bir cihaza bulaşma oranıdır.

4.2.2. SAIR / SIRA Modellemesi

Virüsten koruma yazılımının kullanılması, zararlı yazılım bulaşmış cihazları kurtarmaya yönelik en etkili yaklaşımlardan biri olarak kabul edilmektedir [3]. Bu nedenle bu kısımda SIR modellemesine anti virüs ile donatılmış cihazlar parametresi eklenmiş olan SAIR / SIRA modellemesinin [6] incelemesi sunulmaktadır.

Farklı çalışmalarda iki farklı adlandırmaya da rastlanmış olmakla birlikte bu model için geliştiricilerinin de daha çok tercih ettiği SIRA modeli ifadesi kullanılacaktır. SIRA modellemesi geliştirilirken özetle, bir virüs yayılma dinamiklerini temsil ettiği ve bu model kullanılarak, anti virüs programlarının ekonomik bir şekilde kullanılmasını sağlayan strateji olarak tanımlanabilmektedir [6].

Toplam popülasyon; duyarlı (S) , bulaştırıcı (I), iyileşmiş (R) ve anti virüs ile donatılmış olan (A) olarak 4 gruba ayrılmaktadır. SIRA modellemesinin tanımlaması aşağıdaki denklem (4.4) ile gösterilmiştir [6]:

$$\begin{cases} \dot{S} = N - \alpha_{SA} SA - \beta SI - \mu S + \sigma R \\ \dot{I} = \beta SI - \alpha_{IA} AI - \delta I - \mu I \\ \dot{R} = \delta I - \sigma R - \mu R \\ \dot{A} = \alpha_{SA} SA + \alpha_{IA} AI - \mu A. \end{cases} \quad (4.4)$$

Modelin akış ve ölüm parametreleri şu şekilde tanımlanmaktadır [6]:

N : Yeni cihazların ağa dâhil edilmesini temsil eden giriş oranı,

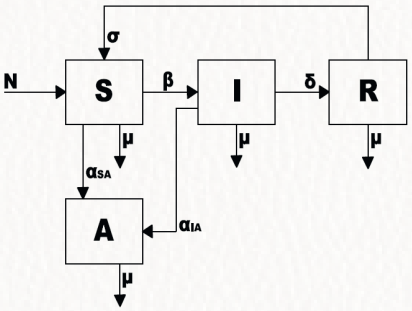
β : Enfekte cihazlarla etkileşimde olan bulaşmaya duyarlı cihaz oranı, SI ile de orantılıdır.

α : Duyarlı olan cihazların dönüşüm oranı SA ile de orantılıdır.

δ : Bulaştırıcı durumdan iyileşmiş duruma geçme oranı,

σ : İyileşmiş durumdan tekrar duyarlı duruma geçme oranı,

μ : Ölüm oranı; ağdan çıkarılan cihazlar (zararlı yazılım dışı nedenler bozulma, eskime vb.)



Şekil 4.4. SAIR – SIRA Modeli [6].

SIRA modellemesinin tanımlaması model genel yapısı Şekil 4.4 ile gösterilmiştir. Burada akış oranı şu şekilde kabul edilir:

$N = 0$, zararlı yazılımın yayılması sırasında ağa yeni cihazların dâhil edilmediğini ve

$\mu = 0$, cihazların eskime süresinin zararlı yazılımın etki süresinden daha uzun olduğunu ifade etmektedir.

Sonuç olarak, Şekil 4.4 ile ifade edilen modelde $N = 0$ ve $\mu = 0$ alınarak Denklem (4.5)'te gösterilen denklem sistemine daha basit bir şekilde dönüştürülmüş olmaktadır.

$$\begin{cases} \dot{S} = -\alpha_{SA} SA - \beta SI + \sigma R, \\ \dot{I} = \beta SI - \alpha_{IA} AI - \delta I, \\ \dot{R} = \delta I - \sigma R, \\ \dot{A} = \alpha_{SA} SA + \alpha_{IA} AI. \end{cases} \tag{4.5}$$

Daha sonra virüs bulaşmadığı hastalıksız denge noktalarının hesaplanmasında $I = 0$ yani bulaştırıcının olmadığı düşünülür. Bu şart Denklem (4.4) ile ifade edilen sisteme uygulanırsa;

$$\begin{aligned} P_1 &= (S, I, R, A) = (0,0,0,T); \\ P_2 &= (S, I, R, A) = (T,0,0,0). \end{aligned} \tag{4.6}$$

olmak üzere iki olasılık hesaplaması yapılır. P_1 denge durumu göz önüne alınırsa, buna karşılık gelen J_{P1} jakobiyeni hesaplanır.

$$J_{P1} = \begin{bmatrix} -\alpha_{SA} T & 0 & \sigma & 0 \\ 0 & (-\alpha_{IA} T - \delta) & 0 & 0 \\ 0 & \delta & -\sigma & 0 \\ \alpha_{SA} T & \alpha_{IA} T & 0 & 0 \end{bmatrix} \tag{4.7}$$

Buradan J_{P1} özdeğerleri: $(-\alpha_{SA} T; -\alpha_{IA} T - \delta; -\sigma; 0)$ şeklinde bulunur.

Sonuç olarak, bütün mümkün parametre değerleri için bakılırsa, bunlar reel ve negatif değerlerdir. Bu da P_1'in asimptotik kararlılığını gerektirir. 0 özdeğeri çatallanma veya merkez manifold oluşturmaz.

Şimdi P_1 denge durumuna göz önüne alınırsa; buna karşılık gelen J_{P2} jakobiyeni hesaplanır.

$$J_{P2} = \begin{bmatrix} 0 & -\beta T & \sigma & -\alpha_{SA} T \\ 0 & (-\beta T - \delta) & 0 & 0 \\ 0 & \delta & -\sigma & 0 \\ 0 & 0 & 0 & \alpha_{SA} T \end{bmatrix} \tag{4.8}$$

Buradan J_{P2} özdeğerleri: $(0; -\beta T - \delta; -\sigma; \alpha T)$ şeklinde bulunur. Yapılan kararlılık analizi bize şunu göstermektedir: bu modelin iki tane virüs bulaşmayan denge noktası vardır, birisi kararsız diğeri asimptotik kararlıdır. Ayrıca bundan yola çıkılarak endemik denge noktalarına da bakılabilir.

4.2.3. Diğer Paradigmatik Model Örnekleri

4.2.3.1. SEIRS Modeli (Mishra ve Saini)

SEIRS modeli varsayımları [1]:

- Ağdaki her bir cihaz duyarlıdır.
- Ağdan kaldırılma oranı her cihaz için eşit ve sabittir (zararlı yazılım dışı nedenler).
- Zararlı yazılımın neden olduğu ağdan kaldırılma oranı sabittir.
- Gecikme süresi ω ve bağışıklık süresi τ sabittir.
- Maruz kalma, bulaşma ve karantina durum süreleri üstel bir dağılım izler.
- Bir bilgisayar artık bulaştırıcı olmadığında iyileşir, p olasılıkla geçici bağışıklık kazanır ve $1-p$ olasılıkla zararlı yazılımın etkileri nedeniyle ağdan kaldırılır.

Bu modelin diferansiyel denklem sistemi Denklem (4.9) ile gösterilmektedir [1]:

$$\begin{cases} S'(t) = bN(t) - \frac{\gamma}{N(t)} S(t)I(t) - \mu S(t) + \alpha I(1-\tau)e^{-\mu t} \\ E'(t) = \frac{\gamma}{N(t)} S(t)I(t) - \frac{\gamma}{N(1-\tau)} S(1-\tau)I(1-\tau)e^{-\mu\omega} - \mu E(t) \\ I'(t) = \frac{\gamma}{N(1-\tau)} S(1-\tau)I(1-\tau)e^{-\mu\omega} - (\mu + \epsilon + \alpha)I(t) \\ R'(t) = p\alpha I(t) - \alpha I(1-\tau)e^{-\mu\tau} - \mu R(t) \end{cases} \quad (4.9)$$

Burada:

$E(t)$: t süresinde zararlı yazılıma maruz kalmış olan cihaz sayısı,

b: Ağdaki yeni bilgisayar oranı,

μ: Zararlı yazılımdan kaynaklanmayan ağdan kaldırılma oranı,

ε: Zararlı yazılımdan kaynaklanan ağdan kaldırılma oranı,

α: Kurtarma hızı ve

γ: İletim hızıdır.

Bu modellemede geçici bağışıklık göz önünde bulundurulur ve sistemin maruz kalma süresi ne kadar uzun olursa, yayılımında o kadar hızlı seyirde olabileceği öngörülmektedir [1].

4.2.3.2. SEIQRS Modeli (Mishra ve Jha)

Bu modelin diferansiyel denklem sistemi Denklem (4.10) ile gösterilmektedir [10]:

$$\begin{cases} S'(t) = A - aS(t)I(t) - dS(t) + \eta R(t) \\ E'(t) = aS(t)I(t) - (d+\mu)E(t) \\ I'(t) = \mu E(t) - (d+\alpha+\gamma+\delta)I(t) \\ Q^I(t) = \delta I(t) - (d+\alpha+\epsilon)Q(t) \\ R'(t) = \gamma I(t) + \epsilon Q(t) - (d+\eta)R(t) \end{cases} \quad (4.10)$$

Bu denklem sisteminde yer alan parametreler:

$Q(t)$: t anında karantinaya alınan cihazların sayısı,

A: Ağa eklenen yeni cihazların sayısı,

d: Cihazların ağdan kaldırılma oranı,

μ: Maruz kalma durumundan bulaştırıcı duruma geçiş oranı,

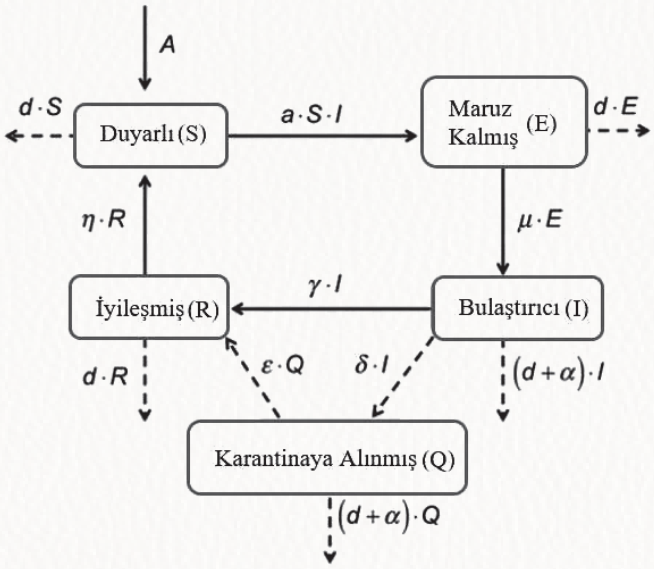
δ : Bulaştırıcı durumdan karantinaya geçiş oranı,

α: Zararlı yazılımın eylemi nedeniyle bir bilgisayarın ağdan kaldırılma oranı,

γ: Anti virüs yazılımının eyleminden kaynaklanan iyileşme oranı,

ε: Bulaştırıcı veya karantinaya alınmış durumdan iyileşmiş duruma geçiş hızı ve

η: Bağışıklık kaybı oranıdır.



Şekil 4.5. SEIQRS modelinin bölmeleri arasındaki dinamiği temsil eden akış şeması [10].

Şekil 4.5 bu modelin farklı bölümleri arasındaki akış şemasını göstermektedir. Bu modelde, temasların sayısı karantinaya alınan sınıfın büyüklüğünden etkilenir ve sonuç olarak hem bulaşıcı dönem hem de karantina oranı arttıkça temel üreme sayısı azalmaktadır [10].

4.2.3.3. SEIRS Modeli (Mishra ve Pandey)

Bu modelin diferansiyel denklem sistemi Denklem (4.11) ile gösterilmektedir [11]:

$$\begin{cases} S'(t) = b - \lambda S(t)I(t) - pbE(t) + qbI(t) - dS(t) + \zeta R(t) \\ E'(t) = \lambda S(t)I(t) - pbE(t) + qbI(t) - \epsilon E(t) - dE(t) \\ I'(t) = \epsilon E(t) - \gamma I(t) - dI(t) - \eta I(t) \\ R'(t) = \gamma I(t) - \zeta R(t) - dR(t) \end{cases} \quad (4.11)$$

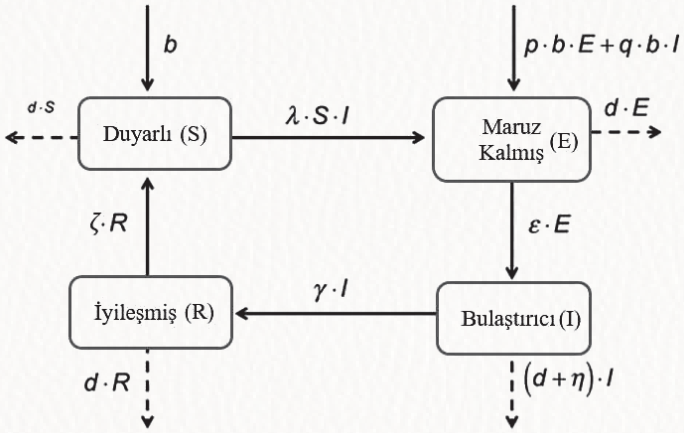
Bu denklem sisteminde yer alan parametreler:

b: Ağa eklenen yeni cihazların sayısı,

d: Cihaz başına doğal ölüm (eskime, bozulma vb.) oranı,

ε: Maruz kalmış durumdan bulaştırıcı duruma geçiş oranı,

γ: Bulaştırıcı durumundan iyileşmiş duruma geçiş oranı,
η: Bulaştırıcı durumunda zararlı yazılıma bağlı ölüm oranı ve
ζ: İyileşmiş durumdan duyarlı duruma geçiş oranıdır.



Şekil 4.6. SEIRS modelinin bölmeleri arasındaki dinamiği temsil eden akış şeması [11].

Bu modelin, farklı bölmeler arasındaki akış şeması Şekil 4.6'da gösterilmektedir. Ayrıca bu model, bilgisayar solucanlarının yayılmasını incelemek için geliştirilmiştir [11].

4.2.3.4. SIR Modeli (Zhu, Yang ve Ren)

Bu model, duyarlı cihazların ve ağdan çıkarılan bulaştırıcı cihazların tanıtıldığı SIR tipi bölmeli bir modeldir. Modeli yöneten denklem sistemi Denklem (4.12) ile gösterilmektedir [12]:

$$\begin{cases} S'(t) = \lambda_1 - \beta_1 S(t)I(t) - \beta_1 S(t)\frac{R_I(t)}{R_N(t)} - \mu_1 S(t) \\ I'(t) = \beta_1 S(t)I(t) - \beta_2 S(t)\frac{R_I(t)}{R_N(t)} - (\mu_1 + \sigma_1)I(t) \\ R'(t) = \sigma_1 I(t) - \mu_1 R(t) \\ {R_S}'(t) = \lambda_2 - \beta_2 \frac{R_S(t)}{N} + \sigma_2 \frac{R_I(t)R(t)}{N} - \mu_2 R_s(t) \\ {R_I}'(t) = \beta_2 \frac{R_S(t)}{N} + \sigma_2 \frac{R_I(t)R(t)}{N} - \mu_2 R_I(t) \end{cases} \quad (4.12)$$

Bu denklem sisteminde yer alan parametreler:

$R_S(t)$: t zamanda duyarlı çıkarılabilir cihazlar sayısı,

$R_I(t)$: t zamanda bulaştırıcı çıkarılabilir cihazlar sayısı,

$R_N(t)$: t zamanda çıkarılabilir cihaz sayısı,

λ_1: Bilgisayarların işlenme oranı,

λ_2: Çıkarılabilir cihazların işlenme oranı,

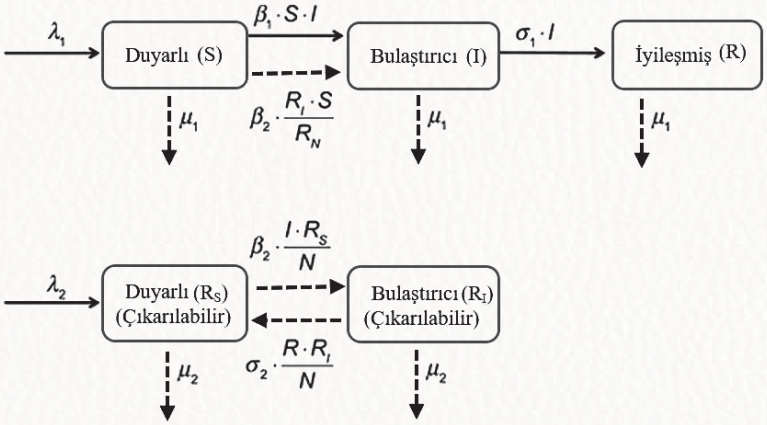
β_1: Duyarlı ve bulaştırıcı bilgisayarlar arasındaki temas, bulaşma kuvveti,

β_2: Bilgisayarlar ve çıkarılabilir cihazlar arasındaki temas, bulaşma kuvveti,

σ_1: (*sırasıyla* σ_2), virüsten koruma etkisinden kaynaklanan bulaştırıcı (*veya* çıkarılabilir) cihazların kurtarma hızı,

μ_1: ağa bağlı bilgisayarların ağ ile bağlantısının kesilme hızı ve

μ_2: çıkarılabilir cihazların ağ ile bağlantısının kesilme hızıdır.



Şekil 4.7. Zhu ve ark.'nın SIR modelinin bölmeleri arasındaki dinamiği temsil eden akış şeması [12].

Bu modelin, farklı bölmeler arasındaki akış şeması Şekil 4.7'de gösterilmektedir. Ayrıca bu model, bilgisayar virüsünün bilgisayarlar ve harici çıkarılabilir aygıtlar arasındaki etkileşimler yoluyla yayılmasını anlamak için geliştirilmiştir [12].

4.3. SONUÇ VE DEĞERLENDİRMELER

Bu bölümde, zararlı yazılımların ve yayılımlarının matematiksel olarak modellenmeleri kapsamlı olarak araştırılmış, incelenmiş ve sunulmuştur. Literatür incelendiğinde yapılan bu çalışma;

- Sunulan bu çalışmanın zararlı yazılım yayılımlarının matematiksel modelleri alanında güncel özellikle de geniş kapsamlı olarak incelenmesi bakımından önemlidir.
- Ulusal literatürde bu konunun yeterince çalışılmamış veya konuya gereken önemin verilmediğini göstermiştir.
- Zararlı yazılımların yapısı ve yayılım modelleri hakkında bilgi eksikliklerini gidermede ve ileride yapılabilecek araştırmalara veya çalışmalara ışık tutabilecek veya faydalı olabilecektir.
- Bundan sonraki süreçte virüslerle aktif olarak mücadele etmede önemli bir boşluğu dolduracaktır.
- Her ne kadar zararlı yazılımların ve yayılımlarının matematiksel model ve süreçlerin gözden geçirilmesi gibi konuları detaylı incelese de bu alanda geliştirilen başlıca yaklaşımları, bu modellerin avantaj ve dezavantajları da gözler önüne sermiş, dezavantajlar içinde çözüm önerileri sunmuştur.

İncelemeler sonucunda; zararlı yazılımların yayılmasını anlamak için önerilen modellerin çoğunun diferansiyel denklem sistemlerine dayandığı görülmektedir. Bunlar, matematiksel açıdan sağlam temellere sahip, dinamiklerinin temel özelliklerini ayrıntılı incelemesine imkân sağlayan tutarlı modeller oldukları için fazlaca tercih edildiği değerlendirilmektedir. Bu avantajlarına rağmen dikkate değer bazı dezavantajları öngörülebilmekte ve literatürde de bu öngörülere destekler nitelikte çıkarımlar [3], [5], [6], [9] mevcut olup bunlar ve bunlara çözüm önerileri aşağıda maddeler halinde verilmiştir:

Tespitler:

- Ağı oluşturan bilgisayarlar arasındaki yerel bulaşmalar hesaba katılmamaktadır.
- Parametre değerleri, ağın tüm öğeleri için genellikle sabit özellik göstermektedir.

- Zararlı yazılım yayılımı ağ yöneticisinin veya diğer kullanıcıların bireysel özelliklerinden etkilenmediği varsayılmaktadır.
- Zararlı yazılımın yayıldığı ağ öğelerin homojen bir şekilde dağıtıldığı ve hepsinin birbirine bağlı olduğu varsayılmaktadır.
- Diferansiyel denklemlere dayalı modellerde, ağdaki genel davranış hakkında iyi sonuçlar elde edebiliyorken ağdaki her cihazın bireysel davranışı eksik kalabilmektedir.
- Ağın her bir öğesinin ayrı dinamiğini modele yansıtılmamaktadır.

Öneriler:

- Sistemin her bir öğesinin bireysel özelliklerini tespit eden bireysel tabanlı ayrık modellerin kullanımıyla ağın her bir elemanının bireysel özellikleri ve nasıl iyileştirileceğine dair sonuçlar çıkarmak mümkün olabilecektir.
- Diferansiyel denklemlere dayalı modellerle gösterilen bu eksiklikler, ağa bağlı bilgisayarların veya cihazların her birinin bireysel özelliklerini hesaba katılarak giderilecektir.
- Ağ boyutu çok büyüdüğünde, gözlemlenen genel davranışın gerçekte olana benzerliğinin çok artacağı değerlendirilmektedir.
- Sunulan modellerin farklı ağ sistemleri üzerinde uygulamaları neticesinde elde edilecek verilerle hem modelin matematiksel olarak gelişimine katkı sunulabileceği hem de elde edilen sonuçlar ile ilgili personellerin karar verme süreçlerine destek sunulabileceği değerlendirilmektedir.
- Bu dezavantajlara sunulan öneriler ile ulaşılabilecek bireysel tabanlı alternatif yaklaşımlarda da aşılması gereken temel bazı sorunlar öngörülebilmektedir. Doğru bir modelleme yapılandırmak için sistemin tüm öğe bilgilerinin bilinmesi gereksinimi ve cihaz sayısının fazla olduğu ağ yapılarında hesaplama yapma maliyetinin çok yüksek olabilmesidir.

Konu ile genel değerlendirmelerim ise aşağıda sunulmuştur.

- Bilişim teknolojileri gelişim gösterdikçe neredeyse tüm iş ve işlemler bu teknolojiler ile hızlı ve kolay yapılır hale gelmektedir. Bunun so-

nucu olarak zararlı yazılımlarının ve yayılımlarının tehditleri, gerek sayı gerekse çeşitlilik açısından artış göstermektedir [13]. Bu konuda birçok önlem alınabilmekle birlikte bu önlemlerin yüksek fayda sağlaması için ilgili zararlı yazılımın yayılım dinamiklerinin bilinmesi oldukça önemlidir. Bu dinamikler bilinerek önlem tekniklerinin, yayılım davranışı ve sonuçlarının üzerindeki etkilerinin daha iyi gözlemleneceği değerlendirilmektedir. Bu yayılım dinamiklerini anlamaya, analizler yapmaya önem verilmez ise; zararlı yazılımların, kişisel / kurumsal veya yerel / küresel boyutlarda ciddi zararlara yol açıp ve büyük olumsuzluklara neden olabileceği belirtilmektedir [13].

- Yüz yıla yakın bir zamandır geliştirilmekte olan SIR modellerinin çözümleri bilgisayar teknolojisinin gelişmesiyle birlikte çok daha hızlı ve güvenilir bir şekilde yapılabilmektedir. Bu modelin hala güncelliğini koruduğunu söylenebilir. Özellikle Covid-19 salgını döneminde de çok yoğun olarak çalışılmış ve çalışılmaya devam etmektedir. Örneklendirmek gerekirse küresel salgının başlangıcından bugüne (bir yıldan biraz fazla bir zaman için) "SIR model" + "Covid 19" anahtar kelimeleri ile Google akademik veri tabanında yapılan aramada 5.420 sonuç çıkmaktadır. Zararlı yazılım yayılımı alanında da geliştirilen modifikasyon modelleri ve çalışma sayıları sıklıkla tercih edildiğini göstermektedir.
- Ülkemizde bu konuya akademik olarak önem verilmesi, daha çok çalışma yapılması, sadece zararlı yazılımlar veya virüsler için değil diğer tüm alanlarda da matematiksel modellerin oluşturulması ve paylaşılmasının hem bu ortamlardaki tehdit ve tehlikelerin daha iyi anlaşılması hem de bunlarla etkili mücadele edilmesi açısından da önem arz ettiğinden, bu konulara daha fazla önem verilmelidir.

KAYNAKLAR

[1]. Mishra B. K. ve Saini D. K. (2007). SEIRS epidemic model with delay for transmission of malicious objects in computer network. Applied Mathematics and Computation 2007; 188: 1476–1482.

[2]. Sun, C. ve Hsieh, Y. H. (2010). Global analysis of an SEIR model with varying population size and vaccination. Applied Mathematical Modelling, 34(10), 2685-2697.

[3]. Ren, J., Yang, X., Zhu, Q., Yang, L. X. ve Zhang, C. (2012). A novel computer virus model and its dynamics. Nonlinear Analysis: Real World Applications, 13(1), 376-384.

[4]. Peng, M., He, X., Huang, J. ve Dong, T. (2013). Modeling computer virus and its dynamics. Mathematical problems in Engineering, 2013.

[5]. Del Rey, A. M. (2015). Mathematical modeling of the propagation of malware: a review. Security and Communication Networks, 8(15), 2561-2579.

[6]. Piqueira, J. R. C. ve Araujo, V. O. (2009). A modified epidemiological model for computer viruses. Applied Mathematics and Computation, 213(2), 355-360.

[7]. Kermack, W. O. ve McKendrick, A. G. (1927). A contribution to the mathematical theory of epidemics. Proceedings of the royal society of london. Series A, Containing papers of a mathematical and physical character, 115(772), 700-721.

[8]. Akpınar, H. (2012). Bulaşıcı hastalıkların yayılımının tahmininde deterministik modellerin kullanılması. Öneri Dergisi, 10(38), 97-103.

[9]. Bilbay, H. (2015). SIR modellerin nümerik çözümleri üzerine. Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı. Doktora Tezi.

[10]. Mishra, B. K. ve Jha, N. (2010). SEIQRS model for the transmission of malicious objects in computer network. Applied Mathematical Modelling, 34(3), 710-715.

[11]. Mishra, B. K. ve Pandey, S. K. (2011). Dynamic model of worms with vertical transmission in computer network. Applied Mathematics and Computation, 217(21), 8438-8446.

[12]. Zhu, Q., Yang, X. ve Ren, J. (2012). Modeling and analysis of the spread of computer virus. Communications in Nonlinear Science and Numerical Simulation, 17(12), 5117-5124.

[13]. Canbek, G. ve Sağıroğlu, Ş. (2007). Kötücül ve casus yazılımlar: kapsamlı bir araştırma. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 22(1), 121-136.

Bölüm 5

KRİTİK ALTYAPILARDA SİBER GÜVENLİK VE SAVUNMA ÖNERİLERİ

Mehmet Yavuz Yağcı - Ebu Yusuf Güven
Sevda Altan - Muhammed Ali Aydın

Kritik altyapılar, insan hayatının her alanında kolaylık sağlamak için gerekli olan karayolları, köprüler, tüneller, demiryolları, kamu hizmetleri ve binaları birbirine bağlayan altyapılar olarak değerlendirilmektedir. Kritik altyapılar kaynak kısıtları ile zorlu fiziksel koşullarda çalışmak üzere kurgulanan bileşenlerden oluşmaktadır. Bu bileşenler zorlu koşullarda uzun yıllar boyunca kesintisiz çalışmak için tasarlanmıştır. Kritik altyapılarda tarihte meydana gelen kesintiler incelendiğinde operatör kaynaklı hatalar ve siber saldırıların ön planda olduğu görülmektedir. Kritik altyapıların aksaması ve durması ciddi ekonomik sorunlara ve can kayıplarına neden olabilmektedir. Kritik altyapılar, risk ve etki alanı açısından değerlendirildiğinde ülkelerin en kırılgan noktalarıdır. Yapılan araştırmalar ve analizler incelendiğinde ise saldırganların öncül hedefleri arasında kritik altyapıların olduğu açıktır. Siber tehditler, enerji üretim ve dağıtım sistemleri, finansal sistemler ve akıllı üretim hatları gibi bilgi sistemleri ile haberleşen kritik altyapılar üzerinde yoğunlaşmaktadır. Kritik altyapılara yönelik siber saldırıların sonuçlarının ciddiyeti yaşanan olaylarda görülmektedir. Uzun yıllar müdahale edilmeden çalışmak üzere tasarlanan kritik altyapılar üzerinde güncelleme ve geliştirme yapmak oldukça zor ve maliyetlidir. Mevcut altyapılar incelendiğinde kullanılan sistemlerin çıkan zafiyetlere karşı sahada yeterli güncelleme sıklığını yakalayamadığı görülmektedir.

Bu yüzden kritik altyapılarda bulunan güvenlik zafiyetleri dikkatle incelenmeli ve mevcut sistemlerde varlığı kontrol edilmelidir. Bu bölümde kritik altyapıları tanımak, olası güvenlik zafiyetlerinin analiz etmek ve olası tedbirler konusunda yapılması gereken çalışmalar üzerinde durulmuş, kritik altyapılar açıklanmış, sıklıkla görülen güvenlik risk senaryoları verilmiş, bilinmesi, yapılması ve alınması gereken önlemler ve sıkılaştırma tedbirleri açıklanmıştır ve sonuçta bölüm değerlendirmesi sunulmuştur.

5.1. GİRİŞ

Gelişen teknoloji ile önemli bir konu haline gelen nesnelerin interneti kavramı sayesinde günlük kullanılan eşyaların akıllanması sağlanmaktadır. Karşılıklı iletişim kurabilen nesneler bu kavramın temelini oluşturmakta ve günlük yaşamda kendine yer edinen akıllı evler, akıllı şehirler ve Endüstri 4.0 konunun en önemli örneklerindendir [1]. Nesnelerin internetinin (IoT) üretim endüstrisine uygulanmış formu Endüstriyel Nesnelerin İnterneti (IIoT) olarak tanımlanmaktadır [2]. Sensörler, robot aksamlar, kontrol sistemleri ile üretim ve tedarik zincirinin izlenmesi ve otomatik olarak yönetilmesine olanak tanıyan IIoT, fabrikalar için bir maliyet olarak nitelendirilmiş olsa da bu sistemde internete bağlanmış olan ve üretim zincirinde bulunan herhangi bir nesne yapması gereken işe diğer nesneler ile iletişim kurarak karar verebilmektedir. Büyük resimde ise bu durum fabrikalara sistem bağlantısı, verimlilik, ölçeklenebilirlik, zaman ve maliyet tasarrufu olarak yansımaktadır [3].

Kritik altyapılar; ulusal güvenlik, halk sağlığı ve güvenliği, ekonomi ve kamu güvenliği için hayati önem taşıyan altyapı ve varlıklar olarak tanımlanan bir organizasyon veya toplumun hayatta kalabilmesi, toplum düzeninin sorunsuz işlemesi için gerekli olan birbirlerine bağımlılıkları bulunan temel sistemleri ifade etmektedir.

Bilgi güvenliği açısından kritik altyapı kavramı; akıllı şehirler, akıllı fabrikalar, nükleer ve kimyasal tesisler, enerji üretim ve dağıtım sistemleri ile sağlık ve finans sektörlerinde bulunan güvenlik problemlerini kapsamaktadır. Ne yazık ki, kritik altyapılarda kapsama problemi, haberleşme sorunu, kısıtlı veri işleme kabiliyeti, uzaktan erişim gereksinimleri gibi olumsuz durumlar bulunmaktadır. Mevcut olumsuzluklar yapının haberleşme yeteneklerinin iyi-

leştirmesine dayalı çözümler ile giderilmeye çalışılmaktadır. Günümüzde Bilgi Teknolojilerinde kullanılan bağlantı ve internet teknolojileri uzak mesafe bağlantılarına çözüm olarak kullanılmaktadır. Gelişen teknoloji trendinde ise IoT teknolojisini kullanan kritik altyapılar birçok bağlantı ve saha problemine çözüm sunmuştur. IoT teknolojisini temel alan kritik altyapılar, sahadan bilgi toplama amacıyla mevcut IoT sensörlerini kullanabildiği gibi var olan IoT haberleşme altyapısını da kullanarak kapsama alanını iyileştirmektedir. Mevcut kritik altyapıların çoğunluğu internetten izole bir şekilde kapalı ağ içerisinde veri aktarımı yapmaktadır. Kapalı ağ yapısı ile sahadan toplanan veriler, kapalı ağ yapısı ile BT sistemlerine taşınmakta ve ardından izleme, raporlama gibi iş geliştirme süreçleri yürütülmektedir.

Kritik altyapılarda halihazırda uygulanan ve gelecekte uygulanması planlanan entegrasyonlar; kararlarını kendi alan, insansız üretim yapabilen, üretim hatlarının akıllanmasına dayalı olan Endüstri 4.0 vizyonunu ortaya çıkarmıştır. İlgi odağı haline gelen Endüstri 4.0 yaklaşımının gerçekleştirilebilmesi ise kritik altyapılarda kullanılan SCADA (Supervisory Control and Data Acquisition) sistemlerinin, IoT ve bulut yapıları ile entegre olmasına dayanmaktadır. Yeni teknolojilere entegre olan SCADA sistemleri üretici ve kullanıcı bazlı problemlerin çözülmesine olanak sağlayacaktır. Endüstri 4.0 yaklaşımının çekiciliği ışığında SCADA sistemlerinin IoT ve bulut bilişim teknolojileri ile entegrasyonu üreticiler, aktif kullanıcılar ve araştırmacılar açısından gelecek vadeden çalışma konuları arasındadır.

Kritik altyapılarda lokal ve uzak sahalar için gerçekleştirilen izleme ve kontrol işlemleri için altyapı olarak SCADA sistemleri kullanılmaktadır. SCADA; üretim tesisi ya da fabrika gibi herhangi bir kritik altyapıda sisteme erişim izni olan bir operatörün uzaktan ayar noktası değişikliklerinin yapılmasına, vana veya anahtarların durumunun değiştirilmesine, alarm izlenmesine ve ölçüm verilerinin toplanmasına izin veren bir sistemdir. Bilgisayar bilimlerinin bakış açısına göre SCADA, dünyadaki fiziksel işlemlerin bilgisayarların hesap yeteneği ile birleştirilmiş sistemlerdir. Otomasyon teknolojisi bakış açısına göre SCADA, kontrol edilmek istenen sisteme göre özelleştirilmiş işlemler barındıran fiziksel çevredeki yapılarla haberleşebilen ve hesaplamalar yapabilen sistemlerdir.

SCADA sistemleri farklı operasyonel alanlarda kullanımına bakılmaksızın temel olarak 4 katmanda incelenmektedir [4]. Mimarinin en alt katmanında sistemin dünya ile fiziksel etkileşimini sağlayan sensörler ve sürücüler bulunmaktadır. Sahada gerçekleşen veya gerçekleşmesi istenen fiziksel olaylar bu alet veya araçlarla izlenebilmekte veya tetiklenebilmektedir. Sensörlerin ve sürücülerin analog veya dijital sinyallerle üst katmana bilgi aktarımı yaptığı ortama kontrol ağı adı verilmektedir. Üst katmanda üretilen kontrol bilgileri ve sahadan toplanan veriler kontrol ağı üzerinden iletilmektedir.

En alt katmanda bulunan devre elemanları ile en üst katmanda bulunan bilgisayar sistemleri birbirlerini doğrudan tanıyan ve iletişim kuran özellikler içermemektedir. İkinci katmanda farklı protokol kullanımı, hesaplama ve haberleşme yeteneği farklılıkları gibi ürün karakteristiklerinden dolayı birbiri ile uyumsuz cihazları haberleştiren ek bileşenler konumlandırılmaktadır. Bu ek bileşenler, farklı haberleşme ortamlarını ve protokolleri destekleyen yetenekleri sayesinde üst katmandaki farklılıklara rağmen alt katmandaki cihazlar için iletişim kurabildiği kontrol sinyallerini üretebilmektedir. Böylece kontrol katmanında bulunan cihaz farklılıkları, süreç ağındaki haberleşme ortamı ve protokol farklılıkları gibi durumlar sistemin genelini etkilememektedir. İkinci katmanda genellikle Uzak Terminal Birimi (Remote Terminal Unit - RTU) ve Programlanabilir Mantık Denetleyici (Programmable Logic Controllers -PLC) gibi saha cihazları bulunmaktadır. RTU, sahadaki dijital veya analog parametreleri okuyup, merkezi izleme birimine aktarma işleminden sorumlu saha cihazıdır. PLC ise, yüksek sıcaklık, titreşim, toz gibi zor koşullara karşı dayanıklı olarak üretilmiş kontrol sistemlerine uyarlanmış kısıtlı hesaplama gücüne sahip endüstriyel amaçlı programlanabilir cihazdır.

İkinci katmandaki cihazlarda düzenlenen ve anlamlandırılan verilerin kontrol merkezine gönderilmesi için süreç ağı katmanı kullanılmaktadır. Süreç ağı fiziksel ortam koşullarına bağlı olarak farklı haberleşme ortamlarını ve protokollerini kullanarak bilgisayar sistemleri ile saha cihazları arasındaki iletişimi sağlamaktadır. SCADA sistemlerinin bilgisayar ağlarıyla kullanılmaya başlamasıyla süreç ağında yerel ağ ve geniş ağ bağlantıları kullanıl-

maya başlanmıştır. Kurulan ağ yapısına ve uzaklığına bağlı olarak kullanılan haberleşme ortamı değişmektedir. Süreç ağı katmanında kullanılan protokoller kullanılan saha cihazına ve kontrol merkezindeki yazılıma bağlı olarak değişiklik gösterebilmektedir. Üreticilerin çoğu geleneksel haberleşme protokollerini baz alarak endüstriyel cihazlarına ait kendi protokollerini geliştirmişlerdir. Bu nedenle farklı üreticilerden alınan cihazların bir arada kullanıldığı SCADA sistemlerini kurmak ve sisteme farklı saha cihazları eklemek zordur.

Sahada yürütülen operasyonun izlenmesi, kontrol edilmesi ve raporlanması işlemlerinde ihtiyaç duyulan bilgi sistemleri en üst katmanda bulunmaktadır. Bilgi sistemlerinin bulunduğu bu katmanda, süreç ağı üzerinden sahadaki cihazlar ile haberleşen sunucu ve donanımsal kontrol bileşenleri mevcuttur. İnsan Makine Arayüzü (Human Machine Interface – HMI) saha ekipmanlarının izlenmesi ve kontrolünde operatörün kullandığı grafiksel arayüzdür. Grafiksel arayüz, bilgisayar üzerinde çalışan bir program veya donanımsal bileşen olarak tasarlanmaktadır. Bu nedenle bilgisayar ağ yapısı ve işletim sistemi kaynaklı hata ve zafiyetleri içerisinde barındırmaktadır.

Kullanılan eski SCADA sistemlerinin izole ağlarda çalışması kritik altyapıları internete bağlı tehditlerden uzak tutmaktayken raporlama ve iş geliştirme süreçleri nedeniyle internet ve kurumsal ağla ile bağlantıları dikkate alınması gereken önemli güvenlik problemlerini oluşturmaktadır. Aslında bir nevi kritik altyapıların güvenliğinin sağlanması SCADA sistemlerini korumaktan geçmektedir. Bu yüzden SCADA sistemlerinin güvenlik zafiyetlerinin araştırılması ve zafiyetlerin giderilmesi kritik altyapıların siber güvenliği konusunda önem arz etmektedir.

SCADA güvenliği, milyonlarca insana elektrik, su, doğal gaz, ulaşım gibi temel hizmet ulaşımının otomatik kontrolünü ve uzaktan yönetimini sağlamaktan sorumlu endüstriyel alanlardaki denetleyici ve veri toplama ağlarını koruma uygulamasıdır. Korunmak istenen ağlar, ülke kritik altyapılarının tamamını ya da bir bölümünü çok kısa sürede çökertebilecek ve güvelik koruması yapılmadığı takdirde korkunç sonuçlara sebep olabilecek siber saldırıların tehdidi altında bulunmaktadır [5].

Bunların yanında SCADA sistemlerinin kuruluşlar için oldukça maliyetli olmasından ötürü bahsedilen harici saldırı ya da dahili hataların neden olabileceği kesintilerin önüne geçilmesi hem kuruluş hem de hizmetten faydalanan ülke ve insanlar adına SCADA sistemlerine yönelik güvenlik önlemlerinin alınması gerekmektedir [6]. Kullanılan eski SCADA sistemlerinin izole ağlarda çalışması kritik altyapıları internete üzerinden gelebilecek tehditlerden uzak tutmaktayken raporlama ve iş geliştirme süreçleri nedeniyle internet ve kurumsal ağla ile bağlantıları dikkate alınması gereken önemli güvenlik problemlerini oluşturmaktadır. Aslında bir nevi kritik altyapıların güvenliğinin sağlanması SCADA sistemlerini korumaktan geçmektedir. Bu yüzden SCADA sistemlerinin güvenlik zafiyetlerinin araştırılması ve zafiyetlerin giderilmesi kritik altyapıların siber güvenliği konusunda önem arz etmektedir. Kritik altyapıların siber güvenliği milyonlarca insana elektrik, su, doğal gaz, ulaşım gibi temel hizmet ulaşımının otomatik kontrolünü ve uzaktan yönetimini sağlamaktan sorumlu denetleyici ve veri toplama ağlarını koruma uygulamasıdır.

Kritik altyapılardan beklenen; aksamalar olmadan, müdahale gerektirmeden, optimum performans ile kararlı bir biçimde uzun yıllar çalışmaya devam etmesidir. Kritik altyapılarda meydana gelen aksaklıklar; anlık gelişen arızalar, siber saldırılar ve planlı bakım çalışmalarından kaynaklı olmaktadır. Anlık arızalar ve siber saldırılar gibi plansız gelişen olaylar karşısında hizmet kesintileri oluşmaktadır. Arızaların giderilmesi siber saldırılara göre daha kolay olduğu için sistemin işleyişe dönmesi daha hızlı olmaktadır. Kritik altyapıları iç ve dış siber tehditlerin neden olabileceği siber saldırılardan korumak hem kuruluş hem de hizmetten faydalanan ülke ve halk için ciddi önem arz etmektedir.

Geçmişten günümüze bu alanda yaşanmış olumsuz durumlar kritik altyapılardaki güvenlik zafiyetlerinin oluşturabileceği sonuçların ciddiyetini ve güvenlik problemlerinin önüne geçilmesi gerektiğini vurgulamaktadır. Örneğin; kritik altyapılara yönelik yapılan siber saldırıların en çarpıcı örneği olan Stuxnet zararlısı, İran'ın nükleer santrallerini hedef alarak nükleer programın durdurulmasını hedef almıştır. Kullanılan santrifüj cihazlarının dönüş hızını etkilemesi ve ana kontrol ekranında bunun izlenmesini engellemesi ile ciddi bir atak vektörü oluşturmuştur. 2021 yılı içerisinde ABD'nin Florida eyaletin-

de içme suyu arıtma tesisinde yaşanan bir diğer olayda ise kısa vadede görme kayıpları ve uzun vadede insan yaşamına son verme ihtimali bulunan kimyasal maddenin içme suyu içerisindeki oranı 100 kat arttırılmıştır [7]. Toplum sağlığı üzerinde ciddi rahatsızlıklara yol açabilecek bu saldırı son anda teknisyen tarafından fark edilmiş ve içme suyunun halka ulaşması engellenmiştir. Her zaman bu kadar şanslı olunamayacağı göz önüne alınırsa eğer kritik altyapıları hedef alan siber saldırıların yoğunlaşılması gereken önemli bir konu ve araştırma alanı olduğu açıktır.

5.2. KRİTİK ALTYAPILARIN KARAKTERİSTİK ÖZELLİKLERİ

Kritik altyapılar, çeşitli endüstriyel sektörler arasında var olan karşılıklı bağımlılıkların yanı sıra diğer sistemler ile arasındaki bağlantılar nedeniyle genellikle "sistemlerin sistemi" olarak anılmaktadır [8]. Kritik altyapılarda meydana gelen olaylar, kademeli ve artan aksaklıklara neden olarak bağlı bulunduğu diğer sistemleri doğrudan ve dolaylı olarak etkileyebilmektedir. Kritik altyapılarda meydana gelebilecek aksamalara en iyi örnek enerji iletim ve dağıtım sistemlerinde görülmektedir. Hem elektrik enerjisi iletimi hem de dağıtım şebekesi endüstrileri, son kullanıcılara elektrik sağlamak amacıyla binlerce kamu ve özel elektrik üreticisi ile birlikte çalışmaktadır [9]. Yüksek miktarda ve düzeyde birbirine bağlı ve dinamik sistemleri çalıştırmak için coğrafi olarak dağıtılmış SCADA kontrol teknolojileri kullanılmaktadır. Bazı SCADA sistemleri, merkezi bir konumdan coğrafi olarak uzak saha kontrol istasyonlarından veri toplayarak ve bunlara komutlar vererek elektrik dağıtımını izlemekte ve kontrol etmektedir. Kritik altyapıların en yaygın bozulma kaynaklarından birinin elektrik şebekeleri olduğu düşünülmektedir [10].

Örnek olarak, bir elektrik güç iletimi SCADA sistemi için kullanılan iletişim ağının kesilmesiyle kademeli bir arıza başlatılabilir [6]. İzleme ve kontrol yeteneklerinin olmaması, büyük bir üretim biriminin devre dışı kalmasına neden olabilir, bu da bir iletim trafo merkezinde güç kaybına yol açabilecek bir olaydır[11]. Bu kayıp, büyük bir dengesizliğe neden olabilir ve güç şebekesinde kademeli bir arızayı tetikleyebilir [11]. SCADA sistemleri ayrıca boru hatları, gemiler, kamyonlar ve raylı sistemler dahil olmak üzere su, petrol ve doğal

gaz dağıtımını ve ayrıca atık su toplama sistemlerini izlemek ve kontrol etmek için kullanılmaktadır. Güç şebekelerinde meydana gelebilecek aksaklıklar, petrol ve doğal gaz üretimini, rafineri operasyonlarını, su arıtma sistemlerini, atık su toplama sistemlerini ve elektrik enerjisi için şebekeye dayanan boru hattı taşıma sistemlerini potansiyel olarak etkileyebilecek geniş alan kesintilerine neden olabilmektedir [13].

Tipik bir SCADA sisteminde, katmanlı ağ mimarileri üzerinde bir dizi ağ protokolü kullanılarak oluşturulmuş çok sayıda kontrol döngüsü, insan arabirimi ve uzaktan tanılama ile bakım aracı içermektedir. Bir kontrol döngüsü, bazı kontrollü prosesleri manipüle etmek için sensörler, aktüatörler ve kontrolörler (örneğin PLC'ler) kullanmaktadır. Sensör, bazı fiziksel özelliklerin ölçümünü üreten ve ardından bu bilgiyi kontrol edilen değişkenler olarak kontrolöre gönderen bir cihazdır. Kontrolör, sinyalleri yorumlar ve bir kontrol algoritmasına ve aktüatörlere ilettiği hedef ayar noktalarına dayalı olarak ilgili manipüle edilmiş değişkenleri üretmektedir. Kontrol valfleri, kesiciler, anahtarlar ve motorlar gibi aktüatörler, kontrolörden gelen komutlara dayalı olarak kontrol edilen süreci doğrudan yönlendirmek için kullanılmaktadır.

Operatörler ve mühendisler; ayar noktalarını izlemek ve yapılandırmak, algoritmaları kontrol etmek, kontrol cihazında bulunan parametreleri ayarlamak ve kurmak için insan arayüzlerini kullanmaktadır. İnsan arayüzü ayrıca süreç durumu bilgilerini ve geçmiş bilgileri de görüntülemektedir. Anormal çalışma durumu veya arızaları önlemek, tanımlamak ve bunlardan kurtulmak için tanılama ve bakım yardımcı programları kullanılmaktadır [13]. HMI tarafından da müdahale edilebilen kontrol döngüleri iç içe veya basamaklı olarak çalışabilmektedir. Bu sayede bir döngü için ayar noktası, başka bir döngü tarafından belirlenen süreç değişkenine dayanmaktadır. Denetim düzeyindeki döngüler ve alt düzey döngüler, milisaniyeler ile dakikalar arasında değişen döngü süreleri ile bir süreç boyunca sürekli olarak çalışmaktadır.

Kritik altyapılarda kullanılan SCADA, DCS, PLC gibi birçok alt sistem tanıtılırken kullanım senaryoları ve aksamaların peş peşe dağılımları örnekler üzerinden paylaşılmıştır. Paylaşılan örneklerde kritik altyapılardaki genel özellikleri ortaya koymaktadır. Kritik altyapıları kontrol, iletişim, güvenilirlik

ve yedekleme özelliklerine göre farklı karakteristik özellikler barındırmaktadır. Bunlar aşağıda kısaca açıklanmıştır.

- **Kontrol Zamanlaması Gereksinimleri:** Kritik altyapılarda çalışan işlemler; çok yüksek hız, tutarlılık, düzenlilik ve senkronizasyon dahil olmak üzere çok çeşitli zamanla ilgili gereksinimlere sahiptir. İnsanlar bu gereksinimleri güvenilir ve tutarlı bir şekilde karşılayamayabilir bu nedenle otomatik olarak görevleri yerine getiren yapılara ihtiyaç duyulmaktadır. Bazı sistemler, iletişim gecikmesini azaltmak ve gerekli kontrol işlemlerini zamanında gerçekleştirmek için hesaplamanın sensöre ve aktüatörlere mümkün olduğunca yakın yapılmasını gerektirebilmektedir.
- **Coğrafi Dağılım:** Kontrol ihtiyacı bulunan sistemler, küçük bir sistemden (tek PLC ile yürütülebilen yerel kontrol süreçleri), geniş alana yayılmış büyük çaplı sistemlere (örneğin, petrol boru hatları, elektrik güç şebekesi) kadar değişen derecelerde dağıtıma sahiptir. Daha büyük dağıtım tipik olarak geniş alan ağları ve mobil iletişim ihtiyacını ifade etmektedir.
- **Hiyerarşi**: Denetleyici kontrol mekanizmaları sistemin mevcut durumuna dayalı kontrol kararlarını desteklemek için birden fazla konumdan veri toplayabilen merkezi bir konumdur. Sistemi izleyen ve kontrol eden operatörlere tüm sistemin kapsamlı bir görünümünü sağlamak için genellikle hiyerarşik/merkezi bir kontrol kullanmaktadır.
- **Kontrol Karmaşıklığı:** Genellikle kontrol işlevleri basit kontrolcüler ve belirli kriterlere göre ayarlanmış algoritmalar tarafından gerçekleştirilebilir. Fakat daha karmaşık sistemler insan tarafından kontrol işlevlerine müdahale edilmesini gerektirmektedir.
- **Kullanılabilirlik:** Sistemin kullanılabilirlik gereksinimleri de tasarımda önemli bir faktördür. Güçlü kullanılabilirlik/çalışma süresi gereksinimleri olan sistemler, tüm iletişim ve kontrol genelinde daha fazla yedek veya alternatif uygulamalar gerektirebilmektedir.
- **Başarısızlıkların Etkisi:** Bir kontrol fonksiyonunun başarısızlığı, etki alanları arasında önemli ölçüde farklı etkilere neden olabilir.

Daha büyük etkiye sahip sistemler, genellikle fazlalık kontroller aracılığıyla operasyonlara devam etme veya bozulmuş bir durumda çalışma becerisi gerektirmektedir.

- **Emniyet:** Sistemin güvenlik gereksinimleri alanı da tasarımda önemli bir faktördür. Sistemler, güvenli olmayan koşulları algılayabilmeli ve güvenli olmayan koşulları güvenli koşullara indirgemek için eylemleri tetikleyebilmelidir. Güvenlik açısından kritik operasyonların çoğunda, insan gözetimi ve potansiyel olarak tehlikeli bir sürecin kontrolü güvenlik sisteminin önemli bir parçasıdır.

5.3. KRİTİK ALTYAPI SEKTÖRLERİ VE UYGULAMALARI

Kritik altyapıların bir ulusun güvenliğiyle yakından ilişkisi olduğu düşünüldüğünde, her ulusun öncelikleri kendi kritik altyapılarını değişiklik gösterebilmektedir. ABD'de yürürlüğe giren Vatanseverlik Yasası ile kritik altyapılarına göre kavramı "Amerika Birleşik Devletleri için o kadar hayati olan fiziksel veya sanal sistemler ve varlıklar ki, bu tür sistemlerin ve varlıkların yetersizliği veya yok edilmesi güvenlik, ulusal ekonomik güvenlik, ulusal halk sağlığı veya güvenliği veya bu konuların herhangi bir bileşimi üzerinde zayıflatıcı bir etkiye sahip olacaktır." şeklinde tanımlanmıştır [1]. NIST (National Institute of Standards and Technology) Siber Güvenlik Platformu (Cybersecurity Framework), Amerika için başlangıçta 14 kritik altyapı belirlenmiş daha sonra da bunu ulusal altyapı koruma planında 16'ya genişletmiştir. Ayrıca NIST tarafından yayınlanan siber güvenlik platformu ile siber güvenlik odaklarının öncelikle bilgi teknolojisi (BT), endüstriyel kontrol sistemleri (EKS), siber-fiziksel sistemler veya daha genel olarak Nesnelerin İnterneti de dahil olmak üzere bağlı cihazlar olup olmadığına bakılmaksızın siber güvenlik odağı haline getirmeye çalışmıştır [35]. Avrupa Birliği tarafında 9 sektör kritik altyapı olarak belirlenmiştir. İngiltere ise toplamda 9 sektörü alt sektörleriyle birlikte ele almıştır [37]. Tablo 5.1'de ABD ve Avrupa Birliği kritik altyapı sektörleri ve uygulamaları yer almaktadır.

Tablo 5.1. Ülkelere göre kritik altyapıları ve uygulamaları

ABD - Ulusal Altyapı Koruma Planı	**ABD - NIST**	**Avrupa Birliği**	**Türkiye**	**Uygulama**
Gıda ve Tarım	Tarım ve Gıda	Gıda		- Gıda temini ve gıda güvenliği ve güvenliğinin sağlanması
Su ve atık su sistemleri	Su	Su	Su Yönetimi	- İçme suyu temini - Su kalitesinin kontrolü - Su miktarının ayarlanması ve kontrolü
Sağlık ve Halk Sağlığı	Halk Sağlığı	Sağlık		- Tıbbi ve hastane bakımı - İlaçlar, serumlar, aşılar ve farmasötikler - Biyo-laboratuvarlar ve biyo-ajanlar
Acil Servisler	Acil Servisler			
Devlet Tesisleri	Hükümet	Kamu Düzeni ve Yasal Düzen ve Güvenlik	Kritik Kamu Hizmetleri	- Kamu ve hukuk düzenini, emniyetini ve güvenliği hizmetleri - Adalet ve gözaltı yönetimi hizmetleri - Devlet işlevleri - Silahlı Kuvvetler - Sivil yönetim hizmetleri - Acil servisler - Posta ve kurye hizmetleri
	Ulusal anıtlar ve simgeler			
Savunma Sanayi	Savunma Sanayi			
Bilgi Teknolojisi	Bilgi ve Telekomünikasyon	Bilgi, İletişim Teknolojileri	Elektronik Haberleşme	- Bilgi sistemi ve ağ koruması - Enstrümantasyon otomasyon ve kontrol sistemleri (SCADA vb.) - İnternet - Sabit telekomünikasyon sağlanması - Mobil telekomünikasyon sağlanması - Radyo iletişimi ve navigasyon - Uydu iletişimi - Yayın
İletişim	Posta			

Enerji Barajlar	Enerji	Enerji	Enerji	- Boru hatları dahil olmak üzere petrol ve gaz üretimi, arıtma, arıtma ve depolama - Elektrik üretimi - Elektrik, gaz ve petrol iletimi - Elektrik, gaz ve petrol dağıtımı
Ulaşım sistemleri	Ulaştırma ve Denizcilik	Ulaştırma	Ulaştırma	- Karayolu taşımacılığı - Demiryolu taşımacılığı - Hava trafiği - İç su yolları taşımacılığı - Okyanus ve kısa deniz taşımacılığı
Finansal hizmetler Kritik Üretim Ticari Tesisler	Bankacılık ve Finans Kritik Üretim	Finans	Bankacılık ve Finans	- Ödeme hizmetleri/ödeme yapıları (özel) - Devlet mali görevi - Özel/Kamu Üretim Altyapıları
Kimyasal Nükleer reaktörler, malzemeler ve atık	Kimya Sanayi ve Tehlikeli Maddeler	Kimya ve nükleer sanayi		- Kimyasal ve nükleer maddelerin üretimi ve depolanması ve işlenmesi - Tehlikeli madde boru hatları (kimyasal maddeler)
-	-	Uzay ve Araştırma		- Uzay Araştırmaları Tesisleri - Uzay Fırlatma Üsleri - Gözlem Üsleri

Kritik altyapıların büyük çoğunluğu bilgi teknolojileri ile entegre olmuştur [37]. Farklı sistemler birbirleriyle bağımlı ve bağlantılı hareket etmekte, dolayısıyla bir tanesine olan siber saldırı, bütün bir sistemi etkileme risklerini ortaya çıkarmıştır [37]. Kritik altyapı hizmetleri servis sağlayıcıları, dünyanın her yerinde zararlı yazılım bulaşmış IoT cihazları yoluyla saldırıya uğrayabilmekte, hizmet kesintileri can ve mal güvenliğini tehlikeye atabilmektedir [36]. Kritik altyapıların bilgi teknolojilerine sızmak ve uzun süre gizlenerek gerektiğinde sistemi bozmak üzerine tasarlanmış zararlı yazılımlar da kritik altyapılar için ciddi tehditler arasında yer almaktadır. Bu sebeple kritik altyapılarda siber güvenlik risklerinin yönetilmesi; insanları, süreçleri, araçları, yazılımlar vb. her türlü parçayı da bir güvenlik unsuru olarak düşünerek sağlanabilmektedir [37].

5.4. KRİTİK ALTYAPILARDA YAŞANAN OLAYLAR

Kritik altyapılarda meydana gelebilecek saldırı veya aksaklıkların sonucunda yıkıcı etkiler ortaya çıkabilmektedir. Kritik altyapılar ülkeler için güvenliği sağlanması gereken alanların başında yer almaktadır. Kritik altyapılarda meydana gelebilecek olayları tahmin edebilmek ve sonuçlarını yorumlayabilmek için geçmişte yaşanan olayları incelemek gerekmektedir.

5.4.1. Maroochy Su Sistemi (2000)

Mart 2000'de Queensland'daki Maroochy Shire'da, atık su sistemlerine bir saldırı yapılmıştır. Radyo frekansları üzerinden haberleşmekte olan atık su pompa istasyonları, belirli bir süre sonra istasyonlar arası bağlantıyı sağlayamamıştır. Bağlantının kaybı sonrasında pompalar planlandığı gibi çalışmamış, alarmlar devre dışı kalmış ve sorunun yaşandığı ilk aşamalarda problemin sistem geçişinden dolayı olabileceği ihtimaline odaklanılmış olsa da bir süre sonra sistemin siber saldırıya uğradığı fark edilmiştir. Siber saldırının dizüstü bilgisayar ve radyo vericisi kullanılarak haberleşme ağına sızılması ile olduğu ve 150 pompa istasyonunun bu durumdan etkilendiği görülmüştür. Bu saldırı, yaklaşık üç ay boyunca bir milyon litreye yakın atık suyun arıtılamaması gibi bir çevre problemine neden olmuştur.

5.4.2. Davis-Besse Nükleer Santrali (2003)

Ocak 2003'te SQL Slammer solucanı, Ohio'nun nükleer santraline bulaşmıştır. Sistemde yayılan solucan operatörlerin sisteme yaklaşık 5 saat boyunca müdahale edebilmesini engellediği rapor edilmiştir. Sistemin eski haline dönmesi ve sürecin yeniden başlatılması 6 saatten fazla süre almıştır. 2000 yıllarında siber güvenlik bilincinin düşük olması ve saldırıların popüler olmaması nedeniyle sistemlerin günümüzden daha savunmasız olduğu bu örnekte görülmüştür. Etkili bir yayılım politikası izleyen Slammer solucanı, savunmasız sistemlerin %90'ına 5 dakika içerisinde bulaşmayı başarabilmiş bir zararlı yazılım örneğidir.

5.4.3. Taum Sauk Hidroelektrik Santrali (2005)

2005 yılında Amerika'da bulunan Taum Sauk hidroelektrik santralinde meydana gelen olay saldırı sonucunda değil, işleyişte meydana gelen bir aksaklık sonucunda olmuştur. Depo doluluğunu ölçen sensörden meydana gelen bir arıza sonucunda depo dolduktan sonra 5 dakika boyunca suyun pompalanmaya devam ettiği belirtilmiştir. Bunun sonucunda depo yüzeyince çökme olmuş ve büyük miktarda su beklenmedik şekilde salınmıştır. Taşan baraj 4 mil çevresindeki tarım arazisinde maddi zarara neden olmuştur.

5.4.5. Tehama Colusa Kanal Kurumu (TCCA) Saldırısı (2007)

Küçük bir California kanal sisteminde eski çalışanın sabotajı sonucunda aksama yaşanmıştır. 17 yıllık şirket çalışanı görevden alınmasına tepki olarak görevden alındığı gün SCADA sisteminin merkezi kontrol sunucusuna yetkisiz bir yazılım yüklemiştir. Personelin içerden yaptığı bu tipte ataklar güvenlik önlemleri alınmış ve ağdan yalıtılmış sistemler olmasına rağmen tespit etmesi ve engellemesi en zor atak tipidir.

5.4.6. Aurora Jeneratörü (2007)

2007 yılında Idaho Ulusal Laboratuvarında "Aurora" isimli siber saldırı ile elektrik şebekelerinin fiziksel bileşenlerinin tahrip edilebileceği gösterilmiştir. Elektrik üretimi için dizel motorlu bir jeneratör Modbus protokolü ile haberleşen kontrol ağı üzerinden kontrol edilmektedir. Saldırgan kontrol ağına erişim sağladıktan sonra, kötü amaçlı yazılımı kontrol merkezine enjekte etmiştir. Kötü amaçlı yazılım, jeneratörün şebeke bağlantısını hızlı bir şekilde açıp kapatarak jeneratörün patlamasına sebep olmuştur.

5.4.7. Ahack Solucanı ile Çelik Fabrikası Enfeksiyonu (2008)

2008 yılında Brezilya'da, internet üzerinden bir çelik fabrikasına giren eski bir yüklenici, şirketin enerji ve yüksek fırın fabrikasında Ahack adında bir solucan yayılmasına neden olmuştur. Otomasyon ağına yayılan solucan finansal kayıplara sebep olmuş, otomasyon ağına yayılmış, sahada bulunan PLC'ler

ile izleme istasyonları arasındaki iletişimi bozarak mali kayıplara neden olmuştur. Ağda istenmeyen paketleri fazla sayıda dolaşması ile SCADA sisteminde hizmet aksaması oluşmuştur.

5.4.8. Bakü-Tiflis-Ceyhan Boru Hattı (2008)

2008 yılında Türkiye'de doğalgaz boru hattında patlama meydana gelmiştir. Saldırganlar kablosuz güvenlik kameralarında bulunan zafiyeti sömürerek ağa dahil olmuştur. Dahil olunan kamera ağından kontrol ağına sızan saldırganlar saha elemanlarına ulaşmışlardır. Sahada meydana gelen sızıntı ve hatalara karşı bulunan alarm sistemleri devre dışı bırakılmıştır. Boru hattındaki basıncın arttırılması sonucunda patlama meydana gelmiştir. Alarmların devre dışı bırakılması sebebiyle patlama, alevlerin görülmesiyle fark edilmiştir.

5.4.9. Gürcistan Nükleer Enerji Santrali (2008)

2008 yılında Gürcistan'da bulunan nükleer enerji santrali 48 saat içerisinde acil kapanmaya zorlanmıştır. Kontrol amaçlı şirket ağında kullanılan bilgisayarda gerçekleşen yazılım güncellenmesinden sonra bilgisayar yeniden başlatılmıştır. Bilgisayar yeniden başlatıldığında başlangıç parametreleri ile sistemi kontrol etmeye çalıştığından dolayı emniyet sistemi devreye girmiş ve reaktörü kapatmıştır.

5.4.10. İran Nükleer Tesislerine Stuxnet Saldırısı (2010)

2010 yılında İran'da bulunan nükleer santral "Stuxnet" isimli bilgisayar solucanından etkilenmiştir. Stuxnet'in amacı PLC içerisindeki programı değiştirerek saldırganın istediği davranışları santrifüj cihazlarına yaptırırken sistem operatöründen sahada meydana gelen değişiklikleri gizlemektir [40]. Virüs Windows işletim sistemine sahip bilgisayarlarda bilinen sertifikalar üzerinden kendine ait sertifikayı yüklemektedir. Yerel ağda yayılırken kendini gizlemek için 4 adet sıfırıncı gün açığını kullanmaktadır. Stuxnet, Windows sistemlerinde ikili dosyalarını gizlemek için rootkit kodunu içermekte ve gerçek sistemler sınırların üzerinde çalışsa da izleme yazılımına kabul edilebilir değerler sunmak için PLC kodunu değiştirmektedir. Ayrıca, tespit edilmekten

kaçınmak ve sürücülerini imzalamak için iki sınırlı dijital sertifikalar kullanılmıştır. Bilinen uç nokta güvenlik ürünlerini taradığı ve bir ürün adı ve sürümüne dayanarak yükünü enjekte ettiği bilinmektedir. Kötü amaçlı yazılımın ilginç özelliklerinden biri, etki alanı adı ve IP adresi de dahil olmak üzere virüslü makinelerin geçmişini tutmasıdır. PLC rootkit'i kullanmak, antivirüsten kaçırma teknikleri, karmaşık işlem enjeksiyonu, çengel kod ve eşler arası güncellemeler Stuxnet'i bugüne kadar gözlemlenen en karmaşık saldırılardan biri haline getirmiştir.

5.4.11. Duqu (2011)

Eylül 2011'de ortaya çıkan Duqu, endüstriyel kontrol sistemlerine saldırı planlanmasında kullanılmak üzere tasarlanan, saldırı senaryosu için gerekli bilgileri toplayan bir yazılımdır. 2011 yılında fark edilmesine rağmen Şubat 2010'dan itibaren aktif olduğuna inanılmaktadır. Truva atı çeşidi olan Duqu, Stuxnet ile benzerlik göstermektedir. Duqu bulaştığı sistemde bulunan dosyaları analiz ederek bilgi çalmayı hedeflemektedir. Saldırganlar, hedef sisteme Duqu yükleyen sıfır günlük bir çekirdek istismarı olan bir Microsoft Word belgesiyle hedeflenen e-postayı kullanmışlardır. Bu güvenlik açığı, saldırganların en yüksek ayrıcalık düzeyiyle kod çalıştırmasına ve güvenlik mekanizmalarını atlamasına neden olmuştur.

5.4.12. Shamoon (2012)

2012 yılında Suudi Aramco ulusal petrol ve doğalgaz şirketini hedef alan Shamoon zararlısı, saldırgan (agresif) ve yüksek yıkıcılığı olan kötü amaçlı bir yazılımdır. Shamoon, bulaştığı bilgisayarda işletim ve dosya sisteminin kalbi olan MBR bölümünü hedef almaktadır. Bu sayede bulaştığı sistemdeki dosyaları erişilemez duruma getirerek zarar vermeyi amaçlamaktadır.

5.4.13. Flame (2012)

Flame, Orta Doğu, Avrupa ve Kuzey Amerika'da çok sayıda ülkeye bulaşan bir siber casusluk solucanıdır. Bu kötü amaçlı yazılım, 2012 yılına kadar keşfedilen en büyük siber casusluk ve şimdiye kadar keşfedilen en karmaşık teh-

ditlerden biriydi. Sıkıştırma ve veritabanı manipülasyonu için birçok kitaplık kullandığı için modüllerin toplam boyutu 20 MB'dir. Flame zararlısı ağı dinleme, ekran görüntüsü alma, giriş-çıkış aygıtlarını denetleme gibi özelliklere sahiptir.

5.4.14. Wiper (2012)

Wiper, 2012 yılında İran'daki enerji, petrol ve gaz şirketlerine ve devlet kurumlarına saldıran bir kötü amaçlı yazılımdır. Bu saldırı, diskin ilk yarısını yok etmeyi amaçlamıştır. Öncelikle sistemin normal çalışması için gerekli olan önemli dosyaları silmiştir. Önemli dosyaların silinmesi sistemin çökmesine neden olmuştur. Saldırganlar, yakalanmamak için farklı teknikler denemişlerdir. İşletim sisteminin önyüklemesini engelleyerek, sistemin sadece BIOS işlemlerini yapabilmesine izin vermişlerdir.

5.4.15. Havex (2014)

Havex, saldırganların sisteme uzaktan erişebilmelerine ve veri sızıntısına neden olabilecek bir arka kapıdır. Ayrıca barındırdığı komut denetim sunucusu iletişimi nedeniyle Uzaktan Erişim Truva Atı (RAT) olarak da sınıflandırılabilir. Havex loader modülü ile ek DLL dosyalarını indirip yüklemektedir. İlgili DLL dosyaları sayesinde komut sunucusu ile kalıcı iletişim kurabilmekte, sistemde yetkili ve kalıcı erişimlere sahip olabilmektedir. Sosyal mühendislik ve oltalama saldırıları ile yayılan Havex, kritik altyapılarda kullanılan OPC protokolünü de kullanabilmektedir.

5.4.16. Almanya Çelik Fabrikası (2014)

Saldırganlar tarafından 2014 yılında Almanya'daki bir çelik fabrikasına sızılarak, oltalama saldırısı ile önce fabrikanın ofis ağına erişim sağlanmış daha sonra da ağdaki yalıtım eksiklikleri nedeniyle ofis ağı üzerinden üretim ağlarına erişilmiştir. Saldırganlar eriştikleri sistemin endüstriyel kontrolleri içerdiğinin farkında olarak, bilgi birikimlerini ve başarılı sızma tekniklerini kullanarak ciddi fiziksel hasara neden olmuşlardır.

5.4.17. Industroyer (2016)

Ukranya'nın başkenti Kiev'in kritik altyapısını hedef alan Industroyer, oldukça yetenekli bir kötü amaçlı yazılımdır. Elektrik dağıtım şebekelerini doğrudan hedef alan ilk kötü amaçlı yazılımdır. İçerisinde komuta kontrol sunucusuna bağlanarak komut almak için bir arka kapı bulundurmaktadır. Arka kapının fark edilmesi ve engellenmesine karşı yedek bir arka kapı bulundurmaktadır. 17 ve 20 Aralık tarihlerinde çalışması üzerine kurgulanmış Industroyer, zaman tetiklemeli bir ana başlatıcı içermektedir. Elektrik dağıtım şebekelerinde tercih edilen IEC 60870-5-101, IEC 60870-5-104, OPC DA ve IEC 61850 endüstriyel protokolleri bünyesinde barındırmaktadır. Saldırıdan kurtulmayı zorlaştırmak ve geride iz bırakmamak amacıyla kayıt defteri ve önyükleme birimlerini silebilecek bir bileşen daha içermektedir.

5.4.18. ClearEnergy Fidye Yazılımı (2017)

ClearEnergy, nükleer ve enerji santralleri, su ve atık tesisleri gibi kritik altyapıları hedef alan bir fidye yazılımıdır. Bu kötü amaçlı yazılım, SCADA ve ICS sistemlerinde saha cihazları üzerindeki güvenlik açıklarını sömürmeyi amaçlamaktadır. Kötü amaçlı yazılımı çalıştırdıktan sonra, bağlı bulunduğu ağ içerisinde PLC cihazlarını arar. Bulduğu PLC cihazlarındaki ladder logic diyagramını elde etmeye çalışır. Elde edilen bilgileri uzak sunucuya aktararak sahadaki süreç konusunda bilgi çıkarımı yapabilmektedir. Ayrıca PLC üzerindeki kodu silme işlevlerini tetiklemeye çalışmaktadır. Mağdur fidyeyi öderse yedeklenen kod geri iade edilmektedir. ClearEnergy, kimlik doğrulama atlamasına neden olan oturum anahtarının kötü tasarımı nedeniyle satıcı Schneider Electric'in UMAS protokolünde bir güvenlik hatasını kullanmaktadır. Güvenlik hatasını sömürerek, PLC cihazında yetki almak için kullanılan oturum anahtarını ele geçirerek tam kontrolü ele alınmaktadır.

5.4.19. Triton (2017)

Sahada yürütülen operasyonda aksaklık ya da saldırı gibi işleyişi normalin dışına çıkaran durumlar meydana geldiğinde emniyet sistemler devreye girerek sistem güvenliğini sağlamaktadır. Triton, SCADA sistemlerinde bulunan

emniyet sistemlerine yönelik bilinen ilk kötü amaçlı yazılımdır. Emniyet sistemlerini hedef alan kötü amaçlı yazılım, iş istasyonlarına uzaktan bağlantı yeteneği geliştirdi. Sahadaki emniyet denetleyicileri yeniden programlayarak, endüstriyel süreci otomatik kapatan bileşenlere müdahale edilmiş oldu.

5.5. KRİTİK ALTYAPILARIN GÜVENLİK ZAFİYETLERİ

5.5.1. Genel Amaçlı İşletim Sistemi Kullanımı

SCADA sistemleri saha elemanlarının durumunu izlemek ve komut göndermek için HMI arayüzlerini kullanmaktadır. HMI arayüzleri cihazlar üzerinde donanımsal olarak bulunabileceği gibi yazılımsal olarak da bir sunucu üzerinde çalışabilmektedir. HMI bileşeninin kurulu olduğu sunucu üzerinde genel amaçlı işletim sistemleri bulunmaktadır. Genel amaçlı işletim sistemleri geleneksel BT sistemlerinin ihtiyaçlarını karşılamak için farklı servisler ve işlemleri bünyesinde barındırmaktadır. İlerleyen yıllarda barındırılan servisler ve işlemlerde güvenlik zafiyetleri keşfedilmektedir. Bu zafiyetlerin giderilmesi ve işletim sisteminin güvenliğinin sağlanması için güvenlik yamaları ve güncellemeler yayımlanmaktadır. Yayımlanan güncellemelerin alınabilmesi için kapalı ağ çalışan SCADA sisteminin internete bağlanması gerekmektedir. Sistemin kısa süreli ve kontrollü internete bağlanması bile sisteme zararlı yazılım yerleşmesine veya sistemde yerleşik halde hareketsiz bekleyen zararlı yazılımların dışarıyla veri alışverişi yapabilmesine olanak sağlamaktadır.

Ayrıca güvenlik yamalarının yayımlanması, zafiyetlerin ortaya çıkışından belirli bir süre sonra gerçekleşmektedir. Bu süre boyunca sistem ilgili zafiyet üzerinden atağa maruz kalabilir. Sistemde önceden bulunan zafiyetler ile birleştirilerek atakların etki alanı arttırılabilir. Bilinen en meşhur saldırılardan biri olan Stuxnet saldırısına ait zafiyetin yamasının yayımlanması 2 yıl sürmüştür [14].

SCADA sistemleri yaşam döngüleri boyunca aralıksız çalışan sistemlerdir. SCADA sistemleri 7 ile 15 yıl arası operasyonel yaşama sahiptir [15]. Bazı işletim sistemi jenerasyonlarının ömürleri SCADA sistemlerinin yaşam sürelerinden kısa olabilmektedir. Windows işletim sistemi genel kullanım ömürleri

incelendiğinde temel desteğin yaklaşık 5 yıl, genişletilmiş desteğin yaklaşık 10 yıl sürdüğü görülmektedir [16]. SCADA sistem yaşam döngüleri ve işletim sistemi ömürleri karşılaştırıldığında, SCADA sistemlerinin güvenlik yamalarının yapılmasının yanında yaşamları boyunca en az bir kez işletim sistemi yükseltmesi gerektiği görülmektedir. Günümüzde Windows XP işletim sistemine destek kesilmiş ve işletim sistemi ile ilgili birçok sömürü kodu paylaşılmıştır. Fakat birçok zafiyet barındıran Windows XP, kütüphane uyumsuzlukları, sistem güncellenememe ve lisans problemleri gerekçesi ile hala SCADA sistemlerinde kullanılmaktadır. Bu durum işletim sistemi kaynaklı atakların önem derecesini ortaya koymaktadır.

5.5.2. Protokol Kaynaklı Zafiyetler

SCADA sistemleri ilk tasarlandıkları yıllarda fabrika, üretim tesisi gibi kapalı alan içerisinde çalışmaktaydı. Saha cihazları ile haberleşmek için kendilerine özel tasarlanmış seri haberleşme hatları kullanılmaktadır [17]. Geçmişte SCADA sistemleri diğer sistemlerden bağımsız olarak kapalı devre haberleşme altyapısı kullanması ve tasarlandıkları yıllarda siber güvenlik perspektifinin yaygın olmamasından dolayı tasarımlarında siber güvenlik ilkelerine önem verilmemiştir. Güvenlik ilke yoksunluğu ile ortaya çıkan SCADA protokollerinde şifreleme, kimlik doğrulaması gibi gereksinimler bulunmamaktadır [18].

Haberleşme altyapılarının gelişimine eski tip SCADA sistemleri küçük eklentiler ile uyum sağlamaya çalışmıştır. Gelişmiş altyapıların kullanılması ile SCADA sistemleri sahada daha geniş alanı kapsayabilmiştir. Yapılan eklentilerin eski çalışan sistemleri kapsayabilmesi için mevcut kullanılan protokollerde köklü değişiklikler yapılmamıştır. Bu nedenle SCADA sisteminin karakteristiğinde bulunan zafiyetler, yerel ağ bağlantıları ile erişilebilir olmuştur. Bu erişilebilirlik zafiyetlerin sömürülme ihtimalini dolayısıyla çarpan değerini arttırmıştır. SCADA sistemleri doğrudan atak uygulanabilecek yapıda olmamasına rağmen ağ bağlantılarından erişilebilir olması sisteme sızılmasına olanak sağlamıştır. Ağa erişim sağlanması sonucunda güvenlik ilke yoksunluğu ile tasarlanan SCADA protokolleri dinlenebilmekte, analiz edilebilmekte, sisteme sahte veriler enjekte edilebilmektedir [19].

5.5.3. Sosyal Mühendislik Saldırıları

Güvenliğin en zayıf halkası olan insan faktörü sosyal mühendislik saldırılarının temelini oluşturmaktadır. Sosyal mühendislik insanlara zafiyetlerinden faydalanarak ikna ve kandırma yöntemleri ile istenilen eylemi yapmasını sağlamaktır [20]. HMI yazılımının çalıştığı bilgisayar ve operatör üzerinden sosyal mühendislik saldırıları gelme ihtimali çok yüksektir. 2010 yılında gerçekleşen Stuxnet saldırısı [14,21] zararlı kod barındıran USB belleğin SCADA sistemini kontrol eden bilgisayara takılması sonucunda olmuştur. Sisteme takılan bellekten bulaşan virüs PLC içerisindeki kodu değiştirmiştir. Bu değişiklik saha cihazlarının hatalı kontrolüne sebebiyet vermiştir. Sistemdeki normal işleyişin öğrenilmesi ve saldırı sırasında normal verinin HMI'ya gönderilmesinden dolayı sistemdeki saldırının tespiti oldukça zorlaşmıştır. Yaşanan bu olay SCADA sistemlerinin internet ile aralarında hava boşluğu olmasına rağmen saldırılara maruz kalma ihtimalini gözler önüne sermiştir. Ayrıca sistem üzerinde bulunan tüm giriş/çıkış portlarının fiziksel olarak kapatılması ve operatörlerin bilinçlendirilmesindeki önem ortaya çıkmıştır. Kontrol bilgisayarının internete bağlı olması ve kullanıcıların mail, sosyal medya gibi genel amaçlı kullanımlarda bulunması da ciddi problemlere sebep olmaktadır.

Sosyal mühendislik saldırıları genellikle e-posta üzerinden gerçekleştirilen oltalama saldırıları üzerine yoğunlaşmıştır [22]. Sahte bir hesap üzerinden aslını taklit ederek gerçekleştirilen saldırı çeşidi, sisteme istenmeyen dosya indirilmesi kurulması veya web oturumu üzerindeki bir zafiyetten sisteme sızılmaya çalışılması şeklinde ilerlemektedir. Ukrayna'da elektrik şebekesine düzenlenen oltalama saldırısı sonucunda saldırganlar ağa erişim yetkisi kazanmıştır [24]. Ağa erişebilen saldırganlar kontrol bilgisayarı ve HMI arayüzünü kullanarak elektrik şebekesinin kontrolünü ele geçirmeye çalışmışlardır.

5.5.4. Kötücül veya Zararlı Yazılım (Malware)

Sistemlerin işlevlerini bozmak, kullanıcıların verisini çalmak, güvenlik özelliklerini devre dışı bırakmak, sisteme erişimi kalıcı hale getirmek için arka kapı açmak, sistem üzerinde komut çalıştırmak gibi zararlı faaliyetleri yapan yazılımlar kötü amaçlı yazılım olarak kabul edilmektedir [30]. Kötü amaçlı

yazılımlar BT için geliştirildiği gibi SCADA sistemleri için de geliştirilmektedir. SCADA sistemlerini doğrudan ya da dolaylı olarak hedef alan Stuxnet [14,21], Flame [24], Duqu [4] en çok bilinen kötü amaçlı yazılımlardır. Saha bileşenleri ile haberleşen ve karakteristik özellikleri açısından zafiyet barındırabilen SCADA sistemlerine kötü amaçlı yazılımların bulaşması, sistemin içerdiği fakat ulaşılması güç durumda bulunan zafiyetlerin sömürülmesine neden olmaktadır.

Sistemde bulunan yüksek yetkili bir işleme bulaşan kötü amaçlı yazılım, elde ettiği yetkiler ile sistem bilgilerini ve konfigürasyonlarını değiştirebilmekte, hatta sistemdeki tüm kontrolü ele geçirebilmektedir. Kontrol merkezine bulaşan kötü amaçlı yazılımlar elde ettikleri yüksek yetkiler ile saldırganların sistemde kalıcı olmasını sağlayan arka kapıları kullanmaktadırlar. SCADA sistemlerinde yaşanan olay kayıtları incelendiğinde keşif aşaması ile başlayan sürecin kötü amaçlı yazılımların bulaştırılması ve sistemde kalıcı olunması ile sonlandığı görülmektedir. SCADA sistemlerinde genel amaçlı işletim sistemleri kullanılması BT sistemlerine yönelik kötü amaçlı yazılımların, SCADA sistemleri üzerinde de başarılı olmasına neden olmaktadır.

SCADA sistemlerine bulaşmış olan en ünlü zararlı yazılım Stuxnet [14,21]'tir. Stuxnet zararlı yazılımı USB bellek aracılığı ile Windows tabanlı bir bilgisayara bulaşmıştır. Bulaştığı işletim sisteminde bulunan sıfırıncı gün açıklarını kullanarak sistem üzerinde yüksek yetkilere sahip olmuştur. Daha sonra kontrol bilgisayarı üzerinden kontrol ağına müdahale edebilme yeteneğine kavuşmuştur. Sahada kullanılan PLC cihazları üzerindeki koda müdahale edebilmiştir. Sahada yapılmaması gereken fiziksel değişimleri gerçekleştirerek ve izleme ekranına normal işleyiş verilerini göndererek amacını yerine getirmiştir.

5.5.5. İleri Düzey Kalıcı Tehditler (APT)

Belirli bir hedefe ait bilgisayar ve bilgisayar ağlarına yetkisiz olarak erişebilen ve yerleştiği sistemlerde uzun zaman boyunca tespit edilmeden barınabilen siber tehditler İleri Düzey Kalıcı Tehditler (Advanced Persistent Threat - APT) olarak adlandırılmaktadır [25]. Genellikle politik ve ekonomik nedenlerle devlet ya da devlet destekli gruplar tarafından oluşturulan APT zararlıları; hükümetler, finans kuruluşları, savunma sistemleri, endüstri, telekom opera-

törleri ve kritik altyapıları hedef almaktadır. İsmini özelliklerinden alan APT, gelişmiş yapıda olması, bulaştığı sistemde kalıcı olmaya çalışması ve bünyesinde birçok tehdidi içermesi ile bilinmektedir [26]. APT'ler kötü amaçlı yazılımlara göre daha gelişmiş yapıda bulunmaktadır. Hedef alınan yapıda bulaşmak için gelişmiş yöntemler kullanmakta ve bulaştığı sistem üzerinden diğer ağ ve sistemlere yayılabilmektedir. Girdikleri sistem içerisinde kendilerini belli etmeden uzun yıllar kalıcı olabilmektedir. Sistemde uzun yıllar kalıcı olabilmesi sistemin tüm davranışlarını öğrenmesine ve saldırı sırasında kullanabilmesine olanak sağlamaktadır. Ayrıca bünyelerinde barındırdıkları fazla sayıda bilgi toplama ve saldırı araçları sayesinde amaçlarını zamanında ve gerektiği şekilde yerine getirmektedir. İlgili hedefteki amacını yerine getirmek için sürekli sistem izlemesi yapmakta ve fark edilmeden yaşamına devam etmektedir. Düşük ve yavaş yaklaşım tekniklerini kullanmakta ve diğer zararlılara göre uzun vadede daha başarılı olmaktadır.

5.5.6. Keşfedilebilirlik

Teknolojik gelişmeler SCADA sistemlerinin uzaktan kontrol edilebilmesine ve sahadan toplanan verilerin bulut tabanlı sistemlerde işlenmesine olanak sağlamaktadır. Bulut altyapısını kullanacak SCADA sistemlerinin kurulum işlemleri, tüm sistemi ve saha cihazlarını programlamak yerine uygulama kurulumu şekline dönüşecektir. Bu sayede merkez yapı tarafından onaylanmış daha efektif ve hızlı kurulum sağlayan bir yapı elde edilecektir. Bulut sistemler ile entegre şekilde çalışabilen SCADA sistemlerinin, kapalı devre çalışan SCADA sistemlerine göre keşfedilmesi daha kolaydır. SCADA sisteminin kolayca keşfedilebilmesi bünyesinde barındırdığı karakteristik özelliklerin kötüye kullanılması ve zafiyetlerin sömürülmesi ihtimalini arttırmaktadır. Sömürülme ihtimalinin artması ulaşılması zor zafiyetlerin çarpan değerini arttırmakta dolayısıyla sistemin siber güvelik risk skorunu etkilemektedir.

Saldırı vektörünün ilk aşaması olan keşfetme, fiziksel olarak ulaşılabilir bir sistemin varlığından haberdar olmakla başlamaktadır. Varlığı tespit edilen sistemlere ilişkin tanımlama, servis ve bileşen tespiti ile saldırı için gerekli bilgiler toplanmaktadır [27]. Toplanan bilgilerin yorumlanması ve zafiyet araştırması ile saldırı vektörü oluşturulmaktadır. Bu nedenle güvenliğinden

emin olunmayan ve güvenlik prosedürleri yapılandırılmamış sistemlerin dış dünya ile iletişimine izin verilmemelidir.

5.5.7. Paylaşımlı Sunucu Kullanımı

Bulut sistemlerle bütünleşmiş çalışan SCADA sistemlerine benzer bir yapıda, İnternet tabanlı kontrol merkezi ile çalışan sistemler bulunmaktadır. Web tabanlı yapının kullanılmasıyla herhangi bir zamanda herhangi bir yerden erişilebilen WebSCADA çözümleri bulunmaktadır [28]. Web tabanlı yapının kullanılması SCADA sistemlerine geleneksel sistemlerden daha esnek ve genişletilebilir bir yapı sunmuştur. Fakat web tabanlı yapının kullanılması sistemin keşfedilebilmesine olanak sağlamaktadır. Ayrıca SCADA sistemine uzaktan bağlanabilmek için bilgi teknolojileri ile ortak kullanımda olan ara sunucular konumlandırılmaktadır.

SCADA sistemlerinde kullanılan paylaşımlı sunucular farklı amaçlar için kullanılan servisler ve işlemler barındırabilir. Paylaşımlı sunucularda kullanılan servislerde bulunan bir zafiyet, sunucudaki tüm servisleri ve işlemleri tehdit eder. SCADA sisteminden bağımsız olarak bulunan bir zafiyet kullanılarak, paylaşımlı sunucuya sızılabilir. Paylaşımlı sunucuya sızılmasından sonra çalışan işlemler ve servisler kontrol edilerek SCADA sisteminin varlığı keşfedilebilir. SCADA sisteminin keşfedilmesinden sonra zafiyet analizi ile saldırı düzenlenebilir.

Paylaşımlı sunucuların güvenliği çalıştırılan servisler ve işlemlerin arasında en zayıf halkaya göre belirlenmektedir. Dolayısıyla paylaşımlı sunuculara bağlı diğer sistemlerin güvenliği de en zayıf halkaya göre değerlendirilmelidir. SCADA sistemleri oldukça güvenli bir kapalı haberleşme yapısında kullanılsa bile paylaşımlı sunucu ile bağlantısı bulunması durumunda risk skoru yükselmektedir.

5.5.8. Konfigürasyon Hataları

Günümüzde Bilgi Teknolojileri ile ortak kullanılan sistemlerde kurulum aşamasında belirli konfigürasyonların yapılması gerekmektedir. Kurulum aşamasında konfigürasyonların eksik yapılması ileride oluşacak hatalara ve zafi-

yetlere neden olmaktadır. SCADA sistemlerinde meydana gelen zafiyetlerin bir kısmı kurulum ve bakım sırasında eksik ya da hatalı konfigürasyondan meydana gelmektedir [29]. Kurulum sırasında eksik konfigürasyonlar ya da varsayılan ayarların kullanılması zafiyet oluşumuna sebep olmaktadır. Ayrıca bakım sırasında eklenen yeni bileşene ait konfigürasyonların eksik yapılması, bileşen özelliklerinin ve güvenlik gereksinimlerinin yeterli olduğu şekilde kullanılmasına engel olmaktadır.

Hatalı ve eksik konfigürasyonların meydana getirdiği durumlarda güvenlik ve emniyet ile ilgili prosedürler uygun olarak işletilememektedir [30]. Prosedürlerin planlanan güvenlik seviyesinde işletilmemesi birçok zafiyete neden olmaktadır. Varsayılan konfigürasyonlarda en çok görülen zafiyet, kullanıcı adı ve şifrelerin tüm ürün grubunda aynı olmasıdır. Her markanın ürün gruplarında aynı kullandığı varsayılan kullanıcı adları ve şifreleri, kullanıcı kılavuzlarında ve internet kaynaklarında paylaşılmaktadır. Fakat kurulum sonrası kullanıcı adı ve şifrelerinin değiştirilmemesi güvenlik prosedürlerinden ilk aşama olan kimlik doğrulamayı devre dışı bırakmaktadır. Bilinen ve varsayılan şifrelerin kullanılması ile kimlik doğrulama adımları kolaylıkla geçilebilmekte ve sistemlerin konfigürasyonlarında değişiklik yapılmasına izin verilmektedir. Sistemde varsayılan olarak bulunan ve kullanılmayan kullanıcı hesapları da konfigürasyon hataları içerisinde bulunmaktadır. Yetkisi düşük olan varsayılan kullanıcıların sömürülmesi ve yetki yükseltme ataklarının yapılması sonucunda sistemde yetkili kullanıcı haline gelebilmektedir. Ayrıca sisteme ağdaki herkesin erişebilmesi eksik konfigürasyondan kaynaklanmaktadır. Sisteme erişebilecek ağ adreslerinin ve erişilmesi gereken portların tanımları beyaz liste yardımı ile yapılmalıdır [31]. Sistem için tasarlanan sınırlara bağlı olarak gerekli konfigürasyonlar kararlaştırılmalıdır. Kurulum ve bakım sırasında çizilen sınırlara göre tüm konfigürasyonlar eksiksiz olarak yapılmalı ve kullanılmayan özellikler kapatılmalıdır.

5.5.9. Üçüncü Parti Kütüphane Kullanımı

Heterojen mimarideki yapıların bir arada kullanımı ve büyük çaplı yazılımların küçük alt modüllere bölünmesi gibi ihtiyaçlar sonucunda kütüphaneler kullanılmaktadır [32]. Kurumsal alanda kütüphaneler, süreçlerin paralel ola-

rak işletilerek hızlandırılmasını amaçlamaktadır. Sistemler oluşturulurken yetkili kişiler tarafından yazılan kütüphaneler kullanıldığı gibi, belirli görevleri yerine getirmek için yazılan ve internette paylaşılan üçüncü parti kütüphaneler de kullanılmaktadır. Yayıncısı bilinmeyen ve teste tabi tutulmamış kütüphanelerin sistemlerde kullanılması, sisteme keşfedilmemiş arka kapı yerleştirme ihtimalini ortaya çıkartmaktadır.

SCADA sistemleri sahada farklı bileşenlerin çeşitli haberleşme ortamlarını kullanarak kontrol merkezine veri aktarması ile bir bütün oluşturmaktadır. SCADA sistemlerinde sahada kullanılan farklı markalara ait PLC cihazları, farklı haberleşme ortamları, farklı endüstriyel protokollerin desteklenmesi gibi ihtiyaçlar kütüphane kullanımına ihtiyaç oluşturmaktadır. SCADA sistemlerinin zafiyetleri değerlendirilirken kullanılan yazılımın ve kütüphanelerin güvenliği de göz önüne alınmalıdır. Sistem kurulumu ve oluşturulması sırasında kullanılması planlanan kütüphanelerin, yazılım güvenliği açısından değerlendirilmesi gerekmektedir. SCADA sistemlerinde kullanılması planlanan kütüphanelerin kararlılık ve güvenlik testlerinden geçirilmesi gerekmektedir. SCADA sistemlerinde kullanılan yazılım, kütüphane ve veritabanı gibi bileşenlerin güvenliğinin önemi Stuxnet saldırısında da görülmektedir. Stuxnet, hedef sistemde kullanılan WinCC yazılımına ait veritabanına erişmiştir. Daha sonra veritabanı içerisinde açık metin olarak bulunan kullanıcı adı ve şifresi bilgilerini okuyabilmiştir [29].

5.5.10. İç Kaynaklı Saldırılar

Bir sistemde sistemin tasarımcısı, yöneticisi ve operatörü olmak üzere iç erişime sahip kullanıcılar ve dışarıdan sınırlı erişime sahip kullanıcılar bulunmaktadır. Dış erişime sahip olan kullanıcılar, sisteme erişim sağlarken farklı katmanlardan ve katmanlar arası yalıtım politikalarından geçmektedir. Bu nedenle dış kaynaklı zararlı aktivitelerin yakalanması kolaydır. İç tehditler her sistem için önemli bir tehlike oluşturmaktadır. Çalışanların ise kasıtlı veya kasıtsız olarak yanlış uygulamalar ile sistemi tehlikeye atması muhtemel bir durumdur. Ek olarak çalışanların işverenden hoşnut olmadıkları durumda da kasıtlı olarak sistemlere zarar verecek davranışlarda bulunabilmesi olasıdır. Sonuçta sistemin işleyişine müdahale edebilmekte veya sisteme zararlı dosya

bulaşmasına neden olabilmektedirler. Özellikle eski çalışanların erişim yetkilerinin alınmadığı durumlarda, kasıtlı olarak sistem işleyişini bozmaya yönelik faaliyetler meydana gelmektedir.

5.5.11. Hizmet Reddi (DoS)

Sistemler genellikle belirli yükü belirli süre içerisinde işleyebilmek üzerine tasarlanmıştır. Sisteme birim zaman içerisinde taşıyabileceği ağ trafiğinden daha fazla trafik göndererek sistemin gelen isteklere cevap veremez duruma gelmesi hizmet reddi saldırısı olarak tanımlanmaktadır. Çalışma anı içerisinde veri akışında gecikme yaşanmaması gereken sistemler gerçek zamanlı sistem kategorisinde değerlendirilmektedir. Kritik altyapılar, çalışma anı içerisinde veri akışında ve sahadaki operasyonda gecikme ve aksama yaşanmaması gereken gerçek zamanlı sistemlerdir. Gerçek zamanlı sistemlerde hizmet reddi saldırısının uygulanması sonucunda ise gönderilen kontrol işaretleri zamanında alınamamaktadır. Bu nedenle sahada durdurulması veya başlatılması gereken fiziksel süreçte aksamalar meydana gelebilmektedir. Meydana gelen aksaklıkların fiziksel zararlara, finansal kayıplara ve can kayıplarına sebep olması beklenen sonuçlar arasındadır.

5.5.12. Dinleme

Haberleşme sırasında harici müdahale ile ya da müdahalesiz olmak üzere akan trafik dinlenilmektedir. Dinleme atakları, hemen hemen tüm iletişim ağlarında göz önüne alınması gereken bir sorundur. Kritik altyapılar da trafik dinlemelerine karşı savunmasızdır. Ağ trafiğini yakalama yöntemleri ise ağ için dağıtılan iletişim ortamına bağlı olarak değişmektedir. Kablosuz iletişim kullanılan bir ağda, paketler kolaylıkla ele geçirilebilmektedir. Uygun ekipmanla donanmış herhangi bir saldırgan, ağdan gelen paketleri kolayca yakalayabilmekte ve inceleyebilmektedir. Birçok endüstriyel protokolde paketler açık metin olarak gönderilmektedir. Bu nedenle, saldırgan kodlanmış bilgileri paketi yakaladığında çıplak gözle okuyabilmektedir. Kritik altyapılarda ağ trafiğinin çoğunluğu sahada toplanan verilerden oluşmaktadır. Sahadaki operasyonel yapının ayrıntılarına hakim olan bir saldırgan ağ trafiğini dinleyerek,

operasyonel yapıdaki durum bilgilerini ele geçirebilmektedir. Operasyonel yapıyı ve ağ trafiğini bilen bir saldırgan özelleşmiş saldırı vektörleri ile gelişmiş saldırılar gerçekleştirebilmektedir.

5.6. KRİTİK ALTYAPILARDA TEHDİT VE TEHLİKELER

5.6.1. Kritik Altyapıya Yönelik "Tehditler ve Tehlikeler" Nelerdir?

Doğal ve insan eliyle gerçekleşen tüm olayların mevcut kritik altyapılara zarar verme, hasar bırakma, kritik altyapıyı yetersiz kılma veya tamamen yok etme potansiyeli bulunmaktadır. Bu yüzden devletler, doğal afetler veya terörizm gibi tek tür tehdit ve tehlikeye odaklanmalarının yanında verimli planlama ve kaynak tahsisine olanak sağlayan kritik altyapılar için tehdit ve tehlike oluşturan tüm etmenleri belirlemelidir.

Uzun zamandır doğal afetler ve fiziksel tehditler ile bağlantılı risklere maruz kalan kritik altyapılar, günümüz teknolojisi ile birlikte siber risklerin etkisi altına daha fazla girmektedir. Endişe uyandıran siber riskler ise kritik altyapılar ile bilgi ve iletişim teknolojilerinin giderek artan bir entegrasyon içerisinde olmasından ve potansiyel güvenlik açıklarından yararlanmaya çalışan düşmanlardan kaynaklanmaktadır. Fiziksel altyapıların süreç kalitesi ve verimliliği için karmaşık siber sistemlere bağımlılığının artması kritik altyapıları uluslararası tehditlerde dahil olmak üzere birçok siber tehditlere karşı savunmasız duruma getirmektedir.

Kritik altyapı unsurları ve sektörler arasındaki bağlantılar ve karşılıklı bağımlılıklar, bir unsurda meydana gelen hasar, kesinti gibi olumsuz bir durum diğer bir unsurda devam eden çalışmayı etkileyebileceği gibi ardışık etkilere de sebep olabilmektedir. Kritik altyapı unsurları ile sektörler arasındaki karşılıklı bağımlılık ve bağlantıları iki yönlü veya tek yönlü olarak anlamak ve belirlemek, potansiyel risk ve açıkları değerlendirmek, olası tehditlere karşı güvenlik ve dayanıklılığı arttırmak için atılacak adımların ve koruma stratejisinin belirlenmesi için oldukça önemlidir. Örneğin, bir elektrik şebeke sisteminin çalışması diğer kritik altyapılardan gelen bilgiye ve diğer sistemler ile iletişimine dayanmak-

tadır. Oluşan bir felaketin ardından acil enerji ihtiyacına yanıt olarak kurtarma operasyonları uygulanmaktadır. Fakat enerji sistemi geri yüklenene kadar su ve atık sistemleri temiz su sağlayamamakta, doğal gaz akışı olmadığı için ısı sağlanamamakta, yedek güç kaynakları arızalanmaya başladığında ise üretim ve telekomünikasyon sistemleri çalışamaz duruma gelmektedir.

5.6.2. Kolay Hedefler ve Kalabalık Yerler

Yeni dünya düzeni, fiziksel güvenlik tehditlerinden siber tehditlere kadar saldırgan faaliyetlerinin arttığı ve yaygınlaştığı bir hal almıştır. Yapılan saldırılar doğası gereği basit ve fırsatçı ya da karmaşık ve organize olabilmektedir. Orlando'dan Yeni Zelanda'ya, San Bernardino'dan Sri Lanka'ya dünya çapında birçok şehirde kolay hedeflere ya da kalabalık ortamlara yapılan saldırıların sayısı artış göstermektedir. Bu artış, mevcut tehdit doğasının değişmekte olduğunu ve küresel farkındalık, uyanıklık, hazırlık ve iş birliği ihtiyacının güçlendirildiğinin göstergesidir. Bu kapsamda ulusal ve uluslararası çalışma ve emekler, kolay hedeflere ve kalabalık yerlere saldırma eğilimi üzerinde durmaya çalışmaktadır. Bu çalışmalara örnek olarak Amerika Birleşik Devletleri, kolay hedeflerin ve kalabalık yerlerin güvenliğini artırmak ve bu konuda yapılan çalışmaları teşvik etmek amacıyla uygulanan eğitim ve kullanılacak kaynak ve materyallerin temini için hükümetin tüm birimleriyle birlikte çalışmaktadır. Uluslararası platformda ise ülkeler, küresel bir güvenlik kültürü oluşturmaya ve ilerletmeye yardımcı olmak için kolay hedeflere ve kalabalık yerlere yönelik saldırılara ilişkin yararlı uygulamaları, alınan dersleri ve deneyimleri paylaşmak için birlikte çalışmaktadır.

Amerika Birleşik Devletleri ve Türkiye tarafından ortaklaşa yürütülen Küresel Terörle Mücadele Forumu Kolay Hedef Koruma Girişimi, 2017 yılında hükümet ve özel sektör ile birlikte farkındalığı arttırmak, hazırlıklı olmak ve terörle mücadele bağlamında kolay hedef korumasına ilişkin bağlayıcı olmayan uluslararası yararlı uygulamaları oluşturmayı amaçlayan bir dizi bölgesel çalıştaya katılmıştır.

Yararlı uygulamalar, vatandaşlarını kolay hedeflere ve kalabalık yerlere yönelik terör saldırılarından korumaya yönelik politikalar, uygulamalar, kılavuzlar, programlar ve yaklaşımlar geliştirmek için birlikte çalışmanın yanı

sıra hükümetleri ve özel sektörü bilgilendirmek ve yönlendirmek amacıyla kullanılmaktadır.

Yoğun tartışmalar sonucunda, devletlerin kendi topraklarında güvenliği sağlama ve sivilleri Birleşmiş Milletler (BM) Şartı uyarınca koruma konusunda birincil sorumluluğun devletlere ait olduğu kabul edilmiştir.

BM Güvenlik Konseyi'nin 2341 (2017) sayılı Kararı ile, kritik altyapıların ve özellikle kamuya açık yerler gibi toplumu etkileyen hassas hedeflerin, kamu-özel sektör ortaklıkları da dahil olmak üzere uygun olduğu şekilde terör saldırılarından korunmasında devletlerin rolü ana hatlarıyla belirtilmiştir.

5.7. KRİTİK ALTYAPI İLETİŞİM PROTOKOLLERİ

Kritik altyapılar, diğer bütün bilgi sistemlerinde olduğu gibi, iletişim protokollerine ihtiyaç duymaktadır. Güvenlik endişelerinin bulunmasına rağmen kullanım alanı çok geniş olan kritik altyapılarda SCADA sistemleri kullanılmaktadır. Bu sistemler, 1960'lı yıllardan beri endüstrinin temelini oluşturmakta, kritik ve hassas zamanlı materyal ve süreçleri yönetmek amacıyla kullanılmaktadır [41]. SCADA sistemlerinde kullanılan protokollerin çoğu master/slave prensibiyle çalışmaktadır. Yaygın endüstriyel kontrol sistemlerinde Modbus, RP-570, Conitel ve Profinet protokolleri kullanılmaktadır.

5.7.1. Modbus

Modbus, şu anda bilinen adıyla Schenider Elektrik tarafınan geliştirilmiş bir veri iletişim protokolüdür. Otomasyon teknolojisinin yapı taşlarından bir olan PLC (Programmable Logic Controller) teknolojisiyle, yapıldığı 1979 yılından itibaren endüstride bir standart haline gelmiştir [42].

Modbus'ın kullanılmasının en önemli sebepleri arasında, kurulumunun ve bakımının kolay olması sayılabilir. Elektrik sektöründe genelde, bir RTU (Remote Terminal Unit) ile SCADA sistemlerine bağlanılmaktadır ve bağlantı olarak RS485 ya da Ethernet kullanılmaktadır [34].

Avantajları

- Protokolün açık kaynak olması özelliği sayesinde yapı birçok araçta kullanılabilmektedir. Bununla birlikte hem geliştirme hemde yardım süreçleri daha kolay ve verimli ilerlemektedir.
- Modbus, kurulumu aylar süren diğer protokollere göre, sadece birkaç gün içerisinde kurulabilmektedir. Bu özelliği ciddi oranda bir zaman kazandırmaktadır.
- Modbus protokolünün ileteceği veri söz konusu olduğunda, çok az sınırlaması vardır.

Dezavantajları

- Modbus, kullanılan bağlantı yöntemine göre bir raporlama sisteminin seçilmesi gereken bir mekanizmadır. Bu yüzden her senaryo ayrı ayrı ele alınmalıdır [43].

5.7.2. Conitel

SCADA sistemlerinde kullanılan bir diğer protokol olan Conitel'in temelleri 1993'te atılmış olup 1994 yılında RTU eklentisi de eklenmiştir. [45].

Avantajları

- Diğer protokollere kıyasla daha kolay bir protokoldür.
- Hata tespit oranları yüksek olduğu için oldukça güvenlidir.
- Özellikle küçük veri blokları konusunda daha verimli çalışmaktadır.

Dezavantajları

- Bit bazında olmadığı için, kurulum için özel donanım gerektirmektedir.
- Hem istasyon adresi hem de veri büyüklüğü konusunda kısıtlamaları bulunmaktadır.
- Büyük veri bloklarında efektif çalışmamaktadır.
- Diğer SCADA protokollerinde olduğu gibi, hata düzeltme yerine hata tespit prensibiyle çalışmaktadır.

5.7.3. Profinet

2003 yılında geliştirilen Profinet iletişim protokolü, endüstride standart haline gelmiş bir diğer protokoldür. Özellikle Siemens sistemlerinde ağırlıklı olarak kullanılan bu protokolün en güçlü yanlarından biri kısa zaman kısıtları altında veri iletimi sağlayabilmesidir. Ethernet bazlı cihazlar arasında hızlı veri iletimi görevini üstlenmektedir ve diğer SCADA protokollerinden farklı olarak provider-consumer modelini izlemektedir [46].

Avantajları

- Profinet, hata giderme (troubleshooting) konusundaki hızıyla diğer protokollere göre zamanın daha büyük bir kısmını çalışır durumda geçirmektedir.
- Sorun çıktığında onaran bir yapı yerine, sorunları çıkmadan öngören ve önlem alan bakım yapısı sayesinde çalışma oranı yüksektir.
- Sistemi büyütmek oldukça kolaydır.
- Hızı ile öne çıkmaktadır.

Dezavantajları

- Ethernet/IP ile uyumluluk açısından karşılaştırıldığında daha iyi değildir.
- Yüksek hızlı bağlantı söz konusu olduğunda, fiyat performans açısından Ethernet/IP, Profinet'e göre daha uygun olarak değerlendirilmektedir.

5.8. KRİTİK ALTYAPI SİMÜLASYONLARI

Siber güvenlik alanındaki simülasyonlar, halihazırdaki bir sistemin güvenlik zafiyetlerini, kötü niyetli saldırganlar ortaya çıkmadan önce tespit etmek için kullanılmaktadır. Simülasyon programlarının çıktıları sonucunda fark edilen zafiyetler düzeltilmekte ve koruyucu önlemler alınmaktadır. Simülasyonların kritik altyapı özelinde kullanılması denemelerin yapılacağı sistemlerin hayati ve pahalı sistemler olması nedeniyle çok daha fazla önem kazanmaktadır. Bilindiği üzere, kritik altyapılar ulusların güvenliği konusunda oldukça hassas noktalardır. Kritik altyapılardaki zafiyetler, milyarlarca dolar hasara yol açа-

bilmekte, milyonlarca insanı etkileyebilmekte, can ve mal kaybına sebep olabilmektedir. Bu yüzden, kritik altyapıların sürekli test ve güvenlik risklerinin yönetilmesi oldukça önemlidir.

Akademik kritik altyapı simülasyon çalışmaları genellikle modelleme uygulamaları kullanmış, bir siber saldırıyı tasarlayıp modele dökerek girilmeye çalışan sistemin zafiyetlerinin tespit ettikleri bir yöntem benimsemişlerdir. Lee et. al. bir Linux sistemini analiz etmiş, ardından DEVS modelleme ve simülasyon ortamını kullanarak bir Linux bazlı bir model geliştirmiştir. Bunun sonucunda, siber saldırının detaylarını tekrardan üretebilmenin yanı sıra, siber saldırı sonucunda sistem değişimlerini de saptayabilmiştir [48]. Ayrık olaylı simülasyonun kullanıldığı bu çalışmada ise girilecek sistemin modellenmesi ARENA üzerinden yapılmış, çıktılar analiz edilmiştir [49]. Literatürdeki simülasyon uygulamalarının modelleme üzerine odaklanmasının sebebi olarak ise, önceden bahsedilen programların halihazırda var olan bir sisteme entegrasyonunun gerekmesi ve endüstriyel ölçekte çalışması gösterilebilir. Araştırmayı hazırlayan bireylerin elinde bu tarz sistemlere ulaşım gibi bir imkân olmadığı durumda, önce bir sistem çeşitli yazılımlar kullanılarak modellenmekte, ardından modellenen bu sistem siber saldırılar düzenlenerek test edilmektedir.

5.8.1. InfectionMonkey

GPL v3 açık kaynak koduyla yazılmış InfectionMonkey, açık kaynak kodlu bir simülasyon programıdır. Google Cloud'da, AWS, Azure ya da şirket içi sistemlerdeki altyapıları test eden InfectionMonkey, Windows, Debian ya da Docker'a kurulabilmektedir. ZT, ATT&CK MITRE ve Breach and Attack saldırılarına karşı simülasyon yapabilmekte ve kimlik hırsızlığı, güvenliği ihlal edilmiş varlıklar, yanlış yapılandırma vb. tehditlere karşı, ağ bazında sürekli otomatik saldırılar düzenleyebilmektedir. InfectionMonkey, kurulumu oldukça kolay olan bir simülasyon sistemidir. Düzenlediği saldırılar ağ operasyonlarını etkilememektedir fakat geniş yelpazeli raporu sayesinde uygulanabilir önerilerde bulunabilmektedir. Bunların yanı sıra, görsel olarak hem ağı hem de saldırganın haritasını çıkarabilmektedir. CPU ve hafıza kullanımının düşük olması da başka bir pozitif yön olarak değerlendirilebilmektedir [50].

5.8.2. NeSSi

Açılımı Network Security Simulator olan Nessi, JIAC platformunu (framework) kullanan açık kaynak kodlu bir yazılımdır. Daha çok saldırı tespit algoritmaları, ağ analizi ve profil bazlı otomatik saldırıları test etmek için kullanılmaktadır. Kurulumu ve çalışması için Java SE 7 ve MySQL gerekmektedir [51].

5.8.3. Foreseeti

Foreseeti, securiCAD tarafından oluşturulmuş, yapay zeka bazlı siber saldırı simülasyon programıdır. Saldırı örüntüleriyle siber riskleri tespit etmekte ve yüksek öncelikli tehditleri, riskleri, zayıflıkları yüksek doğrulukta bulabilmektedir. Büyük bir kısmı otomatikleştirilmiş olan Foreseeti'yi kurmak oldukça kolaydır.

Foreseeti, üç adımla çalışmaktadır. Önce bir model kurulur ve server, router, firewall vb. gibi, test edilecek bütün unsurlar bu modele eklenir. Ardından bir saldırı simülasyonu düzenlenir. Bu saldırının sonucunda ise oluşturulan rapor takip edilerek sistemin genel riskinin azaltılması hedeflenmektedir [52].

5.8.4. AttackIQ

Oldukça popüler güvenlik doğrulama platformlarından biri olan AttackIQ, ofensif/defensif (offansive-defensive) bir sistem olarak ortaya çıkmaktadır. MITRE ATT&CK platformunu kullanan AttackIQ, güvenlik sektörünün liderlerden biridir. Gerçek hayattaki tehditleri simüle edebilmek için özelleştirilmiş saldırı senaryoları kullanılabilmekte ve sürekli güvenlik raporu için saldırılar otomatikleştirilebilmektedir. Bu işlemleri, altyapı üzerinde yük oluşturmadan yapmaktadır. AttackIQ'nun sektör lideri olmasının bir diğer sebebi üst düzey şeffaflık sağlıyor olmasıdır [53]. Bütün bunların yanı sıra, AttackIQ aynı zamanda eğitim olanakları da sağlamaktadır. Telefon, eposta ve internet sitesi desteğinin 24/7 kullanılabildiği program, bir haftalık deneme sürecinin ardından $5000 fiyatından başlamaktadır [54].

5.8.5. XM Cyber

XM Cyber, otomatikleştirilmiş APT üzerinde özelleşmiş bir simülasyondur. Tamamıyla otomatikleştirebilen XM Cyber, sürekli rapor üretebilmekte ve Breach and Attack, güvenlik durum görünürlüğü, saldırma bazlı zafiyet yönetimi, bulut güvenlik yönetimi vb. çözümler sunmaktadır. Microsoft, AWS, Cortex ve Crowdstrike'a entegre edilebilmektedir. İhtiyaca göre saldırı senaryoları oluşturabilmenin yanı sıra, saldırı yollarını görselleştirme ve güncel saldırı metotlarını takip etme gibi artıları da bulunmaktadır. Hedef seçilip çalıştırıldıktan sonra öncelikli çözümlerin verildiği bir rapor sunmaktadır. Avrupa Birliği'nin Genel Veri Koruma Yönetmeliğinin de kullandığı XM Cyber'ın, demo sürecinin ardından tek seferlik $95,000 gibi bir ücreti bulunmaktadır [55].

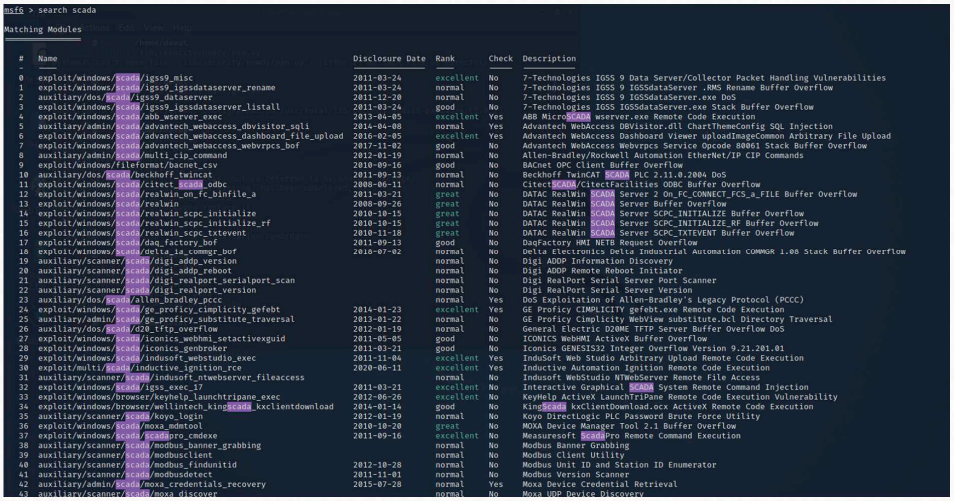
5.9. KRİTİK ALTYAPI SALDIRI ARAÇLARI

Kritik altyapı sistemlerinin test edilmesi ve güvenlik sıkılaştırma faaliyetlerinin yürütülmesi için keşif ve saldırı aşamalarında kullanılacak araçların kullanılması gerekmektedir. Kullanılan protokollerin ve arayüzlerin standart dışı üretilmiş versiyonlarının test ve değerlendirme süreçlerinde geliştirilecek betikler üzerinden saldırı / test faaliyetlerinin gerçekleştirilmesi gerekmektedir. Ağ üzerinde açık portlar ve çalışan servislerin belirlenmesinde NMAP ve ağ üzerindeki paketleri dinlemeye yarayan WireShark uygulamaları her pasif ve aktif saldırı / test senaryosunun başında kullanılmaktadır.

5.9.1. Metasploit Framework

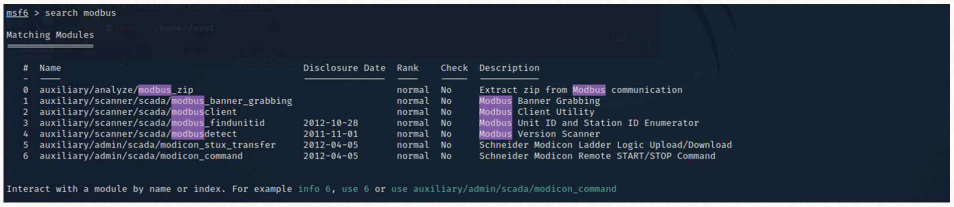
Metasploit açık kaynak kodlu bir açıklık (exploit) platformudur. Metasploit, geleneksel BT sistemlerinde sızma testi yapmak için güçlü bir araç olarak yaygın bir şekilde kabul edilmektedir ancak çok az kişi günümüzde giderek daha önemli bir yere sahip olan SCADA/ICS sektöründe de yeteneklere sahip olduğunun farkındadır. Metasploit Framework birçok SCADA açıklığı (exploiti) barındırdığından ICS-SCADA tarama testi (pentest) için kullanılan en yaygın platformlardan (frameworklerden) biridir [34]. Metasploit aracı açıldı-

ğında Search SCADA komutu çalıştırılarak birçok exploit, auxiliary ve scanner modülleri Şekil 5.1'de görülmektedir.



Şekil 5.1. Metasploit Framework SCADA Modülleri

Endüstriyel kontrol sistemlerinin kullandığı haberleşme protokollerini istismar etmek için kullanılan araçlar Şekil 5.2'de verilmiştir.



Şekil 5.2. Metasploit Framework Modbus Modülleri

5.9.2. ISF - Industrial Control System Exploitation Framework

ISF (Industrial Exploitation Framework), Python ile yazılmış ve açık kaynak proje routersploit tabanlı bir exploitation framework'tür. Çoklu programlanabilir mantık denetleyicisi (PLC) ve Endüstriyel Kontrol Sistemi (ICS) yazılımı ile güvenlik açıklarını test etmemize yardımcı olmaktadır. Endüstriyel kontrol sistemlerinin kullandığı protokoller ISF aracında Tablo 5.2'de bulunmaktadır.

Tablo 5.2. ISF- EKS protokol istemcileri [56]

Name	Parh	Description
modbus_tcp_client	icssploit/clients/ modbus_tcp_client.py	Modbus-TCP Client
wdb2_client	icssploit/clients/wdb2_client.py	WdbRPC Version 2 Client
s7_client	icssploit/clients/ s7_client.py	s7comm Client

ISF aracında bulunan exploitler Tablo 5.3'te bulunmaktadır.

Tablo 5.3. ISF Exploit Modülü [56]

Name	Path	Description
s7_300_400_plc_control	exploits/plcs/siemens/s7_300_400_plc_control.py	S7-300/400 PLC start/stop
s7_1200_plc_control	exploits/plcs/siemens/s7_1200_plc_control.py	S7-1200 PLC start/stop/reset
vxworks_rpc_dos	exploits/plcs/vxworks/vxworks_rpc_dos.py	Vxworks RPC remote dos (CVE-2015-7599)
quantum_140_plc_control	exploits/plcs/schneider/quantum_140_plc_control.py	Schneider Quantum 140 series PLC start/stop
crash_qnx_inetd_tcp_service	exploits/plcs/qnx/crash_qnx_inetd_tcp_service.py	QNX Inetd TCP service dos
qconn_remote_exec	exploits/plcs/qnx/qconn_remote_exec.py	QNX qconn remote code execution
profinet_set_ip	exploits/plcs/siemens/profinet_set_ip.py	Profinet DCP device IP config

ISF'da bulunan port veya daha farklı taramalarda kullanılan Tablo 10.4'de Endüstriyel kontrol sistemleri için kullanılan scapy modülleri Tablo 10.5'te verilmiştir.

Tablo 5.4. ISF tarama modülleri [56]

Name	Path	Description
profinet_dcp_scan	scanners/profinet_dcp_scan.py	Profinet DCP scanner
vxworks_6_scan	scanners/vxworks_6_scan.py	Vxworks 6.x scanner
s7comm_scan	scanners/s7comm_scan.py	S7comm scanner
enip_scan	scanners/enip_scan.py	EthernetIP scanner

Tablo 10.5. ISF Scapy Modülleri [56]

Name	Path	Description
pn_dcp	icssploit/protocols/pn_dcp	Profinet DCP Protocol
modbus_tcp	icssploit/protocols/modbus_tcp	Modbus TCP Protocol
wdbrpc2	icssploit/protocols/wdbrpc2	WDB RPC Version 2 Protocol
s7comm	icssploit/protocols/s7comm.py	S7comm Protocol

5.9.3. RouterSploit Framework

RouterSploit Framework, network cihazlarının güvenlik testlerini yapabilmek ve gömülü cihazlar üzerinde kullanabilmek için yazılmış açık kaynaklı bir güvenlik aracıdır. Şekil 5.3'te RouterSploit Frameworkü ICS/SCADA protokolleri için kullanıllan exploitler görülmektedir.

```
rsf > show exploits
exploits/routers/mikrotik/winbox_auth_bypass_creds_disclosure
exploits/routers/mikrotik/routeros_jailbreak
exploits/routers/netgear/n300_auth_bypass
exploits/routers/netgear/multi_password_disclosure-2017-5521
exploits/routers/netgear/prosafe_rce
exploits/routers/netgear/wnr500_612v3_jnr1010_2010_path_traversal
exploits/routers/netgear/multi_rce
exploits/routers/netgear/r7000_r6400_rce
exploits/routers/netgear/dgn2200_ping_cgi_rce
exploits/routers/netgear/jnr1010_path_traversal
exploits/routers/netgear/dgn2200_dnslookup_cgi_rce
exploits/routers/movistar/adsl_router_bhs_rta_path_traversal
exploits/routers/linksys/1500_2500_rce
exploits/routers/linksys/smartwifi_password_disclosure
exploits/routers/linksys/wap54gv3_rce
exploits/routers/linksys/eseries_themoon_rce
exploits/routers/linksys/wrt100_110_rce
exploits/routers/multi/gpon_home_gateway_rce
exploits/routers/multi/tcp_32764_rce
exploits/routers/multi/rom0
exploits/routers/multi/misfortune_cookie
exploits/routers/multi/tcp_32764_info_disclosure
exploits/routers/ipfire/ipfire_shellshock
exploits/routers/ipfire/ipfire_oinkcode_rce
exploits/routers/ipfire/ipfire_proxy_rce
```

Şekil 5.3. RouterSploit Frameworkü ICS/SCADA protokolleri için exploitleri

5.9.4. Immunity Canvas

Immunity Canvas framework'u içerdiği SCADA+ paketi ile ICS/SCADA sistemlere yönelik birçok exploit barındırmaktadır.

SCADA+ Paketi

Bu, herkese açık TÜM SCADA güvenlik açıklarını tek bir istismar paketinde toplama girişimidir. SCADA ve ilgili güvenlik açıkları, hassas yapıları ve başarılı bir kullanımla ilgili olası büyük etkileri nedeniyle çok özeldir.

SCADA+ Paketinin özellikleri:

- 350'ye yakın istismar bulunmaktadır.
- Düşük gerçek sistemler nedeniyle, yama sıralaması istismarları daha uzun bir süre için geçerlidir.
- Kamuya açık SCADA güvenlik açıklarının çoğunu barındırmaktadır (Eski ve yeni keşfedilen hatalar dahil)
- Kendi derinlemesine araştırma yapar.
- Endüstriyel yazılım ve donanım ortamına odaklanmıştır.
- Sadece SCADA değil, Endüstriyel PC'ler, akıllı çipler ve endüstriyel protokoller de gözden geçirilmektedir.
- Pek çok endüstriyel cihaz, sabit kodlanmış parola vb. gibi zayıflıklardan etkilenmektedir.

5.9.5. Core Impact / EX-Craft

CORE Impact, sızma test aracı olmasının yanında güvenlik açıklarını değerlendirmek ve test etmek için en kapsamlı çözümdür. CORE Impact: sistem, aygıt ve uygulamalar arasında pivot yapan saldırıların çoğaltılmasını güçlendiren ve kötüye kullanıma açık zafiyet zincirlerinin görevde kritik sistemleri ve verilere nasıl büyük riskler oluşturduğunu ortaya koyan tek çözümdür.

Özellikleri

- Ele geçirilen sistemler üzerinden exploit çalıştırma
- Payload olarak "Core Agent" kullanımı
- Harici araçlar ve rapor üretme yeteneği ile tam bir denetim aracı
- Başarılı bir grafik arabirimi bulunmakta
- Çok sayıda uzak ve yerel exploit bulunmakta
- Recon ve exploitler python ile yazılmış ve açık kaynak kodlu
- İnlineEGG ile Shellcode oluşturma

5.10. KRİTİK ALTYAPI SALDIRI YÜZEYLERİ

Saldırı yüzeyleri, bir bilişim sisteminde saldırılabilecek bütün noktaların toplamına işaret eder. Bu noktalar, saldırganlar tarafından sistemlere girmek, kontrol etmek, bilgi çalmak ya da kullanmak için kullanılabilir. Saldırı yüzeylerinin büyüklüğü, kritik altyapılar için daha da büyük bir risk teşkil etmektedir. Kritik altyapılarda oluşacak herhangi bir risk, bu altyapıların hepsinin birbirine bağımlı ve entegre olması sebebiyle, sadece bu altyapıyı değil, daha başka pek çok sistemi de etkileyebilmekte ve tehlikeye atmaktadır [57].

Basit bir ifadeyle saldırı yüzeyi, bir saldırgan tarafından istismar edilebilecek veya kaçınılabilecek güvenlik kontrollerinizdeki tüm boşluklardır. Buna yazılımlar, işletim sistemleri, web uygulamaları, IoT ve mobil cihazlar, web sunucuları, veri merkezlerinin yanı sıra kilitler gibi fiziksel kontroller ve kimlik avı, hedefli kimlik avı ve oltalama gibi sosyal mühendislik saldırılarına karşı savunmasız olabilecek çalışanlar dahildir.

5.10.1. Saldırı Yüzeylerinin Oluşması

Sistemler karmaşıklaştıkça ve büyüdükçe, kontrol edilmeleri de oldukça zorlaşmaktadır. Yazılımın kodunun uzunluğu, karmaşıklığı, diğer sistemlere bağımlılığı arttıkça saldırganların bu sistemleri sömürmesi ve istismar etmesi de kolaylaşmaktadır. Elbette ki sistemlerin hepsinin %100 güvenli olması beklenmemektedir. Özellikle sonradan eklenen, kodun orijinal hali yazılırken düşünülmemiş fonksiyonlar, yazılıma entegre edilen sistemler vb. saldırı yüzeylerinin büyümesine olanak sağlamaktadır [58,60]

Saldırı yüzeyleri sürekli aynı boyutta kalmamaktadır. Bir sistemdeki güvenlik açıkları giderildikçe, saldırı yüzeyleri küçülebilmekte, ya da baştan savma eklenen bir fonksiyon sebebiyle büyüyebilmektedir.

5.10.2. Saldırı Yüzeyi Elementleri

Bir saldırı yüzeyi her sistemde aynı olmak zorunda değildir, ancak pek çok sistemde ortak bulunan elementler bulunmaktadır. Hassas verileri, iş ile ilgili verileri, kişisel olarak tanımlanabilir bilgileri veya korunan sağlık bilgilerini

barındıran veya bunlara erişimi olan her şey özellikle bu yüzeylerde bulunmasa bile incelenmelidir. Saldırı yüzeylerinden bazıları aşağıda sıralanmıştır.

Temel Saldırı Yüzeyi Türler [59];

- Dijital saldırı yüzeyi
- Fiziksel saldırı yüzeyi
- Sosyal mühendislik saldırı yüzeyi

Ağ Yapısına göre;

- İç Ağ
- Dış Ağ
- Kişisel Ağ

Hizmet şekline göre;

- Fiziksel Arayüzler ve Ekranlar
- Cihaz Bileşenleri
- Ağ Hizmetleri
- Yazılımsal API Hizmetleri
- Bulut Hizmetleri
- Web Arayüz
- Mobil Arayüz

Siber İstihbarat

- IP Adresleri
- Domain ve alt domainler
- SSL sertifikaları
- WHOIS kayıtları
- E-mailler
- Görselleştirme

Bilişim sistemleri, somut elementlerine karşın soyut konseptlerdir. Diğer pek çok konuda olduğu gibi sistemin bütün elemanlarını ve unsurlarını haritalamak, sistemin kendisini anlama konusunda atılabilecek en büyük adımlardan

biridir. Sistem tüm bileşenleri ve bağlantıları ile anlaşıldıktan sonra saldırı yüzeyi detaylı bir şekilde çıkarılabilir.

5.11. KRİTİK ALTYAPILAR İÇİN GÜVENLİK ÖNERİLERİ

Kritik altyapılar, ülkelerin temel ihtiyaçlarına (elektrik, doğalgaz, benzin, su, ulaşım…) yönelik hizmetlerin sağlanmasında ana işlevleri sağlayan bilgisayarları ve uygulamaları içermektedir. Kritik altyapılar, sahada bulunan operasyonun izlenmesi ve uzaktan kontrol edilmesine izin verip insanlar için büyük kolaylık sağlamaktadır. Fakat bu kontrol sisteminin uzaktan olması ve bu sistemin işlevselliği öne çıkarıp güvenlikten ödün vermesinden dolayı bazı kamu kurumları ya da ülkelerin kritik altyapılarının zafiyet vermesine neden olabilir. Bu uygulamaların kullanıldığı sistemler ülkenin önemli altyapılarını oluşturduğu için ülkeler korunma ve güvenlik ihtiyacı duymaktadırlar. Bu güvenlik zafiyetini çözmek adına ülkedeki tüm kamu kurumları veya özel kuruluşlar kritik altyapıların siber güvenliğini sağlamak için çeşitli sıklaştırma tedbirlerini uygulamaktadır. Tedbirlerden temel olanlar ise izleyen başlıklar altında incelenmiş ve öneriler yapılmıştır.

i. SCADA ağları tanımlanmalıdır.

SCADA ağında var olan tüm bağlantıların riskini ve bağlantıların gereklilik durumu için yapılan kapsamlı risk analizi ile bağlantıların korunma dereceleri gözlemlenebilmektedir. Böylece iş ağları dahil olmak üzere dahili yerel alan ve geniş alan ağları, internet, kablosuz ağ cihazları ve dahili uydu bağlantıları, modem ve çevirmeli bağlantılar, iş ortaklarına ait bağlantılar, satılıcılar ve düzenleme kurumları gibi bağlantı türlerinin tanımlamaları yapılmakta ve değerlendirilebilmektedir.

ii. Kritik altyapılardaki gereksiz bağlantılar kaldırılmalıdır.

Özellikle internet üzerinden yapılan saldırılarda, bir bağlantıya yapılan saldırı diğer bağlantılarda güvenlik zafiyetlerine oluşturabilmektedir. Bu yüzden güvenli olmayan bağlantılar tespit edilmeli ve bu bağlantıların varlığı ile risk alınmamalıdır. Kritik altyapıların güvenliği sağlamadaki en kesin çözüm ise diğer bağlantılar ile ilişiğinin kesilmesidir. Gereken korumayı sağlamak

için temel hedef ise SCADA ağlarını izole etmektir. "Demilitarized zones" (DMZ'ler) ve veri ambarı kullanımı gibi stratejiler, verilerin SCADA ağından iş ağlarına güvenli bir şekilde aktarılmasını kolaylaştırabilmekte fakat yanlış yapılandırma ile ek riskler ortaya çıkabilecek olması unutulmaması gereken bir sonuçtur. Bu sonucu önlemek için ise stratejiler uygun şekilde tasarlanmalı ve uygulanmalıdır

iii. Kritik altyapılarda ağındaki tüm bağlantıların güvenliği kontrol edilmeli ve güçlendirilmelidir.

Kritik altyapılarda var olan tüm bağlantıların korunma durumunu değerlendirmek için sızma testi veya güvenlik açığı analizi yapılmalıdır. Kritik altyapılarda güvenlik derecesi en zayıf bağlantı noktasıyla eş değer olduğu için giriş noktasında güvenlik duvarları, izinsiz giriş veya saldırı tespit sistemleri (Intrusion Detection System, IDS) ve diğer güvenlik sistemleri gibi önlemlerin alınması oldukça önemlidir. Kritik altyapılarda erişimi engellemek için güvenlik duvar kuralları yapılandırılmalı ve bağlantı onay izni verilirken olabildiğince spesifik olunmalıdır. Aynı zamanda muhtemel ağ güvenliği ihlallerine karşı güvenlik personellerini uyarmak adına her giriş noktasına stratejik olarak IDS'ler yerleştirilmelidir.

iv. Kritik altyapıları güçlendirmek için gereksiz hizmetler kaldırılmalı ya da devre dışı bırakılmalıdır.

Açık kaynak kodlu işletim sistemi üzerine kurulu kontrol sunucularının varsayılan ağ hizmetleri vasıtasıyla saldırılara maruz kalabileceğinden kullanılmayan hizmetler ve arka plan programları kaldırılması ya da devre dışı bırakılması gerekmektedir. Aksi takdirde ilişiği kesilmeyen bağlantılar kritik altyapılarda güvenlik açığı oluşturabilmektedir. Bu yüzden kritik altyapı ağına bağlanacak olan bir hizmetin olumlu ya da olumsuz oluşturabileceği tüm sonuçlar değerlendirilmeden ağ bağlantısına izin verilmemesi gerekmektedir. Hizmet olarak kastedilen terimlere otomatik sayaç okuma, uzaktan faturalandırma sistemi, internet vb. örnek olarak verilebilir. Bu gibi hizmetlerin kaldırılması ya da devre dışı bırakılması sonucunda eksikliklerin oluşacağı ve istenmeyen sonuçlar meydana geleceği öngörülüyor ise daha güvenli yapılandırma ve operasyonel sistemlerdeki tüm değişiklikleri koordine etmek gerekmektedir.

v. Sistemin korunması için özel protokollere güvenilmemelidir.

Kritik altyapılarda kullanılan bazı SCADA sistemleri, saha cihazları ve sunucular arasındaki iletişimi sağlamak için bazı özel protokoller kullanmaktadır. Genel olarak ise SCADA sistemlerinin güvenliği yalnızca bahsedilen protokollerin gizliliği ile sağlanmakta ve korunmaktadır. Belirsiz protokollerin düşük miktarda gerçek güvenliği sağlaması sistemi korumak için özel protokollere ya da fabrika varsayılan ayarlarına güvenilmemesi gerektiğinin bir kanıtıdır. Güvenmemenin yanı sıra SCADA hizmet sağlayıcılarından bir arka kapı ya da satıcı ara yüzünün gösterilmesinin talep edilmesi oldukça önemli bir hamle olarak nitelendirilebilmektedir.

vi. SCADA ağında arka kapı olarak kullanılabilecek ortamlarda güçlü kontroller kullanılmalıdır.

SCADA sistemlerinde arka kapıların veya satıcı bağlantılarının bulunduğu durumlarda, iletişim ve bakım için kullanılan modemler ve kablolu-kablosuz ağların önemli güvenlik açıklarına sebep olabileceğinden ötürü güvenli iletişim sağlamak için güçlü kimlik doğrulama uygulanmalıdır. Gerçekleştirilen bir ağ saldırısı, saldırganın diğer tüm kontrolleri atlayıp SCADA ağına veya kaynaklarına doğrudan erişmesine izin verebilmektedir. Bu tür saldırıların riskini minimum düzeyde tutabilmek için gelen erişim devre dışı bırakılmalıdır.

vii. Sistemler 7/ 24 izlenmelidir.

Siber saldırılara etkin bir şekilde yanıt verebilmek amacıyla ağ yöneticilerini dahili veya harici kaynaklardan kaynaklanan kötü niyetli ağ etkinliği konusunda uyarmayı içeren bir saldırı tespit stratejisinin oluşturulması gerekmektedir. Oluşturulan saldırı tespit sistemlerinde çağrı cihazı yardımıyla kolayca kurulan alarm işlemi 7/24 yapılmalıdır. Bunların dışında herhangi bir saldırıya etkili yanıt verilmesini sağlamak için olaya tepki prosedürleri bulunmalıdır. Ağı izleme işleminin tamamlanması için tüm sistemlerde günlük kayıt yapma etkinleştirilmeli ve şüpheli davranışları tespit etmek amacıyla kaydolan günlüklerin denetimi günlük olarak yapılmalıdır.

viii. Fiziksel güvenlik anketleri yapılmalı ve güvenlik durumunu değerlendirilmelidir.

Özellikle insansız ve korumasız uzak alanlar olmak üzere kritik altyapı ile bağlantısı olan herhangi bir konum saldırıların ana hedefidir. Bu yüzden din-

lenebilecek telefon, bilgisayar ağı, fiber optik kablolar dahil her türlü bilgi kaynağı kontrol edilmeli ve radyo ve mikrodalga bağlantıları gibi sömürülebilecek alanları değerlendirilmelidir. Bu süreçte korumasız uzak alanlarda canlı ağ erişim noktalarına izin verilmemesi kolaylık sağlayabilmektedir.

ix. Oluşabilecek saldırı senaryolarını tanımlamak ve değerlendirmek için kırmızı takım kurulmalıdır.

Olası herhangi bir saldırı senaryosunda saldırının potansiyel etkilerini değerlendirmek ve muhtemel güvenlik zafiyetlerini tespit etmek için kırmızı takım oluşturulmalı, sistemlerin zayıf noktaları hakkında yetkin kişilerden destek alınmalıdır. Edinilen bilgileri değerlendirmek ve uygun koruma stratejileri oluşturmak için kırmızı takım değerlendirmesinden kaynaklanan bilgiler risk yönetim süreçlerine aktarılmalıdır.

x. Personel için siber güvenlik rolü, sorumluluklar ve yetkiler açıkça tanımlanmalıdır.

Gereken sorumluluklar çalışanlara verilerek bilgi teknolojisi kaynaklarının korunması ile ilgili beklentilerin anlaşılması sağlanmalı ve önemli görece sahip personellerin verilen sorumlulukları yerine getirmesi için gereken yetkiler tanımlanmalıdır. Siber güvenlik sorunlarının nasıl başladığı ve sürdüğü ile acil bir durumda kime ya da kimlere bildirilmesi gerektiğini gösteren siber güvenlik organizasyon yapısı oluşturulmalıdır.

xi. Ağ mimarisini belgelenmeli ve kritik işlevlere hizmet eden veya ek koruma düzeyleri gerektiren hassas bilgiler içeren sistemler belirlenmelidir.

Etkili koruma stratejisi oluşturma sürecinin bir parçası olarak güçlü bir bilgi güvenliği mimarisi geliştirilmeli ve belgelenmelidir. Genel koruma stratejisini anlamak ve tek hata noktalarını belirlemek için bilgi güvenliği mimarisini ve bileşenlerini belgelemek kritik öneme sahiptir.

xii. Risk yönetim süreci oluşturulmalıdır.

Bu adım için öncelik, bir ağ koruma stratejisi geliştirmek için kullanmak üzere mevcut bir tehdit değerlendirmesine dayalı temel risk analizi oluşturulmasınındır. Teknoloji dünyasının hızlı değişim ve gelişiminden dolayı her geçen gün yeni tehditlerin oluşması sebebiyle risk değerlendirme süreci yürütülme-

lidir. Risk yönetiminin temeli, mevcut bir ağ koruma stratejisi ile kalan riskin belirlenmesi ve bu riskin yönetim tarafından kabul edilmesidir.

xiii. Derinlemesine savunma ilkesine dayalı bir ağ koruma stratejisi oluşturulmalıdır.

Derinlemesine savunma, herhangi bir ağ koruma stratejisinin parçası olması gereken temel ilkedir ve savunma geliştirme sürecinin tasarım aşamasında erkeden düşünülmeli ve ağla ilgili tüm teknik karar verme süreçlerinde bütünleyici bir değerlendirme olarak ele alınmalıdır. Hata noktalarından ve güvenlik problemlerinin etkilerinden kaçınmak için siber güvenlik savunma mekanizması katmanlı olarak organize edilmeli ayrıca, her katmanın aynı katmandaki diğer sistemlere karşı korunması gerekmektedir.

xiv. Siber güvenlik gereksinimleri net bir şekilde belirlenmelidir.

Kamu kurumları veya özel şirketler personellerinin olaylardan sorumlu tutulmasını sağlamak için zorunlu gereksinimlere sahip yapılandırılmış güvenlik programlarına ihtiyaç duymaktadırlar. Resmileştirilmiş politikalar ve prosedürler tipik olarak bir siber güvenlik programı oluşturmak ve kurumsallaştırmak için kullanılmaktadır. Kurumların siber güvenliğin tutarlı ve standartlara dayalı olması için resmi bir program veya politika oluşturması gerekir. Böylece bireysel inisiyatife bağlılık ortadan kaldırılır. Ayrıca politika ve prosedürlerin yerine getirilmesinden sorumlu çalışanların, belirli siber güvenlik sorumlulukları ve bu sorumlulukları yerine getirmemenin sonuçları hakkında bilgilendirilmesi gereklidir. Gereksinimler ise arka plan kontrollerinin yapılması ve ağ ayrıcalıklarının kesinlikle gerekli olanlar ile sınırlandırılması da dahil olmak üzere, içeriden kötü niyetli kişilerden gelen tehdidi en aza indirmek için belirlenmelidir.

xv. Yapılandırma yöntemi belirlenmelidir.

Yapılandırma yöntemi, güvenli bir ağın devamlılığını sağlamak için temel bir yönetim sürecidir. Yapılandırma yönetiminin hem donanım yapılandırmalarını hem de yazılım yapılandırmalarını kapsaması gerekmektedir. Donanım veya yazılımdaki değişiklikler, ağ güvenliğini zayıflatan güvenlik açıklarını kolayca ortaya çıkarabilmektedir. Bundan dolayı yönetim süreçleri ağın güvenli kalmasını sağlamak, herhangi bir değişikliği değerlendirmek ve kontrol etmek için kullanılması gerekmektedir.

xvi. Öz değerlendirmeler yapılmalıdır.

Kurumsal şirketlerin en önemli özellikleri sorunları kendi kendine tanımlayabilen, temel neden analizleri yürütebilen, bireysel ya da sistematik sorunları ele alıp etkili düzeltme teknikleri uygulayabilen kuruluşlar olmalarıdır. Kısaca öz değerlendirme yapabilen kurumlar olmalarıdır. Etkili bir siber güvenlik programın parçası olan öz değerlendirme süreçleri, güvenlik açıkları için rutin taramayı, ağın otomatik denetimini, kurumsal ve bireysel performansın öz değerlendirmelerini içermektedir.

xvii. Sistemler yedeklenmeli ve afet kurtarma planlamaları oluşturulmalıdır.

Muhtemel bir saldırı durumunda hızlı şekilde kurtarma yapabilmek için olağanüstü durum kurtarma planı yapılmalı ve ilave olarak sistem yedeklenmelidir. Yedekleme, ağın hızlı şekilde yeniden yapılandırılmasına olanak tanımaktadır. Bu planlamaların çalıştıklarından ve personelin bu planlar hakkında bilgi sahibi olduğundan emin olmak için olağan üstü durum kurtarma planlarını rutin olarak uygulanması gerekmekte ve uygulanan planlardan alınan geri dönüşler ile planlarda gerekli değişikliklerin yapılması gerekmektedir.

5.12. SONUÇ VE DEĞERLENDİRMELER

Kritik altyapılar, çeşitli sektörlerin ve uygulamaların karşılıklı bağımlılıkları ile bir arada çalışan sistemler bütünüdür. Bulundukları ülkelere, hedef aldıkları sektörlere ve uygulamalara göre farklılık göstermektedir. Bu farklılıklar kritik altyapıların kontrol zamanlaması gereksinimleri, coğrafi koşullar, hiyerarşi, kontrol karmaşıklığı, kullanılabilirlik, hata yayılımı ve emniyet olarak çeşitli karakteristik özellikler göstermesine neden olmaktadır.

Ülkeler kritik altyapılardaki güvenlik ve emniyet konularını ulusal güvenlik kapsamında değerlendirmektedir. Ülkeler mevcut geleneksel bilgi teknolojilerine yönelik önlem ve standartlara benzer çalışmaları kritik altyapılar için de gerçekleştirmektedir. Ülkelerin kendi kritik altyapılarını inceleyerek önlem almaları ve ulusal standartlar konusunda çalışmalar yapması ulusal siber güvenlik riskinin azalmasına katkı sağlayacaktır. Avrupa Birliği gözünden

kritik alt yapılar değerlendirildiğinde toplamda 9 sektörün bu tanım içerisine alındığı görülmektedir. Genel kapsamda işleyişinde aksama meydana gelmesi durumunda yaşamsal faaliyetlerde duraksama gerçekleştirme potansiyeli olan sektörler bu kapsamdadır. Kritik altyapılarda meydana gelen hata ve siber saldırılar sonucunda yıkıcı etkilerin ortaya çıkacağı geçmişte yaşanan olaylar ile deneyimlenmiştir. Kritik altyapılarda bulunan riskleri analiz etmek, siber güvenlik zafiyetlerini ve etki alanını değerlendirmek, güvenli modeller tasarlamak için yaşanan olaylardan ders çıkarımı yapılması gerekmektedir.

Kritik altyapıların siber güvenliğini sağlamak için güvenlik zafiyetleri araştırılmalıdır. Bu kitap bölümünde kritik altyapılarda sık görülen güvenlik zafiyetleri araştırılmış ve paylaşılmıştır. Güvenlik zafiyetlerinin oluşmasına neden olan hatalı düşünce ve tasarımların düzeltilebilmesi için analiz edilmiştir. Kritik alt yapılarda zafiyetlerin araştırılması, analiz edilmesi ve konsept kanıtları üzerinde çalışılabilmesi için simülasyonlara ihtiyaç duyulmaktadır. Simülasyonlar sayesinde gerçek dünyada yıkıcı etkilere neden olabilecek zafiyetlerin doğrulanması zararsız bir şekilde gerçekleşebilmektedir. Simülasyonlar üzerinde saldırıları gerçeklemek, mevcut saldırı vektörlerini uygulamak için birtakım saldırı araçları kullanılmaktadır. Bu saldırı araçları kritik altyapılara ilişkin zafiyetlerin araştırılması ve kurulu altyapılarda sızma testleri uygulanması amacıyla kullanılmaktadır.

Kritik altyapılara yönelik yapılan araştırmalar ve zafiyet incelemeleri sonucunda kritik altyapıların güvenliğini sağlamak için çeşitli sıkılaştırma tedbirleri oluşturulmuştur. Kritik altyapılarda fiziksel nesneler ile bilgisayar teknolojilerini bir araya SCADA sistemleri sıkılaştırma tedbirlerinin en yoğun uygulandığı sistemlerdir. Bu nedenle SCADA sistemlerinin haberleşme ağının, kurum içerisinde var olan diğer bütün ağlardan fiziksel olarak ayrı şekilde tasarlanması ve ağlar arası geçiş ihtimalinin olmaması gerekmektedir. Kritik altyapılarda kullanılan bazı cihazlara servis/teknik destek gerekçeleri ile internet ve kurumsal ağlar üzerinden geçişe izin veren yapılar kurulmaktadır. Kurulan bu yapıların erişim kuralları üzerinden kısa süreli olarak oluşturulması hatta zorda kalmadıkça kullanılmaması önerilmektedir. Ağda akan trafiğin ulaştığı tüm noktaların kontrol edilmesi, ağdaki tüm cihazların tanınması gerekmektedir. Ayrıca ağda kullanılan geleneksel güvenlik cihazları yerine uygulamaya yönelik, cihazları ve protokolleri analiz edebilen endüstriyel

cihazların kullanılması gerekmektedir. İzleme ekranlarında bulunan işletim sistemleri özelleştirilerek ihtiyaç duyulmayan tüm kütüphane ve servislerin kaldırılması veya durdurulması gerekmektedir. Kritik altyapılardaki fiziksel nesnelerin izlenmesine ek olarak ağdaki iletişimde sürekli olarak izlenmelidir. Belirli aralıklarda sistem ve personeller üzerinde değerlendirme çalışmaları yapılmalıdır. Personellere ihtiyaç duyabilecekleri siber güvenlik bilgisi ihtiyaç duyulmadan önce sağlanmalıdır. Sistemleri hedef alabilecek saldırı senaryoları tasarlanmalı, tatbikatları yapılmalı ve personellere görev dağılımları verilmelidir. Sistemler önem derecesine göre belirli periyotlarda yedeklenmelidir. Tüm çalışmaların perspektifinde sisteme ilişkin afet kurtarma planları ve risk yönetimi süreçleri oluşturulmalıdır.

Günümüz dünyasında ulusal güvenliği sağlamanın en önemli adımlarından biri kritik altyapıların dahili ve harici düşmanlardan saklanması ve korunmasıdır. Kritik altyapıların saklanması ancak onlara erişimin zorlaştırılması ve paylaşılan sıkılaştırma tedbirlerinin uygulanması ile mümkün olabilmektedir. Korunması ise güvenlik zafiyetlerinin derinlemesine incelenmesi, tedbirlerinin alınması ve daha güçlü bir yapıya bürünmesi ile sağlanabilmektedir.

Teşekkür

Bu çalışma İstanbul Üniversitesi – Cerrahpaşa bünyesinde İstanbul Kalkınma Ajansı tarafından desteklenen YMP-0061 Nesnelerin İnterneti Ekosistemi Güvenlik Test ve Değerlendirme Merkez'i araştırmacıları tarafından hazırlanmıştır. Yazarlar İstanbul Kalkınma Ajansına teşekkür eder.

KAYNAKLAR

[1] S. Berger, O. Bürger, and M. Röglinger, "Computers & Security Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy," *Comput. Secur.*, vol. 93, p. 101790, 2020.

[2] G. Falco, C. Caldera, and H. Shrobe, "IIoT Cybersecurity Risk Modeling for SCADA Systems," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4486–4495, 2018.

[3] S. Tweneboah-Koduah and W. J. Buchanan, "Security risk assessment of critical infrastructure systems: A comparative study," *Comput. J.*, vol. 61, no. 9, pp. 1389–1406, Sep. 2018.

[4] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Comput. Secur.*, vol. 70, pp. 436–454, Sep. 2017.

[5] S. McLaughlin *et al.*, "The Cybersecurity Landscape in Industrial Control Systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016.

[6] L. Rosa, T. Cruz, P. Simões, E. Monteiro, and L. Lev, "Attacking SCADA systems: A practical perspective," *Proc. IM 2017 - 2017 IFIP/IEEE Int. Symp. Integr. Netw. Serv. Manag.*, pp. 741–746, 2017.

[7] "Florida water treatment plant was involved in second security incident before poisoning attempt: report | ZDNet." [Online]. Available: https://www.zdnet.com/article/florida-water-treatment-plant-was-involved-in-second-security-incident-before-poisoning-attempt-report/. [Accessed: 12-Sep-2021].

[8] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, MD, Jun. 2015.

[9] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids – A comprehensive survey," *Comput. Stand. Interfaces*, vol. 56, pp. 62–73, Feb. 2018.

[10] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: Solutions and challenges," *J. Inf. Secur. Appl.*, vol. 52, p. 102500, Jun. 2020.

[11] M. R. Tür, R. Bayındır, and S. Vadi, *Siber Güvenlik ve Savunma Problemler ve Çözümler*, 1.baskı. Ankara: Grafiker Yayınları, 2019.

[12] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.

[13] T. Akhtar, B. B. Gupta, and S. Yamaguchi, "Malware propagation effects on SCADA system and smart power grid," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, vol. 2018-Janua, pp. 1–6.

[14] R. B. Benisha and S. Raja Ratna, "Prevention of Cyber Attacks in Control Systems: A Review," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2018, pp. 419–424.

[15] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Priv.*, vol. 9, no. 3, pp. 49–51, 2011.

[16] C. M. Lewandowski *et al.*, "Operating System Concepts," *Wiley Sons*, vol. 1, no. 3, pp. 40–46, 2013.

[17] "Yaşam Döngüsü SSS - Windows | Microsoft Docs." [Online]. Available: https://docs.microsoft.com/tr-tr/lifecycle/faq/windows. [Accessed: 15-Nov-2020].

[18] W. Knowles, J. M. Such, A. Gouglidis, G. Misra, and A. Rashid, "Assurance techniques for industrial control systems (ICS)," in *CPS-SPC 2015 - Proceedings of the 1st ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, co-located with CCS 2015*, 2015, pp. 101–112.

[19] A. Homay, C. Chrysoulas, B. El Boudani, M. de Sousa, and M. Wollschlaeger, "A security and authentication layer for SCADA/DCS applications," *Microprocess. Microsyst.*, p. 103479, Nov. 2020.

[20] G. Hayes and K. El-Khatib, "Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol," in *2013 3rd International Conference on Communications and Information Technology, ICCIT 2013*, 2013, pp. 179–184.

[21] J. M. Hatfield, "Virtuous human hacking: The ethics of social engineering in penetration-testing," *Comput. Secur.*, vol. 83, pp. 354–366, Jun. 2019.

[22] E. N. M., Liam O., Chien, "W32.Stuxnet Dossier," 2011. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[23] A. Binks, "The art of phishing: past, present and future," *Comput. Fraud Secur.*, vol. 2019, no. 4, pp. 9–11, Apr. 2019.

[24] "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks - The Henry M. Jackson School of International Studies." [Online]. Available: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/. [Accessed: 21-Nov-2020].

[25] K. Thakur, M. L. Ali, N. Jiang, and M. Qiu, "Impact of Cyber-Attacks on Critical Infrastructure," *Proc. - 2nd IEEE Int. Conf. Big Data Secur. Cloud, IEEE BigDataSecurity 2016, 2nd IEEE Int. Conf. High Perform. Smart Comput. IEEE HPSC 2016 IEEE Int. Conf. Intell. Data S*, pp. 183–186, 2016.

[26] Y. Qi, R. Jiang, Y. Jia, and A. Li, "An APT attack analysis framework based on self-define rules and mapreduce," in *Proceedings - 2020 IEEE 5th International Conference on Data Science in Cyberspace, DSC 2020*, 2020, pp. 61–66.

[27] B. Stojanović, K. Hofer-Schmitz, and U. Kleb, "APT datasets and attack modeling for automated detection methods: A review," *Comput. Secur.*, vol. 92, p. 101734, May 2020.

[28] D. N. Jones, E. Padilla, S. R. Curtis, and C. Kiekintveld, "Network discovery and scanning strategies and the Dark Triad," *Comput. Human Behav.*, vol. 122, p. 106799, Sep. 2021.

[29] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[30] D. Upadhyay and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations," *Comput. Secur.*, vol. 89, p. 101666, Feb. 2020.

[31] K. S. Kiangala and Z. Wang, "An Industry 4.0 approach to develop auto parameter configuration of a bottling process in a small to medium scale industry using PLC and SCADA," *Procedia Manuf.*, vol. 35, pp. 725–730, Jan. 2019.

[32] R. R. R. Barbosa, R. Sadre, and A. Pras, "Flow whitelisting in SCADA networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 6, no. 3–4, pp. 150–158, Dec. 2013.

[33] J. Tian, W. Xing, and Z. Li, "BVDetector: A program slice-based binary code vulnerability intelligent detection system," *Inf. Softw. Technol.*, vol. 123, p. 106289, Jul. 2020.

[34] İ. Erkek and E. Irmak, *Siber Güvenlik ve Savunma Biyometrik ve Kriptografik Uygulamalar*, 1. Basım. 2020.

[35] M. Barrett, "Framework for improving critical infrastructure cybersecurity," in Proceedings of the Annual ISA Analysis Division Symposium, 2018, vol. 535, pp. 9–25.

[36] I. F. Mikhalevich and V. A. Trapeznikov, "Critical Infrastructure Security: Alignment of Views," 2019 Syst. Signals Gener. Process. F. Board Commun. SOSG 2019, May 2019, doi: 10.1109/SOSG.2019.8706821.

[37] J. E. Rubio, R. Roman, and J. Lopez, "Analysis of cybersecurity threats in industry 4.0: The case of intrusion detection," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, vol. 10707 LNCS, pp. 119–130.

[38] H. Y. Erkal , "ENERJİ GÜVENLİĞİNE YÖNELİK TEHDİTLER VE ENERJİ GÜVENLİĞİ POLİTİKALARINDAKİ DEĞİŞİM", Ahi Evran Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, vol. 2, no. 2, pp. 63-78, Dec. 2019

[39] International Telecommunication Union, "Overview Cybersecurity," ITU-T X.1205 Recomm., vol. 1205, no. Rec. ITU-T X.1205 (04/2008), pp. 2–3, 2008, [Online]. Available: https://www.itu.int/rec/T-REC-X.1205-200804-I.

[40] "İRAM raporu: İran 2010'dan sonra operasyonel siber saldırı kapasitesini artırdı." [Online]. Available: https://www.aa.com.tr/tr/bilim-teknoloji/iram-raporu-iran-2010dan-sonra-operasyonel-siber-saldiri-kapasitesini-artirdi/2197020. [Accessed: 11-Dec-2021].

[41] "What is SCADA? Supervisory Control and Data Acquisition," 2018. [Online]. Available: https://oleumtech.com/what-is-scada. [Accessed: 11-Dec-2021].

[42] B. Drury, "Control Techniques Drives and Controls Handbook (2nd Edition) - Knovel," 2009. [Online]. Available: https://app.knovel.com/web/toc.v/cid:kpCTDCHE08/viewerType:toc/root_slug:control-techniques-drives/url_slug:control-techniques-drives/? [Accessed: 28-Aug-2021].

[43] "Top 3 Pros and Cons of the Modbus Protocol." [Online]. Available: https://www.dpstele.com/blog/top-three-pros-and-cons-of-modbus-protocol.php [Accessed: 28-Aug-2021].

[44] ABB Substation Automation, "REC 501 RP 570 Protocol Description Technical Description Manual." 1997.

[45] P. Christensson, "Protocol Definition," 2019. [Online]. Available: https://techterms.com/definition/protocol [Accessed: 28-Aug-2021].

[46] "PROFINET System Description Technology and Application PROFINET System Description." [Online]. Available: http://us.profinet.com/wp-content/uploads/2012/11/PROFINET_SystemDescription_ENG_2014_web.pdf [Accessed: 28-Aug-2021].

[47] "EtherNet/IP versus PROFINET | DigiKey." [Online]. Available: https://www.digikey.com/en/articles/ethernet-ip-versus-profinet [Accessed: 28-Aug-2021].

[48] J.-S. Lee, J.-R. Jung, J.-S. Park, and S.-D. Chi, "Linux-Based System Modelling for Cyber-attack Simulation," Lect. Notes Artif. Intell. (Subseries Lect. Notes Comput. Sci., vol.3397, pp. 585–596, 2004, doi: 10.1007/978-3-540-30583-5_62.

[49] M. E. Kuhl, J. Kistner, K. Costantini, and M. Sudit, "Cyber attack modeling and simulation for network security analysis," Proc. - Winter Simul. Conf., pp. 1180–1188, 2007, doi: 10.1109/WSC.2007.4419720.

[50] "Homepage | Infection Monkey." [Online]. Available: https://www.guardicore.com/infectionmonkey/ [Accessed: 28-Aug-2021].

[51] "NeSSi2." [Online]. Available: http://www.nessi2.de/index.html [Accessed: 28-Aug-2021].

[52] "foreseeti - foreseeti." [Online]. Available: https://foreseeti.com [Accessed: 28-Aug-2021].

[53] "SC Media | AttackIQ Platform v2.15." [Online]. Available: https://www.scmagazine.com/product-test/-/attackiq-platform-v2-15 [Accessed: 29-Aug-2021].

[54] "The Security Optimization Platform - AttackIQ." [Online]. Available: https://attackiq.com/ [Accessed: 29-Aug-2021].

[55] "Home | XM Cyber." [Online]. Available: https://www.xmcyber.com [Accessed: 28-Aug-2021].

[56] "ICSsploit (Industrial Control System Exploitation)" [Online]. Available: https://github.com/tijldeneut/icssploit [Accessed: 29-Aug-2021].

[57] P. K. Manadhata and J. M. Wing, "An attack surface metric," IEEE Trans. Softw. Eng., vol. 37, no. 3, pp. 371–386, 2011.

[58] "6 Brand Threats That Affect Your Organization - The Tools and Actionable Intelligence to Takedown Threats | RiskIQ." [Online]. Available: https://www.riskiq.com/brand-protection-resources/ [Accessed: 28-Sep-2021].

[59] "What is an Attack Surface? (And How to Reduce It)," okta, 2021. [Online]. Available: https://www.upguard.com/blog/attack-surface. [Accessed: 11-Dec-2021].

[60] "Saldırı Yüzey Analizi – SwordSec." [Online]. Available: https://swordsec.com/tr/cozumler/saldiri-yuzey- analizi/ [Accessed: 28-Sep-2021].

Bölüm 6

BİYOMETRİK SİSTEMLERDE GÜVENLİK: SALDIRI VEKTÖRLERİ VE SAVUNMA YOLLARI

Ceren Güzel Turhan - Eyüp Burak Ceyhan - Şeref Sağıroğlu

Bilişim teknolojilerindeki gelişmeler ile kullanıcı adı, şifre gibi doğrulama mekanizmalarının yerini günümüzde daha güvenli olmaları sebebiyle biyometrik sistemler almıştır. Birçok alanda yaygın olarak kullanılan biyometrik sistemlerin beklenildiği şekilde güvenli sistemler olup olmadığını belirlemek üzere çalışmalar yürütülmüştür. Yapılan araştırmalarda biyometrik sistemlere kolaylıkla sızabildiği görülmüştür. Bu nedenle, biyometrik sistemler üzerinde olası güvenlik açıklıklarının tanımlanması ihtiyacı ortaya çıkmıştır. Bu bölümde biyometrik sistemlerde saldırganlar tarafından hedef alınabilecek saldırılar üzerine bir literatür incelemesine yer verilmiştir. İncelenen çalışmalarda ele alınan saldırılar bu çalışmada genelleştirilerek sınıflandırılmış ve literatürdeki tüm örneklerine göre çok daha kapsamlı yeni bir saldırı vektörleri modeli sunulmuştur. En az performans hedefi kadar önemli olan güvenlik kriterini sistemlerin sağlayabilmeleri için önerilen yeni saldırı vektörleri modelinde tanımlanan saldırı noktalarına karşı alınabilecek tüm önlemler sunulmuştur. Bu bölümde sunulan saldırı vektörleri modeli ve korunma yöntemleri ile güvenli biyometrik sistemler sağlanabileceği gibi biyometrik sistemlerde güvenlik konusunda önemli derecede farkındalık oluşturulacağı, yeni tehditlerin engellenmesine katkılar sağlayacağı öngörülmektedir.

6.1. GİRİŞ

İnsanlar yüz, ses gibi fiziksel özellikleri dikkate alarak binlerce yıl süredir çevrelerindeki insanları tanıyabilmektedirler. 19. yüzyılın ortalarında kriminal tanıma biriminde çalışan bir kişinin tespiti ile insanlar arasındaki ön önemli ve en ayırt edici özelliklerden birinin parmak izi olması dikkat çekmiştir. Bir dizi yasal izinlerin alınması ile suçluların parmak izleri alınarak bir veritabanında kaydedilmeye başlanmıştır. İlk olarak güvenlik sebebi ile alınan parmak izleri günümüzde çok sayıda sivil uygulamada kişi tanıma amacıyla kullanılır hale gelmiştir [1].

Güvenlik amacıyla kullanılan üç farklı doğrulama mekanizması mevcuttur. Bunlardan ilki pasaport, pin, anne kızlık soyadı gibi bildiklerimizin doğrulanmasıdır. Doğrulama işlemini sahip olduğumuz bir kart şifresi veya akıllı kart ile de gerçekleştirmemiz mümkündür. Son olarak ise kendimize ait olan biyometrik diye nitelendirilen karakterleri doğrulama mekanizması olarak kullanabilmekteyiz. Tüm doğrulama mekanizmaları arasından şüphesiz en güvenilir olanı biyometriktir [2]. Biyometriğin kişiye özgü özellikler olması adına diğer doğrulama mekanizmalarına göre kopyalanmasının, taklit edilmesinin daha zor olması ve günümüz teknolojik gelişmeleri biyometrik sistemlerin yaygınlaşmasına neden olmuştur.

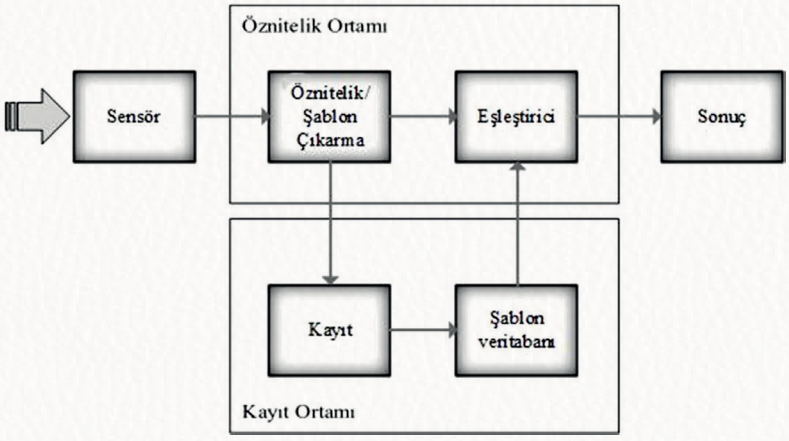
Basit bir biyometrik sistem temel olarak dört ana modülden oluşmaktadır. Bu modüller biyometrik verilerin sisteme alındığı sensör modülü, alınan veriden öznitelik vektörlerinin elde edildiği öznitelik çıkarımı modülü, elde edilen öznitelik vektörlerinin şablonlar ile karşılaştırıldığı eşleştirme modülü ve yapılan eşleştirme sonucunda kullanıcının kimliğine karar verilen karar modülü [3] olup, Şekil 6.1'de temel bir biyometrik sistem modeli gösterilmektedir.

Biyometrik sistemler doğrulama ve tanıma işlemlerini yapmak üzere oluşturulan sistemler olarak iki gruba ayrılmaktadır. Doğrulama sistemlerinde veritabanında daha önceden kaydedilen bir şablon ile karşılaştırma yapılarak kişinin tanımlanması hedeflenmektedir. Tanımlama sistemlerinde ise veritabanında yer alan tüm şablonlar ile karşılaştırma yapılarak özelliğin kime ait olduğu tespit edilmeye çalışılmaktadır [4]. Biyometrik sistemler sensör modülünde dışarıdan alınan biyometrik verinin karakterine göre adlandırılmaktadır. Bu sistemlerde kullanılan biyometrik olarak nitelendirilebilecek karakterler fiziksel ve davranışsal olarak iki grupta ele alınmıştır. Fiziksel karakterler, parmak izi, yüz, iris gibi özellikler iken el yazısı, ses ve tuş basım

örüntüsü gibi özelliklerde davranışsal özellikler olarak tanımlanabilmektedir [5]. Biyometrik sistemlerin diğer doğrulama mekanizmalarına göre daha güvenli olması beklenmesine rağmen incelenen çalışmalarda biyometrik sistemlerde mevcut olan çok sayıda saldırı vektörlerinin mevcut olduğu görülmektedir. Literatürde biyometrik sistemlerde kullanılmak üzere geliştirilen algoritmaların tersine sistemlerde olası saldırı vektörlerine odaklanılan çalışmaların çokta fazla olmadığı görülmüştür.

Bu kitap bölümünde; biyometrik sistemlerin maruz kalabileceği saldırı vektörleri incelenmiş, bunun için daha önce literatürde tanımlanan çeşitli modeller araştırılmış [7]-[52], araştırmalar ve modeller bir araya getirilerek kapsamlı bir şekilde ele alınmış, saldırı vektörleri dikkate alınarak biyometrik sistemlerin güvenliğini sağlamak için alınması gereken önlemlere yer verilmiş, karşılaşılabilecek yeni saldırı vektörlerini de içine alan yeni model geliştirmek için saldırı vektörlerini oluşturan tüm saldırıları içine alabilecek önlemler özetlenmiştir.

Bu kitap bölümü, 6 başlıktan oluşmaktadır. Bölüm 6.2'de biyometrik sistemlerde güvenlik sağlamak üzere saldırıya maruz kalabilecek saldırı vektörleri tanımlanmıştır. Bölüm 6.3'te saldırılar sınıflandırılmıştır. Bölüm 6.4'te önceki bölümde tanımlanan saldırı vektörlerine karşı biyometrik sistemlerde güvenlik sorununu çözmek üzere alınabilecek önlemler sunulmuştur. Bölüm 6.5'te biyometrik sistemlerde kullanılmak üzere geliştirilen standartlar ele alınmıştır. Son bölümde ise çalışmada yapılanlar özetlenerek, ileride yapılacak çalışmalara yönelik değerlendirmelere yer verilmiştir.

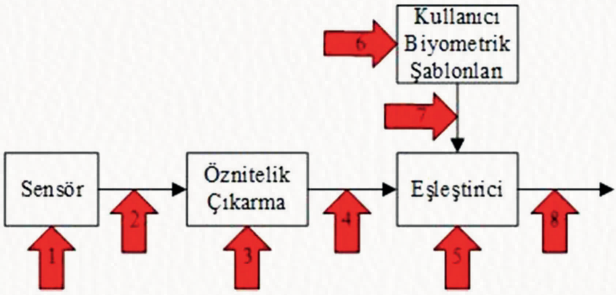


Şekil 6.1. Genel bir biyometrik sistem gösterim model gösterimi

6.2. BİYOMETRİK SİSTEMLERE YAPILAN SALDIRI MODELLERİ

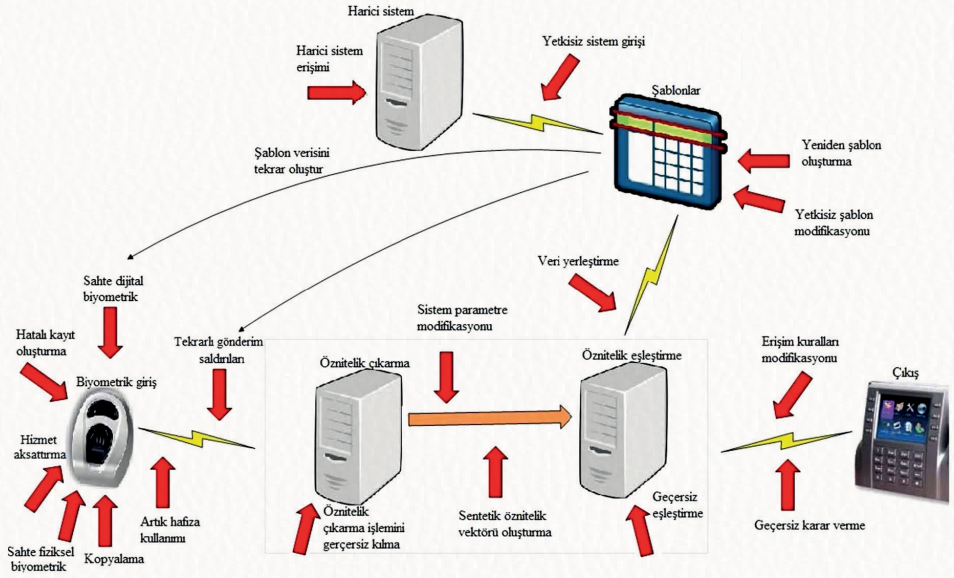
Biyometrik sistemlerin güvenli bir şekilde kişisel kimlik doğrulama ve kimlik belirleme işlemlerini gerçekleştirmek amacıyla yaygın olarak kullanılması, bu sistemlerde güvenlik kavramını oldukça önemli kılmaktadır. Bütün çalışmalar incelendiğinde biyometrik sistemlerde güvenlik sorunları olarak genellikle bu sistemlere sızmak üzere kullanılan sahte parmak izi, yüz kullanılarak yapılan aldatma yaklaşımlarının ele alındığı görülmüştür. Bu bölümde biyometrik sistemlerde bulunan tüm olası açıklar ele alınacaktır. Olası saldırılar ele alınmadan önce bu bölümde ve devam eden bölümlerde bahsi geçecek terimler ele alınmıştır. Biyometrik sistemlerde 3 çeşit kullanıcı bulunmaktadır. Bunlar taklitçi, saldırgan ve yetkili kullanıcıdır. Taklitçi, yetkili bir kişi gibi görünerek biyometrik sistemlere giriş yapmaya çalışan kişidir. Saldırgan, biyometrik sistemlere çeşitli saldırılar düzenleyerek servis erişimini engellemeye ya da yetkisiz giriş yapmaya çalışan kişidir. Yetkili kullanıcı ise biyometrik sisteme giriş yetkisine sahip olan kişidir. Güvenlik açıkları biyometrik sistemlerde güvenlik zayıflığı olarak da nitelendirilen saldırılara zemin olabilecek tasarım eksiklikleridir. Biyometrik sistemler üzerindeki saldırıya maruz kalınabilecek noktalar saldırı vektörleri olarak ele alınmıştır. Tehdit terimi olası saldırılar olarak nitelendirilmiştir. Aldatmaca ise taklitçi tarafından yapay, kopyalanan biyometrik verilerin biyometrik sistemlere erişilebilmek üzere kullanılmasıdır. Biyometrik sistemlerinin geniş kitlelerce kullanımından önce çeşitli performans ölçüm çalışmalarına tabi tutulması gerekmektedir. Biyometrik sistemlerin performansı yanlış kabul oranı (FAR), yanlış ret oranı (FRR), gerçek kabul oranı (GAR), ROC eğrisi gibi ölçütler ile belirlenebilmektedir [6]. FAR, yetkisi olmadığı halde biyometrik sisteme erişimi sağlanan sisteme giriş sayısının toplam sisteme giriş deneme sayısına oranıdır. Bu oran sisteme gerçek kullanıcı gibi girebilen taklitçi sayısını ifade etmektedir. Bu oranın yüksek olması sisteme girebilecek taklitçi sayısının yüksek olduğu anlamına geldiğinden güvenlik adına önemli bir sorundur. Bu sebeple, biyometrik sistemlerde FAR oranı düşürülmeye çalışılmaktadır. FRR ise taklitçi olarak nitelendirilerek sisteme girişine izin verilmeyen gerçek kullanıcı sayısını belirlemek üzere kullanılan bir ölçüttür. Bu ölçütün yüksek olması sistem kullanıcılarının sisteme erişememesine neden olduğundan biyometrik sistemlerde istenilmeyen bir duruma neden olmaktadır.

Biyometrik sistemlere saldırı vektörleri ile erişilerek bu sistemlerin güvenliği ortadan kalkmaktadır. Bu nedenle, bu vektörlerin önceden bilinerek sistemlerin bu noktalara karşı dayanıklı hale getirilmesi gerekmektedir. Biyometrik sistemlerde saldırı vektörlerini modellemek üzere çeşitli çalışmalar yapıldığı görülmüştür. Konuyu ele alan ilk çalışma Ratha ve arkadaşları [7] tarafından yapılan çalışmadır. Bu çalışmada, biyometrik sistemlerde yetkisiz kişilerce erişilen bir biyometrik verinin değiştirilemez bir karakter olmasından dolayı çok önemli bir kayıp olacağı düşüncesiyle biyometrik sistemlerde güvenlik unsurunu sağlamaya odaklanılmıştır. Çalışmada, güvenlik ve gizlilik sağlayan bir biyometrik sistem sunmak üzere olası güvenlik açıklarına da değinilmiştir. Önerilen modelde, 8 saldırı vektörü belirlenmiştir. Bu saldırı vektörleri, 1'den 8'e kadar numaralandırılmış kırmızı oklarla Şekil 6.2'de gösterilmiştir. Bu saldırı vektörleri sırasıyla sahte biyometrik, tekrarlı gönderim, öznitelik çıkarımı işleminin etkisiz kılınması, öznitelik vektörünün değiştirilmesi, eşleştiricinin etkisiz kılınması, veritabanında saklanan şablonlara yetkisiz erişim, şablon verisinin değiştirilmesi ve eşleştirici sonucunun değiştirilmesidir. Cukic ve Bartlow [8] ise çalışmalarında bir saldırı ağacı şeklinde çalışmalarını modelleyerek sunmuşlar, sundukları bu çalışmada ise 22 güvenlik açığı ile 20 olası saldırı vektörünü içeren daha kapsamlı bir çalışma olmuştur. Jain ve arkadaşları [9] ise biyometrik sistemlerde karşılaşılan sorunları Kılçık Modeli diye adlandırdıkları bir yaklaşım ile kategorize ederek, saldırıları düşman saldırıları ve sıfır çaba saldırıları olarak iki grupta ele almışlardır. Roberts [10] çalışmasında; 18 saldırı vektöründen oluşan bir model sunmuş, olası saldırı vektörü ile bu saldırı vektörlerine karşı savunma yollarının neler olabileceğini göstermiş, sunduğu model ise Türkçeleştirilerek yapılan saldırılar ve isimleri oklarla gösterilerek Şekil 6.3'te verilmiştir.



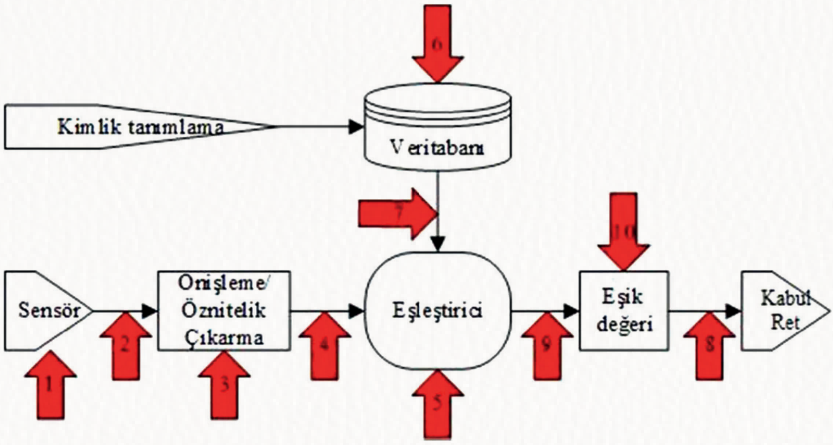
Şekil 6.2. Ratha ve arkadaşlarının biyometrik sistem saldırı vektörleri modeli ([7] nolu kaynaktan Türkçeye çevrilmiştir.)

Galbally [11] çalışmasında; saldırı vektörlerini Jain ve arkadaşlarının [9] yaptığı kategorizasyonu dikkate alarak geliştirmiş ve genişletmiş, kötü niyetli saldırılarını doğrudan ve dolaylı saldırılar olarak kategorize ederek ele almış, ve yaptığı kategorizasyonu da 10 saldırı vektöründen oluşan ve Şekil 6.4'te verilen model üzerinde açıklamıştır. Ayrıca, Ratha ve arkadaşlarının [7] önerdiği saldırı vektörlerine ek olarak önerdiği modelde 4 ve 5 ile tanımlanan saldırı vektörleri 9 ve 10 numara ile gösterilen saldırı vektörleri olarak tekrar ifade edilmiştir.

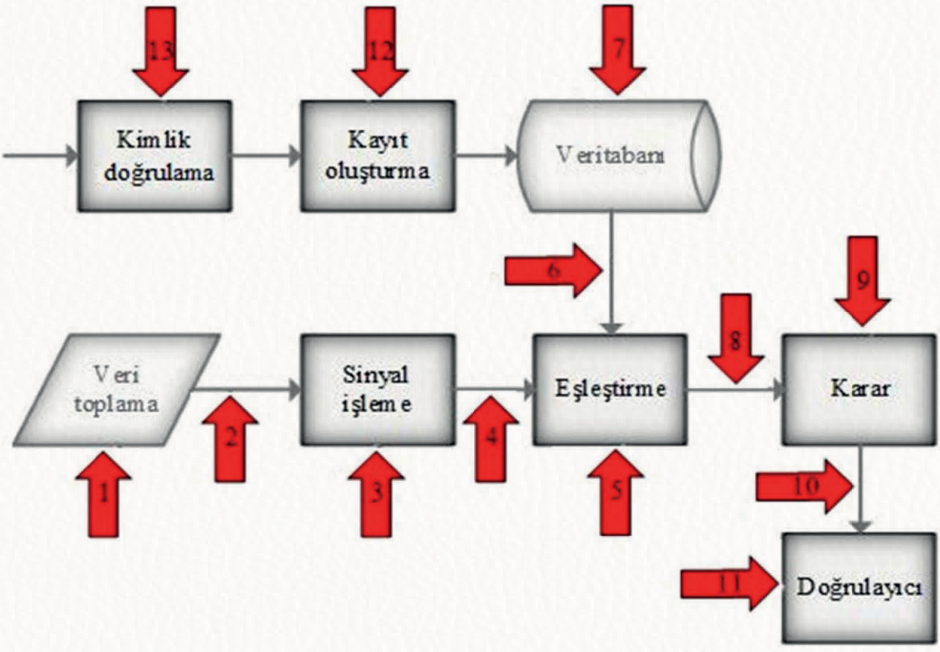


Şekil 6.3. Roberts'ın biyometrik sistem saldırı vektörleri modeli ([10] nolu kaynaktan Türkçeye çevrilmiştir.)

Alaswad ve arkadaşları [12] ise biyometrik sistemler üzerinde saldırı vektörlerini 13 saldırı vektörü ile ifade etmişlerdir. Tanımladıkları saldırı vektörleri Şekil 6.5'te gösterilmiş olup, saldırıların biyometrik sistemlerde gerçekleştirilen işlemlerin her aşamasında yapılabileceğini göstermektedir.



Şekil 6.4. Galbally'nin önerdiği biyometrik sistemlerde saldırı vektörleri modeli ([11] nolu kaynaktan Türkçeye çevrilmiştir.)



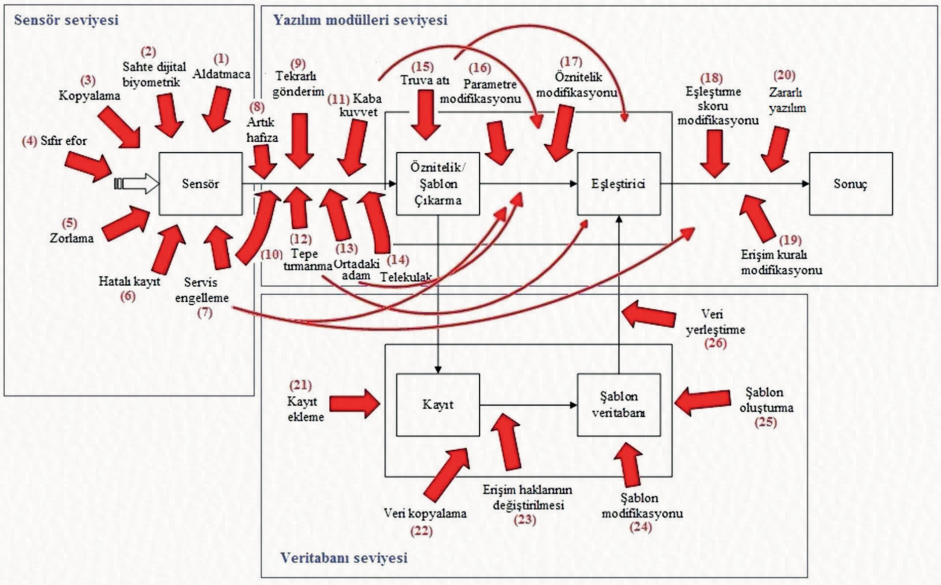
Şekil 6.5. Alaswad ve arkadaşlarının biyometrik sistem saldırı vektörleri modeli ([12] nolu kaynaktan Türkçeye çevrilmiştir.)

6.3. SALDIRILARIN SINIFLANDIRILMASI

Bu kısımda, daha önce tanımlanan modellerden [7]-[12], saldırı türlerinden, sınıflarından ve yeni saldırılardan [13]-[17] ve [19]-[23] yararlanılarak kapsamlı bir saldırı vektör modeli sunulmuştur. Oluşturulan modelde saldırı vektörleri;

- sensör seviyesi saldırıları,
- yazılım modülleri seviyesi saldırıları ve
- veritabanı seviyesi saldırıları

olmak üzere 3 gruba ayrıştırılmış ve bu çerçevede yeni bir bakış açısı oluşturulmuş ve sunulmuştur. Oluşturulan biyometrik sistem saldırı vektör modeli Şekil 6.1'de verilen genel biyometrik sistem modeli üzerinde gösterilerek, biyometrik sistemlerde saldırılara maruz kalınabilecek noktalar, olası saldırı vektörleri yeniden çizilerek Şekil 6.6'da kapsamlı olarak verilmiştir.



Şekil 6.6. Biyometrik sistem saldırı vektör modeli

Ayrıştırılan ve modeli oluşturan saldırı vektörler türlerinin detayları da Tablo 6.1'de tanımlanmıştır [7]-[12]. Tablo 6.1'de verilen sınıflandırma seviyesine göre

de saldırılar alt başlıklarda tek tek açıklanmış, farklı tablolarda (Tablo 6.1-6.3 ve Tablo 6.4-6.8) ise detaylandırılmıştır. Sensör Seviye saldırıları S ile, Yazılım Modüllerine saldırılar Y ile ve Veritabanına saldırılar V ile gösterilmiştir.

6.3.1. Sensör Seviyesi Saldırıları

Yapılan incelemelerde; sensör seviyesinin saldırılara en çok maruz kalan saldırı bölgesi olduğu ve sisteme giriş sırasında saldırı gerçekleştirmenin daha çok tercih edildiğinden bu seviyede karşılaşılabilecek saldırılara odaklanılmıştır. Tablo 6.2'de sensör seviyesinde gerçekleştirilebilecek saldırılar literatürden toparlanarak özetlenmiştir [10, 12-17, 19-20]. Tablodan görülebileceği gibi, bu seviyede karşılaşılabilecek olan 8 farklı saldırı söz konusu olup bu sensör seviyesi saldırıları S1'den S8'e kadar bir gösterimle tablo da ifade edilmiştir. Bu saldırılar devam eden bölümde ele alınmıştır.

Tablo 6.1. Saldırı vektör türleri

Saldırı no	Saldırı	Seviye
1	Aldatmaca saldırı	Sensör
2	Sahte dijital biyometrik oluşturma	
3	Kopyalama saldırısı	
4	Sıfır çaba saldırısı	
5	Zorlama saldırısı	
6	Hatalı kayıt oluşturma	
7	Hizmet engelleme saldırısı	
8	Artık hafıza kullanma	
9	Tekrarlı gönderim saldırısı	Yazılım modülleri
10	Servis engelleme saldırısı	
11	Kaba kuvvet saldırısı	
12	Tepe tırmanma saldırısı	
13	Ortadaki adam saldırısı	
14	Telekulak saldırısı	
15	Truva atı saldırısı	
16	Parametre modifikasyonu	
17	Öznitelik modifikasyonu	
18	Eşleştirme skoru modifikasyonu	
19	Erişim kuralı modifikasyonu	
20	Zararlı yazılım	
21	Kayıt ekleme	Veritabanı
22	Kullanıcı verilerinin kopyalanması	
23	Erişim haklarının değiştirilmesi	
24	Şablon modifikasyonu	
25	Şablon oluşturma	
26	Depolama kanalı engelleme ve veri yerleştirme	

Sahte Fiziksel Biyometrik (Aldatmaca) Saldırıları; biyometrik sistemlere yetkisiz şekilde giriş yapabilmek üzere sahte fiziksel biyometrik veri kullanmak en önemli güvenlik açıklarından birini oluşturmakta ve bu saldırı vektörü de literatürde aldatmaca olarak bilinmektedir. **Aldatmaca saldırıları**, yetkisiz giriş sırasında kullanılacak olan ilgili kişiye ait biyometrik verinin fiziksel olarak yapay bir şekilde oluşturulmasını ve bu sahte biyometrik ile sisteme giriş yapılmasını hedeflemektedir. Bu saldırı için sahte bir biyometrik karakterden başka herhangi bir şeye gerek duyulmadığı için aldatmaca, saldırganlar tarafından diğer saldırı türlerine göre daha çok tercih edilen saldırı çeşitlerinden biridir [13]. Aldatmaca saldırısını gerçekleştirebilmek için hiç ya da yok denecek kadar az teknik bilgiye ihtiyaç duyulması bu saldırı türünün kolaylıkla uygulanmasına neden olmaktadır [10].

Tablo 6.2. Sensör Seviyesi Saldırıları

Saldırı	Açıklama
S1	Sahte bir fiziksel biyometrik verinin sensöre sunulması
S2	Sahte bir dijital biyometrik verinin sensöre sunulması
S3	Sensör üzerinde kalan bir biyometrik izin kopyalanarak sisteme erişim için kullanılması
S4	Saldırganın kendi biyometrik karakteri ile çaba harcamadan sisteme erişebilmesi
S5	Saldırganın fiziksel zorlama ile kullanıcının biyometrik verisini kullanarak sisteme erişimi
S6	Saldırganın yetkili kullanıcı kaydı sırasında kendi biyometrik verisini sisteme giriş olarak sunarak kayıt oluşturması
S7	Saldırganın sensörün çalışmasını engellemek ya da sensöre zarar vermek üzere yaptığı fiziksel saldırı
S8	Saldırganın hafızada kalan son kullanıcıya ait biyometrik veriyi kopyalayarak sisteme erişmesi

Şekil 6.7. Aldatmaca saldırılarında kullanılan sahte yüz örnekleri [14].

Aldatmaca saldırıları; biyometrik doğrulama teknolojileri kullanarak bilgi güvenliği sağlamaya çalışan şirketler için önemli bir sorundur. Lenovo, Asus ve Toshiba marka dizüstü bilgisayarların bazı modellerinde (Lenovo Veriface III, Asus SmartLogon V1.0005, Toshiba Face Recognition 2.0.2.32) gömülü bulunan biyometrik sistemlerde sahte biyometrikler ile kolaylıkla sistemlere erişilebildiği 2009 yılında düzenlenen Black Hat Konferansında Hanoi Üniversitesi Güvenlik ve Güvenlik Açığı Araştırma Grubu tarafından gösterilmiş olup, Şekil 6.7'de aldatmaca saldırısı için kullanılan sahte yüz örneklerine yer verilmiştir. Bu yüz örneklerini oluşturmak için silikon, kauçuk, fotoğraf ve video dosyaları kullanılmıştır [14].

(a) Silikon (b) Kauçuk (c) Film (d) Kağıt (e) Jelatin

Şekil 6.8. Aldatmaca saldırılarında kullanılan sahte parmak izi görüntüleri [16]

Apple tarafından 2013 yılında parmak izi sensörü özelliği ile piyasaya sürülen iPhone 5s'e yapışkanla kaplanan bir parmak ile erişilebileceği gösterilmiştir [15]. Şekil 6.8'de aldatmaca saldırılarında kullanılmak üzere oluşturulan sahte parmak izi örneklerine yer verilmiştir. Şekildeki sahte parmak izleri sırasıyla silikon, kauçuk, film, kağıt ve jelatin kullanılarak elde edilmiştir [16]. Benzer şekilde, Samsung Galaxy S5 telefonunda bulunan parmak izi sensörü sahte bir parmağı doğrulayarak akıllı telefona yetkisiz erişime izin vermiştir [17].

Sahte Dijital Biyometrik Saldırılar; biyometrik verinin bir sensör ile alınması sırasında fiziksel biyometrik karakter yerine sahte dijital bir biyometrik karakter kullanılarak gerçekleştirilmektedir. Bu saldırılar iki şekilde düzenlenebilmektedir. Bunlardan ilki kimlik sahteciliği saldırıları diye bilinen dijital bir biyometrik veri ile yapılan saldırılardır. İkinci durumda ise daha önceden sisteme erişimine izin verilen bir kaynak biyometrik veriden tekrarlı gönderim saldırısı ile elde edilen dijital verinin sisteme giriş olarak verilmesi ile saldırı söz konusu olmaktadır [10].

Kopyalama Saldırıları; özellikle parmak izi ya da avuç izi teknolojilerine konu olmaktadır. Sensör yüzeylerine, derinin yağlı yapısı nedeniyle par-

mak izi ya da avuç izi okutulurken iz bırakılması söz konudur. Bırakılan bu izlerin pudra, japon yapıştırıcısı ve sıcak su içeren bir plastik çanta gibi materyaller kullanılarak kopyalanması mümkün olmaktadır. Kopyalanan biyometrik veriler ile saldırganlar tarafından sisteme erişim kolaylıkla sağlanabilmektedir.

Sıfır Çaba Saldırıları; dışarıdan herhangi bir saldırı olmaksızın sistemin kendisinden kaynaklanmaktadır. Sistemde tanımlanan FAR ve FRR olasılıkları yüksek olduğu durumda yetkisiz bir kişinin hiçbir çaba harcamadan sisteme erişimi mümkün olabilmektedir [19].

Zorlama Saldırıları; doğru bir biyometrik veriyi elde etmek üzere gerçek bir kullanıcının saldırgan tarafından fiziksel olarak zorlanmasıdır [20].

Hatalı Kayıt Oluşturma Saldırıları; biyometrik sistemi kullanacak olan yetkili kullanıcının kayıt işlemleri sırasında sisteme yapılan saldırılardır. Bu saldırılar ile sistemde yer almayan birinin kaydı yapılabilmektedir. Kayıt oluşturabilmek için kimlik kanıtlama adı verilen bir işlem söz konusudur. Kayıt sırasında kişiden biyometrik veri toplanması sırasında sistem bu saldırılara maruz kalabilmektedir. Bu işlem sırasında sisteme daha sonra giriş için hedeflenen bir kimliği tanımlayan hatalı bir dokümanla kayıt oluşturularak bu kayıt ile elektronik doğrulama işlemi gerçekleştirilebilmektedir. Bu saldırı ile sahte biyometrik veriler sisteme eklenerek daha sonra bu biyometrik veriler aracılığıyla sisteme yetkisiz giriş hedeflenmektedir [12].

Hizmet Engelleme Saldırıları (DoS); giriş cihazına zarar vererek ya da cihazın hata üretmesine neden olarak sistemi bozmaya ya da çalışmasını aksatmasına yönelik saldırılardır. Bellek taşması saldırıları olarak da bilinir. Saldırı örnekleri olarak optik parmak izi sensörü ya da kamera sensörüne ani flaş parlaması ile zarar vermek gösterilebilir. Silikon sensörüne kısa devre yaptırmak, sensörü suya batırmak servis engellemeye yönelik saldırılardır [12]. Sıcaklık, ışık ve toz gibi çevre koşulları da sensörlerin performansını düşürerek alınan verinin kalitesini düşürmektedir [10].

Artık Hafıza Kullanma Saldırıları; bazı biyometrik sistemlerde sensör hafızasında son birkaç biyometrik verinin tutulabilmesi söz konusudur. Saldırgan sensör hafızasında tespit ettiği veriyi elde ederek sisteme tekrar giriş için kullanabilmektedir [10].

6.3.2. Yazılım Modülleri Seviyesinde Saldırılar

Bu düzeyde saldırılar [10, 20-23], sensör düzeyinde alınan verinin işlenmesinden veritabanlarında saklanan şablon verileri ile karşılaştırılmak üzere iletimine kadar süre zarfı boyunca karşılaşılabilecek olan saldırılar ve karşılaştırma işlemi sonrasında eşleştirme skoru oluşturma sırasında karşılaşılabilecek olan saldırılardır.

Tablo 6.3. Yazılım modülleri seviyesinde karşılaşılabilecek saldırılar

Saldırı	Açıklama
Y1	Saldırganın yetkili birey biyometrik veri örneğini iletim kanallarından alarak sisteme yeniden erişim için kullanması
Y2	Saldırganın sistemin çalışmasına engel olması için iletişim bağlantısını koparması
Y3	Saldırganın kaba kuvvet saldırısı ile giriş verisi oluşturarak sisteme giriş sağlaması
Y4	Saldırganın tepe tırmanma saldırısı ile giriş verisi oluşturarak sisteme giriş sağlaması
Y5	Saldırganın sensör ile yazılım modülleri arasındaki iletim kanalları üzerinde iletilen biyometrik veriyi değiştirmesi
Y6	Saldırganın iletim kanallarında iletilen biyometrik veriyi dinlemesi
Y7	Saldırganın öznitelik çıkarımı işleminde elde edilen öznitelikleri değiştirmesi (Truva atı saldırıları)
Y8	Saldırganın sistem parametrelerini değiştirebilmesi
Y9	Saldırganın servis engelleme saldırıları ile öznitelik çıkarımı işlemini geçersiz kılması
Y10	Saldırganın yazılım modülleri arasında bulunan iletim kanallarında iletilen öznitelik vektörünü ortadaki adam saldırısı ile elde etmesi
Y11	Saldırganın kaba kuvvet saldırısı ile elde ettiği sentetik öznitelik vektörü sisteme dahil edilebilmesi
Y12	Saldırganın tepe tırmanma saldırısı ile elde ettiği sentetik öznitelik vektörü sisteme dahil edilebilmesi
Y13	Saldırganın eşleştirme skorunu değiştirebilmesi
Y14	Saldırganın erişim kuralını değiştirebilmesi
Y15	Saldırganın uygulamaya zararlı yazılım yerleştirmesi

Tablo 6.3'te görüldüğü gibi yazılım modülleri seviyesinde karşılaşılabilecek 15 farklı saldırı mevcuttur. Bu saldırılar arasından ilk olarak sensör ile yazılım modülleri arasındaki iletim kanalında yer alan saldırı vektörleri ele alınmıştır. Bu saldırı vektörleri Tablo 6.3'te Y1-Y6 arasında ifade edilen saldırılardır.

Tekrarlı Gönderim Saldırıları; Yetkili kişilere ait biyometrik şablon verilerinin temassız akıllı kart gibi kaynaklarda şifresiz bir şekilde saklandığı

sistemlerde, şablon verilerine erişim ve bu verileri tekrar kullanarak sisteme giriş için yapılan işlemlere tekrarlı gönderim saldırıları adı verilmektedir [10].

Hizmet Engelleme Saldırıları (DoS); iletim kanalları üzerinden sistemi bozmaya ya da çalışmasını aksatmasına yönelik yapılan saldırılardır. Bu saldırı ile iletim bağlantısı koparılarak alınan biyometrik verinin işlenmesi engellenmeye çalışılmaktadır.

Tablo 6.4. FAR olasılığına göre sisteme giriş için gereken saldırı sayıları ve gereken zaman ([21] nolu kaynaktan Türkçeye çevrilmiştir.)

Saldırı sayısı	Zaman	FAR olasılığı
10^{11}	1,16 gün	9×10^{-24}
10^{12}	11,5 gün	9×10^{-23}
10^{13}	115 gün	9×10^{-22}
10^{14}	3,17 yıl	9×10^{-21}
10^{15}	31 yıl	9×10^{-20}

Kaba Kuvvet Saldırıları; rastsal bir şekilde sürekli olarak biyometrik veriler oluşturularak sisteme erişilmesi hedeflenmektedir. Çok büyük sayıda biyometrik giriş kümesi oluşturularak sisteme giriş yapabilen veri elde edilmeye çalışılmaktadır. Tablo 6.4'te biyometrik bir sistemdeki FAR oranına göre sisteme erişim için gereken zaman ve kaba kuvvet saldırı sayısı örneklenmiştir. Eşik değeri sabit olarak 0,37 olan bir biyometrik sistem için tabloda da görülebileceği gibi FAR olasılığı küçüldükçe yapılması gereken saldırı sayısı ve gereken zaman artmaktadır [21].

Tepe Tırmanma Saldırıları; iteratif olarak daha önceden belirlenen bir başarı oranına ulaşana kadar saldırganın sentetik biyometrik verisi ile şablon oluşturma işlemi gerçekleştirilir. Her bir iterasyonda şablon, eşleştirici sonuçlarına göre modifiye edilecektir. Hedeflenen değere ulaşıldığında sisteme girişine izin verilecek olan şablon oluşturulmuş olacaktır [22].

Ortadaki adam saldırıları; sensör düzeyinde alınan biyomerik veri, sistemde bir tehdit oluşturmadan değiştirilebilmektedir. Bu saldırı ile hatalı verinin sisteme eklenmesi sayesinde yeniden gönderim saldırısı düzenlenir. Veritabanından şablon verisi tekrar elde edilerek sisteme erişim sağlanabilmektedir [10].

Telekulak Saldırıları; sensör düzeyinde sisteme kabul edilen biyometrik veri iletim kanallarında dinlenerek yetkisiz kişilerce elde edilebilmektedir. Elde edilen biyometrik veri aracılığıyla saldırgan tarafından sisteme erişim söz konusu olabilmektedir [20].

Öznitelik çıkarımı adımında saldırılar elde edilecek öznitelik kümesini değiştirmek üzere düzenlenmektedir. Bu adımda düzenlenebilecek saldırı Tablo 6.3'te Y7 ile ifade edilmiştir. Öznitelik kümesinin daha önceden saldırgan tarafından tanımlanan bir öznitelik kümesine denk gelecek şekilde oluşturulması sağlanabilmektedir.

Öznitelik çıkarımı ve eşleştirici adımları arasındaki iletim kanalında saldırılar öznitelik çıkarımı adımında elde edilen öznitelik vektörünü değiştirmek ve yerine sonraki adımlarda işlenmek üzere hatalı veriyi sisteme almak üzere gerçekleştirilmektedir. Y8 olarak ifade edilen saldırı ile FAR/FRR gibi eşleştirme mekanizmasında önemli olan, sistem parametrelerinin değiştirilerek hatalı olan verinin sisteme alınmasının sağlanmaktadır. Hizmet engelleme saldırıları ile (Y9) bu seviyede sistemin çalışması engellenebilmektedir [10]. İletim kanalında iletilen öznitelik vektörü ortadaki adam saldırısı (Y10) ile elde edilebilmektedir. Kaba kuvvet (Y11) ve tepe tırmanma (Y12) saldırıları ile elde edilen sentetik öznitelik vektörleri mevcut öznitelik vektörü yerine değerlendirilmek üzere sisteme dâhil edilmektedir. Böylece sistemde kaydı olmayan bir biyometrik veri ile sisteme saldırgan tarafından erişim söz konusu olabilmektedir.

Eşleştirme adımında eşleştirme yapıldıktan sonra Y13 ile gösterilen saldırılarla eşleştirme skoru gibi eşleştirme kriterlerinin değiştirilerek FAR oranını üzerinde bir skor oluşturularak sisteme erişim hedeflenmektedir. Bu saldırı sırasında yetkili kullanıcının sisteme girişi sırasında değişik bir durum ortaya çıkmadığı için saldırının sistem yöneticileri ve/veya kullanıcıları tarafından fark edilmesi zor olmaktadır [10]. Eşleştirme skoru yerine eşleştirme işlemi sonucunda alınan erişim kararının uygulama arayüzüne aktarımı sırasında değiştirilmesi amacıyla saldırı düzenlenerek hatalı kabul sağlanabilmektedir. Y14 olarak ifade edilen bu saldırı atlatma saldırısı olarak da bilinmektedir. Tepe tırmanma saldırıları ile eşleştirici karar sonucu değiştirilebilmektedir. Sinyal işleme sonucu dikkate alınmaksızın üzerine veri eklenerek sistemin tüm aday kullanıcılara erişiminin açık tutulması mümkün olmaktadır [23].

6.3.3. Veritabanı Seviyesinde Saldırılar

Biyometrik sistemlerin yazılım modülleri seviyesinde, eşleştirme skoru oluşturmak üzere elde edilen biyometrik şablonlar ile veritabanlarında tutulan şablonlar arasında gerçekleştirilen karşılaştırmalar bu seviyede tamamlanmaktadır [10,12,19]. Bu seviyede karşılaşılabilmesi olası saldırılar Tablo 6.5'te verilmiştir.

Tablo 6.5. Veritabanı seviyesinde karşılaşılabilecek saldırılar

Saldırı	Açıklama
V1	Saldırganın sisteme sonradan veri ekleyerek kaydını oluşturması
V2	Saldırganın tüm kullanıcı şifre ve şablon bilgilerine erişmesi
V3	Saldırganın yetkisiz olarak sisteme erişimi ile erişim haklarının değiştirilmesi
V4	Saldırganın yetkisiz olarak şablonu değiştirmesi
V5	Saldırganın şablonu yeniden oluşturması
V6	Saldırganın eşleştirme sonucu olarak kullanılabilmek üzere sisteme veri eklemesi

Kayıt ekleme; saldırganın biyometrik sistem veritabanına kendi kaydını erişim haklarını değiştirerek ekleyebilmesi amacıyla yapılan saldırılardır.

Kullanıcı Şablonlarına Erişim; biyometrik sistem veritabanına erişen saldırgan, veritabanında yer alan kullanıcı şifre ve şablon verilerine erişerek bu verileri elde edebilecektir.

Erişim Haklarının Değiştirilmesi; biyometrik istem admin haklarının elde edilmesi ile sisteme yetkisiz bir şekilde erişilerek kullanıcı hak ve izinlerinin değiştirilmesi amacıyla gerçekleştirilen saldırılardır [10].

Yeniden Şablon Oluşturma; sentetik öznitelik vektörü oluşturmak üzere tepe tırmanma saldırılarına benzer şekilde sentetik şablon oluşturulabilmektedir. Servis engelleme saldırıları ile veritabanında saklanan şablon verileri yok edilebilir. Taklitçi diye adlandırılan sisteme sızmaya çalışan kişi, kendisine ait şablon verisi ile veritabanında tutulan şablonları değiştirebilmektedir [19].

Yetkisiz Şablon Modifikasyonu; şablon verileri silinerek yeniden oluşturulmak yerine yetkisiz kişilerce erişilerek değiştirebilmektedir. Böylece hatalı kabul ve hatalı ret söz konusu olabilmektedir [12].

Depolama kanalı engelleme ve veri yerleştirme; hem veritabanı hem de sistem olumsuz şekilde etkilenmektedir. Saldırgan veritabanından karşılaştırma işlemi için gelecek olan şablonları silmek ya da modifiye etmek yerine engelleyerek istediği hatalı veri şablonunu eşleştiriciye gönderebilmektedir [10].

6.4. BİYOMETRİK SİSTEMLERE YAPILAN SALDIRILARDAN KORUNMA YOLLARI

Kimlik doğrulama ve belirleme amacıyla birçok alanda kullanılmakta olan biyometrik sistemlerde kullanılan biyometrik karakterlerin şifreler gibi değiştirilemeyen kişiye özgü nitelikler olmaları bu sistemler üzerinde gizlilik ve güvenlik kavramını ön plana çıkarmaktadır. Biyometrik sistemlerin korunması ve olası savunma yöntemlerinin geliştirilmesi için konuya kapsamlı bakmak, saldırıları ve saldırı vektörlerini iyi tanımak, teknik ve teknolojileri bilmek, uygulama aşamalarını anlamak, olası riskleri bilmek ve korunma adımlarını ve savunma yollarını geliştirmek gereklidir. İncelenen çalışmalardan [7, 10, 12, 24-52] da faydalanarak biyometrik sistemlerde güvenliği sağlamak için; öncelikli olarak olası saldırı vektörleri tanımlanmış, olası saldırı vektörlerine göre farklı yaklaşımlar önerilmiş, mevcut saldırılardan korunabilmek üzere savunma yolları sensör seviyesinde, yazılım modülleri seviyesinde ve veritabanı seviyesinde ele alınmıştır.

Tablo 6.6. Sensör seviyesinde karşılaşılabilecek saldırılar ve önlemler

Saldırı	Önlem
Aldatmaca	Gerçeklik tespiti
	Güvenlik yanıtı
	Hafızada kalan biyometrik verinin silinmesi
	Rastsal biyometrik veri
	Çoklu biyometrik veri kullanımı
	Çok karakteristikli biyometrik sistemler
	Çok faktörlü doğrulama
	Ayırt edici olmayan biyometrik
Kopyalama	Rastsal biyometrik veri
Servis aksattırma	Güvenli cihaz
	Çok faktörlü doğrulama

6.4.1. Sensör Seviyesinde Korunma Yöntemleri

Bu bölümde sensör seviyesinde en çok karşılaşılan tehditler olan aldatmaca saldırıları, kopyalama saldırıları ve servis engelleme saldırılarına karşı alınabilecek önlemler ele alınmıştır. Biyometrik sistemlerin biyometrik veri girişinde karşılaşılabilecek olumsuzluklar ve çözüm yolları Tablo 6.6'da özetlenmiştir. Özellikle aldatmaca saldırıları daha önceki bölümlerde bahsedildiği gibi biyometrik sistemlerin en çok maruz kaldıkları saldırı çeşididir.

Aldatmaca saldırılarına çözüm olmak üzere gerçeklik tespitine yönelik çalışmalar ön plana çıkmıştır. Bu amaçla çeşitli sensörler aracılığıyla sıcaklık [24], koku [25], oksijen miktarı [26], kan akışı [27], spektrum bilgisi [28] gibi bilgiler ile deri teri [29,30], morfolojik karakteristikler [31], deri deformasyonu ve elastikiyeti [32] ve de varyans [33] gibi bilgiler kullanılarak biyometrik karakterlerin gerçeklik tespiti yapılmaya çalışılmıştır. Bu sensörler aracılığıyla yapılan ölçümlerde sentetik bir biyometrikten elde edilen değerler ile gerçek bir veriden elde edilen değerler farklı olacaktır.

Güvenlik yanıtı doğrulama mekanizması ile güvenli bir şekilde sistemin doğrulanabilmesi için kullanıcıdan şifre yerine istenen bilgiler istenmektedir. Anne kızlık soyadı bu amaçla en yaygın olarak kullanılan bilgilerden biridir. Biyometrik sistemlerde ise benzer bir mantıkla kullanıcının söylenen bir cümleyi tekrarlaması, göz kırpması, başını sallaması gibi isteklerde bulunularak sahte biyometrik verilerin tespit edilmesi hedeflenmiştir [10].

Biyometrik sistemlerde kullanılan bazı sensörler yerel olarak okunan biyometrik verileri hafızalarında geçici olarak saklayabilmektedir. Bu nedenle sensörlere yapılacak artık hafıza saldırılarına karşı sensörler hafızalarında tutulabilen verilerin düzenli olarak takip edilerek hafızadan silinmesi gerekmektedir [10].

Rastsal biyometrik veri yöntemleri aldatmaca saldırılarına karşı kullanılabilecek farklı bir yaklaşımdır. Bu yaklaşımda farklı zamanlarda, rastsal bir şekilde, farklı kombinasyonlarda biyometrik karakter girilerek saldırganların sisteme erişimleri engellenmeye çalışılmıştır. Bu yaklaşım ile kopyalama saldırılarına karşı da önlem alınmış olacaktır [12].

Çoklu biyometrik veri kullanımı ile aldatmaca saldırılarına karşı biyometrik sistemlerin güven içinde tutulabileceği ifade edilmiştir. Bu yaklaşımla birden fazla biyometrik veri aynı anda doğrulanmaya çalışılacağı için yetkisiz kişile-

rin sisteme sahte biyometrik verilerle erişimi daha fazla zorlaştırılabilecektir. Bu sistemler böylece daha karmaşık bir hal almakla birlikte birden fazla sensör gibi donanımlara gerek duyacaktır [10].

Multi-modal olarak adlandırılan çok karakteristikli biyometrik sistemlerde, günümüzde kullanılan sensörlerin aynı anda birden fazla veriyi okuyabilmeleri kabiliyetinden yararlanılarak tek bir veriden ortalama bir öznitelik vektörü elde edilmesi yerine ağırlıklandırılmış öznitelik vektörü oluşturulması sağlanabilmektedir [10]. Tek karakteristiğe sahip sistemlerde gürültü, kullanıcıdan kaynaklı olarak alınan veride mevcut olan varyasyon gibi problemler verilerin doğru bir şekilde işlenerek eşleştirilememesine neden olmaktadır. Multi-modal sistemler ile daha doğru bir eşleştirme yapabileceği için biyometrik sistem daha düşük FAR olasılığında çalışabilecektir. Böylece sahte bir biyometrik veri ile her okuma işlemi sırasında aynı biyometrik verinin sisteme alınması ile oluşturulan öznitelik vektörünün sisteme kabul edilme olasılığı düşecektir. Bu yaklaşımla aldatmaca saldırılarına karşı daha gürbüz bir sistem elde edilebilecektir [34].

Çok faktörlü doğrulama sistemlerinin aldatmaca saldırılarına karşı kullanımı önerilen bir diğer yaklaşımdır. Bu yaklaşımda çoklu biyometrik karakterler yaklaşımlarına benzer olarak bir biyometrik karakter ve bir akıllı kart veya PIN gibi doğrulama mekanizmaları bir arada kullanılarak güvenliği arttırmak hedeflenmiştir [12]. Hizmet engelleme saldırılarına karşı da bu yaklaşım kullanılabilmektedir. Böylece saldırgan çok sayıda doğru olmayan erişim denemesi yapamayıp sistemin çalışmasına engel olamayacaktır [35].

Ayırt edici bir özelliği olmayan yaş, cinsiyet gibi biyometrik sistemlerde kullanılabilecek bilgiler ayırt edici olmayan biyometrik diye adlandırılmaktadır. Ayırt edici olmayan biyometrikler ile fiziksel veya davranışsal biyometrik karakterler bir arada kullanılarak sahte bir biyometrik verinin sisteme erişimi engellenebilecektir [10].

6.4.2. Yazılım Modülleri Seviyesinde Korunma Yöntemleri

Bu düzeyde, sensörler aracılığıyla alınan verinin işlenmesinden saklanan şablonlar ile karşılaştırmasına kadar olası saldırılar dikkate alınarak savunma yolları tanımlanmıştır. Tablo 6.7'de öncelikli olarak bu seviyedeki ilk iletim kanalı olan biyometrik verinin alınması ile öznitelik çıkarımı işlemi

için iletimi arasındaki kanal sırasında karşılaşılabilecek saldırılara karşı alınabilecek önlemler ele alınmıştır. Tabloda ayrıca öznitelik çıkarımı işlemi, öznitelik vektörünün eşleştiriciye iletimi ve eşleştirme işlemleri sırasında karşılaşılabilecek saldırılara karşı savunma yolları özetlenmiştir. Birçok biyometrik sistemde alınan biyometrik veri, veri işleme için yerel ya da uzak bir iş istasyonuna iletilmektedir. Bu iletim sırasında ve alınan verinin öznitelik çıkarımı işlemine aktarımı için iletimi sırasında verilerin okunamaması ve değiştirilememesi gerekmektedir. Veri iletimi sırasında karşılaşılabilecek olan telekulak saldırılarına karşı önlem olarak, veri güvenliğini sağlamak üzere biyometrik veriler şifreli ve güvenli kanallar üzerinde iletilmelidir. Biyometrik sistemlerde karşılaşılabilecek olan artık hafıza saldırılarına karşı düzenli olarak sensör hafızasının kontrol edilmesine ek olarak rastsal biyometrik veriler kullanılarak hafızada tutulan farklı bir biyometrik veri kullanılması yoluyla sisteme saldırgan tarafından erişim engellenebilmektedir [12].

Tablo 6.7. Yazılım modülleri seviyesinde olası saldırılar ve önlemler

Saldırı	Önlem
Artık hafıza kullanımı	Hafızada kalan biyometrik verinin silinmesi
	Rastsal biyometrik veri
Tekrarlı gönderim saldırıları	Simetrik/Asimetrik şifreleme
	E-imza
	TTL etiketi
	Steganografi
	Güvenlik yanıtı
Kaba kuvvet saldırıları	Süre aşım politikaları
Tepe tırmanma saldırıları	Karşılıklı doğrulama
	Şifrelenmiş güvenli iletim kanalı
Ortadaki adam saldırıları	PKI sertifikası
	Şifrelenmiş güvenli iletim kanalı
	Steganografi
	Filigran
Telekulak saldırısı	Şifrelenmiş güvenli iletim kanalı
Truva Atı saldırıları	Truva atı saldırılarına karşı gürbüz algoritmalar
Sistem bileşenleri modifikasyonu	İşaretlenmiş bileşenler
Eşleşme skoru modifikasyonu	Hata ayıklayıcı
Zararlı yazılım saldırıları	Kod imzalama, biyometrik standartlar

Tekrarlı gönderim saldırılarına karşı ise simetrik ya da asimetrik şifreleme algoritmaları kullanılarak biyometrik veriler şifrelenmelidir. E-imza teknolojisi kullanılarak biyometrik sistemlerde güvenlik ve bütünlük sağlanabilecektir. Şifreleme anahtarlarının biyometrik sistem dışında tutulması, sistemi daha güvenli kılacaktır. TLL etiketleri kullanılarak iletim kanalları için tanımlı bir zaman kısıtı oluşturularak tekrarlı gönderim saldırıları engellenebilecektir [12]. Sistem içerisinde güvenli cevap mekanizması ile doğrulama istenerek tekrarlı gönderim saldırılarına karşı önlem alınmış olacaktır [10].

Ortadaki adam saldırılarına karşı sistem güvenliğini sağlamak üzere şifrelenmiş güvenli kanal ve açık anahtar kullanımı önerilmiştir [12]. Tekrarlı gönderim ve ortadaki adam saldırılarına karşı steganografi ile veri saklama önerilmiştir. Filigran yaklaşımı [36] ile iletim sırasında verinin üzerinde herhangi bir değişiklik yapılabilmesine engel olunabilecektir.

Kaba kuvvet saldırısı sırasında saldırganın sisteme erişim için hedeflenen skoru elde edene kadar deneme yapabilmesine engel olmak üzere süre ve eşleştirme deneme kısıtlaması aşım politikaları uygulanabilmektedir [10].

Sensörler aracılığıyla alınan verinin işlenmesi sırasında karşılaşılabilecek en önemli sorun öznitelik şablonunun truva atı programları ile değiştirilmesidir. Bu soruna çözüm olmak üzere truva atı saldırılarına karşı gürbüz algoritmaların kullanımı önerilmiştir. Truva atı saldırılarına karşı savunma olarak C ve C++ programlama dilleri için önerilen güvenli kod çalıştırma yaklaşımları kullanılabilmektedir [19].

Eşleştirme adımında karşılaşılabilecek olan truva atı programları ile skor değiştirme saldırılarına karşı güçlü biyometrik algoritma kullanımı önerilmiştir. Sistem bileşenlerinin değiştirilmesi eşleştirme işlemi için kritik öneme sahip olduğundan sistem bileşenlerine yönelik saldırılara karşı bileşenlerin işaretlenmesi bir önlem olarak sunulmuştur. Eşleşme skorunu değiştirmek üzere yapılan saldırılar kod bütünlüğü kontrol metodolojilerinden yararlanılarak çözülebilmektedir. Tepe tırmanma saldırıları ile istenen skorun yakalanabilmesi sorununa karşı güvenli iletişim kanalı, karşılıklı doğrulama mekanizması gibi yaklaşımlar önerilmiştir. Uygulamaya yönelik olarak zararlı yazılım yerleştirme saldırılarına karşı kod imzalama ve BioAPI gibi biyometrik standartların kullanılması gibi önlemler sunulmuştur [12].

6.4.3. Veritabanı Seviyesinde Korunma Yöntemleri

Bu seviyede veritabanlarında tutulan şablon verilerine yönelik saldırılar en çok karşılaşılan saldırılar olmuştur. Karşılaşılabilecek saldırılar ve çözüm yolları Tablo 6.8'de özetlenmiştir.

Saldırgan, veritabanına doğrudan erişim yolunu bulabilir ise sistemde kayıtlı olan bir kişinin şablon verisini çalarak yerine kendi biyometrik karakteristiğine ait şablonu verisini yerleştirebilir. Bu saldırıları engellemek üzere ortak veritabanı güvenlik metodolojileri uygulanarak güvenlik sağlanabilmektedir. Veritabanında şablon verilerini saklamadan önce şifreleme ve özetleme yaklaşımlarını kullanmak anlamlı olabilmektedir. Şablon verilerini harici veritabanları yerine akıllı kartlar üzerinde tutmak bir diğer önlem olarak değerlendirilmiştir [12].

Tablo 6.8. Veritabanı seviyesinde karşılaşılabilecek saldırılar ve önlemler

Saldırı	Önlem
Yetkisiz şablon oluşturma ve modifikasyonu	Veritabanı erişim kontrolleri
	İşaretlenmiş şablon
	Şifrelenmiş, özetlenmiş şablon
	Akıllı kartlarda şablon depolama
	Niceleme şeması, bulanık şemalar, güvenli şablon
	İptal edilebilir biyometri, bulanık atlama şemaları
	Kriptografik teknikler

Biyometrik şablonları saldırılardan korumak üzere geliştirilen çeşitli yöntemlere yönelik çalışmalara rastlanmıştır. Bu çalışmalar üç kategoride ele alınmıştır. İlk kategoriyi biyometrik verinin kendisini korumak üzere geliştirilen yaklaşımlar oluşturmaktadır [19]. Niceleme şemaları, bulanık şemalar ve iptal edilebilir biyometri güvenli şablon yaklaşımları bu kategoride ele alınabilecek yaklaşımlardır. [37] numaralı çalışmada biyometrik şablonları korumak üzere geliştirilen bir niceleme şeması yaklaşımı sunulmuştur. Güvenli şablon yaklaşımı bir özet haline getirilen biyometrik bilgiden gürültülü ortamlarda veriyi başarıyla yeniden oluşturabilmek üzere [38-40] numaralı çalışmalarda kullanılmıştır. [41-44] numaralı çalışmalarda güvenli şablon yaklaşımı tabanlı pratik kodlama şemaları geliştirilmiştir. Biyometrik sistemlerde saklanan biyometrik verilerin gizliliğini arttırmak üzere tersine çevrilemeyen dönüşüm kavramı [7] ortaya atılmıştır. Tersine çevrilemeyen dönüşümü sağlayan biyo-

metrik yapı ise iptal edilebilir biyometri olarak ifade edilmiştir. Bu kavramın performans değerlendirmelerini yapmak üzere çok sayıda durum çalışması ele alınmıştır [45-47]. Biyometrik bilgilerden elde edilen anahtarlar kullanılarak veritabanında verileri şifrelemeye dayanan bulanık atlama şeması [48-52] numaralı çalışmalarda kullanılmıştır. İkinci kategoride ek donanımlar kullanılarak şablonların biyometrik sistemlerde güvenli tutulması üzerine çalışmalar yer almaktadır [19]. Son kategori altında ise kriptografik tekniklere dayalı protokoller ile biyometrik verileri korumaya çalışan yaklaşımlar yer almaktadır.

6.5. BİYOMETRİK SİSTEMLERDE GÜVENLİK STANDARTLARI

Günümüzde birçok alanda kullanılan biyometrik sistemlerin maliyetini düşürürken kalitesini ve güvenilirliğini artırmak üzere biyometrik standartlar ortaya çıkmıştır. Ulusal ve uluslararası organizasyonlar tarafından sunulan biyometrik standartlara ek olarak çeşitli endüstri konsorsiyumları ile araştırma gruplarının standart çalışmaları söz konusudur. Uluslararası Standart Organizasyonu (ISO), Uluslararası Elektroteknik Komisyonu (IEC) gibi organizasyonlar uluslararası standartlar sunmaktadır. ISO ve IEC organizasyonları bir birlik komitesi oluşturarak ISO/IEC JTC1 adı altında bilgi teknolojileri alanında faaliyet göstermek üzere SC17, SC27 ve SC37 standartlarını geliştirmişlerdir. Özellikle SC37 biyometri ile ilgili olarak biyometrik uygulama arayüzü, biyometrik veri değişim formatları, biyometrik veri değerlendirme kriterleri ve performans testlerinin standart hale getirilmesini hedeflemektedir. Bu standart dikkate alınarak geliştirilen biyometrik sistemlerde bu çalışmada yazılım modülleri seviyesi olarak ele alınan seviyede doğrudan güvenlik sağlamak mümkün olacaktır. ISO/IEC 30107-1:2016 standardı ise biyometrik sistemlerin sensör seviyesi ile ilgili olan bir standart olarak sensöre yönelik yapılabilecek saldırıları önlemeyi hedeflemektedir. Bu standarda göre PAD olarak ifade edilen biyometrik veri sunum saldırı tespit platformu (framework) tanımlanarak saldırı vektörleri modelimizde aldatmaca saldırıları olarak ifade ettiğimiz saldırıları önlemeye odaklanılmıştır.Bunlara ilave olarak son yıllarda güncellenen pek çok biyometrik standartları vardır. ISO/IEC 19794, ISO/IEC 19795, ISO/IEC 19784, ISO/IEC 19785, ISO/IEC 24709, ISO/IEC 24722, IEEE 2410-2021,IEEE P2884 ve IEEE 2790-2020 bunlardan bazılarıdır.

Bunun yanında bu alana katkı veren çok sayıda organizasyon mevcuttur [53,54].

- Amerika'da Amerikan Ulusal Standartlar Enstitüsü'ne bağlı olarak faaliyet gösteren Uluslararası Bilgi Teknolojileri Standartları Komitesi (INCITS) çok sayıda teknik komiteden oluşmaktadır. M1 adıyla bilinen komite, biyometrik standartlara odaklanan INCITS komitelerinden biridir.
- İngiltere'de benzer şekilde İngiliz Standartlar Enstitüsü'nün IST/44 standardı mevcuttur. BioAPI Konsorsiyum (BioAPI) ve Biyometrik Konsorsiyum (BC) biyometrik sistemler alanında standart geliştiren iki önemli konsorsiyum olarak hizmet vermektedir.
- IBIA International Biometrics & Identification Association
- FIDO (Fast IDentity Online) Alliance
- IEEE Biometric Open Protocol Standard
- OASIS Biometrics Technical Committee
- Natural Security Alliance.

Bu bölümde ele alındığı gibi biyometrik sistemler üzerine gerek ulusal gerekse uluslararası organizasyonlar tarafından çok sayıda standart geliştirilmiştir. Bu standartların kullanımı ile maliyet ve kalite hedeflerine ek olarak güvenirlik sağlanması amaçlanmıştır. Standartlar, biyometrik sistemlerde güvenliği sağlama konusunda yol gösterici olmak üzere kullanılmaktadır. Biyometrik sistem geliştiricileri, standartlarda ifade edilen gereksinimleri yerine getirerek bu çalışmada belirtilen güvenlik açıklıklarına karşı gürbüz sistemler elde edebileceklerdir. Ayrıca standartlar biyometrik sistemler için test metodolojileri olarak kullanılabilmektedir. Biyometrik standartlara ek olarak test metodolojileri olmak üzere kullanılabilecek platformlar mevcuttur. Bu platformlar aracılığıyla geliştirilen sistemlerin güvenlik değerlendirmelerinin yapılması mümkündür.

6.6. SONUÇ VE DEĞERLENDİRMELER

Bu kitap bölümünde biyometrik sistemlere yapılacak saldırılar ile ilgili olarak kapsamlı bir araştırma yapılmış, saldırılar gruplandırılmış ve seviyelendirilmiş, biyometrik sistemlere yapılabilecek saldırılar ve bunların sistemi nasıl zafiyete uğratacağı örnekler ile birlikte sunulmuş, biyometrik sistemlerin gü-

venliği konusunda bir farkındalık oluşturulmaya çalışılmış ve biyometrik sistemlerde saldırganlar tarafından hedef olabilecek saldırı vektörleri literatürdeki örneklerine göre çok daha kapsamlı şekilde değerlendirilmiş ve korunma yöntemleri sunulmuştur. Sunulan çalışmada;

- Güncel saldırı vektörleri dikkate alınarak biyometrik sistemlerin güvenliğinin yüksek oranda sağlanması için yeni saldırı vektörleri modeli önerilmiştir.
- Önerilen bu model literatürde bulunan mevcut 6 model dikkate alınarak, daha çok saldırı vektörü tanımlanarak daha kapsamlı olacak şekilde tanımlanmıştır.
- Literatürdeki çalışmalarda en fazla 13 veya 20 saldırı dikkate alınmış olsa da bu çalışmada 29 saldırı vektörü dikkate alınarak bir öneride bulunulmuştur.
- Hem saldırı sayısı hem de saldırılara karşı koymayı kolaylaştırmak için kavram çalışması seviyelendirilmiştir. Bunlar; sensör seviyesi, yazılım modülleri seviyesi ve veritabanı seviyesi olarak kategorize edilerek ele alınmıştır. Daha önceki çalışmalarda da ele alınan saldırılardan bazıları, farklı seviyeler altında sınıflandırılmıştır.
- Bu saldırılara karşı alınabilecek önlemlerin neler olması gerektiğine de ayrıca yer verilmiştir.
- Önerilen modeller ve yapılan incelemeler neticesinde yeni model sonuç bölümünde kritik edilmiş ve karşılaştırmalar yapılmıştır.

Elde edilen bilgiler bulgular ışığında bu konu değerlendirildiğinde;

- Literatürdeki çalışmaların daha çok biyometrik sistemlerin performans kriterine odaklanıldığı, yapılan saldırılara ve güvenlik ihlallerine ve risklerine yeterince odaklanılmadığı,
- en fazla tehdit içerdiği görülen sensör ve veritabanı saldırıları üzerine odaklandığı,
- biyometrik sistemlerde her bir seviyeye özgü güvenlik açıklıkları bulunabileceği,
- literatürde aksi ifade edilmesine rağmen yazılım modülleri seviyesinde sistemlere daha çok sayıda saldırı yapılabileceği,
- biyometrik sistemler için performans gereksinimi kadar önemli olan diğer bir konunun güvenlik olduğu,

- güncel tehditler incelendiğinde biyometrik sistemlerin daha fazla saldırıya maruz kalabileceği

gözlemlenmiştir.

Sonuç olarak;

- sunulan çalışma ile biyometrik teknolojilerde hedeflenen, performansı yüksek ve güvenli sistemlerin sağlanabilmesi için sistemlerin tasarlanması sırasında dikkate alınması gereken tüm unsurlar açık bir şekilde ortaya koyulmuştur. Bu unsurlarla birlikte biyometrik sistemler için geliştirilen standartların benimsenmesi yararlı olacaktır. Bu standartlar ve önerilen saldırı vektörleri modeli dikkate alınarak daha güvenli, güvenilir, yüksek performanslı ve düşük maliyetli biyometrik sistemler geliştirmek mümkün olacaktır.
- Günümüzde kullanılan biyometrik teknolojilerin güvenlik sorunları ve çalışmada sunulan unsurlar göz önünde bulundurularak, güvenliği sağlayacak olan yaklaşımlara duyulan gereksinimlerin tekrar gözden geçirilerek, özellikle 6698 KVK Kanununa dikkate alındığında üzerinde daha fazla durulması gerekmektedir.
- Gelecek çalışmalarda biyometrik sistemler için geliştirilecek olan güvenli ve performansı yüksek yeni yaklaşımlara odaklanılması bu çalışma kapsamında sunulan saldırı vektörlerinin engellenmesine yönelik çalışmalar yapılmalıdır.
- Günümüzde biyometrik verilerin her ortama kolaylıkla entegre edilebildiği, kolaylıkla paylaşılabildiği, istenilmeyen veya arzu edilmeyen olaylarla karşılaşılması, suistimal veya istismar edilebileceği bilinmektedir. Bu hususların farkında olunması, çözümün teknolojilerden değil kişilerin dikkatine de bağlı olduğu unutulmamalıdır.
- Biyometrik verilerin değiştirilemeyecek kalıcı veriler olduğu unutulmamalıdır. Bu husus dikkate alınarak faydalı teknolojiler geliştirilmesi, olası risklerin bilinmesi ve verilerin korunması, kişisel verileri kullanırken/paylaşırken/işlerken/saklarken çok dikkatli olunması ve kanuna uygun olarak bu işlemlerin yapılması, nitelikli kişisel veri mahremiyetine gereken önemin verilmesi gereklidir.
- Bu çalışma kapsamında saldırı vektörü sadece genel bir biyometrik sistem üzerinde gösterilmiştir. Günümüz sistemleri incelendiğinde

buradaki modelin çok basit kalacağı her zaman hatırda bulundurulmalı, burada sunulan veya aktarılan saldırı vektörlerinden daha büyük ve kapsayıcı modellere ihtiyaç olduğu hatırda bulundurulmalı ve yeni çalışmalar yapılmalıdır.

KAYNAKLAR

[1]. Jain, K., Ross, A. ve Prabhakar, S., "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, Cilt 14, No 1, 4–20, 2004.

[2]. Liu, S. ve Silverman, M., "A practical guide to biometric security technology", IT Professional, Cilt 3, No 1, 27–32, 2001.

[3]. Delac, K. ve Grgic, M. "A survey of biometric recognition methods", Proceeding of 46th International Symposium Electronics in Marine, 184–193, 2004.

[4]. Prabhakar, S., Pankanti, S. ve Jain, A. K. "Biometric recognition: Security and privacy concerns", IEEE Security & Privacy, Cilt 1, No 2, 33–42, 2003.

[5]. Tolba, A. S., El-Baz, A. H. ve El-Harby, A. A., "Face recognition: A literature review", International Journal of Signal Processing, Cilt 2, No 2, 88–103, 2006.

[6]. Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L. ve Ross, A, "Biometrics: a grand challenge", Proceedings of the 17th International Conference on Pattern Recognition (ICPR2014), Cilt 2, 935–942, 2004.

[7]. Ratha, N. K., Connell, J. H. ve Bolle, R. M., "Enhancing security and privacy in biometrics-based authentication systems", IBM systems Journal, Cilt 40, No 3, 614–634, 2001.

[8]. Cukic, B. ve Bartlow, N., "Biometric system threats and countermeasures: a risk based approach", Proceedings of the Biometric Consortium Conference (BCC05), 2005.

[9]. Jain, A. K., Ross, A. ve Pankanti, S., "Biometrics: a tool for information security", IEEE Transactions on Information Forensics and Security, Cilt 1, No 2, 125–143, 2006.

[10]. Roberts, C., "Biometric attack vectors and defences", Computers & Security, Cilt 26, No 1, 14–25, 2007.

[11]. Galbally, J., "Vulnerabilities and attack protection in security systems based on biometric recognition", IEscuela Politecnica Superior, Universidad Autónoma de Madrid, PhD Dissertation, 2009.

[12]. Alaswad, A. O., Montaser, A. H. ve Mohamad, F. E., "Vulnerabilities of biometric authentication threats and countermeasures", International Journal of Information & Computation Technology, Cilt 4, No 10, 947–958, 2014.

[13]. Uludag, U. ve Jain, A. K. "Attacks on biometric systems: a case study in fingerprints", Proceeding of Electronic Imaging 2004, International Society for Optics and Photonics, 622–633, 2004.

[14]. Zhang, Z., Yi, D., Lei, Z. ve Li, S. Z., "Face liveness detection by learning multispectral reflectance distributions", Proceeding of IEEE International Conference on Automatic Face & Gesture Recognition and Workshops (FG 2011), 436–441, 2011.

[15]. Hadid, A., "Face biometrics under spoofing attacks: vulnerabilities, countermeasures, open issues, and research directions", Proceeding of IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 113–118, 2014.

[16]. "Cti resources", [Online]. http://www.ctiresources.com.my/products-solutions/biometrics.html

[17]. Smith, D. F., Wiliem, A. ve Lovell, B. C., "Face recognition on consumer devices: Reflections on replay attacks", IEEE Transactions on Information Forensics and Security, Cilt 10, No 4, 736–745, 2015.

[18]. Chong, R., Flory, C., Lerums, J. ve Long, D., "Fido password replacement: Spoofing samsung galaxy s5 fingerprint biometric authenticator using a latent fake fingerprint approach", http://insurehub.org/sites/default/files/reports/FIDO\%20Final\%20Report.pdf

[19]. Jain, A. K., Nandakumar, K. ve Nagar, A., "Biometric template security", EURASIP Journal on Advances in Signal Processing, Cilt 2008, No 113, 2008.

[20]. Campisi, P., Security and Privacy in Biometrics, Springer, 2013.

[21]. Kong, A., Zhang, D. ve Kamel, M., "A study of brute-force break-ins of a palmprint verification system", Proceedings of the International Conference on Audio-and Video-Based Biometric Person Authentication, Cilt 3546, 447–454, 2005.

[22]. Maiorana, E., Hine, G. E. ve Campisi, P., "Hill-climbing attacks on multibiometrics recognition systems", IEEE Transactions on Information Forensics and Security, Cilt 10, No 5, 900–915, 2015.

[23]. Breebaart, J., Yang, B., Buhan-Dulman, I. ve Busch, C., "Biometric template protection", Datenschutz und Datensicherheit-DuD, Cilt 33, No 5, 299–304, 2009.

[24]. Kallo, P., Kiss, I., Podmaniczky, A. ve Talosi, J., "Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus", US Patent 6 175 641, 2001.

[25]. Baldisserra, D., Franco, A., Maio, D. ve Maltoni, D, "Fake fingerprint detection by odor analysis", Proceeding of International Conference on Biometric Authentication, 265–272, 2006.

[26]. Reddy, P. V., Kumar, A., Rahman, S. ve Mundra, T. S., "A new antispoofing approach for biometric devices", IEEE Transactions on Biomedical Circuits and Systems, Cilt 2, No 4, 328–337, 2008.

[27]. Lapsley, P. D., Lee, J. A., Pare Jr, D. F. ve Hoffman, N., "Anti-fraud biometric scanner that accurately detects blood flow", Us Patent 5 737 439, 1998.

[28]. Coli, P., Marcialis, G. L. ve Roli, F., "Power spectrum-based fingerprint vitality detection", Proceeding of IEEE Workshop on Automatic Identification Advanced Technologies, 2007.

[29]. Derakhshani, R., Schuckers, S. A., Hornak, L. A. ve O'Gorman, L., "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners", Pattern recognition, Cilt 36, No 2, 383–396, 2003.

[30]. Parthasaradhi, S. T., Derakhshani, R., Hornak, L. ve Schuckers, S. A., "Time-series detection of perspiration as a liveness test in fingerprint devices", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Cilt 35, No 3, 335–343, 2005.

[31]. Moon, Y. S., Chen, J. S., Chan, K. C., So, K. ve Woo, K. C. "Wavelet basedfingerprint liveness detection", Electronics Letters, Cilt 41, No 20, 1112–1113, 2005.

[32]. Antonelli, A., Cappelli, R., Maio, D. ve Maltoni, D., "Fake finger detection by skin distortion analysis", IEEE Transactions on Information Forensics and Security, Cilt 1, No 3, 360–373, 2006.

[33]. Zhang, Y., Tian, J., Chen, X., Yang, X. ve Shi, P., "Fake finger detection based on thin-plate spline distortion model", Proceeding of International Conference on Biometric Authentication, Cilt 4642, 742–749, 2007.

[34]. Ross, A. ve Jain, A. K., "Multimodal biometrics: An overview", Proceeding of IEEE 12th European Signal Processing Conference, 1221–1224, 2004.

[35]. Gorman, L. O., "Comparing passwords, tokens, and biometrics for user authentication", Proceedings of the IEEE, Cilt 91, No 12, 2019–2040, 2003.

[36]. Pankanti, S. ve Yeung, M. M., "Verification watermarks on fingerprint recognition and retrieval", Proceeding of. International Society for Optics and Photonics, Electronic Imaging'99, 66–78, 1999.

[37]. Linnartz, J. P. ve Tuyls, P., "New shielding functions to enhance privacy and prevent misuse of biometric templates", Proceeding of 4th International Conference Audio-and Video-Based Biometric Person Authentication, 393–402, 2003.

[38]. Sutcu, Y., Li, Q. ve Memon, N., "Protecting biometric templates with sketch: Theory and practice", IEEE Transactions on Information Forensics and Security, Cilt 2, No 3, 503–512, 2007.

[39]. Li, Q., Sutcu, Y. ve Memon, N., "Secure sketch for biometric templates", Proceeding of Advances in Cryptology (ASIACRYPT 2006), 99–113, 2006.

[40]. Sutcu, Y., Li, Q. ve Memon, N., "Secure biometric templates from fingerprint-face features", Proceeding of IEEE Conference on Computer Vision and Pattern Recognition (CVPR'07), 1–6, 2007.

[41]. Draper, S. C., Khisti, A., Martinian, E., Vetro, A., & Yedidia, J. S., "Using distributed source coding to secure fingerprint biometrics", Proceeding of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2007), Cilt 2, 129-132, 2007.

[42]. Sutcu, Y., Rane, S., Yedidia, J. S., Draper, S. C. ve Vetro, A., "Feature transformation of biometric templates for secure biometric systems based on error correcting codes", Proceeding of IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'08), 1–6, 2008.

[43]. Vetro, A., Draper, S. C., Rane, S., & Yedidia, J., "Securing biometric data", Distributed source coding, 293–323, 2009.

[44]. Davida, G. I., Frankel, Y. ve Matt, B. J., "On enabling secure applications through off-line biometric identification", IEEE Symposium on Security and Privacy, 148–157, 1998.

[45]. Ang, R., Safavi-Naini, R. ve McAven, L., "Cancelable key-based fingerprint templates", Information Security and Privacy, 242–252, 2005.

[46]. Ratha, N. K., Chikkerur, S., Connell, J. H. ve Bolle, R. M., "Generating cancelable fingerprint templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, Cilt 29, No 4, 561–572, 2007.

[47]. Ratha, N., Connell, J., Bolle, R. M. ve Chikkerur, S., "Cancelable biometrics: A case study in fingerprints", Proceeding of IEEE 18th International Conference on Pattern Recognition (ICPR 2006), Cilt 4, 370–373, 2006.

[48]. Cohen, G. ve Zemor, G., "The wiretap channel applied to biometrics", Proceeding of IEEE International Symposium on Information Theory (ISIT), 1–5, 2004.

[49]. Ignatenko, T. ve Willems, F., "On privacy in secure biometric authentication systems", Proceeding of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'07), 2007.

[50]. Tuyls, P. ve Goseling, J., "Capacity and examples of template-protecting biometric authentication systems", Biometric Authentication, 158–170, 2004.

[51]. Nagar, A., Nandakumar, K. ve Jain, A. K., "Biometric template transformation: a security analysis", Proceeding of International Society for Optics and Photonics, IS&T/SPIE Electronic Imaging, 2010.

[52]. Upmanyu, M., Namboodiri, A. M., Srinathan, K. ve Jawahar, C. V., "Efficient biometric verification in encrypted domain", Advances in Biometrics, 899–908, 2009.

[53]. Deravi, F., "Biometrics standards", Advances in biometrics, 473–489, 2008.

[54]. https://biometrics.mainguet.org/basics/standards.htm

Bölüm 7

DAĞITIK HİZMET ENGELLEME / AKSATTIRMA SALDIRILARI (DDoS) VE KARŞI ÖNLEMLER

Süreyya Atasever - İlker Özçelik - Şeref Sağıroğlu

DDoS (Distributed Denial-of-Service) Dağıtık Hizmet Engelleme/Aksattırma Saldırılarının interneti tehdidi gün geçtikçe artmaktadır. Güncel veriler ve hazırlanan güvenlik raporları tehditlerin her geçen gün de artacağına yönelik veriler sunmaktadır. Tehditlerin artmasına paralel olarak alınan önlemlerde çeşitlenmektedir. Bu bölümünde; DDoS tanımı ve tarihsel gelişimine kronolojik olarak değinilmiş ve saldırıların ne zaman ve nasıl başladığından hangi amaçlar için kullanıldığına kadar saldırılarının sebepleri ayrıntılı bir şekilde irdelenmiştir. DDoS ile ilgili çalışma alanları genel başlığı içerisinde literatürde yapılan DDoS çalışmaları saldırı türleri, saldırı araçları ve DDoS savunma yöntemleri olarak gruplandırılmış ve ayrıntılarıyla açıklanmıştır. Saldırı çeşitleri başlığı altında; DDoS saldırılarının çeşitlerine ve boyutlarına değinilmiş ve saldırılar ayrıştırılarak incelenmiştir. DDoS Saldırı araçları başlığında; saldırıları gerçekleştirilen araçlar kronolojik sıra ile açıklanmış, tarihsel gelişiminin yanında hangi aracın hangi çeşit DDoS saldırısı meydana getirdiği, sistemlerin kaynağını mı yoksa bant genişliğini mi tüketmeyi hedef aldığına dair ayrıntılı açıklamalar sunulmuştur. DDoS Savunma Yöntemleri konusu ise iki farklı perspektiften ele alınmış ve değerlendirilmiştir. Takip eden başlıklarda ise DDoS algılama ve müdahale başlıklarında savunma süreçleri ayrıntılı bir şekilde açıklanmış, karşı önlemler ele alınmış ve önerilerimiz sunulmuştur. Sonuç olarak, önemli araştırma ve çalışma alanlarından birisi olan DDoS konusunun kapsamlı ve ayrıntıları olarak ele alınmış, incelenmiş ve ilgilenen araştırmacılara kapsamlı bir kaynak olmayı hedeflemektedir.

7.1. GİRİŞ

İnternet; kişilerin bilgiye kolay ulaşmasını sağlayan büyük bir bilgi ağıdır. Kişiler sosyal hayatın içerisinde, eğitim öğretim ortamında ve iş yaşamında özetle teknolojiye erişimin gerekli olduğu her ortamda artık internete erişmektedir. Gelişen teknoloji ile beraber yaşamımızın merkezine yerleşen internet kullanımı, yaşamımızı oldukça kolaylaştırdığı gibi çeşitli risk ve tehditleri de yanında getirmektedir. Yaşanabilecek olumsuzluklara karşı internetin bilinçli kullanımı ve güvenliğini sağlamak oldukça önemli bir problem haline gelmiştir. Bilgi ve ağ güvenliği kavramlarının hayatımızda daha fazla yer etmesinin temel sebebi; internet üzerinde artan risk ve tehditlerdir. Artan risklere bağlı olarak alınan tedbirlerde çeşitlenmiş ve önem kazanmıştır. Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması sırasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür [1]. Ağ güvenliği ise bilgi güvenliği tanımına benzer şekilde, dijital ortamda yer alan bilgilerin güvenli bir şekilde taşınması olarak tanımlanabilir.

Saldırgan, ağa usulsüz olarak katılan, ağda yer alan bilgilere erişip, bu bilgileri kötü amaçlar için kullanan kişi olarak en genel şekilde tanımlanabilir. Bu durum ağı saldırılara ve saldırganlara karşı korumak geniş bir çalışma alanı oluşturur. Bu saldırılar ağ üzerinden hizmet vermeyi durdurarak kişileri ve kurumları büyük zararlara uğratmaktadır. Bu saldırılardan, tehdidi her geçen gün artan saldırı türlerinden birisi de hizmet engelleme (DoS/DDoS) saldırılarıdır. Veri alışverişi için hazır bulunan ağa veya servise karşı yapılan DoS/DDoS saldırısı ile kullanıcıların hizmet alması engellenmektedir.

Bu çalışmanın ilk bölümü DDoS tanımı, DDoS saldırılarının nedenleri, hedefleri ve DDoS saldırı sınıfları konu başlıklarından oluşur. İkinci bölüm ise DDoS saldırılarının çalışma alanlarının açıklanması için ayrılmıştır. Bu çalışmada ana hedef; DDoS u anlamak adına geçmişten günümüze geldiği yeri bilmektir. Aynı zamanda bilimsel çalışmalarda her geçen gün önemi artan DDoS savunma konusunda ayrıntılı bir sınıflandırma yapılmıştır. Yapılan sınıflandırma ile DDoS alanında çalışmak isteyen araştırmacılara toplu bir kaynak sunulmaktadır.

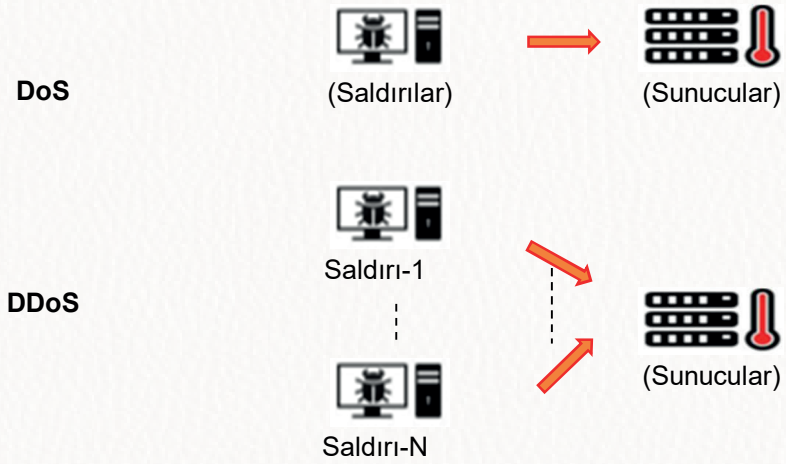
7.2. DAĞITIK HİZMET ENGELLEME/AKSATTIRMA SALDIRILARI (DDoS)

Yirminci yüzyılın sonlarında başlayan, büyük firmaları zarara uğrattığı 1999 Haziran'ında bilindik hale gelen Dağıtık Hizmet Engelleme saldırıları (DDoS) internet üzerinde yıkıcı zararlar veren büyük tehditlerden birisidir [2-4]. DDoS saldırıları ciddi maddi kayıplara yol açmaktadır. Yankee grubun açıklamasına göre 2000 yılının Şubat ayında Amazon, Yahoo, eBay gibi önemli sitelere karşı yapılan saldırıların yaklaşık olarak 1.2 milyar dolar zarara uğratıldığı tespit edilmiştir. 2001 yılının Eylül ayında ise Microsoft'un yaklaşık olarak 500 milyon dolar kaybettiği belirtilmiştir [3-5]. Dünyada en bilindik DDoS saldırısı; Ekim 2002'de Ana veya Kök Sunuculara (Root server) yapılmış olup 13 DNS kök sunucunun (root DNS server) 8'i bundan etkilenmiştir. 2010 yılında Wikileaks internet sitesine yardım yasaklarından dolayı Mastercard, PayPal, Visa ve Postfinance internet siteleri, DDoS saldırısına maruz kalarak belirli bir süre hizmet vermemiştir [2-6]. Bank of America, JP Morgan Chase, US Bancorp, Citigroup, PNC Bank isimli Amerika bankaları, 2012 yılında maruz kaldıkları DDoS saldırısı sebebiyle üç gün boyunca hizmetleri kesintiye uğramış ve ciddi bir yavaşlama yaşamışlardır. 2013'te, istenmeyen (spam) e-postaların %80'e varan bir kısmına hizmet veren istenmeyen eposta filtreleme kuruluşu olan Spamhaus, 300 Gbps hızında ilerleyen ve o zamana kadar kaydedilen en büyük DDoS saldırısına maruz kalmıştır. Maruz kalınan saldırı İngiltere genelinde ağ kesintilerine neden olmuştur. 2015'in son gününde meydana gelen DDoS saldırısı, BBC'nin sitelerinin yaklaşık üç saat süreyle hizmet vermemelerine sebep olmuştur. Netflix, PayPal, Visa, Amazon ve The New York Times dahil olmak üzere birçok büyük şirketin ağ altyapısı için çok önemli rolü olan, DNS sağlayıcısı Dyn, 2016 yılında Mirai botneti aracılığıyla DDoS saldırısına maruz kalmıştır. Milyonlarca geliştirici tarafından kullanılan popüler bir çevrimiçi kod yönetimi hizmeti olan GitHub'ın 2018 yılında maruz kaldığı DDoS saldırısı, GitHub'ın sistemlerini yaklaşık 20 dakikalığına devre dışı bırakmıştır. 2020'de Amazon Web Servisini kullanan kimliği belirsiz bir kuruluş uğradığı DDoS saldırısının 2,3 terabayt büyüklüğünde olduğu açıklanmış ve saldırı üç gün sürmüştür.

DoS/DDoS saldırıları ağın genel trafiğini bozan saldırılardır. Ağ anormalliği; ağ trafiğinde her zaman ki duruma kıyasla kalıpların (pattern) bazılarında ilginç ve uyumsuz davranışların sergilenmesidir [5-7]. DoS/DDoS ağda anor-

mal davranışlar oluşmasına sebep olur. DoS; tek bir kaynaktan hedefe yönelik yapılan saldırılar olarak tanımlanırken; DDoS, birçok kaynaktan hedefe yönelik yapılan saldırılar olarak en genel şekilde tanımlanabilir. DoS (Denial of Service) ifadesi, hizmet engelleme anlamına gelen ve saldırı sırasında tek kaynağı kullanan yapılardır. DDoS (Distributed Denial of Service), dağıtık hizmet engelleme anlamındadır. Burada dağıtıklığın karşılığı birden çok kaynaktan tek bir hedefe yönelik saldırının düzenlenmesidir. Bu saldırılar Şekil 7.1'de temsili olarak gösterilmiştir. Kaynakların çoğalması, bu tip saldırıların sezilmesini, saldırılara karşı önlem alınmasını ve savunma yapılmasını zorlaştırmaktadır.

DDoS hizmet engelleme saldırılarında, saldırgan ağ trafiğini engelleyerek hedefteki sisteme veya hizmete erişimi kesmeye çalışır. DDoS saldırıları; sınırlı ve yenilenemez kaynak tüketimine yönelik olabileceği gibi sistem yapılandırma bilgisinin değiştirilmesi veya imha edilmesine yönelik ya da ağ bileşenlerinin fiziksel olarak yok edilmesi veya değiştirilmesine yönelik de gerçekleştirilebilir [6-8].



Şekil 7.1. Hizmet engelleme ve dağıtık hizmet engelleme saldırıları [9]

DDoS saldırıların boyutları her geçen gün artmaktadır. Botnetlerin gücünün artması ve yüksek hızlı ağ teknolojileri ile modern DoS saldırıları 400 Gbps seviyelerine ulaşmıştır. Bu durum, internet için ciddi bir tehlike arz etmektedir [7]. DDoS saldırılarının 2015 yılında yaklaşık olarak 500 Gbps seviyesine

ulaştığı gözlemlenirken, 2016'da bu değer yaklaşık olarak 800 Gbps seviyesini bulmuştur. Symantec İnternet Güvenliği 2017 Risk Raporuna göre; Mirai botnetinin, Brian Krebs web sitesine yönelik yaptığı saldırı bu zamana kadar raporlanan en büyük DDoS saldırısıdır ve 620 Gbps seviyesini bulmuştur. Hatta raporun yayınlandığı tarih olan Nisan 2017'de, Fransız ISP olan OVM, 1Tbps seviyesinde DDoS saldırısına maruz kalmıştır [8]. Arbornet 2018 kayıtlarına göre Mart ayında 1.7 TBps gücünde saldırı tespiti yapılmıştır [9]. 2020 yılında ise Amazon web servisinin yaptığı bir açıklamaya göre ismini vermek istemedikleri bir müşterisinin 2,3 Tbps gücünde bir saldırıya maruz kaldığı ve bu saldırının taraflarınca hafifletildiği açıklaması yapılmıştır [10]. Saldırıya maruz kalma oranları, ülkeler bazında incelendiğinde ise Türkiye'nin dünya sıralamasında ikinci sırada yer alması, ülkemizde bu konuya daha çok önem verilmesini bizlere göstermektedir [11].

7.3. DDOS SALDIRI NEDENLERİNİN TARİHSEL GELİŞİMİ

DDoS saldırılarının gerçekleştirilme sebepleri kronolojik olarak incelendiğinde; saldırı motivasyonun beş temel evrede geliştiği gözlemlenmektedir. Bu saldırıların başlangıcı olarak bilinen 1988 yılında saldırının gerçekleştirilme nedeni merak ve eğlenceyken, günümüze gelindiğinde saldırıları motivasyonunda değişiklikler olmuş ve bunlar ise Şekil 7.2'de özetlenmiştir [7]. Bu bölümde DDoS saldırılarının zaman içerisindeki motivasyonundaki değişim detaylı olarak incelenmektedir.

Şekil 7.2. DDoS saldırılarının temel motivasyonları [7].

Doğrudan ve dolaylı olarak yapılan saldırıların önemlileri aşağıda kısaca açıklanmıştır. Bunlar:

- Tarihte, bilgisayar dünyasında ilk hizmet engelleme saldırısı olarak bilinen Morris virüsü, 1988 yılında Rober Tappan Morris tarafından eğlence amaçlı yazılmıştır. Morris'in, kodlama sırasında yaptığı bir yanlış sonucu ortaya çıkan bu program, Morris solucanı, sadece birkaç gün içinde günümüz İnternetinin öncüsü olan Arpanet'i gezmiş ve internete bağlı olan bilgisayarların %10′unun ağlarını çalışmaz hale getirmiştir [8].
- 1999 yılında, amatör bilgisayar korsanlarının DDoS'un araç olarak kullanılmasına örnek olan Melissa virüsünün, kısa süre içerisinde bilgisayar ve elektronik posta sistemlerine vermiş olduğu zararın ise 80 milyon dolardan daha fazla olduğu tespit edilmiştir [8].
- Takip eden yıllarda ise DDoS saldırıları daha ciddi maddi kayıplara yol açmaya başlamış olup Amazon, Yahoo, eBay gibi önemli sitelere karşı yapılan saldırıların yaklaşık 1.2 Milyar dolar zarar vermiş [9], 2001 yılının Eylül ayında ise Microsoft'un yaklaşık olarak 500 milyon dolar kaybettiği raporlanmıştır [10].
- DDoS saldırılarının sosyal eylem aracı olarak kullanıldığı 2010 yılında, Wikileaks internet sitesine yardım yasaklarından dolayı Mastercard, PayPal, Visa ve Postfinance internet siteleri DDoS saldırısına maruz kalarak belirli bir süre hizmet verememiştir [11].
- Anonymous, belirli bir yapılanmaya sahip olmayan haktivist bir gruptur ve sosyal protestolar için DDoS saldırılarını kullanan en bilindik örgütlerden birisi olarak tanımlanmaktadır [12].
- Wikileaks; Anonymous grubunun ilk gerçekleştirdikleri eylem olmayıp, 2008 yılında Scientology Kilisesi'nin haksız olarak vergi muafiyetine sahip olduklarını düşündükleri için Anonymous tarafından Scientology Kilisesinin, internet sitesi DDoS saldırıları ile kullanılmayan hale getirilmiş ve telefon hatları kilitlenmiştir [13].
- 2009 yılında ise Twitter sosyal medya sitesine yönelik yapılan saldırı ile twitter hesaplarına kullanıcılar saatlerce erişilememiştir [14].
- 2011 yılında ise Lulzsec adını kullanan saldırgan grup, Amerikan Gizli Teşkilatı internet sitesinin sunucusuna erişip aşırı talep isteği göndererek Amerikan Gizli Teşkilatı internet sitesini kullanılmaz duruma getirmiştir [15].

- 2012 yılında ise Türk Hava Yolları çalışanlarının grevlerine destek olmak amacıyla Anonymous tarafından gerçekleştirilen saldırıda, Türk Hava Yolları çevrimiçi uçuşlar sayfası DDoS saldırısına maruz kalmış ve uçuşlarda gecikmeler yaşanmıştır [16].

Yapılan saldırıların detaylarına bakıldığında ise aşağıda verilen saldırı örnekleri de bizlerin daha detaylı olarak bu saldırılara bakmamızı ve ciddiyetinin farkında olmamıza verilebilecek örneklerdir. Bunlar ise;

- 2007 yılında ilk defa DDoS, Estonya'ya karşı siber savaş aracı olarak kullanılmıştır. Estonya hükümeti, Sovyet döneminden Bronz heykeli taşıyınca Rusya duruma sert tepki göstermiştir. Tam bu tarihlerde siber saldırılar ile önce siyasi hedefler daha sonra da medya üzerinden halkın bilgi edinme olanaklarını kısıtlanmış, bankacılık sektörü yani ekonomi hedef alınmıştır. Estonya, saldırılara çözüm üretemeyince internet ile bağlantılar geçici süre durmuştur. Saldırılar 3 hafta sürmüş, tarihteki en büyük DDoS saldırısı olmasa da ilk defa suç unsuru içeren istenmeyen epostalar ve botnetler (spammers, botnets) ile, bir ülkenin ulusal güvenliğini tehdit edilmiştir. Bundan Rusya devlet olarak sorumlu tutulsa da bu hiçbir zaman ispatlanamamıştır. Bu olayla birlikte, siber suçlar artık ulusal ve uluslararası güvenlik için olası bir tehdit haline gelmiş ve içerisinde bulunduğumuz sayısal dünyanın aslında savunmasız olduğunu bir kez daha bizlere göstermiştir [17].
- Diğer bir siber olay ise, Rusya ile Gürcistan arasında sınır şeridinde yer alan Güney Osetya bölgesi için 2008 yılında çıkan anlaşmazlık ile ortaya çıkmıştır. Cephede yaşanılan savaş sanal ortama taşınmıştır. Gürcistan'da gerçekleşen DDoS saldırısı ile Gürcistan devlet kurumlarına ait sistemlere uzun süre erişilememiştir [18].
- Başka bir saldırı örneği ise 2012 yılında yaşanmıştır. İran, Amerikan bankalarına, binlerce yüksek güçlü uygulama sunucusu içeren botnetler kullanarak büyük bir DDoS saldırısı başlatmıştır. Saldırı da, saniyede 60 GB'i aşan veri selleri oluşturmak için "itsoknoproblembro" olarak bilinen yeni bir siber silah aracı kullanmıştır. Önemli finans kurumları yavaşlama ve ara sıra görülen kesintiler yaşamışlardır. En büyük üç ABD bankasına yönelik yapılan saldırıların İran'dan kaynaklandığı açıklansa da bu durum hiçbir zaman ispatlanamamıştır [19].

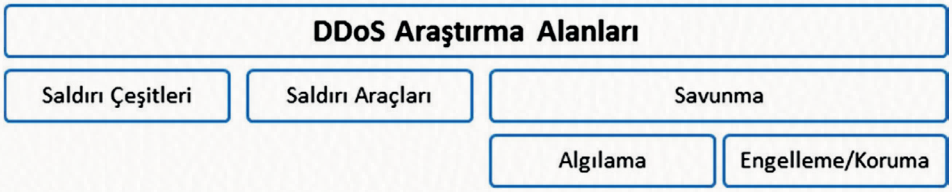
- İsveç Ulusal Hava Trafik Sistemine Kasım 2015 yapılan saldırı için, İsveç yetkilileri bu saldırıların Rusya odaklı olduklarını işaret etmişlerdir [20].
- Ekim 2018'de İsveç'te gerçekleşen DDoS saldırısı sonucu trenlerin güzergahını düzenleyen bilgisayar programı çökmüş, bu saldırıdan sonra şirket bazı trenleri durdurmuş, bazı trenleri ertelemek zorunda kalmış ve rezervasyonlarını kapatmıştır.
- 2019 yılında ise Türk Telekom Genel Müdürlüğünden yapılan açıklamaya göre Garanti Bankasına düzenlenen saldırı Türk Telekom ve Vodafone alt yapısını etkilemiş ve belirli bir süre hizmet verilememiştir [21].
- 2020 yılında ise dünyanın zorlu bir dönem içerisinde, bulunduğu küresel salgında, Ulusal Eğitim Bilgi Ağına (EBA) yönelik gerçekleşen saldırı sonucunda gün boyunca EBA'ya erişim sağlanamamıştır.
- Bebek alışveriş portalında yüksek ilgi gören e-bebek mağazası ve uzaktan eğitim sürecinde Sivas Cumhuriyet Üniversiteside DDoS saldırılarına maruz kalmıştır [22].

7.4. DDOS ÇALIŞMA ALANLARI

DDoS saldırıları akademi dünyası ve güvenlik mühendisleri tarafından da çok tercih edilen çalışmaların başında yer almaktadır. Ağ güvenliği stratejileri belirlenirken güçlü ve etkili bir ağ güvenliğinin DDoS saldırılarını kapsayıcı olması oldukça önemlidir. Şekil 7.3, DDoS saldırılarının araştırma alanlarına genel bir çerçeve çizmektedir. Literatürde DDoS saldırıları üzerine yapılan çalışmalara bağlı olarak çalışma alanları temelde üç kategoride gruplanır. Bunlar; saldırı çeşitleri, saldırı araçları ve savunma mekanizmalarıdır. DDoS çalışmalarının yapıldığı ilk zamanlarda DDoS saldırılarının tanımlanması ve özelliklerinin belirlenmesine odaklanılmıştır [23-27]. Ayrıca saldırı araçlarının özellikleri, avantaj/dezavantajları ve sınıflandırması ile ilgili çalışmalar da bulunmaktadır [23], [27].

Gerek saldırı tiplerini belirlerken gerekse de saldırı araçları üzerinde yapılan çalışmaların ana hedefi mevcut olarak kullanılan veya ihtiyaç duyulan savunma yeteneğini geliştirmektir. Bu sayede saldırılara dayanıklı bir güven-

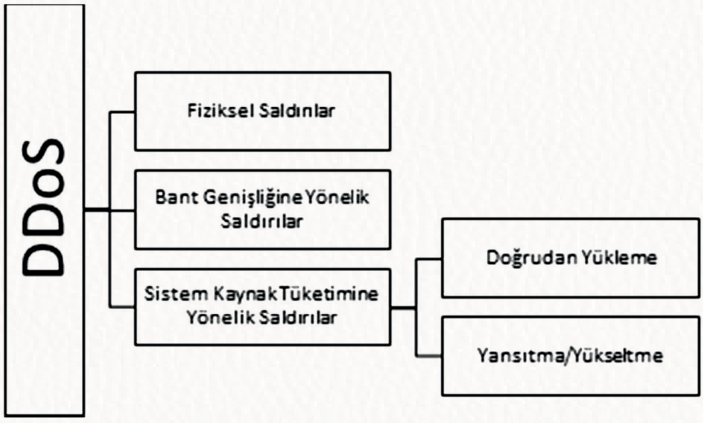
lik altyapısı oluşturmaktır. Şekil 7.3'te verildiği gibi DDoS saldırılarına karşı gerçekleştirilen savunma çalışmaları ise algılama ve engelleme aşamalarını içermektedir.



Şekil 7.3. DDoS çalışma alanları

7.5. DDOS SALDIRI TÜRLERİ

Literatür incelendiğinde; DDoS saldırıları farklı araştırmacılar tarafından farklı ölçütlere göre sınıflandırıldığı gözlemlenmektedir [26-30]. Bu çalışmada; DDoS saldırıları, hedefe zarar verme yöntemlerine bağlı olarak sınıflandırılmaktadır. DDoS saldırı sınıfları, fiziksel saldırılar, bant genişliğine yönelik yapılan saldırılar ve sistem kaynakları tüketimine yönelik yapılan saldırılar olmak üzere üç ana kategoride Şekil 7.4'de gösterildiği gibi incelenmektedir. Aşağıda yer alan bölümlerde bu üç kategoriye ait olan DDoS saldırıları teknik olarak tanımlanmakta ve incelenmektedir.



Şekil 7.4. DDoS saldırı türleri

7.5.1. Fiziksel Saldırılar

Fiziksel DDoS saldırılarında, fiziksel olarak hizmetin engellemesi veya sekteye uğratılması ana hedeftir. Bu müdahale doğrudan veya dolaylı olarak gerçekleştirilebilir. Bir sistemin çalışması için gerekli altyapıya yapılacak fiziksel bir müdahale veya bu altyapıya uzun vadede zarar verecek sistem ayarlarındaki değişiklikler fiziksel saldırı sınıfında sayılabilir. Almanya'da gerçekleşen DDoS saldırısı, fiziksel saldırıların önemine dair en iyi örneklerinden birisidir. Bu saldırıda bir demir çelik üretim fabrikasının bilgisayar sistemi kötücül bir yazılımla, saldırganların eline geçmiş, yüksek sıcaklıkta ki fırınların ayarları uzaktan erişilerek değiştirilmiş ve bu sayede üretimin durması sağlanmıştır [31]. İran nükleer santraline yönelik yapılan fiziksel saldırıda santral santrifüjlerinin dönüş hızı, Stuxnet isimli kötücül bir yazılım yardımı ile azaltılarak, uzun sürede üretim aksaması gerçekleştirilmiştir [32]. New York'ta bulunan Bowman Avenue Dam adlı baraja yapılan saldırı da ise saldırganlar baraj kapaklarını, sisteme uzaktan erişerek açmaya çalışmış ancak saldırı anında kanal kapısının elle kontrol ediliyor olmasından dolayı fiziksel hasar engellenmiştir [33].

7.5.2. Bant Genişliğine Yönelik Yapılan Saldırılar

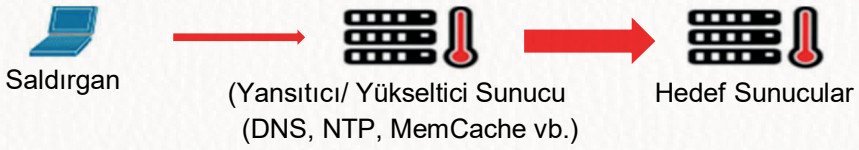
DDoS saldırıları; bant genişliğini tüketmeye yönelik yapılsa da kapsamlı veya volümetrik (hacimsel) saldırılar adını almaktadır. Kapsamlı (volümetrik) saldırılar, kötü amaçlı yazılım (malware) bulaşmış veya enfekte olmuş sistemler vasıtası ile doğrudan veya halka açık ağ servislerini suistimal edip yansıtma/yükseltme yapılarak gerçekleştirilebilir [34].

Siber saldırganlar, kötü amaçlı yazılım bulaşmış cihazları uzaktan kontrol ederek, hedefe giden yolda trafik akışını artırır ve hedefte hizmet aksamasına veya engellenmesine sebep olabilirler. Genellikle botnet (robot network) olarak adlandırılan bu uzaktan kontrol edilebilir ağlar; kontrolü ele geçirilmiş bilgisayarlar, sunucular ve benzeri ağ cihazları kullanılarak DDoS saldırıları gerçekleştirmektedir. Bu tür saldırılarda saldırgan, saldırı yapacağı ağa botnetler yardımı ile çok fazla sayıda paket göndererek ağın bant genişliğinin tükenmesine sebep olmaktadır. Böyle bir saldırıda, Internet Kontrol İletisi Protokolü (ICMP), Kullanıcı Veri Bloğu Protokolü (UDP) ve İletişim Denetim Protokolü (TCP) gibi farklı ağ katmanı protokolleri kullanılabilir [34].

Saldırıların büyüklüğü genellikle saniyede bit veya paket olarak ölçülmektedir. Arbor Network'ün 2017 yılında yayınladığı internet güvenliği raporuna göre; DDoS saldırılarının %65'i hacimsel (volümetrik) niteliği yüksek saldırılar [18] olup gerçekleştirilme yöntemlerine göre doğrudan ve yansıtma/yükseltme (reflection/amplification) saldırıları olarak ta iki kategoride incelenmektedir [33]

Doğrudan gerçekleştirilen DDoS saldırılarında; saldırgan, saldırı komutunu, kontrol ve komuta merkezine (CCC) iletir, komut komuta merkezi, kontrolü ele geçirilmiş ağ cihazlarına hedefe yönelik trafik göndermesi için komut verir [34]. Bu sistemde yer alan katmanlı yapı ile saldırganın kimliği gizlenir ve böylece kaynak hakkında ipucu bulunamaz [35]. Bu yöntemle oluşturulan yüksek seviyedeki trafik hacmi, hedefin bant genişliğini kaplamakta ve hedefte hizmet aksaması veya engellemesi gerçekleştirilmektedir.

Doğrudan saldırılara; ICMP veri seli veya UDP veri seli örnek olarak verilebilir. Günümüzde bilinen yüksek hacimli veri seli saldırıları, güvenlik seviyesi düşük IoT cihazlarını kullanan Mirai Botneti aracılığı ile gerçekleştirilmiştir.



Şekil 7.5. Yansıtma/Yükseltme ile saldırı boyutunu (volümetrik) büyütme saldırıları

Hedefin bant genişliğine yönelik yansıtma/yükseltme yöntemi ile yapılan saldırılar Şekil 7.5'de gösterilmektedir. Saldırgan bu saldırılarda herkes tarafından kullanılabilen, zafiyeti bulunan sunucuları bir yükseltme/yansıtma aracı olarak kullanır. Yansıtma/Yükseltme aracı olarak kullanılan bu sunucular; herkes tarafından erişilebilmektedir. Bu sunuculara DNS, NTP, Memcache örnek olarak verilebilir. Saldırgan; sahteleştirdiği paketleri sunucuya gönderir. Yansıtıcı/Yükseltici ise paketleri kendi üzerinden hedef bilgisayara gönderir. Bu işlemi gerçekleştirirken paketler sunucu üzerinden yansıtılmış veya yükseltme faktör değerine göre yükseltilmiş olarak gönderilir. Sonuç olarak fazlalaşan paket sayısı ile birlikte hedefin bant genişliğinde taşma meydana gelir ve hedefte hizmet aksar veya engellenir.

Yansıtma saldırılarında, saldırganlar, saldırı trafiğini hedefe göndermek için reflektör adı verilen bileşenden faydalanmaktadır. Saldırgan sahte IP kullanan paketleri, reflektör görevi gören ve ara katman olarak kullanılan bilgisayarlara gönderir. Yükseltme saldırılarında ise ara katman olarak kullanılan bileşen amplifikatör adını alır ve hedefe gönderilen paketler, kullanılan protokole bağlı olarak farklı oranlarda yükseltmektedir. Bu yükseltme katsayısı; yükseltme faktör değeri olarak adlandırılmaktadır. Yükseltme faktör değeri, yansıtma/yükseltme DDoS saldırılarında önem taşımaktadır. Bu yükseltme katsayısı; yükselticiden hedefe giden paket boyutunun, saldırgandan yükselticiye giden paket boyutuna bölünmesi ile hesaplanmaktadır. Yansıtma/Yükseltme saldırılarında kullanılan protokoller ve bu protokollerin yükseltme katsayıları Tablo 7.1'de gösterilmektedir [36].

Tablo 7.1. Kullanılan protokollere bağlı yükseltme katsayıları [36]

Protokol	*Yükseltme Katsayısı*
NetBios	3.8
BitTorrent	3.8
SNMPv2	6.3
DNS	28-54
NTP	556.9
Memcache	10.000 – 50.000

Günümüzde gerçekleştirilen saldırılarda genellikle yansıtma ve yükseltme saldırıları aynı anda gerçekleştirilmektedir. Bu saldırılara örnek olarak; Smurf, Fraggle, NTP Yükseltme, DNS Yükseltme, Memcache Yükseltme verilebilir. Smurf saldırılarında; ICMP Echo istekleri (ping) yönlendiricilerin yayın adreslerine gönderilir. ICMP Echo isteği alan aygıt bağlı olduğu her bir cihaz ile sahte kaynak adrese Echo yanıtı gönderir. Fraggle saldırılarında, bir ağdaki bir yönlendiricinin yayın adresine çok miktarda sahte UDP trafiği gönderilerek hizmet engellenir. Fraggle saldırıları, Smurf saldırılarına çok benzer fakat günümüzde yönlendiriciler yayın adreslerine yönlendirilen paketleri iletmedikleri için çoğu ağ artık Smurf ve Fraggle saldırılarına karşı tedbirlidir [36].

NTP, internet'e bağlı makinaların saatlerini ayarlamak için kullandığı ağ zaman protokolüdür. NTP amplifikasyon saldırılarında, DDoS saldırganı NTP selinden yararlanır. Saldırgan, NTP altyapısını aldatmak için, açık olan NTP

sunucuları yardımı ile ağ da veri selleri oluşturur [37], DNS (alan adı sistemi) internet sitelerinin isimlerini IP adreslerine yönlendiren bir veritabanına sahip sunucu bilgisayar olarak tanımlanabilir. DNS yükseltme saldırısı; saldırganın kurbanın açık olan bir DNS çözümleyicisine sahte bir IP adresi kullanarak DNS sorgusu yapması ile başlar. Saldırgan tarafından botnetler aracılığı ile çok sayıda sahte sorgunun gönderilmesi ve birkaç DNS çözümleyicinin aynı anda yanıt vermesi ile hedef ağda hizmet aksaması meydana gelir [36]. NTP yükseltmesi ve DNS yükseltmesi gibi DDoS yükseltme saldırılarına benzer şekilde çalışan Memcache saldırıları da yükseltme saldırılarına örnektir. Memcache; web sitelerini ve ağları hızlandırmak için kullanılan bir veritabanı önbellekleme sistemidir [37]. Memcache sunucuları, UDP protokolünü kullanarak çalışma seçeneğine sahiptir. UDP protokolünde paketler, alıcı taraftan cevap beklemeden gönderilir. Saldırgan, hedefin IP adresinden geliyormuş gibi UDP taleplerini Memcache sunuculara gönderir. Memcache sunucuların temel özelliğinden kaynaklı olarak, cevap talebe göre kat kat büyür. Bu yükseltilmiş cevaplar hedefin internet sitesine doğru büyük miktarda gereksiz trafik oluşturur. Bu sayede hedefte hizmet aksaması veya engellemesi meydana gelir.

7.5.3. Sistem Kaynak Tüketimine Yönelik Yapılan Saldırılar

Sistem kaynaklarını, sabit disk, işlemci, geçici bellek tüketimi için protokol zafiyetlerinden faydalanılarak gerçekleştirilen saldırılardır. Bu saldırılar da ağa gönderilen yüksek paket sayısı bulunmamaktadır. Bu saldırılara; Fork Bomb, HTTP GET/POST, Slowloris örnek olarak verilebilir [31]. Fork Bomb, çatal bomba olarak bilinen DDoS saldırısıdır. Sistemin CPU ve bellek tüketime yönelik sistem zafiyetlerinden faydalanılarak yapılır. Unix ve Linux sistemlerinde var olan bir işlemi tekrar tekrar çalıştırma mantığına dayanır. Saldırının arkasında yatan temel fikir ise bir işlemin (process) kendi başına yeni kopyalarını tekrar tekrar başlatması ve sonsuz bir döngü oluşturması ile işlemciyi ve belleği yormaktır. Microsoft Windows işletim sistemlerinin Unix fork sistem çağrısına eşdeğer bir işlevi olmadığı için bu saldırı Microsoft Windows işletim sistemlerinde yapılamaz [38].

HTTP istemcisi bir sunucuya HTTP isteği, genellikle GET veya POST çağrıları kullanılarak gönderilir. Post istekleri dinamik olarak oluşturulmuş kaynaklara erişmek için kullanırken, GET isteği resimler gibi standart ve statik

içeriği almak için kullanılmaktadır. Saldırgan genellikle sunucuyu, mümkün olduğunca çok işlem gerektiren yoğun istek göndererek meşgul eder. HTTP GET sel saldırıları uygulama katmanına yönelik yapılan en popüler DDoS saldırılarından birisidir [39].

TCP, günümüzde en çok kullanılan iletişim protokolüdür. TCP protokolünün zafiyetlerinden faydalanan saldırganlar, kolaylıkla uygulama katmanı DDoS saldırılarını gerçekleştirebilir. Uygulama katmanına yönelik, kaynak tüketimini hedef alarak yapılan saldırılara; Slowget, Slowpost, Slowloris örnek olarak verilebilir. Uygulama katmanına yönelik yapılan DDoS saldırılarında, kaynak tüketimi, hafızada daha fazla yer tutma işlemine dayalı olarak gerçekleştirilir. Sürekli gönderilen istek mesajı ile beraber sistem belleğinde oluşan kuyruk nedeniyle hedef, isteklere cevap veremez duruma gelir. İstemci sunucudan gelen veriyi yavaş okuduğunda ve/veya istemci sunucuya veriyi yavaş gönderdiğinde sunucu kaynakları gereğinden uzun süre meşgul edilir [31].

7.6. DDOS SALDIRI ARAÇLARI

DDoS saldırganları, kurban olarak seçtikleri sistemlerin kaynaklarını tüketmek için çeşitli araçlar kullanmaktadır. DDoS saldırı araçları çeşitlilik göstermekle beraber bu araçların birçoğu ücretsiz yazılım ve/veya açık kaynak kodlu proje olarak paylaşılmaktadır [40]. Günümüzde birçok DDoS saldırı aracı bulunmaktadır. Aşağıda yer alan kısımda kronolojik olarak bazı popüler DDoS saldırı araçları incelenmiştir.

- **TrinOO** [41], DDoS saldırganlarının, kurban sistemin bant genişliğini tüketmeye yönelik, UDP paket seli (flood) saldırısının başlatılması için kullanılan araçlardan birisidir. TFN [41], kurban sistemin hem bant genişliğine hem de kaynak tüketimine yönelik yapılan saldırıları gerçekleştirebilen Trin00 daha gelişmiş versiyonu olarak bilinen bir başka DDoS saldırı aracıdır. UDP paket selinin yanı sıra TCP SYN paket seli, ICMP paket seli saldırılarını başlatabilir. TFN2K [41], TFN saldırı aracının bir türevidir ve hem bant genişliğine hem de kaynak tüketimine yönelik saldırıları gerçekleştirebilir. SYN, UDP ve ICMP taşma saldırılarını başlatabilir. TFN2K, saldırı bileşenleri arasında şifreli mesajlar ekleme özelliğine sahiptir.

- **Stacheldraht** [42], hem bant genişliğini hem de sistem kaynaklarının tüketimini hedef alan bir saldırı aracıdır. Stacheldraht, SYN paket seli, UDP paket seli ve ICMP paket seli saldırılarını gerçekleştirebildiği gibi son versiyonunda TCP ACK, NULL, MSTREAM VE HAVOC paket seli saldırıları ve SMURF saldırılarını gerçekleştirebilmektedir [115].
- **Shaft** [43], gelişmiş bir şifreleme mekanizması olmamakla beraber basit Sezar şifreleme tekniğini kullanır. Hem bant genişliğini hem de sistem kaynaklarının tüketimini hedef alan bir saldırı aracıdır. ICMP, UDP ve TCP SYN paket seli saldırılarının başlatılması için kullanılan araçlardan birisidir.
- **Trinity** [44], 2000 yılında ortaya çıkmış bir saldırı aracıdır. Trinity saldırı aracı IRC kanalına özel bir anahtar kullanarak katılır, bir kere kanala katıldıktan sonra Trinity ajanları uygun komutun gönderilmesini bekler. Trinity ajanlarının aracının paket seli meydana getirmek için oluşturulan komut biçimi şu şekildedir [45]:

<paket taşma türü> <ajanın şifresi> <kurbanın IP adresi> <saniye cinsinden paket seli için geçen sürenin uzunluğu>

Hem bant genişliğini hem de sistem kaynaklarının tüketimini hedef alan bir saldırı aracıdır. UDP, TCP SYN, TCP ACK, TCP NUL ve HAVOC paket seli saldırılarını gerçekleştirebilmektedir.

- **Knight** [46], Windows işletim sistemlerinde çalışacak şekilde tasarlanmış, hem bant genişliğini hem de sistem kaynaklarının tüketimini hedef alan bir saldırı aracıdır. UDP paket seli saldırılarını ve SYN saldırılarını gerçekleştirebilmektedir.
- **Kaiten** [46], virüslü hedef bilgisayarlar, bir IRC kanalı aracılığıyla saldırı komutları alır böylece hem bant genişliğini hem de sistem kaynaklarının tüketimini hedef alan bir saldırı aracıdır. UDP, TCP, SYN ve PUSH + SYN paket seli saldırılarını başlatabilen DDoS saldırı aracıdır.
- **BlackEnergy** [47], 2007 yılında ilk defa Arbor Network tarafından raporlanmış, HTTP temelli saldırganlar üreten DDoS saldırı aracıdır. Saldırı, e-posta üzerinden bir Word belgesi veya PowerPoint eki aracılığıyla dağıtılır ve kurbanları meşru görünen dosyayı açmaya teşvik eder. Bu şekilde hem bant genişliğini hem de sistem kaynaklarının tüketimini

hedef alır. Sahip olduğu çalışma zamanı şifreleyicisi, antivirüs yazılımı tarafından tespit edilememesine neden olur [48]. ICMP, TCP SYN, UDP, HTTP , DNS paket seli saldırılarını başlatabilmektedir.

- **LOIC (Düşük Yörüngeli İyon Topu)** [48], 2008 yılında Praetox Teknoloji tarafından C# programlama dili ile geliştirilmiş açık kaynaklı ağ stres testi ve DDoS saldırı aracıdır. Bu araç Windows, Linux, OS X, Android, IOS işletim sistemlerinde çalışmaktadır. LOIC, belirli bir ana bilgisayarın hizmetini kesintiye uğratmak için sunucuyu TCP, UDP veya HTTP paketleri ile doldurarak, hedef internet sitesinde bir DoS/DDoS saldırısı gerçekleştirir. LOIC saldırıları, sistem günlüklerinde kolayca tespit edilir ve saldırı, kullanılan IP adreslerine kadar izlenebilir [49]. LOIC, Scientology Kilisesi'nin internet sitelerine saldırmak için Anonymous tarafından ayrıca Ekim 2010'da Amerika Kayıt Endüstrisi Birliği internet sitesine saldırmak için ve Anonymous tarafından Aralık 2010'daki WikiLeaks'e karşı çıkan şirketlerin ve kuruluşların internet sitelerine saldırmak için tekrar kullanılmıştır [50-52]. LOIC ağ kaynaklarını ve 3., 4. ve 7. ağ katmanlarında saldırı trafiği oluşturmak için kullanılır.
- **RUDY** [53]; 2010 yılında Raviv Raz tarafından geliştirilen 7. katman DoS saldırıları oluşturmak için hazırlanmış bir saldırı aracıdır. Ağ stres testi aracı olarak Pyhton'da yazılmıştır. RUDY; HTPP POST mesajı açıklığından yararlanarak düşük ve yavaş seviyeli DoS saldırıları düzenleyebilmektedir. RUDY kaynak kodlarına, GitHub paylaşım internet sitesinden erişilebilmektedir [54]. Sistem kaynaklarını tüketmek ve 7. ağ katmanında saldırı trafiği oluşturmak için kullanılır.
- **HULK** [55], HTTP dayanılmaz yük kralı olarak nitelendirilen HULK saldırı aracıdır. 2012 yılında Barry Shteiman tarafından Pyhton programlama dilinde yazılmıştır. HTTP paket seline benzer ve internet sunucuların kaynaklarını istila etmek için tasarlanmıştır. HULK, sunuculardaki yükü artırmanın yanı sıra herhangi bir saldırı tespit ve önleme sisteminden kaçınmak amacıyla her talepte benzersiz bir model oluşturur. Sistem kaynaklarını tüketmek ve 7. ağ katmanında saldırı trafiği oluşturmak için kullanılır.
- **SADDAM** [43]; pek çok farklı protokoldeki ağ trafiğini yansıtmak veya güçlendirmek için, genel kullanıma açık sunucuların kimlik de-

netimi kontrolü zayıflığından veya güvenlik açığından yararlanır. Offensive Python tarafından Python programlama dilinde 2015 yılında geliştirilmiştir. DNS (Alan Adı Sunucu), NTP (Ağ Zaman Protokolü), SNMP (Basit Ağ Yönetim Protokolü), SSDP (Basit Servis Bulma Protokolü) Yükseltme yansıtma saldırılarını düzenleyebilir. SADDAM kaynak kodlarına GitHub paylaşım internet sitesinden erişilebilmektedir [56]. Sistem kaynaklarını tüketmek ve 7. ağ katmanını saldırı trafiği oluşturmak için kullanılır.

- **Memcrashed-DDoS** [57]; 2018'de ön tampon bellekte keşfedilen açıklık saldırganların güçlü yansıtma DDoS saldırısı başlatmasına ve yürütmesine izin vermiştir. Bu güvenlik açığı "Memcrashed" olarak adlandırılmıştır ve 2018 yılında 1,35 TBps büyüklüğündeki GitHub'a düzenlenen saldırının sebebi bu araçtır. Bu saldırı aracının kaynak kodlarına GitHub paylaşım internet sitesinden erişilebilmektedir [58]. Sistem kaynaklarını tüketmek ve 7. ağ katmanını saldırı trafiği oluşturmak için kullanılır.

Yukarıda kronolojik olarak sıralanan DDoS saldırı araçları sayı olarak çok daha fazladır. Bu bölümde popüler saldırı ve stres testi araçları listelenmiştir. LOIC saldırı aracından sonra geliştirilen saldırı araçları, yeni özellikler eklemek yerine saldırı hacmini nasıl arttırılır sorusuna odaklanmaktadır. Bu saldırı araçlarının ana hedefi en az efor ile saldırı trafiği oluşturup ana trafiği yavaşlatmaktır.

7.7. DDOS SAVUNMA

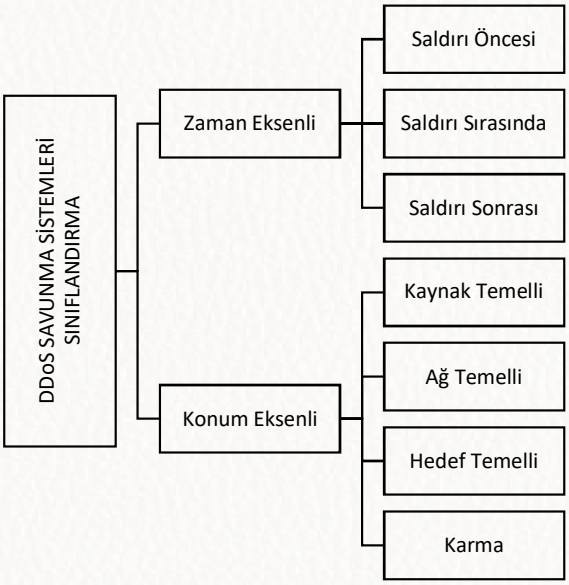
DDoS saldırılarına karşı yeterli savunma ağ yöneticileri için de ağ uzmanları için de hala çözülmesi zor olan problemlerden biridir. Birçok gerçek zamanlı DDoS saldırı algılama yöntemi literatürde bulunmakta fakat günümüzde tüm DDoS saldırı sınıfları için geçerli gerçek zamanlı bir mekanizma yoktur. Ayrıca önerilen savunma sistemleri genellikle hesaplama karmaşıklığı yüksek yöntemlerden oluşur.

Bir DDoS saldırganı, ağa anında paket seli yapmak için çok sayıda düğüm kullanır. Saldırganın hazırlık faaliyetlerinin erken tespiti, saldırı ile etkin mücadele için çok önemlidir. DDoS'a karşı temel savunma hem algılama hem de müdahale yeteneklerinin bir arada kullanılması ile gerçekleştirilir.

DDoS savunma mekanizmaları saldırıya ne zaman ve ne nerede müdahale edildiğine bakılarak iki sınıfta incelenebilir. Ayrıca, DDoS savunma algılama ve müdahale süreci olmak üzere iki ana kategoride incelenebilir. Bu çalışmada her iki kategori içinde ayrıntılı değerlendirme gelecek olan başlıklarda yer almaktadır.

7.7.1. DDoS Savunma Sistemi Sınıflandırması

DDoS Saldırılarına karşı savunma yapılırken savunma mekanizmasının ne zaman ve nerede devreye girdiğine göre savunma sistemleri iki ana başlıkta değerlendirilebilir. Şekil 7.6, DDoS savunma sistemi sınıflandırmasını ayrıntılı olarak sunmaktadır. Zaman eksenine bağlı savunma ise saldırı öncesi, saldırı sırasında ve saldırı sonrası olmak üzere üç alt başlıktan oluşur. Saldırı mekanizması gerçekleştirildiği yere bağlı olarak kaynak temelli, hedef temelli, ağ temelli ve hibrit olmak üzere dört alt başlıkta incelenir.



Şekil 7.6. DDoS savunma sistemleri sınıflandırma

Şekil 7.6'da verilen sınıflandırma aşağıda verilen alt başlıklarda kısaca gösterilmektedir.

7.7.1.1. Savunma Zaman Eksenli DDoS Saldırıları

DDoS saldırılarına karşı savunma, ne zaman gerçekleştirildiğine bakıldığında üç kategoride incelenir. Savunma; saldırı öncesinde, saldırı sırasında ve saldırı sonrasında gerçekleştirilebilir. Saldırı öncesi savunma denildiğinde akla gelen saldırı önleme sistemleridir. Saldırı sırasında savunmadan bahsedildiğinde ise sistem saldırı algılama olarak nitelendirilebilir. Saldırı sonrası savunma ise saldırı kaynağını tanımaya ve yanıtlamaya yönelik gerçekleştirilir.

Saldırı Öncesi; alınan önlemler en genel kapsamda sistemlerin saldırıya uğramaması için sistem açıklıklarının giderilmesini kapsar. Saldırıdan önce, saldırı önlemede kullanılan mekanizmalarının çoğu, DDoS saldırıları başlatmak için kullanılabilecek güvenlik açıklarını örneğin güvensiz protokoller, zayıf kimlik doğrulama şemaları ve savunmasız bilgisayar sistemleri düzeltmeyi amaçlar [59]. Böylece sistemler için daha fazla güvenlik sağlanabilir. Önleme mekanizmaları, saldırı kaynaklarına, ara ağlara, varış noktalarına veya bunların birleşimine konuşlandırılabilir [59]. Saldırı öncesi alınan önlemler DDoS saldırı tehdidini tamamen ortadan kaldıramaz [60].

Saldırı Sırasında; DDoS saldırı sırasında gerçekleşen savunma saldırı algılama işlemlerini kapsar. Saldırı sırasında kullanılan sistemler saldırı hedefe ulaşmadan önce saldırıyı durdurmayı ya da saldırının hedefe en az zararı vermesini hedefler. DDoS saldırılarını hedefe ulaşmadan tespit etmek için kullanılan çeşitli mekanizmalar vardır [60-63]. Bazı algılama mekanizmaları, ağ bağlantıları belirli bir seviyede sıkıştığında kapasite temelli olarak saldırı akışlarını tespit eder [63-66]. Bazı mekanizmalar ise DDoS saldırı trafiğini, anormal kalıplar keşfedildiğinde yani anormallik temelli olarak tespit eder [66-69]. Anormallik temelli mekanizmalar, çeşitli yerlerde ve zaman noktalarında trafik akışının bazı özelliklerini izler ve trafiğin normal davranışını öğrenirler. Ardından, izledikleri ve topladıkları bilgilere dayanarak, kaynakların trafik modelleri ve kullanım şekilleri üzerinde bir değişiklik tespit edebilirler [70].

Saldırı Sonrası; DDoS saldırısı tespit edildiğinde, savunma sistemi saldırı sırasında saldırının kaynağını belirlemeye ve saldırı trafiğini engellemeye çalışabilir. Saldırı sonrası sistemleri ise saldırı hedefe ulaştıktan sonraki aşamada ise müdahale ve geri izleme gerçekleştirilir [71] . Saldırıya müdahale de kullanılan en yaygın yöntemlerden birisi de filtrelemedir [71]. Filtreleme mekanizmaları ile saldırının sisteme vereceği zarar durdurulabilir veya en aza indirilebilir. Filtreleme işlemi bağımsız gerçekleştirilebileceği gibi işbirliğine

dayalı da yapılabilir [72]. Saldırı geri izleme mekanizmaları ise saldırı gerçekleştikten sonra saldırının kimliğini belirlemeye yönelik yapılan çalışmaları kapsar [72]. Saldırı etkisini en aza indirgemek ve savunma hizmetlerin kullanılabilirliğini en üst düzeye çıkarmak, saldırı mekanizmalarının tamamında ana odak noktadır [69-73].

7.7.1.2. Savunma Konum Ekseninde DDoS Saldırıları

DDoS saldırılarına karşı savunma mekanizmaları yerleştirildiği konuma bağlı olarak dört sınıfta incelenir [70]. Savunma mekanizması kaynak da yer alıyor ise kaynak temelli, hedef de yer alıyorsa hedef temelli, ağ da yer alıyorsa ağ temelli ve birden fazla yerde konumlandırılmış ise karma olarak isimlendirilir. Saldırı algılama mekanizmaları, kaynakta, hedefte, ara ağlarda veya bunların bir kombinasyonuna konumlandırılabilir.

Kaynak temelli savunma mekanizmaları; DDoS saldırı trafiğini kaynakta tespit etmek ve süzmek üzere tasarlanmıştır. Bu mekanizmalar, saldırı kaynaklarının yakınına konumlandırılır ve kaynağın yerel ağının kenar yönlendiricilerinde veya kaynakların kenar yönlendiricilerine bağlanan Özerk Sistemin (Autonomous System) erişim yönlendiricilerinde savunma gerçekleştirilir [74]. DDoS saldırılarına karşı kaynak temelli tasarlanan mekanizmalara; kaynağın kenarında giriş/çıkış filtresi (ingress/egress) yönlendiriciler [75], D-WARD [76], çevrimiçi paket istatistikleri için çoklu düzey ağaç (MULTOPS) [77], Tabletlenmiş Çevrimiçi Paket İstatistikleri (TOPS) [80], MANAnet'in ters güvenlik duvarı [78], örnek olarak verilebilir [51]. Fiziksel olarak saldırı kaynağı kaynak dışında farklı bir noktada olduğunda sadece kaynak temelli bir savunma mekanizmasını kullanmak, DDoS saldırılarına karşı savunmada kötü bir tercih olur. Bu sebeple savunma mekanizmasını konumlandırırken sadece kaynak temelli konumlandırma tercih edilmemektedir.

Hedef temelli savunma mekanizmaları; DDoS saldırılarına karşı müdahaleyi saldırının hedef aldığı yerde yani kurbanda yapmak üzere tasarlanmıştır [74]. Hem uç yönlendiricilerde, hem de hedeflerin özerk sistemlerinin erişim yönlendiricilerin de savunma için konumlandırılabilir. Bu konumda yer alan mekanizmalar yardımı ile istenirse kurban yakından gözlemlenebilir, kurban davranışlarını modellenebilir ve herhangi bir anormallik tespit edebilir. Hedefe dayalı DDoS savunma mekanizmalarına, IP Geri izleme mekanizmaları [80], yönetim bilgi tabanı (MIB) [81], paket işaretleme ve filtreleme meka-

nizmaları [82], geçmişe dayanan IP filtreleme [83], hop-sayısı filtreleme [84], yol tanımlayıcı (Pi) [85], paket tıkanıklığı seviyesine göre düşen paket skoru (packetscore) [86] örnek olarak verilebilir. Hedef temelli savunma mekanizmalarının çoğu, saldırı kurbana ulaşmadan, saldırıyı doğru bir şekilde tespit edemez ve cevaplayamaz. Kurbana giden yolda kaynak israf edebilmektedir; bu sebeple hem kaynak hem de hedef temelli mekanizmaların dezavantajları göz önüne alındığında daha etkin kullanım alanına sahip olduğu düşünülen ağ temelli DDoS savunma mekanizmaları önerilmiştir [52].

Ağ temelli savunma mekanizmaları; DDoS saldırılarına karşı müdahaleyi ağlar içerisinde ve özellikle özerk sistemlerin yönlendiricileri üzerinde konumlanarak gerçekleştirmeye çalışır [87]. Saldırı trafiğini tespit etmek ve ara ağlarda saldırıyı durdurmak bu savunma mekanizmalarının ana hedefidir. Ağ temelli DDoS savunma mekanizmalarına; rota temelli paket filtreleme [88], kötü amaçlı yönlendiricileri saptama ve filtreleme örnek olarak verilebilir [89]. Ağ temelli konumlandırılan savunma mekanizmaları, genellikle yönlendiriciler için yüksek depolama ve işleme masrafına neden olmaktadır [52]. Her bir yönlendirici hedefe giden yolu kullanarak gereksiz algılama ve yanıt üretirse bu durum ek yük getirir. Bu sebeple yönlendiricilerde ki ek yükü azaltmak için bloom filtreleri [90], paket örnekleme [91] gibi farklı yaklaşımlar önerilmektedir. Fakat yine de yönlendiriciler için bu yaklaşımlar yeterli olmamaktadır.

Kaynak temelli, hedef temelli ve ağ temelli konumlandırılan DDoS savunma mekanizmaları merkezi savunma mekanizmaları olarak adlandırılır. Merkezi savunma mekanizmalarında dağıtım noktaları arasında işbirliği olmamakla birlikte algılama ve tepki merkezi bir noktadan yapılır [52]. Merkezi savunma mekanizmalarının dezavantajları göz önüne alınarak karma şekilde konumlandırılmış savunma mekanizmaları önerilmiştir [53].

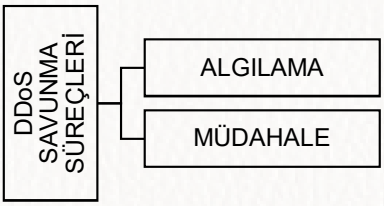
Karma savunma mekanizmaları; merkezi savunma mekanizmalarının aksine, kaynak, varış veya ara ağlar gibi birden çok yere konumlandırılabilir ve dağıtım noktaları arasında genellikle işbirliği bulunmaktadır [52]. Örneğin, algılama mağdur tarafta yapılabilir, yanıt mağdur tarafından başlatılabilir ve diğer düğümlere dağıtılabilir. Karma DDoS savunma mekanizmalarına; Tıkanıklık Kontrolü (ACC) ve geri çağırma [92], TRAK [93], DEFCOM [94], COSSACK [97], Etkin İnternet Trafiği Filtreleme (AITF) [95] ve DurdurOnu (StopIt) [96] bunlara örnek olarak verilebilir. DDoS savunma ile ilgili ça-

lışmalar avantajları göz önünde bulundurulduğunda karma DDoS savunma mekanizmaları üzerine yoğunlaşmaktadır. Yakın zamanda önerilen mekanizmaların çoğu karma kategoriye aittir.

DDoS savunma mekanizmalarının ana hedefi, DDoS saldırılarını mümkün olan en kısa sürede ve mağdurlara ulaşmadan tespit etmek, saldırı kaynaklarını belirlemek ve saldırıyı durdurmaktır. Bu hedef en iyi karma yani dağıtılmış olarak konumlandırılan DDoS savunma mekanizmaları ile başarılabilir [54].

7.7.2. Savunma Süreçleri Temelli DDoS Saldırıları

DDoS saldırılarına karşı savunma süreçleri DDoS saldırı algılama ve DDoS saldırılarına karşı müdahale olarak Şekil 7.7'de gösterildiği üzere genel olarak iki başlık altında incelenir [59]. Bu başlıkların ayrıntılı değerlendirmesi ilerleyen bölümlerde sunulmuştur.



Şekil 7.7. DDoS savunma süreçleri

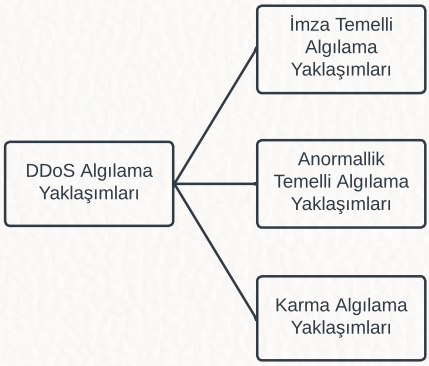
7.7.2.1. DDoS Algılama

DDoS algılama konusunda literatür incelendiğinde; saldırı algılama işlemi ya saldırı algılamayı ya da saldırı trafiği algılamayı hedef alarak iki şekilde gerçekleştirilir. Saldırı algılama işlemi gerçekleştirilirken saldırının var olup olmadığını test eder. Saldırı trafiği algılamada ise saldırı esnasında zararlı trafiğin gerçek kullanıcı trafiğinden ayrıştırılması hedeflenir. Bu iki durumda da saldırı algılamada da birbirlerine benzer yöntemler kullanır [59-61].

DDoS saldırı trafiği algılama teknikleri; ağ trafiğini meşru (legitimate) veya kötücül (malicious) amaçlı olarak sınıflandırır. İyi bir saldırı sezme sisteminin performansı, normal trafik verilerinden saldırı trafik verilerinin en iyi şekilde ayrıştırılması, doğru algılama (true detection) oranının yüksekliği ve algılama

hata oranının düşüklüğü ile değerlendirilir. Bahsedilen yöntemler literatürde yaygın olarak kullanılan yöntemlerdir. Bu yöntemlerin yanı sıra saldırı sezme sisteminin performansını değerlendirmek için kullanılan diğer ölçütler; doğruluk, **duyarlılık,** yanlış pozitif ve doğru pozitif oranlarını gösteren ROC Eğrileri, gerçek verilerin tahmin edilen sonuçlar ile karşılaştırıldığı karışıklık matrisi, işlem süresi, tüketilen bellek miktarı, zaman içerisinde işlenen paket sayısı, saldırıya cevap verme zamanı yani zaman gecikmesi, uygulama karmaşıklığıdır [98].

DDoS algılama yaklaşımları Şekil 7.8'de gösterildiği gibi imza temelli, anormallik temelli ve karma olmak üzere üç sınıfta incelenir [32].



Şekil 7.8. DDoS algılama yaklaşımlarının sınıflandırılması

i. DDoS İmza Temelli Algılama

İmza temelli algılama teknikleri, veri tabanında saklanan, bir dizi kural ve bilinen saldırı imza kalıplarını kullanır. Ağ trafiği algılama sistemi tarafından izlenir ve kötü amaçlı trafiği saptamak için mevcut imza kalıpları ile karşılaştırılır. Bu teknikler kural temelli algılama olarak da isimlendirilir. İmza temelli yöntemlerin en önemli avantajları; bilinen saldırı tespitinde doğruluk oranının yüksek ve yanlış pozitif oranının düşük olmasıdır. Öte yandan bu yöntemler daha önceden sistem tarafından bilinmeyen saldırıları tespit edemez. DDoS saldırı kalıplarının varlığı, sistem yöneticisinin, hedef sistemin deneyimlediği DDoS saldırı türünün kesin belirlenmesine olanak tanır. Bu yöntemlerin ihtiyaç duyduğu imza veritabanını güncel tutmak zahmetli ve masraflı bir görevdir.

ii. DDoS Anormallik Temelli Algılama

Anormallik temelli DDoS saldırı trafiği algılama yaklaşımı, bir süre boyunca ağ/sistem trafik davranış modelinin izlenmesine veya öğrenilmesine dayanır. Bu sebeple davranışsal yaklaşım olarak ta tanımlanabilir. Bu yaklaşımda temel amaç; beklenen bir davranıştan sapmaların belirlenmesidir. Anormallik temelli çözümlerin bilinmeyen ve bilinen saldırı modellerinin türevlerine karşı etkili olduğu bilinmektedir. İmza temelli yaklaşımların bilinmeyen saldırılar için ihtiyaç duyduğu imza veritabanını güncel tutmak zahmetli olduğu için saldırı trafiğini ayırt etmek amacıyla verimliliği daha yüksek olan ve bilinmeyen saldırılar üzerinde de etkisi bulunan anormallik yaklaşımına ait yöntemler sıklıkla kullanılmaktadır.

Anormallik temelli yöntemler istatistik ve öğrenme temelli olmak üzere genel olarak iki kategoride incelenebilir. Öğrenme temelli modellerin çıkış noktası istatistiktir fakat bu modellerin optimizasyonu ve tahmin başarısı bilgisayar bilimleri ile ilerletilmiştir [55]. Genelde terminolojik farklar olmakla birlikte istatiksel yöntemlerle öğrenme temelli yöntemlerin birbirinden ayıran en önemli nokta istatiksel modellerin açıklanabilirliği, öğrenme temelli modellere göre daha fazladır [56]. **Öğrenme temelli yaklaşımlar**, büyük ölçekli uygulamalarda tercih edilir ve sisteme yeni gelen verinin tahmin yakınlığı ile ilgilenir. **İstatiksel yöntemlerde**; profillenen ağ trafiğindeki anormal davranış ancak anormal bir sapma değeri var ise göz önüne sunulur.

Öğrenme temelli yöntemler; normal trafik akışının ve/veya saldırı trafiğinin uygun algoritmalarla modellenip sisteme öğretilmesidir. Bu yöntemlerdeki öğrenme süreci danışmanlı ve danışmansız olmak üzere iki şekilde gerçekleşebilir. **Danışmanlı öğrenme** hem normal hem de anormallik sınıfları için etiketli örnek eğitim veri kümelerinin kullanılabilirliğini varsayar. Yaklaşım, normal ve anormallik sınıfları için tahmini bir model oluşturmak için kullanılır. Öğrenilen modeller, anormallik olan trafiği belirlemek için test edilecek trafikle karşılaştırılır. Yarı danışmanlı öğrenme, eğitim verisinde sadece normal sınıf için etiket örnekleri olduğunu varsayar. Anormal sınıf için etiket kullanımına gerek olmadığı için danışmanlı tekniklerle karşılaştırıldığında çok daha pratiktir [56]. Danışmansız öğrenme yaklaşımında model etiketlemeyi kullanmaz veya ihtiyaç duymaz.

DDoS saldırı trafiğini ayırt etmek için kullanılan yöntemler; imza temelli, anormallik temelli ve karma olmak üzere üç grupta sınıflandırılır. Bu üç sı-

nıfın ilki olan imza temelli algılamanın, bilinen saldırı imza tespitinde doğruluk oranı yüksek ve düşük yanlış pozitif oranına sahip olması avantajıdır. Fakat imza veritabanını güncel tutmak, zahmetli ve masraflı bir görevdir. Ayrıca imza örneğinin yanlış beyan edilmesi, yüksek yanlış negatif oranla sonuçlanır. Bilinmeyen ve sıfırıncı gün açıklıklarını tespit edememesi ise imza temelli algılamanın en önemli dezavantajıdır. Bilinmeyen saldırı ve sıfırıncı gün açıklıklarının tespiti için anormallik temelli yaklaşımlar geliştirilmiştir.

DDoS saldırı trafiği ayırt etme yöntemlerinin; verimlilik, işletim yükü ve ölçeklenebilirlik parametreleri ışığında değerlendirilmesi Tablo 7.2'de gösterildiği gibidir.

Tablo 7.2. DDoS savunma metotlarının karşılaştırılması

YAKLAŞIM		Verimlilik	İşletim Yükü	Ölçeklenebilirlik
İmza Tabanlı				+
Hibrid			+	
Anomali	İstatiksel			+
	Makine Öğrenmesi ve Veri Madenciliği	+	+	
	Yapay Zeka	+	+	

DDoS saldırı trafiği ayrımında kullanılan yöntemleri kıyaslarken, kullandığımız kıstaslardan biri olan *verimlilik*, sistemin verdiği kararlardaki doğruluk oranının yüksekliği ve hata oranın düşüklüğü ile ilişkilidir. Saldırı trafiği ayırt etme yöntemleri ve algoritmaları incelendiğinde anormallik temelli yöntemlerin bilinmeyen saldırı ayrımını yaparken verimliliği diğer yöntemlere kıyasla daha iyidir. İmza temellinin ise bilinen saldırı algılamada verimliliği anormallik temelli algılamaya göre daha yüksektir.

Anormallik tespiti için kullanılan istatistiksel yöntemler ve öğrenme temelli yöntemler mevcut teknikler, kullanılan algoritmaya bağlı olarak gruplanabilir ve bu yöntemlerin beraber kullanılması mümkün olabilmektedir.

– **İstatistiksel Yöntemler**; istatistiksel anormallik tespitinde, ağ trafiğinin belirli öznitelikleri, izlenen trafik profilinin/kalıbının oluşturulmasında ve bu profilden beklenmeyen aşırı değişimleri algı-

larken kullanılır. Algılama sırasında izlenen ağ trafiği, oluşturulan bu profil ile kıyaslanır. Literatürde yer alan istatiksel yöntemlerden bazıları; Gauss Modeli [99], Jensen-Shannon Ayrım Konsepti [100], Entropi Temelli Algılama [101], Kovaryans Matrisi ve Entropi, Korelasyon Özellikleri, Sürekli Zamanlı Bayes, Oyun Teorisidir [102].

- **Öğrenme Temelli Yöntemler**; veri madenciliği, büyük miktarda veriden bilginin çıkarılmasıdır [103]. Veri madenciliği, daha önce bilinmeyen, geçerli modelleri ve büyük veri setlerindeki ilişkileri keşfetmek için istatistiksel modelleri, matematiksel algoritmaları ve makine öğrenim yöntemlerini analiz aracı olarak kullanan disiplinlerarası bir alandır [103]. Makine öğrenmesi teknikleri ile karar destekleri sağlanabilir ve ağ saldırı tespit sistemi için kullanılacak otomatik kurallar oluşturulabilir. Makine öğrenmesinde sınıflandırma; etiketli veri örnekleri kullanılarak gerçekleştirilir Sınıflandırma algoritması; normal ağ trafiğini inceleyerek tanımlanmış sınıfları öğrenir. Daha sonra sınıfının belli olmadığı test verilerinde, veriyi öğrenilen sınıflardan biri ile eşleştirir. Veri kümesinde sınıfları belirten değerlere etiket adı verilir. Sınıflandırma işlemi iki aşamada gerçekleştirilir. İlk aşamada; bir eğitim veri kümesi kullanılarak istenilen sınıflar öğrenilir. İkinci aşamada ise öğrenilen sınıflar ile test verisi kıyaslanarak sınıflandırma yapılır. Veri kümeleri etiketlenerek, veri kümesi içerisindeki sınıflar sisteme tanıtılarak öğrenme gerçekleştiği için sınıflandırma denetimli öğrenme olarak da isimlendirilir. Makine öğrenmesinde kümeleme, sistemin saldırı trafiği ayrımı yaparken herhangi bir eğitim verisi kullanmadığı bir yöntemdir. Temel olarak, benzer özellikler gösteren verilerin gruplanmasına dayanır. Aynı kümede bulunan verilerin benzerlikleri fazladır. Farklı kümelerin birbirlerine benzerliği ise azdır. Kümeleme yapılırken sisteme yardımcı bilgi (etiket) verilmez. Bu sebeple kümeleme temelli yöntemleri denetimsiz öğrenme olarak da isimlendirilir.
- **Yapay zeka** çalışmalarının amacı, insan zekasını örnek alarak, insan zekası gerektiren görevleri yapabilecek makineler geliştirmek ve yapılması gereken tekrarlı işleri bilgisayar yardımı ile verimli bir şekilde yerine getirmektir [104]. Yapay zeka, karmaşık problemlere çözüm

bulmak ile ilgilenen yöntemler bütünü olarak tanımlanabilmektedir. Yapay zeka yaklaşımı; DDoS saldırı trafiği ayırt etme sırasında ağda yer alan yeni anormallikleri, etkili bir şekilde tespit etmek için sürekli bir öğrenme süreci gerektirir. DDoS saldırı trafiği ayırt etme çalışmalarında yapay zeka kullanımı [60-64], 2015 yılından bu yana devam etmektedir [105].

Anormallik temelli yaklaşımlar içerisinde de makine öğrenmesi ve yapay zeka yöntemlerinin ***verimliliği*** istatiksel yöntemlere göre daha iyidir. Bunun en önemli sebeplerinden biri makine öğrenmesi yaklaşımı eğitim verisi yardımı ile sistemi öğrenirken, istatiksel yaklaşım, profilini çıkardığı ağdaki ani değişimleri gözlemler. İstatiksel yaklaşımlarda, ağda meydana gelen yavaş değişimleri algılamak güçtür. Diğer taraftan; makine öğrenmesi yaklaşımında öğrenme sırasında aşırı uyarlama (overfitting) gerçekleşebilir, bu durumda sanal ayrıştıramama düzeyini olumsuz şekilde etkiler. Normal trafik verisine yetersiz erişim, eğitilen algoritmanın verimliliği üzerinde olumsuz etkilidir. ***İşletim yükü;*** uygulanan yöntemin sistemlere getirdiği ekstra işlem yüküdür. İşletim yükünün yüksek olması sistemin daha yavaş çalışmasına sebep olur. Gerçek zamanlı ve gerçek zamanlıya yakın algılama yapılmak istenen sistemlerde, sistemin yavaşlaması, algılama süresini negatif yönde etkiler. Makine öğrenmesi ve yapay zeka yaklaşımları; eğitim sırasında yüksek işlem kapasitesine ve zamana ihtiyaç duyarken, test aşamasında gerekli işlem kapasitesi, eğitim aşamasındaki gerekli işlem kapasitesinden daha düşüktür. Diğer yöntemlerle kıyaslandığında makine öğrenmesi ve yapay zeka temelli yöntemler istatistiksel ve imza temelli yöntemlere nazaran daha yavaştır. Bu yöntemlerin gerçek zamanlı algılama sistemlerinde kullanılabilmesi için yüksek kapasiteli sistemlere ihtiyaç vardır. İmza temelli yöntemlerde sistemlerde imza veritabanının büyümesi ile doğru orantılı olarak algılama süresi ve işlem yükü artar. İstatiksel yöntemlerde; ağ trafiği özniteliklerinin takibi yapılır ve sistem işletim yükü sabittir. ***Ölçeklenebilirlik***; veri boyutu artışına rağmen sistemin performansında ciddi kayıpların yaşanmaması olarak tanımlanabilir. İstatiksel yöntemler diğer yöntemlere kıyasla daha iyi ölçeklenebilir seviyeye sahiptir. İmza temelli yaklaşımlarda kullanılan veri tabanın boyutunun artması, algılama yapılacak veri hızının artmasına bağlı ölçeklendirme problemleri yaşanabilir. Yapay zeka ve makine öğrenmesi yaklaşımlarının ölçeklenme seviyeleri düşüktür.

iii. DDoS Karma Algılama

Karma temelli algılama yaklaşımı, imza temelli ve anormalliğe dayalı teknikleri beraber kullanır. Bu yaklaşım, daha yüksek algılama oranı elde etmek için her iki tekniğin tamamlayıcı özelliklerini birleştirir [31]. Karma yaklaşımda; hem imza hem de anormalliğin sunduğu avantajları sağlarken, verimli ve etkili bir şekilde birlikte çalışmak için farklı algoritmalar elde etmek masraflıdır ve karmaşıklığı fazladır.

Bilinen DDoS imzalarını tanımlamak için imza temelli sınıflandırma yaklaşımı kullanılır. Bu yaklaşım, bilinen DDoS saldırı düzenlerine karşı etkili bir çözüm olsa da, bilinmeyen DDoS saldırı imzalarını tespit edememesi nedeniyle bugün önemini giderek kaybetmektedir. Anormallik temelli çözümlerin sistem tarafından daha önce gözlemlenmemiş saldırı türlerine karşı etkili olduğu bilinmektedir [31]. Normal trafik davranışı, veri madenciliği, makine öğrenmesi, yapay zeka ve istatistiksel yöntemler gibi modelleme teknikleri kullanılarak, normal bir davranışsal profil elde etmek üzere modellenir. Bu modelleme, saldırı olmayan süre zarfında paket özelliklerinin çıkarılmasını ve normal davranışı profillemeyi içerir. Saldırı döneminde; gelen paket karakteristiklerindeki değişim incelenip DDoS saldırıları tespit edilir. Karma çözümler, imza ve anormallik temelli teknikleri birleştirerek bu yaklaşımların tamamlayıcı niteliklerinden yararlanmaya çalışmaktadır.

7.7.2.2. DDoS Müdahale

DDoS saldırısını önleme mekanizmalarının temel işlevi; kötücül yaklaşımları belirleme, bu yaklaşımların kaydını tutma, önleme/engelleme ve bu yaklaşımları güvenlik yöneticilerine raporlamadır. Saldırı önleme sistemleri; ağ trafiği hattına yerleştirilir. Kötü amaçlı paketler ile karşılaştığında alarm verir, kötü amaçlı paketleri iptal eder, bağlantıyı sıfırlar ve/veya rahatsız edici IP adresinden gelen trafiği engeller [6]. Saldırı önleme mekanizmaları filtre temelli mekanizmalardır.

Filtre temelli yaklaşımda ise paketler trafiğe girmeden önce bir dizi kurala göre oluşturulan filtrelere tabi tutulur. Filtreleme sonucunda paketlere ya geçmeleri için izin verilir ya da sisteme girmeden önce paketler engellenir. Düşman (hostile) paketlerin filtrelenmesi ve ortadan kaldırılması sistemin DDoS'tan zarar görmemesi için önemlidir. Filtreleme esas olarak bir paketin sisteme girmesine izin veren veya reddeden bir kuraldır [74]. Genellikle yönlendirici üzerine kuru-

lurlar. Bunun sebebi bir alan adı girmeden önce yönlendiriciler paketleri kontrol eder ya kabul eder ya da reddeder. Bu kural dizileri çok sayıda makinaya zarar vermeyi amaçlayan saldırıları engelledikleri için hayati önem taşır [107]. Filtreleme mekanizmalarını daha kapsamlı değerlendirebilmek için literatürde iki tip sınıflandırma mevcuttur. Bunlardan ilki işbirliği özelliklerine dayanmakta ikincisi ise tepki noktasına, (yanıt süresine) dayalı sınıflandırmadır. Alt başlıklarda bu iki tarz sınıflandırma incelenecektir.

Bazı durumlarda, makinelerin veya düğümlerin, filtre uygulaması ve seçimi ile ilgili karar vermek için işbirliği yapması gerekebilir [74]. Filtreleme mekanizmasının tek bir cihazda kurulu olması *bireysel filtreleme* adını alırken, ağda yer alan cihazlarda kurulu ve bu cihazların beraber işbirliği yapması *kooperatif filtreleme* adını alır.

- **Kooperatif filtreleme**, işbirliği yapılan makineler arasında savunma sırasında iletişim kuran ve filtreleme kararlarını veren filtreleme mekanizmasıdır. Bu sistemin etkin çalışabilmesi için tüm filtreleme aşamalarında iletişim kurması gerekir.
- **Bireysel filtreleme**, filtreleme mekanizması tek bir cihazda kurulur ve çalışır. Sistem kendi filtrelerini belirler ve oluşturur. İşbirliği yapmak, iletişim kurmak veya diğer cihazlara güvenmek zorunda olmadığı için kullanımı kolaydır. Saldırılara karşı tepki süresi, işbirliği nedeniyle ortaya çıkan gecikme ve iletişim masraflarından zarar görmediğinden daha kısadır.

Bir filtreleme savunma mekanizması; DDoS saldırısı başlamadan önce veya saldırı esnasında etkinleştirilebilir. DDoS savunmasında kullanılan filtreleme sistemleri zaman ekseninde proaktif ve reaktif filtreleme olarak iki sınıfta incelenebilir [74].

- **Proaktif filtreleme**, DDoS saldırısı başlamadan önce kullanılan, önleyici mekanizmadır. Bu sistemlerin, gelen kötü amaçlı paket tahmininde başarılı olması gerekir. Sürekli aktif olması gerektiği için savunma sisteminde ilave yüke neden olur.
- **Reaktif Filtreleme**, DDoS saldırısı başladıktan gerçekleştirilen filtreleme yöntemidir. Saldırının ilk tespiti ile reaktif sistem tetiklenir. Ardından, reaktif filtreleme işlemi devreye girer ve DDoS paketlerinin ağ boyunca yayılmasını engeller. Saldırı tespiti sonrası aktif olduğu için savunma sistemine ilave yük oluşturmaz.

Tablo 7.3. Filtreleme mekanizmaları [74].

FİLTRELEME YAKLAŞIMI	ÜSTÜNLÜKLER	DEZAVANTAJLAR
Bireysel + Proaktif	- Kolay dağılım - Hızlı müdahale	Sürekli aktif olduğu için ektra yük
Kooperatif + Proaktif	- Kolay dağılım - Hızlı müdahale - Kolay dağılım - Hızlı müdahale	- Senaryo zor - Saldırı daha gerçekleşmeden tüm katılımcılar işbirliğini kabul eder
Bireysel + Reaktif	- Kolay dağılım - Hızlı müdahale - Kolay dağılım	- Kısa süreli aktif olursa başarılı - Büyük ölçüde yetersiz
Kooperatif + Reaktif	İşbirlikçi	Saldırı gerçekleşince aktif

Filtreleme modellerinin her birinin kendine özgü pozitif ve negatif yanları bulunur. Ağ yöneticileri ihtiyaçları doğrultusunda en uygun modeli belirlemesi gerekir. Yukarıda verilen tanımlara dayanarak dört farklı filtreleme temelli savunma mekanizması vardır. Bunlar; bireysel+proaktif, kooperatif+proaktif, bireysel+reaktif ve kooperatif+reaktif yöntemlerdir [74]. Tablo 7.3, filtreleme mekanizmalarının avantaj ve dezavantajlarını detaylı olarak sunmaktadır.

7.8. SONUÇ VE DEĞERLENDİRMELER

Bu kitap bölümünde kapsamlı olarak ele alınan DDoS, öncelikle tanım ve tarihsel gelişim, kronolojik bakış, saldırıların ne zaman ve nasıl başladığından hangi amaçlar için kullanıldığına kadar saldırıların sebepleri, ayrıntıları nasıl yapıldığı ve bunların nasıl önlenebilceği ve müdahale edilebileceği irdelenmiş ve konu genel olarak değerlendirilmiştir.

DDoS saldırıları, bu saldırılarla mücadele ve alınması gerekli önlemler genel olarak değerlendirildiğinde;

- Literatürde DDoS başlığı ile ilgili kapsamlı çalışmalar yapıldığı, çalışmaların ve çalışma alanlarının gruplandırıldığı, saldırılarının çeşitlerine ve boyutlarına göre ayrıştırıldığı, verdiği zararların arttığı ve saldırı yüzeyinin büyüdüğü görülse de DDoS saldırılarının her geçen gün arttığı bundan sonra da bu saldırıların artarak devam edeceği görülmektedir.
- DDoS saldırılarına karşı koyma, tespit ve sistemleri savunma ve çalışır konumda tutma konusunda çalışmaların olduğu, savunmanın ger-

çekleştirildiği zamana ve konuma göre bunların çözülmeye çalışıldığı, algılama ve müdahale ile bunların durdurulmaya veya hizmetlerin sürdürülmeye çalışıldığı görülmektedir.

- Bu bölümde gözden geçirilen DDoS saldırıları bizlere bu saldırıların gün geçtikçe daha karmaşıklaştığını, saldırı boyutunun büyümekte olduğunu, şirket, kurum ve ülkelere büyük zararlar verdiklerini göstermektedir. Bundan sonra da bunun devam edeceği aşikar olup geleceğe hazırlık yapmak, yaşanmış olaylardan dersler almak veya çıkarmak, bu saldırılara karşı dayanıklılığı artırmak için kapasite, yetenek ve altyapıları güçlendirmek, önceden senaryolar geliştirip sistemleri test etmek ve tatbikatlar yapmak ve hizmet sürekliliğini sağlamak gereklidir.
- Saldırılara karşı koymada yetişmiş insan gücü ve bilgi birikimi çok önemlidir. Yapılan çalışmalara bakıldığında, ülkemizde bu konudaki çalışmaların yetersiz olduğu, ülkemizde bu konuda eğitim-öğretim faaliyetleri yürüten üniversitelerimizde konunun kapsamlı olarak çalışılması gerekmektedir. Bu konuda inovatif çözümler geliştirilmeli, teknolojiler üretilmeli, bilgi birikimini artırıcı tezler yapılmalıdır. Bunların yapılabilmesi içinde, açık kaynak veriler araştırmacılara sunulmalı ve gerçek veriler ile çalışmalar yapılmalıdır.
- DoS/DDoS saldırılarından korunmak, sistemleri savunmak ve saldırılara karşı dayanıklılığı arttırmak için izleme ve iyileştirme faaliyetlerine ağırlık verilmelidir. Kurumlar, eğitim faaliyetlerine önem vermeli ve bunun sürekli olmasına dikkat etmelidirler. Bunun için politikalar üretilmeli ve uygulanmalı, DDoS saldırılarına dayanıklı sistemler geliştirilmeli ve kurulan sistemler hizmete alınmadan önce mutlaka test edilmelidir.
- Yapılan çalışmalarda gerçekçi sonuçlar elde edebilmek için DoS/DDoS gibi yıkıcı saldırıların önceden test edilmesi, büyük ölçekli test yatakları kurulmalı ve bunlar araştırmacıların erişimine sunulmalıdır.
- Test amaçlı olarak kullanılan benchmark veri setleri detaylı incelenmeli, bu veri setlerinin günümüz operasyonel ağlarındaki trafiği ne derece temsil ettiği incelenmeli ve geliştirilen modellerin gerçek saldırılara karşı ne kadar etkili olabileceği kapsamlı olarak değerlendirilmelidir.

– Özellikle yıkıcı etkileri olan DDoS saldırıları gibi uygulaması her zaman mümkün olmayan saldırılara dair verilerin araştırmacılar ile paylaşıldığı ulusal veri merkezleri kurulmalı ve araştırmacılara açılmalıdır.
– Son kullanıcı ve sistem mahremiyeti göz önünde tutularak, DDoS çalışmalarında kullanılmak üzere operasyonel ağlardan anonimleştirilmiş veriler toplanmalı, toplanan veriler ulusal veri merkezleri üzerinden araştırmacıların erişimine sunulmalıdır. Ülkemizde de DDoS üzerine raporlar hazırlandığı ve yayımlandığı [98] görülse de bu ve buna benzer çalışmaların hem sayısının hem de niteliğinin geliştirilmesi gereklidir.

KAYNAKLAR

[1]. G. Canbek, Ş. Şağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi 9 (165-174), 2006

[2]. A. Srivastava, B.B. Gupta, A. Tyagi, Sharma A, Anupama Mishra A, "A Recent Survey on DDoS Attacks and Defense Mechanisms", ACM Computing Surveys 2009.

[3]. (Online) Available: "Anomaly detection" Cisco Systems http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.html

[4]. K. Kalkan, G.Gür, F. Alagöz, " Filtering-Based Defense Mechanisms Against DDoS Attacks: A Survey" IEEE Systems Journal, (Volume: PP, Issue: 9) 2016.

[5]. N. Hoque , H. Monowar, Bhuyan, R.C.Baishya, Bhattacharyya D.K., Kalita J.K. "Review Network attacks:Taxonomy,tools and systems" Journal of Network and Computer Applications 40 (2014) 307–324

[6]. (Online) Available: "Denial of Service Attacks", CERT, http://www.cert.org/tech_tips/denial_of_service.html, (Erişim Tarihi: Ağustos 2017)

[7]. S. Atasever, İ. Özçelik, Ş. Sağıroğlu, (2019). "Siber Terör ve DDoS" Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23 (1), 238-244 . DOI: 10.19113/sdufenbed.507948.

[8]. (Online) Available: "On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus." http://www.findingdulcinea.com/news/on-this-day/July-August-08/On-this-Day--Robert-Morris-Becomes-First-Hacker-Prosecuted-For-Spreading-Virus.html

[9]. (Online) Available: "A Brief History Of Ddos Attacks." https://eugene.kaspersky.com/2016/12/06/a-brief-history-of-ddos-attacks/.

[10]. E. Luiijf, "Definitions of Cyber Terrorism, Cyber Crime and Cyber Terrorism Investigator's Handbook", Chapter 2, Syngress, 2014, Pages 11-17.

[11]. Ş.,Sağıroğlu, "Dünyada ve Ülkemizde Siber Terör ve Güvenlik," presented at the TÜBAV Konferansları, Ankara, 2017.

[12]. P. Olson, 2012, "We Are Anonymous – Inside the Hacker World of LulzSec, Anonymous, And the Global Cyber Insurgency", Little Brown, pp. 423

[13]. (Online) Available: IEEE Spectrum: Technology, Engineering, and Science News. (2018). Unmasking the "Anonymous" Hackers. [online] Available at: https://spectrum.ieee.org/tech-talk/telecom/security/unmasking-the-anonymous-hackers

[14]. (Online) Available: "Ddos Nedir? - Shiftdelete.Net". Teknoloji Haberleri - Shiftdelete.Net. https://shiftdelete.net/ddos-nedir?

[15]. (Online) Available: "CIA DDoS attack" https://www.washingtonpost.com/national/national-security/ciaweb-site hacked/2011/06/15/AGGNphWH_story.html?noredirect=on&utm_term=.3a9a44174b32.

[16]. (Online) Available: "DDoS Nedir?," http://www.next.web.tr/konu/ddos-nedir.11171/

[17]. (Online) Available: "Estonya Siber Saldırısı" https://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf.

[18]. "Arbournet Security Report," 2019, (Online) Available: https://www.netscout.com/asert

[19]. "Counterterrorism And Cybersecurity." 2015. Cham: Springer International Publishing.

[20]. (Online) Available: "İsveç DDoS", https://siberbulten.com/siber-saldirilar-2/ddos-aldirilari-isvecte-trafigini-etkiledi/

[21]. (Online) Available: "Türk Telekom DDoS Saldırısı" https://www.hurriyet.com.tr/teknoloji/turkiyeye-siber-saldiri-soku-turk-telekomdan-flas-aciklama-geldi-41360791

[22]. (Online) Available: "EBA Siber Saldırısı" https://www.webtekno.com/meb-eba-siber-saldiri-h99785.html#

[23]. A. Srivastava, B.B. Gupta, A. Tyagi, A. Sharma, A. Mishra A, "A Recent Survey on DDoS Attacks and Defense Mechanisms", ACM Computing Surveys (2009).

[24]. N. Hoque, H. Monowar. B., Baishya R.C., D.K. Bhattacharyya, J.K. Kalita "Review Network attacks:Taxonomy,tools and systems" Journal of Network and Computer Applications 40 (2014) 307–324.

[25]. (Online) Available: "CERT, Denial of Service Attacks," http://www.cert.org/tech_tips/denial_of_service.html,

[26]. A. Mitrokotsa , C. Douligeris, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Computer Networks, 44 (2004) 643–666.

[27]. D.Karig, R, Lee, "Remote denial of service attacks and countermeasures," Dept. of Electrical Eng., Princeton University, Tech. Rep., 2001.

[28]. J.K. Kalita, 2016 "DDoS Attacks - Evolution, Detection, Prevention, Reaction, And Tolerance."

[29]. İ. Özcelik,Y. Fu, R. Brooks, "DoS Detection is Easier Now", 2013 Second GENI Research and Educational Experiment Workshop.

[30]. İ.Özçelik, "DoS Attack Detection and Mitigation" 2015, (Doctor of Philosophy's Thesis)

[31]. Z, Kim, K. Zetter, B. Barrett, E. Dreyfuss, L. Newman, WIRED Staff, Issie Lapowsky, and Emily Dreyfuss. 2018. "A Cyberattack Has Caused Confirmed Physical Damage For The Second Time Ever". WIRED. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

[32]. (Online) Available: https://siberbulten.com/siber-saldirilar-2/ddos-aldirilari-isvecte-trafigini-etkiledi/https://blog.cyberage.com.tr/2017/02/03/siber-saldirilar-fiziksel-dunyamizi-etkileyebilir-mi/

[33]. A., Basheer, G. Manimaran. 2006. "Distributed Packet Pairing For Reflector Based Ddos Attack Mitigation". Computer Communications 29 (12): 2269-2280.

[34]. C.,Rossow . (2014). "Amplification Hell: Revisiting Network Protocols for DDoS Abuse." 10.14722/ndss.2014

[35]. (Online) Available: https://security.radware.com/ddos-knowledge-center/ddospedia/fraggle-attack/

[36]. (Online) Available: https://www.incapsula.com/ddos/attack-glossary/dns-amplification.html

[37]. (Online) Available: https://www.corero.com/resource-hub/ntp-amplification/

[38]. Arbor Sert, " DDoS and Security Reports: The Arbor Networks Security Blog," 2011. Available at: http://ddos.arbornetworks.com/2012/02/ddos-tools/.

[39]. (Online) Available: "http Flood" https://www.imperva.com/learn/ddos/http-flood/?redirect=Incapsula

[40]. https://resources.infosecinstitute.com/topic/dos-attacks-free-dos-attacking-tools/#gref (Erişim Tarihi : Şubat 2021)

[41]. C, Paul. (2000). "Distributed Denial of Service: Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht" CIAC-2319. 19.

[42]. (Online) Available: https://www.usenix.org/legacy/publications/library/proceedings/sec2000/invitedtalks/dittrich_html/timeline.html

[43]. İ. Özçelik, R. Brooks "Distributed Denial of Service Attacks Real-world Detection and Mitigation"

[44]. B,,Hancock "Trinity v3, a DDoS tool, hits the streets," Computers & Security, vol. 19, pp. 574-574, 2000..

[45]. N.L Sven Dietrich, D. Dittrich, "Analyzing Distributed Denial Of Service Tools: The Shaft Case," in Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, Louisiana, USA, December 3– 8, 2000, p. 12.

[46]. Bysin, ―knight.c sourcecode," 2001. Available at: http://packetstormsecurity.org/distributed/ knight.c.

[47]. D. McPherson, ―Worldwide Infrastructure Security Report," Arbor Networks, January 19th, 2010, avilable at: http://ipv6.org.sa/sites/default/files/World_ Infrastructure _Security_Report_ 2011.pdf.

[48]. J. Nazario,, ―BlackEnergy DDoS Bot Analysis,‖ Arbor Networks, 2007. Available at: http://atlaspublic.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Ana lysis.pdf.

[49]. N, Tom (March 3, 2012). "Low Orbit Ion Cannon: Exposed". The Powerbase. Archived from the original on March 6, 2012. Retrieved March 4, 2012.

[50]. S., Pratima. (2015). "DDoS Tools: Classification, Analysis and Comparison".

[51]. M., Asher (December 9, 2010). "The Aussie who blitzed Visa, MasterCard and PayPal with the Low Orbit Ion Cannon". The Age. Melbourne.

[52]. (Online) Available: https://www.zdnet.com/article/wikileaks-has-been-under-ddos-attack-for-the-last-five-days/

[53]. (Online) Available: https://www.imperva.com/learn/ddos/rudy-r-u-dead-yet/

[54]. (Online) Available: https://github.com/nosperantos/RUDY

[55]. E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah and R. Alfaris, Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art International Journal of Computer Applications, vol. 49, no. 7, pp. 24-32, Jul. 2012.

[56]. (Online) Available: https://github.com/OffensivePython/Saddam

[57]. (Online) Available: https://www.knownhost.com/wiki/developmental/memcrashed-what-is-it-memcache

[58]. (Online) Akamai, "Memcached Reflection Attacks: A New Era For DDoS", https://www.akamai.com, 2017

[59]. S.T. Zargar, J. Joshi, D. Tipper, (2013). "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials, 15(4), 2046-2069.

[60]. S. Behal, K. Kumar, M. Sachdeva, "D-FAC: A novel ϕ-Divergence based distributed DDoS defense system,Journal of King Saud University" - Computer and Information Sciences, 2018.

[61]. T Vissers, T.S. Somasundaram, L.Pieters, K. Govindarajan, P. Hellinckx "DDoS defense system for web services in a cloud environment." Future Generation Computer System 37 (2014) 37–45.

[62]. A. Mitrokotsa, C. Douligeris, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Computer. Network, 44 (2004) 643– 666.

[63]. M. Zakarya, "DDoS verification and attack packet dropping algorithm in cloud computing." World Application Science Jorunal (11) 2013 18–24.

[64]. J. Mirkovic, P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," SIGCOMM Computer Communication 34 (2004) 39–53.

[65]. Q.Yan,, F.R. Yu, Q. Gong, Q., &J. Li, (2015). "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey," some research issues, and challenges. IEEE communications surveys & tutorials, 18(1), 602-622.

[66]. O.Osanaiye,, K. Choo,, & M. Dlodlo, (2016)." Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework." Journal of Network and Computer Applications, 67, 147-165.

[67]. A. Khraisat., I. Gondal,, P. Vamplew,., & J. Kamruzzaman, (2019). "Survey of intrusion detection systems: techniques, datasets and challenges". Cybersecurity, 2(1), 1-22.

[68]. B.B. Gupta, . O. P. Badve, (2017). "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment." Neural Computing and Applications, 28(12), 3655-3682.

[69]. T. Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), 1550147717741463.

[70]. R.Sahay,, G.Blanc, Z., Zhang, ., & H. Debar, (2015, February). Towards autonomic DDoS mitigation using software defined networking. In SENT 2015: NDSS workshop on security of emerging networking technologies. Internet society.

[71]. P. Kamboj,, M. Trivedi, M. C., Yadav, V. K., & Singh, V. K. (2017, October). "Detection techniques of DDoS attacks: A survey". In 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON) (pp. 675-679). IEEE.

[72]. K.M. Prasad, A.R.M. Reddy, K.V. Rao, (2014). "DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey." Global Journal of Computer Science and Technology.

[73]. R, Vishwakarma, A.K. Jain, (2020). "A survey of DDoS attacking techniques and defence mechanisms in the IoT network." Telecommunication systems, 73(1), 3-25.

[74]. K, Kalkan, G. Gür, Ş. Şentürk, Dağıtık Servis Dışı Bırakma Saldırılarına Karşı Filtreleme Tabanlı Savunma Mekanizmaları",18. Akademik Bilisim Konferansı, 2016.

[75]. P. Du, A. Nakao, (2010, May). "DDoS defense deployment with network egress and ingress filtering." In 2010 IEEE international conference on communications (pp. 1-6). IEEE.

[76]. J. Mirković, (2003). "D-WARD: DDoS network attack recognition and defence "(Doctoral dissertation, Ph. D. thesis, Computer Science Department, University of California, Los Angeles).

[77]. T. Gil, M. Poletto, (2001, August). "MULTOPS: A Data-Structure for Bandwidth Attack Detection". In USENIX security symposium (pp. 23-38).

[78]. S. Dorbala, Y., Kishore, R., & N. Hubballi, (2015, June). "An experience report on scalable implementation of ddos attack detection." In International Conference on Advanced Information Systems Engineering (pp. 518-529). Springer, Cham.

[79]. (Online) Cs3, Inc. MANAnet DDoS White Papers. Available: http://www.cs3-inc.com/mananet.html.

[80]. M.Sung J. Xu (2003). "IP traceback-based intelligent packet filtering: A novel technique for defending against Internet DDoS attacks". IEEE Transactions on parallel and Distributed Systems, 14(9), 861-872.

[81]. J.,Yu, H., Lee, H., Kim, M. S., Park, D. (2008)." Traffic flooding attack detection with SNMP MIB using SVM." Computer Communications, 31(17), 4212-4219.

[82]. M. Choo C., Wing C. Lau, Y. Kim and H. J. Chao, "Transient performance of PacketScore for blocking DDoS attacks," 2004 IEEE International Conference on Communications, 2004, pp. 1892-1896 Vol.4, doi: 10.1109/ICC.2004.1312849.

[83]. T. Peng, C. Leckie, and K. Ramamohanarao, Protection from distributed denial of service attacks using history-based IP filtering, ICC '03. May, Vol.1, pp: 482- 486, 2003.

[84]. K., Yoohwan L., Wing & Chuah, Mooi Choo. (2006). "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks." Dependable and Secure Computing, IEEE Transactions on. 3. 141-155. 10.1109/TDSC.2006.25.

[85]. W.Haining J.Cheng. (2007). "Defense Against Spoofed IP Traffic Using Hop-Count Filtering". Networking, IEEE/ACM Transactions on. 15. 40 - 53. 10.1109/TNET.2006.890133.

[86]. Y. Kim, W. Cheong Lau, M. Choo Chuah,H. J. Chao, "Packetscore: statistics-based overload control against distributed denial-of-service attacks," IEEE INFOCOM 2004, 2004, pp. 2594-2604 vol.4, doi: 10.1109/INFCOM.2004.1354679.

[87]. M. Abliz, "Internet Denial of Service Attacks and Defense Mechanisms", University of Pittsburgh, Department of Computer Science, Technical Report. TR-11-178, March 2011.

[88]. K. Park, H. Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets", in Proc. ACM SIGCOMM, August 2001.

[89]. K. A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, R. A. Olsson, "Detecting Disruptive Routers: A Distributed Network Monitoring Approach", in Proc. 1998 IEEE Symposium on Security and Privacy, May 1998.

[90]. M. R. Sharma, J. W. Byers, "Scalable Coordination Techniques for Distributed Network Monitoing", in Proc. PAM, pp. 349-352, 2005.

[91]. R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, S. Shenker, "Controlling high bandwidth aggregates in the network", presented at Computer Communication Review, pp.62-73, 2002

[92]. K. Kumar, A.L., Sangal, A., Bhandari (2011). "Traceback techniques against DDOS attacks: A comprehensive review". 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011), 491-498.

[93]. D. Yau, J. C. S. Lui, F. Liang, Defending against distributed denial of service attacks using max-min fair server centric router throttles, IEEE international conference on Quality of Service. 2002.

[94]. R. Chen, J. M. Park, "Attack Diagnosis: Throttling distributed denial-of-service attacks close to the attack sources", IEEE Int'l Conference on Computer Communications and Networks (ICCCN'05), Oct. 2005.

[95]. R. Chen, J. M. Park, R. Marchany, "TRACK: A novel approach for defending against distributed denial-of-service attacks", Technical Report TR-ECE-06-02, Dept. of Electrical and Computer Engineering, Virginia Tech, Feb. 2006.

[96]. X. Liu, X. Yang, Y. Lu, "To filter or to authorize: network-layer DoS defense against multimillion-node botnets," in Proc. ACM SIGCOMM conference on Data communication (SIGCOMM '08), NY, USA, pp. 195-206, 2008

[97]. C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, R. Govindan, "Cossack: Coordinated Suppression of Simultaneous Attacks", in Proc. DARPA Information Survivability Conference and Exposition, Vol. 1, pp. 2 13, Apr. 2003.

[98]. (Online), https://www.barikat.com.tr/docs/LoDDoS_ddos_degerlendirme_raporu.pdf

[99]. D. Erhan, E. Anarım, (2020, October)." Istatistiksel Yöntemler ile DDoS Saldırı Tespiti DDoS Detection Using Statistical Methods." In 2020 28th Signal Processing and Communications Applications Conference (SIU) (pp. 1-4). IEEE.

[100]. P, Shamsolmoali, M. Zareapoor, (2014, September). "Statistical-based filtering system against DDOS attacks in cloud computing." In 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1234-1239). IEEE.

[101]. İ,Özçelik, R.R. Brooks, (2015). "Deceiving entropy based DoS detection." Computers & Security, 48, 234-245.

[102]. H. Bedi, S., Roy, S., S. Shiva, (2011, April). "Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows." In 2011 IEEE symposium on computational intelligence in cyber security (CICS) (pp. 129-136). IEEE.

[103]. H. Jiawei, J. Micheline Kr, "In The Morgan Kaufmann Series in Data Management Systems, Data Mining (Third Edition)," Morgan Kaufmann,2012, Pages 1-38, ISBN 9780123814791, https://doi.org/10.1016/B978-0-12-381479-1.00001-0.

[104]. O. Torkul, S. Gülseçen,, G. Çağıl,, M.K. Uçar, M. İnal, M., Erol, Ç., Selvi, İ. H. "Mühendislikte yapay zeka ve uygulamaları", 2020.

[105]. B. Zhang, T. Zhang, Z. Yu, "DDoS detection and prevention based on artificial intelligence techniques," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, pp. 1276-1280, doi: 10.1109/CompComm.2017.8322748.

Bölüm 8

AĞ VERİ KATMANI PROGRAMLAMA VE SİBER GÜVENLİK

Özgür Yürekten

Bu bölümünde; ağ yazılımlaştırma yaklaşımını oluşturan yazılım tanımlı ağlar ve ağ fonksiyonu sanallaştırma teknolojileri, OpenFlow protokolünün programlama için sunduğu özellikler, veri katmanının programlanabilmesi için kullanılan P4 programlama dilinin kabiliyetleri, P4 programlama dili özelliklerinin siber güvenliğe sağladığı katkılar özetlenmektedir. Sonrasında da veri katmanı programlama ile geliştirilebilen siber güvenlik çözümleri ve açıklanarak bu alanda yapılabilecek çalışmalar değerlendirilmiştir.

8.1. GİRİŞ

Her geçen gün yeni teknolojilerin hayatımıza girmesi ve günlük alışkanlıklarımızın bu teknolojilere bağlı olacak şekilde değişmesi, bilişim altyapılarındaki ihtiyaçları da sürekli değiştirmektedir. İnternete bağlı cihaz sayısı ve İnternet kullanımı her geçen gün artış gösterirken nesnelerin interneti, bulut bilişim, otonom sistemler, büyük veri ve veri analizi teknolojileri ile geliştirilen yeni uygulamalar ve ürünler, hayatımızı kolaylaştırırken aynı zamanda kullandıkları ağ altyapıları üzerindeki yükü de artırmaktadır. Bu alanlardaki İnternet kullanım artış oranları öngörülebilmesine rağmen dünya genelinde yaşanan COVID-19 pandemi sürecinde bilişim teknolojilerine olan bağımlılığı beklenmedik sürede çok fazla artırmıştır. Bu süreçte toplumlar fiziksel

olarak yakın olmadan fakat günlük çalışmalarını devam ettirmek için uzaktan çalışma kültürüne kısa sürede adapte olmuştur. Eğitim sektörü, hizmet sektörü, kamu hizmetleri İnternet üzerinden sunulan servislerle bağımlı hale gelmiştir. 2020 yılının başlarında İnternet trafiğinin %30 arttığı raporlanmıştır [1]. Yeni teknolojiler ve bilişim teknolojileri ile sunulan hizmetler; yüksek bant genişliğine sahip, hızlı, güvenli ve ölçeklenebilir ağ altyapılarına ihtiyaç duymaktadır. Klasik ağ mimarileri gelişen bu ihtiyaçların karşılanmasında yetersiz kaldığı için son dönemde ağ teknolojilerinde yeni yaklaşımlarla yoğun çalışmalar yürütülmekte ve bu yaklaşımları kullanan teknolojiler hızla hayata geçirilmektedir. Bu yaklaşımların başında ağ yazılımlaştırma gelmektedir. Ağ yazılımlaştırma kapsamda da yazılım tanımlı ağlar (Software Defined Networking - SDN) ve ağ fonksiyonu sanallaştırma (Virtual Network Functioning - VNF) teknolojileri ön plana çıkmaktadır.

Ağ yazılımlaştırma teknolojileri, klasik ağ teknolojileri ile çözülmesi zor olan siber güvenlik problemlerinin daha kolay üstesinden gelinebilmesine yönelik kabiliyetler ve fonksiyonlar sunmaktadır. Siber güvenliğin artırılması için en temelde yüksek hız ve bant genişliği sunan dinamik güvenlik fonksiyonlarına ihtiyaç duyulmaktadır. Bu ihtiyaçların karşılanması için ağ yazılımlaştırma yaklaşımında P4 [2] gibi alan özel programlama dilleri ile ağ cihazları programlanmakta ve ağ cihazlarının donanımla sundukları hızlardan faydalanılabilmektedir. Bu kitap bölümünün ikinci kısmında ağ yazılımlaştırma ve teknolojileri hakkında özet bilgi sunulmaktadır. Üçüncü kısımda, ağ yazılımlaştırma için kullanılan OpenFlow protokolü ve P4 programlama dilinin kabiliyetleri anlatılmaktadır. Dördüncü kısımda ise veri katmanı programlama ile geliştirilebilecek siber güvenlik fonksiyonları ve bu alanda sunulan çözümler paylaşılmaktadır. Son kısımda bölüm özeti, veri katmanı programlama alanındaki araştırma konularına ve önerilerine yer verilmektedir.

8.2. AĞ YAZILIMLAŞTIRMA TEKNOLOJİLERİ

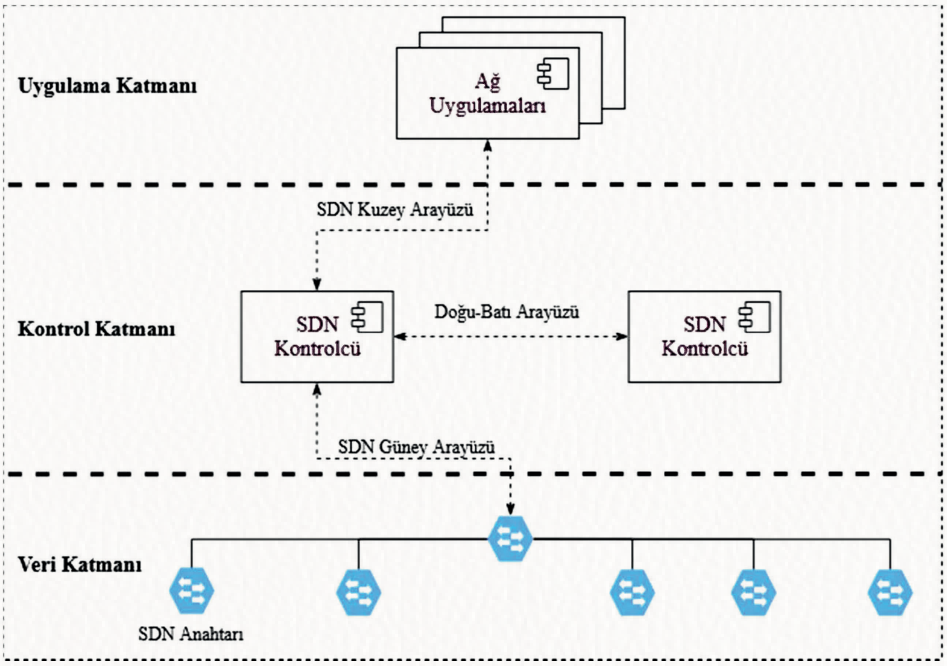
Ağ yazılımlaştırma; ağ fonksiyonlarının, protokollerinin ve servislerinin üzerlerinde çalıştıkları donanımlardan ayrılmasını sağlayan mimariler olarak tanımlanabilir [3]. Ağ yazılımlaştırma için iki mimari öne çıkmaktadır. İlk mimari, klasik ağlarda veri ve kontrol katmanlarının ayrılmasını sağlayan yazılım tanımlı ağ mimarisi, diğeri de ağ fonksiyonlarının donanıma bağımlı olmadan dinamik olarak yönetilebilmesini sağlayan ağ fonksiyonu sanallaştırma mimarisidir.

8.2.1. Yazılım Tanımlı Ağlar

Klasik ağlarda her bir ağ cihazının yapılandırması ve yönetimi, o cihazın üreticisinin sunduğu arayüzlere ve kabiliyetlere bağlıdır. Klasik ağlarda ağ kontrol katmanı ile veri yönlendirme katmanı bütünleşik olarak ağ cihazlarında yer almaktadır. Bu durum da ağ cihazlarının merkezi olarak yönetilebilmesini, ağ fonksiyonlarının dinamik olarak ölçeklendirilebilmesini ve cihazlar üzerinde kolay bakım yapılabilmesini zorlaştırmaktadır. Ağ yönetiminin donanımlardan bağımsız olarak gerçekleştirilebilmesini sağlayan ağ yazılımlaştırma yaklaşımının uygulanabilmesini sağlayan mimarilerin başında yazılım tanımlı ağlar (Software Defined Networking – SDN) gelmektedir. SDN, kontrol katmanını veri yönlendirme katmanından ayırarak ağlarının daha esnek yönetimini sağlayan bir ağ mimarisidir. SDN; ağlar üzerinde mantıksal olarak merkezi yönetim ve programlanabilir arayüzler sunar, ağ anahtarları yönetimi için yeni protokollerinin geliştirilebilmesini sağlar, mantıksal sanal ağların tanımlanabilmesini ve ağın merkezi olarak izlenebilmesini kolaylaştırır [4]. Bu özelliklerinden faydalanmak için SDN veri merkezlerinde, omurga ağlarında, kurumsal ağlarda ve kablosuz ağlarda yaygın olarak kullanılmaktadır [5].

SDN mimarisi, Şekil 8.1'de gösterildiği gibi üç katmandan ve katmanlar arası iletişim arayüzlerinden oluşmaktadır [6]. Veri katmanında yer alan anahtarlar gelen paketleri sadece programlanabilir akış tablolarına göre yönlendirmektedir. Bu tablolar da, kontrol katmanında yer alan SDN kontrolcüleri tarafından güncellenebilmektedir. Gelen paketler akış tabloları ile eşleşmemesi durumunda paketler karar için SDN kontrolcüsüne gönderilebilmektedir. SDN kontrolcü ile veri katmanında yer alan anahtarlar, SDN güney arayüzü ile eş zamanlı ve eş zamanlı olmayan mesajlar kullanarak haberleşmektedir. SDN ürünlerinde güney arayüzü olarak çoğunlukla endüstri standardı olan OpenFlow [7] protokolü kullanılmaktadır. Bir anahtar aynı anda sadece bir SDN kontrolcü tarafından yönetilebilmektedir. SDN kontrolcülerinin ölçeklenebilirliğini sağlamak için SDN ağlarında birden fazla kontrolcünün konumlandırılabilmesi mümkündür. SDN kontrolcülerinin birbirleri arasındaki koordinasyon doğu-batı arayüzleri kullanılarak gerçekleştirilir. SDN mimarisindeki uygulama katmanında farklı amaçlar için (güvenlik fonksiyonları, ağ erişim yönetimi, vb.) geliştirilmiş uygulamalar yer alabilmektedir. Bu uygulamalar, SDN kontrolcünün sunduğu ve

SDN kontrolcüsüne özel kuzey arayüzleri ile ağ katmanını yönetebilmekte ve izleyebilmektedir.



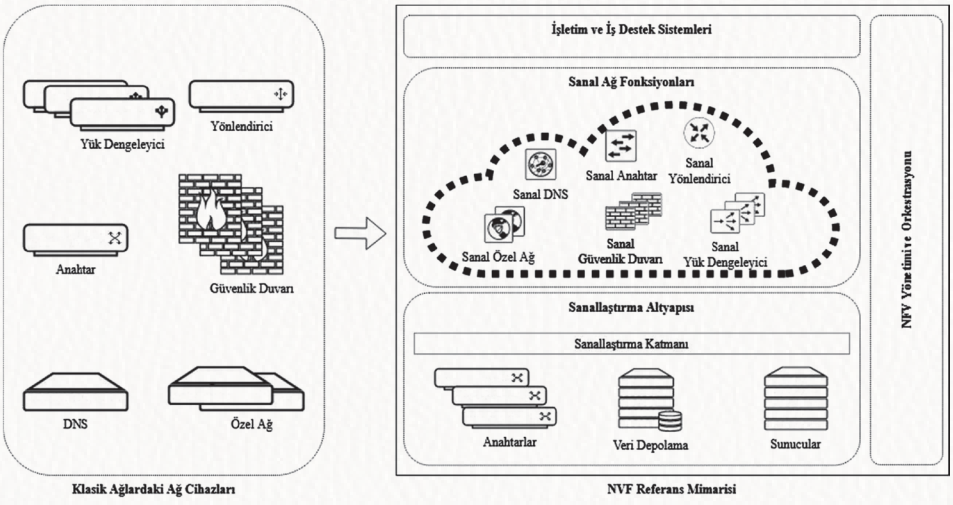
Şekil 8.1. Yazılım tanımlı ağ mimarisi

SDN mimarisi kullanılarak oluşturulan ağlarda ağ cihazlarının yönetimi ve geliştirilen üçüncü parti yazılımlarla ağ trafiğinin yönetimi merkezi olarak gerçekleştirilebilmektedir. Bu kapsamda ağ güvenliğinin artırılabilmesi için SDN mimarisini kullanan güvenlik fonksiyonları ve çözümleri geliştirilebilmektedir. SDN mimarisinden faydalanılarak güvenlik duvarı, saldırı tespit sistemi gibi klasik güvenlik fonksiyonlarının yanında DDoS, tarama, dinleme, IP sahteciliği, web uygulama saldırıları ile zararlı yazılımların önlenmesine yönelik çözümler de geliştirilebilmektedir [8]. Bütün bu çözümlerin geliştirilmesinde SDN mimarisinin tüm katmanlarında bulunan bileşenlerden faydalanılması gerekmektedir. Özellikle performansı etkilemeden yüksek hızlı ağ trafiği üzerinde işlemlerin yapılabilmesi için veri katmanında bulunan anahtarların kabiliyetlerine üst seviyede ihtiyaç duyulmaktadır. Bu da SDN mimarisinde yer alan anahtarların da programlanabilir olması ile sağlanmaktadır.

8.2.2. Ağ Fonksiyonu Sanallaştırma

Ağ sanallaştırmanın tam olarak uygulanabilmesi için ikinci bir gereksinim de ağ üzerinde konumlandırılmış cihazlarının üzerinde çalıştıkları donanımlardan bağımsız hale getirilmesidir. Ağ fonksiyonu sanallaştırma (Network Function Virtualization - NFV) mimarisi uygulanarak donanıma bağımlı ağ cihazlarının ve fonksiyonlarının standart bilgi teknolojileri sanallaştırma altyapılarının içine taşınması ve bunların sanallaştırma ortamlarından yönetilmesi sağlanabilmektedir [9]. Şekil 8.2'de klasik ağlardaki ağ cihazlarının referans NFV mimarisine uygun taşınması gösterilmektedir.

Klasik ağlarda güvenlik duvarı, yük dengeleyici, anahtar, yönlendirici, özel ağ, saldırı tespit sistemi gibi çeşitli cihazlar yer almaktadır Eşdeğer sanal fonksiyonu bulunmayan cihazların fonksiyonlarının sanal ortamlara taşınması aşamasında üretici firmaların sundukları ürünler veya ağ fonksiyonlarını yerine getiren alternatifler kullanılmaktadır. Bazı durumlarda da mevcut cihazlar işletim sistemi seviyesinde sanallaştırılarak NFV mimarisine dâhil edilmektedir. Ağ cihazlarının her biri sanallaştırıldıktan veya eşdeğer sanal ürünler seçildikten sonra sanallaştırılmış ağ ortamında NFV yönetim ve orkestrasyonu kullanılarak yapılandırılmaktadır.



Şekil 8.2. Ağ fonksiyonlarının NFV referans mimarisine uygun sanallaştırılması [10]

NFV mimarisi 4 ana bileşenden oluşmaktadır. Bu bileşenlerden ilki sanallaştırma altyapısıdır. Bu altyapı, yönettiği donanım kaynaklarını ve sanallaştırma altyapısını kullanarak NFV mimarisine sanal hesaplama, depolama ve ağ yönetimi kabiliyetleri kazandırmaktadır. NFV mimarisinde yer alan sanal ağ fonksiyonları bileşeni de sanal kaynakları kullanarak sanal ortamlarda çalışan sunuculardan oluşmaktadır. NFV mimarisindeki üçüncü önemli bileşen olan NFV yönetim ve orkestrasyon bileşeni, NFV mimarisinde tüm altyapının ve NFV ile sunulan fonksiyonların merkezi koordinasyonunu sağlamaktadır. Ağ yapılandırma, hata yönetimi, envanter yönetimi, talep yönetimi gibi kurumsal ve operasyonel hizmetleri sunmak için geliştirilen ve NFV mimarisinde dördüncü temel bileşen olarak yer alan işletim ve iş destek sistemleri, sanal ağ fonksiyonları ile haberleşerek işlevlerini yerine getirmektedir.

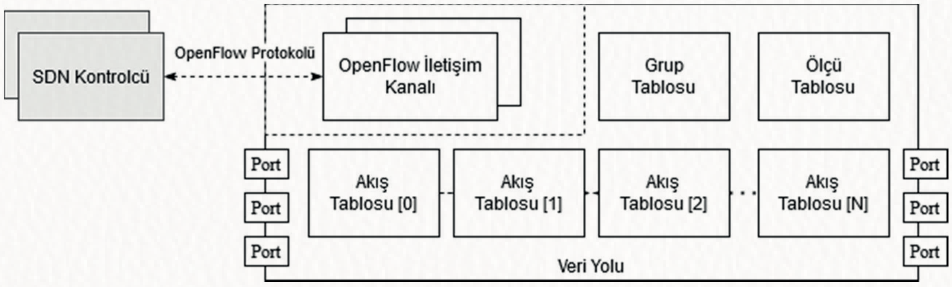
NFV ile ağ fonksiyonlarının dinamik olarak oluşturulabilmesi, ölçeklendirilebilmesi, yerinin değiştirilebilmesi mümkün olabilmektedir. Ayrıca NFV; ağ işletiminin merkezi olarak yürütülebilmesine, daha yüksek güvenlik ve erişilebilirlik sağlayacak yeni ağ fonksiyonlarının geliştirilebilmesine, ağ fonksiyonlarının ve altyapılarının kolaylıkla bakımlarının yapılabilmesine olarak sağlamaktadır. Ağ fonksiyonu sanallaştırma, siber güvenlik için çeşitli ağ güvenlik fonksiyonlarının geliştirilebilmesini ve uygulanabilmesini kolaylaştırmıştır. Fakat bu mimaride de ağ paketlerinin hızlı şekilde işlenebilmesini sağlayacak altyapılara ihtiyaç duyulmaktadır.

8.3. AĞ YAZILIMLAŞTIRMA VE AĞ VERİ KATMANI PROGRAMLAMA

8.3.1. OpenFlow Protokolü ve OpenFlow Destekli Anahtarların Yapı Taşları

OpenFlow protokolü, SDN kontrolcü ile SDN anahtarları arasındaki mesajlaşma için endüstri standardı olarak tanımlanmıştır. Şekil 8.3'te OpenFlow destekli bir SDN anahtarının temel bileşenleri gösterilmektedir. Bir SDN anahtarda SDN Kontrolcü ile iletişim, anahtar üzerinde bulunan OpenFlow iletişim kanalları üzerinden gerçekleşmektedir. Kurulan bağlantı üzerinden SDN anahtarları yapılandırılabilmekte, SDN anahtarları ve ağ trafiği ile ilgili

bilgiler SDN kontrolcüsüne aktarılabilmekte ve SDN Kontrolcü tarafından ağ trafiği yönetilebilmektedir. SDN anahtarında ağ paketleri, anahtarın portundan girerek tanımlanan akış tablolarından geçmekte ve bu işlemler tamamlandıktan sonra paketler; yönlendirilmekte, düşürülmekte, değiştirilmekte veya gönderilmesine karar verilen yeni paketler hazırlanarak anahtarın çıkış portlarına yönlendirilmektedir. Paketler akış tablolarında ilerlerken farklı bir akış tablosuna veya grup tablosuna yönlendirilebilmektedir. Ayrıca paketler işlenirken belirli ölçülere yönlendirilerek paketlerin ölçülere uygun olarak işlenmesi sağlanabilmektedir.



Şekil 8.3. OpenFlow destekli bir SDN anahtarının temel bileşenleri [7]

Aşağıdaki alt başlıklarda OpenFlow protokolü ağ yazılımlaştırma fonksiyonlarının geliştirilmesinde aktif olarak kullanılabilecek özellikler açıklanmaktadır.

8.3.1.1. SDN Kontrolcüler ve SDN Anahtarları Arasındaki Mesajlaşma

OpenFlow protokolünde; SDN kontrolcünün başlattığı, SDN anahtarlarının gönderdiği ve OpenFlow haberleşme altyapısının yönetimini sağlayan mesajlaşma tipleri tanımlanmıştır.

SDN kontrolcüsünün başlattığı mesajlar *kontrolcüden-anahtarlara mesajlar* olarak isimlendirilmektedir. Bu mesajlar çoğunlukla SDN kontrolcünün anahtarlardaki akış ve grup tablolarındaki kayıtların güncellemesi (flow_mod, group_mod), anahtardaki portların yapılandırması (port_mod) ve anahtarın belirli portlarından paketler göndermesi (packet_out) için kullanılmaktadır. Ayrıca anahtarların özelliklerinin sorgulanması ve değiştirilmesi, akış tablo-

larının özelliklerinin değiştirilmesi, anahtarlardaki OpenFlow iletişim kanalının rolünün değiştirilmesi, mesajlar arası bağımlılıkların yönetilmesi gibi farklı işlevler için de SDN kontrolcüsü anahtarlara bu tipte mesajlar gönderebilmektedir.

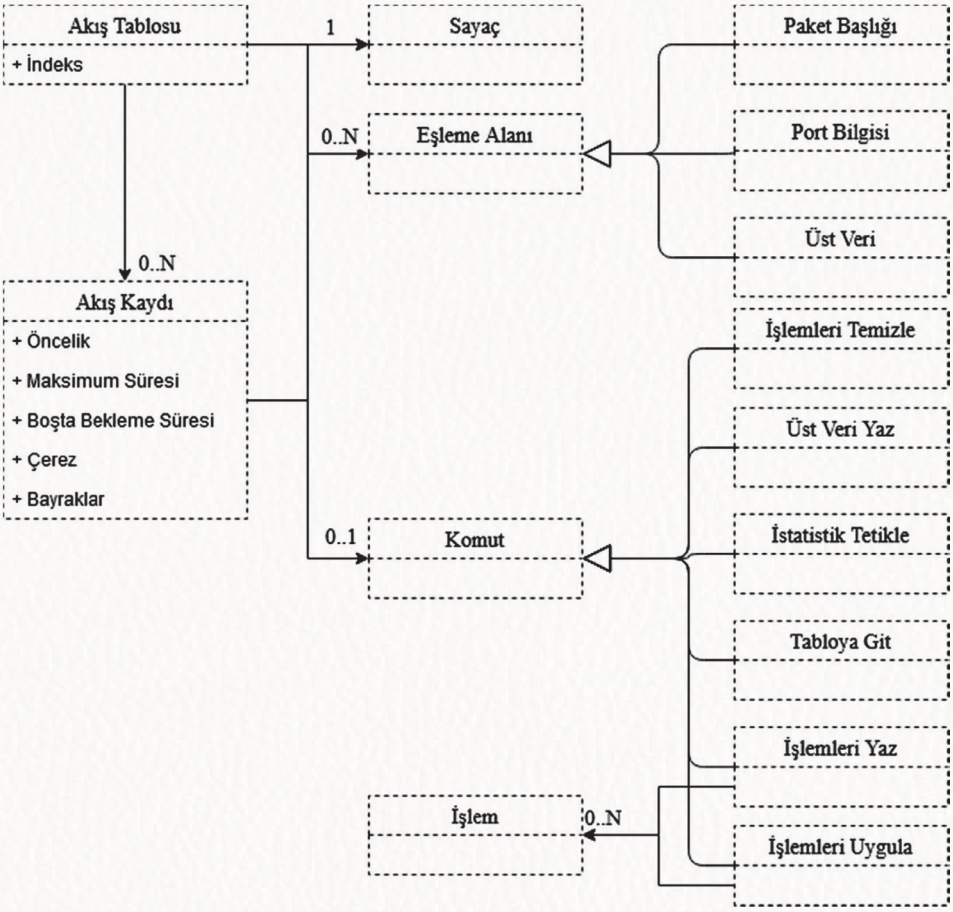
SDN anahtarlarının gönderdiği mesajlar *eş zamanlı olmayan mesajlar* olarak isimlendirilmektedir. Bu mesajlar, SDN anahtarında gerçekleşen bir olayın SDN kontrolcüye iletilmesini sağlar. Bu kapsamdaki en önemli mesaj, paket ile ilgili yapılması gereken kararın verilmesi için yeni paketin SDN kontrolcüye iletilmesini sağlayan gelen paket (packet_in) mesajıdır. Paketin geldiği port, gönderilme sebebi, en son işlem yapılan tablo ve akış kaydı bilgilerini içerecek şekilde gelen paket mesajı oluşturulur ve SDN kontrolcüye iletilir. Ayrıca anahtar; bir akış tablosundan bir kaydın silinmesi, akış tablosunda güncellemeler olması ve anahtarın bir portunun durumunun değişmesi gibi olayların da SDN kontrolcüye iletilmesi için de eş zamanlı olmayan mesajlar gönderebilir. Ağda birden fazla SDN kontrolcü bulunması durumunda anahtar tarafından OpenFlow iletişim kanalının seçilmesi ve güncel durumun SDN kontrolcüleri ile paylaşılması bu tip mesajlarla gerçekleştirilir.

OpenFlow haberleşme altyapısının yönetimi için hem SDN kontrolcü hem de SDN anahtarları tarafından başlatılabilen *simetrik mesajlar* kullanılır. OpenFlow bağlantısının başlatılması için kullanılan selamlaşma, mesajlar işlenirken karşılaşılan hataların iletilmesi ve bağlantının devam ettiğini kontrol için kullanılan istek ve cevaplar bu tip mesajlardır.

8.3.1.2. Programlanama İçin Kullanılan OpenFlow Tabloları

SDN anahtarlarda akış, grup ve ölçü tablosu olmak üzere üç tür tablo bulunmaktadır. Bu tablolar farklı amaçlarla kullanılmaktadır. Tüm paketler için akış tabloları kullanılması zorunludur. Diğer iki tablo türünün kullanımı programlama ihtiyaçlarına göre belirlenmekte ve bu tablolar sadece kendilerine paket yönlendirildiğinde devreye girmektedir.

SDN anahtarlarda birden fazla akış tablosu tanımlanabilmektedir. Tablolara eklenecek kayıtlarla başka bir akış tablosuna ve grup tablosuna yönlendirilebilmektedir. Bir akış tablosunun ve akış kaydının veri modeli Şekil 8.4'te gösterilmiştir.



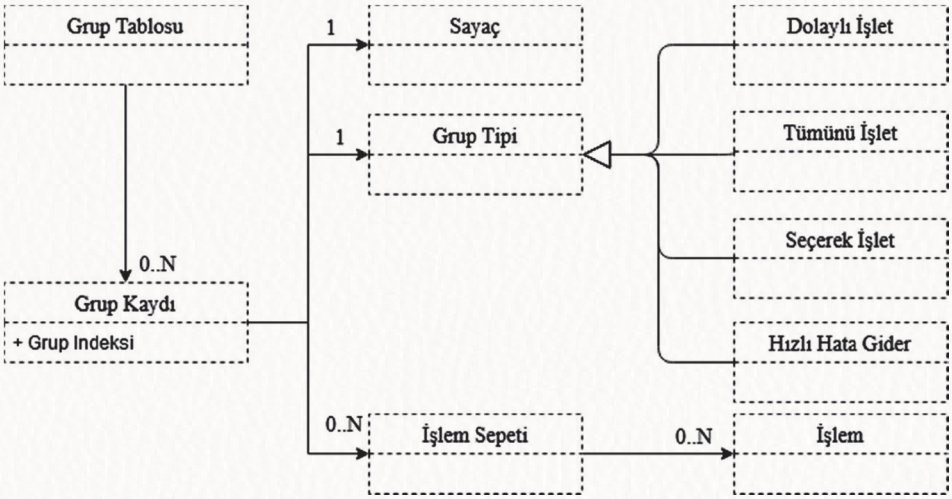
Şekil 8.4. OpenFlow akış tablosu veri modeli

Bir akış tablosunda birden fazla akış kaydı yer alabilmektedir. Her bir akış tablosu ve akış kaydı için farklı sayaçlar SDN anahtar tarafından yönetilmektedir. SDN anahtarında bir paket işlenmeye başlandığında öncelikle ilk akış tablosunda bulunan kayıtlarla eşleşip eşleşmediği kontrol edilmektedir. Birden fazla eşleşme olduğunda akış kaydında yer alan öncelik değeri en yüksek olan seçilmekte ve seçilen kayıtta tanımlanan komutlar çalıştırılmaktadır. Komutlar çalıştırılarak; paket güncelleme, düşürme, SDN kontrolcüsüne aktarma, bir porta gönderme, başka tabloya yönlendirme, bir ölçüye dâhil etme gibi işlemler gerçekleştirilebilmektedir.

Bir akış kaydında; eşleme alanları, işletilecek komutlar, kaydın öncelik değeri, maksimum ve boşta bekleme süresi ve çerez gibi veriler ile sayaç bilgileri bulunmaktadır. Bu kayıtlar SDN kontrolcü tarafından akış güncelleme (flow_mod) mesajları ile güncellenmektedir. Eşleme alanları; port, paket başlıkları ve paket için geçici verilerin yönetimini sağlayan üst verilerden oluşabilmektedir. Paketlerin bir kayıtla eşleşmesi durumunda çeşitli komutlar işletilebilmektedir. Akış kaydında yer alan komutlarla; paketler için yönetilen üst veriler güncellenebilmekte, başka bir tabloya yönlendirilebilmekte, istatistik bilgisi için tetikleme yapılabilmekte, paketler üzerinde uygulanacak işlemler seçilebilmekte, silinebilmekte veya belirlenen işlemler paketler üzerinde hemen uygulanabilmektedir.

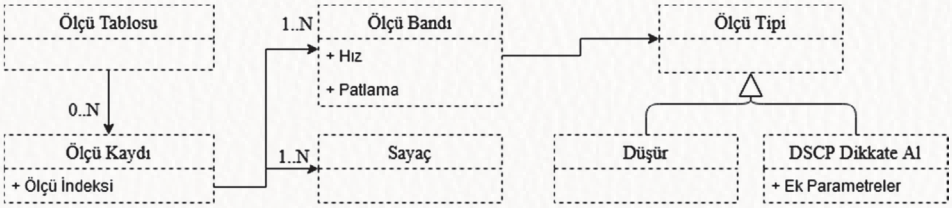
Paketler üzerinde uygulanabilecek işlemler (Örneğin; paket başlıklarının güncellenmesi, pakete VLAN başlığı eklenmesi) OpenFlow protokolünde tanımlanmıştır. OpenFlow protokolü, üreticilerin protokol tarafından desteklenmeyen deneysel komutlar ve işlemler ekleyebilmelerine olanak sağlamaktadır. OpenFlow protokolünde tanımlanan tüm komut ve işlemler zorunlu olmadığı için SDN anahtarlarının yetenekleri üreticiden üreticiye değişebilmektedir. Bu durum da birden fazla SDN anahtar tarafından desteklenen SDN uygulamalarının geliştirilebilmesini zorlaştırmaktadır.

SDN anahtarlarda bir tane grup tablosu bulunmaktadır. Grup tablosunun yapısı Şekil 8.5'te gösterilmektedir. Grup tablosunda birden fazla grup kaydı yer alabilmekte ve her bir kayıtta birden fazla işlem sepeti oluşturulabilmektedir. Her bir işlem sepetinde de birden fazla işlem yer alabilmektedir. Paketler akış tablolarından bir grup kaydına yönlendirilebilmektedir. Grup tablosuna yönlendirme yapıldığına, grup kaydının tipine göre bir veya birden fazla işlem sepeti seçilerek bu sepetlerdeki işlemler uygulanabilmektedir. Grup tipi *dolaylı işlet* olarak tanımlanan grup kaydında sadece bir işlem sepeti tanımlanabilmektedir. Bu kayıt tipine yönlendirilen paketler için hemen ilgili işlem sepetinde yer alan işlemler işletilmektedir. Grup tipi *tümünü seç* olarak tanımlanan grup kaydında yer alan tüm işlem sepetleri, *seçerek işlet* olarak tanımlanan grup kaydında ise anahtar tarafından işletilen bir algoritma (paket özeti vb.) ile işlem sepetlerinin biri seçilerek işletilmektedir. Grup tipi *hızlı hata gider* olan grup kaydında her bir işlem sepeti bir anahtar portu veya port grubu ile eşleştirilmektedir. Bu eşleştirmede aktif olarak tespit edilen ilk işlem sepeti seçilerek işletilmektedir.



Şekil 8.5. OpenFlow grup tablosu veri modeli

SDN anahtarlarda bir tane ölçü tablosu bulunmakta ve bu ölçü tablosunda birden fazla ölçü kaydı oluşturulabilmektedir. Şekil 8.6'da ölçü tablosunun yapısı sunulmaktadır. Her bir ölçü kaydı için birden fazla ölçü bandı tanımlanabilmektedir. Her ölçü bandı için hız ve patlama değerleri belirlenmektedir. Paketler akış tablolarında işlenirken ölçü tablosundaki bir ölçü kaydına yönlendirilebilmektedir. OpenFlow protokolünde sadece paketleri düşüren ve IP paketi içerisinde yeralan DSCP değerini dikkate alarak düşüren iki ölçü bandı türü tanımlanmıştır.



Şekil 8.6. OpenFlow ölçü tablosu veri modeli

8.3.1.3. OpenFlow ile Desteklenen Protokoller ve Protokol Başlıkları

Akış tablolarında paketlerin eşleştirilmesi için port bilgisi, paket başlıkları ve paket için oluşturulan işlem hattı bilgileri kullanılmaktadır. Paket başlıklarının veya işlem hattı bilgilerinin, akış tablosundaki kayıtlardaki eşleşme alanları ile

birebir aynı olması veya belirli bir maskeleme ile benzer olması durumunda önceliği yüksek akış kaydı seçilerek ilgili kayıttaki komutlar çalıştırılmaktadır. OpenFlow protokolünde bir paket için kullanılabilecek toplamda 44 eşleşme alanı bulunmakta ve OpenFlow ile 12 ağ protokolü desteklenmektedir [7]. SDN anahtarları, paketi ayrıştırarak OpenFlow protokolünde tanımlanan protokollerin belirli paket başlıklarını çıkarmaktadır. Bu kapsamda OpenFlow; ETH, VLAN, IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, ARP, MPLS ve PBB ağ protokollerini desteklemekte ve bu protokollerde tanımlanan başlıklardan 38 tanesini ayrıştırabilmektedir. Paket başlıklarının yanında paket için tanımlanan giriş portu, fiziksel port, üst veri, tünel numarası gibi 6 işlem hattı bilgisi de akış tablolarında eşleşme kriteri olarak kullanılabilmektedir.

OpenFlow protokolünde paket başlıklarının ve paket için oluşturulan işlem hattı bilgilerinin kopyalanabilmesinde kullanılmak üzere yazmaçlar tanımlanmıştır. Fakat protokolde yazmaçların akış tablolarında eşleşme kriteri olarak kullanılabilmesi isteğe bağlı olduğu belirtilmiştir.

8.3.1.4. OpenFlow ile Paketler Üzerinde Yapılabilen İşlemler

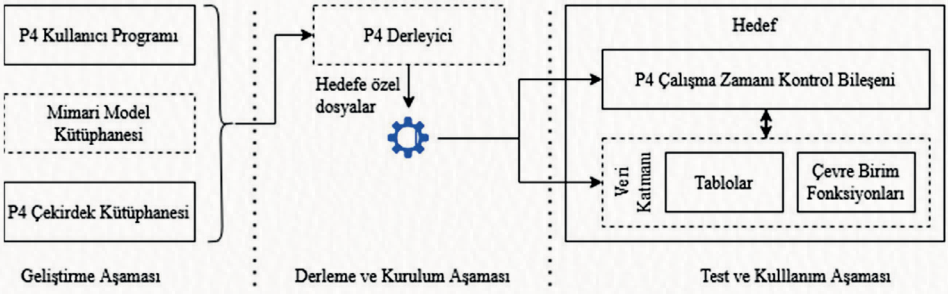
OpenFlow protokolü ile SDN anahtarlarında paketler üzerinde deneysel olarak tanımlanabilecek işlemlerin yanında 18 standart işlem gerçekleştirilebilmektedir [7]. Üreticiler OpenFlow protokolünde deneysel işlemler tanımlayarak daha fazla paket işleme kabiliyeti sunabilmektedir. Örneğin, Open vSwitch ile NSH [11] protokolünün anahtar üzerinde gerçekleştirilebilmesi için deneysel işlemler gerçekleştirilebilmektedir.

Bu işlemler akış tablo kayıtlarındaki komutlarda, grup tablo kayıtlarındaki işlem sepetlerinde yer alabilmektedir. Komutlarda veya işlem sepetlerinde hiçbir işlem yer almadığı durumlarda paket düşürme işlemi gerçekleştirilmektedir. On sekiz standart işlemden 6 tanesi paketteki TTL verisinin değiştirilmesi, diğer 6 tanesi de pakete MPLS, VLAN ve PPB etiketlerinin eklenmesi veya paketlerden bu etiketlerin çıkarılması için kullanılmaktadır. OpenFlow protokolü ile paketlerin başlıkları güncellenebilmekte (set-field) ve başlıklardaki değerler başka alanlara kopyalanabilmektedir (copy-field). Bunların haricinde paketlerin bir porta (output), grup tablosuna (group) ve bir ölçüye (meter) yönlendirilebilmesi mümkün olmaktadır. Ayrıca, çıkış portuna yönlendirilen paketler için kullanılacak kuyruğun numarasının güncellenebilmesi (set-queue) sağlanabilmektedir.

8.3.2. P4 Programlama Dilinin Yapı Taşları

P4 programlama dili, paketlerin veri katmanında nasıl işleneceğini tanımlamak için kullanılan alana özel üst seviye bir programlama dilidir [2], [12]. P4 ismi protokol bağımsız paket işlemcilerinin programlanması anlamına gelen İngilizce "Programming Protocol-independent Packet Processors" ifadesindeki kelimelerin ilk harflerinden türetilmiştir. P4 destekli hedef donanımlar, ağ protokolüne ve hedef donanımlara bağımlı kalmadan paketlerin işlenebilmesini sağlamakta ve paket işleme sürecinin tekrar yapılandırılabilmesine olanak sunmaktadır. P4 programlama dilinin başlangıçta anahtarlama cihazlarının programlanmasında kullanılması düşünülse de daha sonra kapsamı genişletilmiş ve ağ arayüz kartlarında, sanal anahtarlarda, FPGA kartlarında da kullanılabilmesi sağlanmıştır. Bu sebeple P4 programlama ile geliştirilen uygulamaların yükleneceği ortamlar farklılaşabilmekte ve bu ortamlar *hedef* olarak isimlendirilmektedir.

Şekil 8.7'de bir hedefin P4 ile programlanması için gerçekleştirilen aşamalar ve bu aşamalarda kullanılan bileşenler gösterilmektedir. Hedeflerde programlanabilir veri katmanı ve P4 çalışma zamanı [13] kontrol bileşeni bulunmaktadır. P4 çalışma zamanı kontrol bileşeni ile veri katmanındaki tablolar güncellenebilmekte ve çevre birim fonksiyonları kullanılabilmektedir.



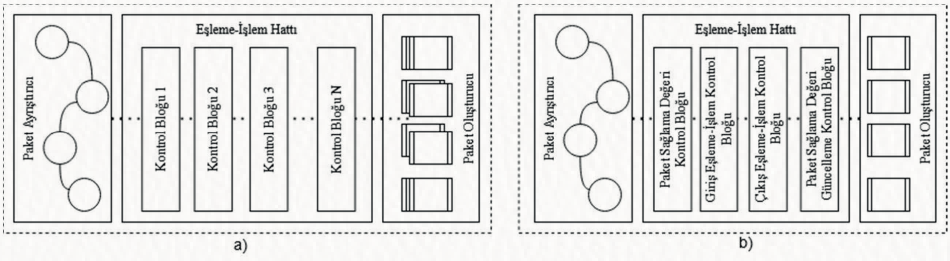
Şekil 8.7. Bir hedefin P4 dili ile programlanması [12]

Üreticiler, sundukları hedef ortamlar ile birlikte uygun P4 derleyicilerini ve hedefin kullandığı mimari model kütüphanelerini de sağlamaktadır. Geliştiriciler P4 çekirdek kütüphanelerini ve üreticilerin sağladığı mimari model kütüphanelerini kullanarak programlarını geliştirmektedir. Geliştirilen programlar ve ilgili kütüphaneler derlenerek hedefe yüklenebilmesi için gerekli dosyalar üretilmektedir. Üretilen dosyalar; hedefteki veri katmanının yapı-

landırılması için kullanılabilecek dosyalarını ve veri katmanının yönetimini sağlayacak uygulama programlama arayüzlerini (API) içermektedir.

Veri katmanının programlanabilmesi için geliştirilen P4 dilinde hedeflerin destekleyebileceği mimari modeller tanımlanabilmektedir. Bir hedef kendisine özel bir model kullanabileceği gibi birden fazla mimari modeli de destekleyebilmektedir. Örneğin, Xilinx NetFPGA SUME kartı için SimpleSumeSwitch mimari modeli kullanılırken, BMv2 sanal anahtarı [14] V1Model, SimpleSumeSwitch ve P4QueueDisc gibi mimari modelleri desteklemektedir [15].

Şekil 8.8'de tanımlanabilecek P4 genel mimari modelinin ve BMV2 sanal anahtarı tarafından desteklenen V1Model mimari modelin blokları gösterilmektedir. P4 genel mimari modelinde bir hedef, paket ayrıştırıcı ve paket oluşturma blokları arasında eşleme-işlem hattı oluşturulabilmektedir. Bu hatta birden fazla kontrol blokları geliştiriciler tarafından tanımlanabilmektedir. Şekil 8.8b'de V1Model mimari modelinin blokları gösterilmektedir. Bu model altı bloktan oluşmaktadır. İlk ve son bloklar P4 genel mimarisinde yer alan ayrıştırma (parser) ve paket oluşturma (deparser) bloklarıdır. Eşleme-işlem hattı dört bloktan oluşmaktadır. Bu hattaki ilk blok sağlama değerinin kontrolünü (checksum verification) sağlayan kontrol bloğudur. Bu blokta paket başlıklarındaki sağlama (checksum) değerlerinin doğru olup olmadığı kontrol edilerek geçerli içeriğe sahip paketlerin işlenebilmesi sağlanmaktadır. Paket bu bloktan geçtikten sonra sırası ile giriş (ingress) ve çıkış (egress) eşleme-işlemlerini gerçekleştiren blokları izlemektedir. Bu bloklarda paketler üzerinde P4 programlama ile iş mantığına uygun işlemler gerçekleştirilmektedir. Paket bu bloklardan geçtikten sonra paket başlıklarındaki bilgilerin güncellenmiş olması durumunda başlıklarda bulunan sağlama değerlerinin güncellenmesi için son bir kontrol bloğundan daha geçmektedir. Tüm eşleme-işlem hattı blokları tamamlandıktan sonra paket oluşturma bloğunda paket başlıkları tekrar oluşturulabilmektedir.



Şekil 8.8. a) P4 genel mimari modeli [12] b) V1Model mimari modeli [16]

Çıkış için oluşturulan paket başlıkları gelen paketin başlıklarının aynısı olabileceği gibi programlama ile paket bağlıkları tamamen de değiştirilebilmektedir. Örneğin gelen paketlerin VxLAN protokolü ile taşınması için paket oluşturma bloğunda yeni taşıyıcı başlıkları eklenebilmekte veya VxLAN ile taşınan paketlerin hedef istemciye gönderilebilmesi için taşıyıcı başlıklar çıkarılabilmektedir.

8.3.2.1. P4 programlama Dilinin Genel Yapısı

P4 alana özel programlama dilinin yapısı çoğunlukla C programlama diline benzemektedir. Kodlara yorum ekleme, başka kaynak dosyaları içerme, koşullu ifade tanımlama, veri tipleri tanımlama gibi özellikler C programlama dilinden alınmıştır. P4 programlama dilinde dinamik olarak değişebilen veri tipleri desteklenmemekte olup struct, enum, error gibi veri yapıları ile birlikte bit ve bit dizileri tanımlanabilmektedir. Şekil 8.9'da P4 programlama dilinin en temel yapılarını göstermek için oluşturulan örnek kod parçaları yer almaktadır.

P4 programlama dili ile tanımlanan yapılar paketler işlenirken kullanılabilmektedir. Ağ protokollerinin başlıklarını ayrıştırmak için ve başlıklarda değişiklik yapmak için başlık (header) anahtar kelimesi ile yapılar oluşturulabilmektedir. Bu yapılar paketlerin bit dizisinin sırası ile nasıl anlamlandırılması gerektiğini belirtmek için P4 diline özel yapılardır. Birden çok veri yapısını birlikte tutabilmek için yapı (struct) tanımlamaları P4 dilinde yapılabilmektedir.

Paketlerin işlenebilmesi için P4 programlamaya özel ayrıştırıcı (parser) ve kontrol (control) kod blokları tanımlanabilmekte ve bu bloklarla mimari modele uygun uygulamalar geliştirilebilmektedir. Şekil 8.9b'de sırası ile Ayrıştırıcı, Blok1 ve PaketOlusturucu yapıları ile hedef mimariye uygun bir uygulama paketi geliştirilmiştir. Bu örnek uygulamada, ağ paketlerinin Ethernet ve IP adresleri ayrıştırıcıda çıkarılmakta, Blok1'de paketin IP başlığındaki TTL değeri kontrol edilerek paket içeriğinin yönlendirme süresinin dolup dolmadığı test edilmekte ve çıkış portu belirlenmektedir. Son blokta da ayrıştırılan Ethernet ve IP başlıkları pakete tekrar eklenerek çıkış paketi oluşturulmaktadır.

```
#ifdef   _P4_BASLIKLAR_
#define  _P4_BASLIKLAR_

#include <core.p4>

#define MAKSIMUM_DEGER 100
const   bit<16> IP_PROTOKOLU = 0x800

typedef bit<48> EthernetAdresi;
typedef bit<32> IPAdresi;

header ipv4_t {
   bit<64>  ipIlkDegerleri
   bit<8>   ttl;
   bit<8>   protokol;
   bit<16>  saglamaDegeri;
   IPAdresi kaynakAdres;
   IPAdresi hedefAdres;
}

header ethernet_t {
   EthernetAdresi hedefAdres;
   EthernetAdresi kaynakAdres;
   bit<16>        ethernetTipi;
}

struct basliklar {
   ethernet_t ethernet;
   ipv4_t     ip;
}

struct ustveri {
   bool   gecerli;
   bit<9> hedefPort;
}

#endif
```

a)

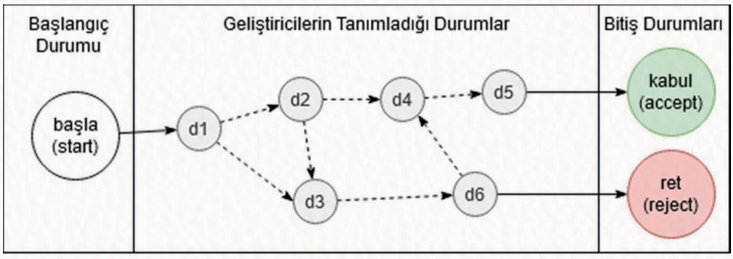
```
#ifdef    _P4_UYGULAMA_PAKETI_
#define   _P4_UYGULAMA_PAKETI_

#include "p4_basliklar.p4"

parser Ayristirici(packet_in p, out basliklar b) {
   state start {
      transition etherneti_ayristir;
   }
   state etherneti_ayristir {
      p.extract(b.ethernet);
      transition ip_ayristir;
   }
   state ip_ayristir {
      p.extract(b.ip);
      transition accept;
   }
}
control Blok1 (inout basliklar b,
               inout ustveri u,
               inout standart_metadata_t s) {
   apply {
     if (b.ip.ttl > 0) {
        u.gecerli = True;
     }
     u.hedefPort = 3;
   }
}
control PaketOlusturucu (inout basliklar b,
                         packet_out o) {
   apply {
     o.emit(b.ethernet);
     o.emit(b.ip);
   }
}

Switch(Ayristirici(),Blok1(),PaketOlusturucu()) main;
#endif
```

b)

Şekil 8.9. Bir P4 uygulamasının başlıklarını (a) ve bloklarını (b) tanımlayan örnek kod dosyaları

8.3.2.2. P4 Programlama Dili ile Paketlerin Ayrıştırılması

P4 programlama dilinde durum makinesi tanımlanarak paket başlıklarının ayrıştırılabilmesi sağlanmaktadır. Şekil 8.10'da tanımlanabilecek örnek bir durum makinesi gösterilmiştir.



Şekil 8.10. Paketlerin ayrıştırılma için örnek durum makinesi ve ön tanımlı durumlar

Durum makineleri kullanılarak paketlerde istenilen başlıklar ayrıştırılabildiği gibi etkin çalışma için sadece istenen başlıkların ve alanların ayrıştırılması sağlanabilmektedir. Şekildeki durum makinesinin ilk durumu başla (start) durumudur. P4 ayrıştırıcı bu durumun tanımlandığı kod bloğunu çalıştırarak süreci başlatır. Geliştiriciler paketlerin ayrıştırılabilmesi için istenildiği kadar durum tanımlayabilmektedir. Verilen örnekte kullanıcı tarafından altı durum (d1 – d6) tanımlanmıştır. Ayrıştırıcı, durum makinesinin son durumu kabul veya ret oluncaya kadar durumların tanımlandığı kod bloklarını çalışmaya devam eder. Durum kod bloklarında sonraki durum belirlenmeden sona erdiğinde veya ayrıştırma işleminde hata oluştuğunda durumun ret durumuna geçmiş olduğu kabul edilerek ayrıştırma süreci sonlandırılır.

Durum kod bloklarında; paketlerin değerlerinin kontrol edilmesi, ayrıştırılarak paketin başlıklarındaki alanlara aktarılması ve sonraki duruma karar verilmesi işlemleri yapılabilir. Sonraki duruma geçiş için belirli değerlere bakarak karar verilebileceği gibi doğrudan diğer bir duruma geçiş de yapılabilmektedir.

Şekil 2.9b'de yer alan ayrıştırıcıda başla durumuna ek olarak *etherneti_ayristir* ve *ip_ayristir* adında durumlar tanımlanmıştır. Bu durumlarda sırası ile Ethernet başlık bilgileri ve IP başlık bilgileri ilgili veri yapılarına kopyalanmaktadır. IP paketinin ayrıştırılması için *ipv4_t* veri tipi kullanılmaktadır. Geliştirilecek uygulamada IP başlığının ilk 64 bitinin kullanılmayacağı kararlaştırılarak bu değerler ayrıştırılmadan bütün olarak bir alana kopyalanmıştır. Fakat IP başlığındaki diğer alanların uygulamada kullanılacağı düşünülerek her biri ayrıştırılmıştır. Örnekteki durum makinesinde IP paketi ayrıştırıldıktan sonra kabul durumuna erişildiği için paket ayrıştırma süreci sonlandırılmaktadır. Ethernet ve IP başlığı içermeyen paketlerin ayrıştırmasında hata oluşacağı için son durum ret olarak belirlenerek ayrıştırma süreci sonlandırılır. Paketin ayrıştırılmayan kısımları paket oluşturma bloğunda belirlenen başlıkların arkasına eklenerek çıkış paketi oluşturulmak için kullanılmaktadır.

8.3.2.3. P4 Programlama Dili ile Tanımlanabilen Kontrol Blokları

P4 programlama dili ile birden fazla kontrol (control) bloğu tanımlanabilmekte ve bir kontrol bloğunun içinde diğer kontrol blokları değişken tanımlaması ile oluşturularak çağrılabilmektedir. Genel olarak eşleme-işlem hattı blokları ile paket oluşturma blokları bu veri yapıları ile tanımlanmaktadır. Bir kontrol bloğunda sabit değerler, değişkenler, işlemler ve tablolar tanımlanabilmektedir. Örnek bir kontrol bloğu Şekil 8.11'de gösterilmiştir.

```
control Yonlendirici(inout basliklar b, inout ustveri meta, inout standard_metadata_t s) {
    bool gecerli = False;

    action dusur() {
        mark_to_drop(s);
    }
    action yonlendir(bit<32> sonrakiIP, bit<9> port) {
        meta.sonrakiIP = sonrakiIP;
        s.egress_spec = port;
        b.ip.ttl = b.ip.ttl - 1;
    }
    table yonlendirme_tablosu {
        key = {
            b.ip.hedefAdres: lpm;
        }
        actions = {
            yonlendir;
            dusur;
            @defaultonly NoAction;
        }
        size = 16384;
    }
    apply {
        if(yonlendirme_tablosu.apply().hit){
           gecerli = True;
        }
    }
}
```

Şekil 8.11. Örnek kontrol bloğu yapısı

Bu kontrol bloğunda *gecerli* adı ile bir değişken tanımlanmış ilk değeri atanmıştır. Sonrasında "düşür" ve "yönlendir" adı ile iki adet işlem tanımlanmıştır. İlk işlemde P4 çekirdek kütüphanesinde tanımlanan işlem kullanılarak paketin düşürülmesi için paket işaretlenmektedir. İkinci işlemde, yönlendirilecek sonraki IP adresi ve çıkış portu belirlenmekte ve paketin IP adresindeki TTL değeri bir azaltılmaktadır. Tanımlanan bu işlemler tablolarda ve kontrol bloğunun çalıştırıldığı *uygula* (*apply)* adı ile belirtilen bölümde kullanılabilmektedir.

Bir kontrol bloğunda birden fazla tablo tanımı yapılabilmektedir. Tanımlanan bu tablolar ve işlemler kontrol bloğunun *uygula* kod bölümünden çağrılabilmektedir. Örnekte kontrol bloğunun uygulama bölümünde yönlendirme tablosunun uygulanması sağlanmaktadır. Bu tablo ile eşleşme olduğunda da kontrol bloğunda tanımlanan *geçerli* isimli değişkenin değeri değiştirilmektedir. IP yönlendirme yapılabilmesi amacı ile kullanılan *yönlendirme tablosunda* eşleme kriteri olarak paketin IP başlığındaki hedef adresi kullanılmaktadır. Tabloda eşleme sonrasında kullanılabilecek işlemler de (*actions*) belirtilmektedir. Bu tablo uygulandığında ve bir eşleşme durumunda düşür ve yönlendir isimli işlemler gerçekleştirilebilmektir. Bir eşleşme olmadığında da yine P4 çekirdek kütüphanesinde tanımlanan ve bir değişiklik yapmayan işlem ger-

çekleştirilmektedir. Oluşturulan tablolara eklenebilecek maksimum kayıt sayısı da ayrıca belirtilebilmektedir. Örneğin bu tabloda maksimum tablo kayıt sayısı 16384 olarak belirlenmiştir.

8.3.2.4. Kontrol Katmanından Veri Katmanının Yapılandırılması

Kontrol bloklarında tanımlanan tablolar ve diğer yapılar, kontrolcü katmanından güncellenebilmektedir. Bu tabloların güncellenmesi için P4 çalışma zamanı bileşeni ile iletişim kurulması gerekmektedir. Bu bileşen gerekli güncellemelerin yapılabilmesi için arayüz sunmakta ve bu arayüz kullanılarak yeni kayıtlar eklenebilmekte, kayıtlar güncellenebilmekte, listelenebilmekte veya silinebilmektedir. Bu işlemlerin gerçekleştirilebilmesi için gerekli arayüzler geliştirilen uygulamanın derlenmesi sürecinde oluşturulmakta ve bu bileşene yüklenmektedir. Şekil 8.12'de BMv2 sanal anahtarına komut satırından bağlanarak üç kayıt eklenmesini sağlayan kod örneği sunulmaktadır. İlk iki kayıt belirtilen IP adreslerinin 3 numaralı port ve 10.0.3.12 IP adresi kullanılarak yönlendirileceği belirtilmektedir. Son kayıtta da 10.0.4.0/24 IP bloğundaki tüm paketlerin düşürülmesi için güncelleme yapılmıştır.

```
simple_switch_CLI --thrift-port 9091

> table_add yonlendirme_tablosu yonlendir 10.0.1.1/32 => 10.0.3.12 3
> table_add yonlendirme_tablosu yonlendir 10.0.2.1/32 => 10.0.3.12 3
> table_add yonlendirme_tablosu dusur     10.0.4.0/24 =>
```

Şekil 8.12. BMV2 sanal anahtarına bağlanma ve tanımlı tabloya örnek kayıt ekleme

8.3.2.5. Veri Katmanında Ağ Durum Bilgilerinin Yönetimini Sağlayan Bileşenler

P4 programlama dili, tabloların yanında ağ durum bilgilerinin yönetimi için bazı yapılar sunmaktadır. Bunların başında ölçüler, sayaçlar ve yazmaçlar gelmektedir. Bu yapılar kullanılarak dinamik ve akıllı ağ fonksiyonları tanımlanabilmektedir. Şekil 8.11'de sunulan uygulama örneği, ağ durum bilgilerini içeren yapıları barındıracak şekilde genişletilmiş ve Şekil 8.13'te sunulmuştur. Bu örnekte tanımlanan ölçü eşik değerlerini aşmayan paketler yönlendirme tablosu ile eşleştirilmektedir. Bu tabloda bir eşleşme gerçekleştiğinde paketin geldiği porttaki son IP adresi yazmaçlar kullanılarak saklanmaktadır. Paket geçerli bir paket değilse veya tanımlanan ölçünün

eşik değerlerinin dışında ise paket düşürülmek için işaretlenmekte ve her bir porttan düşürülen paket sayıları tanımlanan sayaç ile sayılmaktadır. Bu örnekte de görüldüğü gibi ölçüler, yazmaçlar ve sayaçlar ağ durum bilgilerinin takip edilebilmesi için kullanılabilecek en önemli yapılardır. Bu yapıların haricinde durum bilgilerinin yönetimi için P4 uygulamasında kontrol bloklarının dışında tanımlanan genel değişkenler de ağ durum bilgilerini saklamak için kullanılabilmektedir.

```
control Yonlendirici(inout basliklar b, inout ustveri meta, inout standard_metadata_t s) {
    bool gecerli = False;
    direct_meter<bit<32>>(MeterType.packets) olcu1;
    counter(512, CounterType.packets_and_bytes) sayac1;
    register<bit<32>>(512) yonlendirilenSonIP;
    action dusur() {
        mark_to_drop(s);
    }
    action yonlendir(bit<32> sonrakiIP, bit<9> port) {
        meta.sonrakiIP = sonrakiIP;
        s.egress_spec = port;
        b.ip.ttl = b.ip.ttl - 1;
    }
    table yonlendirme_tablosu {
        key = {
            b.ip.hedefAdres: lpm;
        }
        actions = {
            yonlendir;
            dusur;
            @defaultonly NoAction;
        }
        meters = olcu1;
        size = 16384;
    }
    apply {
        olcu1.read(meta.olcu_sonucu);
        if(meta.olcu_sonucu == 0 && yonlendirme_tablosu.apply().hit){
           gecerli = True;
           bit<32> ip = 0;
           yonlendirilenSonIP.read(ip, (bit<32>) s.ingress_port);
           if(ip != b.ip.kaynakAdres){
              yonlendirilenSonIP.write((bit<32>) s.ingress_port, b.ip.kaynakAdres);
           }
        }
        if(gecerli == False || meta.olcu_sonucu > 0) {
           dusur();
           sayac1.count((bit<32>)s.ingress_port);
        }
    }
}
```

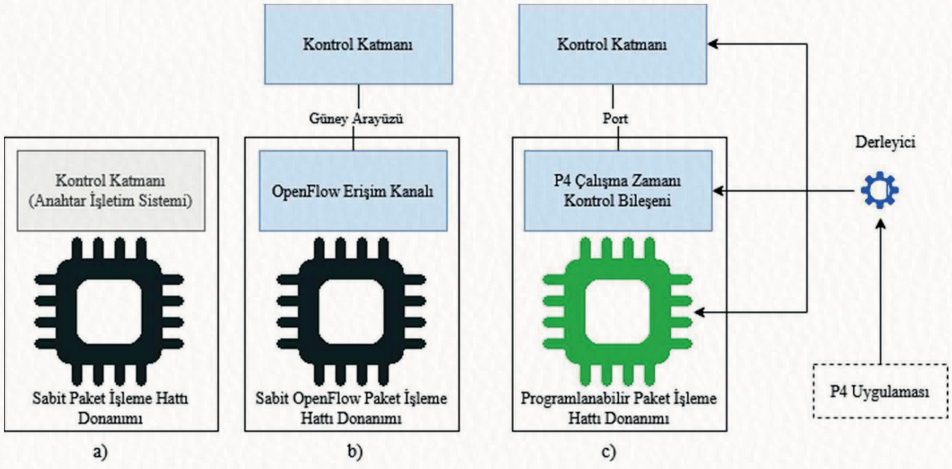
Şekil 8.13. Ağ durum bilgilerini içeren yapıların kullanıldığı P4 uygulama örneği

Ağ durum bilgilerini saklayan yapılar, geliştirilen uygulamaların kontrol bloklarından erişile bildiği gibi P4 çalışma zamanı bileşeni kullanılarak kontrol katmanından da erişilebilmektedir. Örneğin kontrol katmanından sayaçların değerleri okunabilmekte ve yazmaçlar güncellenebilmektedir.

8.3.3. OpenFlow Protokolü ve P4 Programlama Dilinin Karşılaştırılması

Klasik ağ anahtarı, OpenFlow destekli ve P4 destekli anahtarların yapıları ile sundukları arayüzler farklılık göstermektedir. Bu anahtarların yapılarındaki temel farklılıklar Şekil 8.14'te gösterilmektedir. Klasik anahtarlarda veri katmanı ve kontrol katmanı anahtar içinde yer almaktadır. Diğer iki anahtar mimarisi ile ağ yazılımlaştırma için çeşitli özellikler sunulmaktadır.

OpenFlow destekli anahtarlarda üreticiler tarafından OpenFlow protokolünün özelliklerini destekleyecek şekilde geliştirilmiş sabit veri katmanı donanımları yer almaktadır. Anahtarlarda OpenFlow erişim kanalları bulunmakta ve bu kanallar kullanılarak anahtar yapılandırılabilmektedir. Bu anahtarlarda bulunan sabit işleme hattı OpenFlow protokolünde tanımlanan işlem hattına uygun geliştirilmiştir. OpenFlow mesajları kullanılarak bu sabit işleme hattı donanımları üzerinde aşağıdan yukarı programlama yaklaşımı ile uygulamalar geliştirilebilmektedir.



Şekil 8.14. Klasik (a), OpenFlow (b) ve P4 (c) anahtarlarının yapısı ve arayüzleri [15], [17]

P4 programlama dilinde uygulama seviyesinde tasarım yapılmakta ve bu tasarımlara göre donanımlar programlanabilmektedir. Bu süreç de yukarıdan aşağıya programlama yaklaşımı olarak adlandırılmaktadır. P4 destekli anahtarlarda P4 çalışma zamanlı bileşeni bulunmaktadır. Bu bileşenin sunduğu porttan bağlantı kurularak programlanabilir işleme hattı donanımları kontrol

katmanından yapılandırılabilmektedir. Geliştirilen uygulamaların ilgili parçaları programlanabilir işleme hat donanımına, P4 çalıma zamanı bileşenine ve kontrol katmanına yüklenebilmektedir.

Ağ yazılımlaştırma için OpenFlow veya P4 destekli anahtarlar kullanılarak uygulamalar geliştirilebilir. OpenFlow protokolünün sunduğu özellikler ve P4 programlama dili kabiliyetleri kullanılarak gerçekleştirilebilecek veri katmanı programlamanın karşılaştırmalı özeti Tablo 8.1'de sunulmuştur. Karşılaştırmada veri katmanı programlama için sağlanabilecek temel 12 özellik tanımlanmış ve bu özelliklere göre OpenFlow protokolü ve P4 programlama dili ayrı ayrı değerlendirilmiştir.

Tablo 8.1. OpenFlow protokolü ve P4 programlama dilinin sunduğu özellikler

Özellik	OpenFlow Protokolü	P4 Programlama Dili
Desteklenen ağ protokolleri	Tanımlanmış 12 ağ protokolü desteklenmektedir.	Uygulama ile istenilen ağ protokolü desteklenebilmektedir.
Kontrol katmanı ile anahtar arasındaki iletişim	Anahtarda bulunan OpenFlow iletişim kanalı üzerinden OpenFlow protokolü kullanılır.	Anahtarda bulunan P4 Çalışma zamanını bileşenine bağlanılarak geliştirilen uygulamanın arayüzleri kullanılabilir.
Eşleşme tabloları	Sıfır numaralı indeksten başlayan ön tanımlı akış tabloları programlama için kullanılmaktadır.	İstenilen tablolar istenilen eşleme kriterleri ve işlemlerle oluşturulabilmektedir.
Akış tablolarında eşleştirilme için kullanılan alanlar	OpenFlow 1.5.1'de paket ve işleme hattı verilerinden 44 tanesi akış tablosu eşleştirme kriteri olarak kullanılabilmektedir.	Paket ve işleme hattı bilgilerinin yanında tanımlanan değişkenler de tablolarda eşleştirme kriteri olarak kullanılabilmektedir.
Paketler üzerinde yapılabilecek işlemler	OpenFlow 1.5.1'de 18 işlem tanımlanmıştır. Üreticiler kendi işlemlerini tanımlayabilmektedir.	Paket üzerinde yapılacak işlemler uygulama ile tanımlanabilmektedir.
Paket başlığı güncelleme	Sadece paketin alanları güncellenebilmekte ve pakete VLAN, MPLS ve PBB etiketleri eklenebilmekte / çıkarılabilmektedir.	Paket başlığı uygulama ile tamamen değiştirilebilmektedir (yeni başlık ekleme, başlığı güncelleme, başlık çıkarma, vb.).
Paket işleme hatları	Ön tanımlı tablolardan oluşan sabit hatlar tanımlanmıştır. Tablolar arasındaki geçişler tablodaki komutlarla yapılabilmektedir.	Uygulama seviyesinde hatlar tanımlanabilmekte, hatlar arası geçiş ve kullanılacak tablolar yazılım ile belirlenmektedir.
Paketlere uygulanacak ortak işlemler için fonksiyon tanımlama	Bir veya birden fazla işlemin fonksiyon olarak çalıştırılabilmesi için seçilen bir akış tablosu veya grup tablosu kayıtları kullanılabilmektedir.	Standart fonksiyonlar için işlem tanımlaması yapılarak kontrol bloklarından çağrılabilmektedir.

Özellik	OpenFlow Protokolü	P4 Programlama Dili
Değişken tanımlama ve kullanımı	Değişken tanımlanamamakta, ön tanımlı üst veri kayıt alanları paket işleme hattında değişken olarak kullanılabilmektedir.	Ağ durumsal bilgilerini saklamak veya paket işleme hatlarında kullanılmak üzere değişkenler tanımlanabilmektedir.
Yazmaç kullanımı	Sadece paketteki alanların değerlerinin kopyalanabilmesi için kullanılmaktadır.	Yazmaçlar, herhangi bir değeri ve ağ durumsal bilgilerinin saklanabilmesi için kullanılabilmektedir.
Ölçü kullanımı	Birden fazla ölçü ve ölçü bandı tanımlanabilmektedir. OpenFlow 1.5.1'de standart olarak iki tane ölçü bandı tipi (düşür ve DSCP ile düşür) tanımlanmıştır.	İstenilen şekilde ölçüler tanımlanabilmekte ve ölçü değerleri tablolarda, karşılaştırmalarda ve diğer işlemlerde kullanılabilmektedir.
Sayaç kullanımı	Tablolar, kayıtlar ve diğer nesneler için ön tanımlı paket ve paket uzunluğu ile ilgili sayaçlar bulunmaktadır.	Uygulama ile istenilen sayaçlar tanımlanabilmekte ve istenilen durumlar için kullanılabilmektedir.

OpenFlow protokolü ağ yazılımlaştırma adına daha kısıtlı özellikler sunmaktadır. Üreticiler bu kısıtları giderebilmek için eklentiler geliştirebilmektedir. P4 programlama dili ile daha esnek uygulamalar geliştirilebilmektedir. Fakat P4 programlama dili ile karmaşık aritmetik işlemler, ondalık sayı tanımlamaları, kriptografik işlemler ön tanımlı olarak yapılamamaktadır. Bu özellikleri üreticiler hedeflere çevre birimleri ekleyerek tanımladıkları mimari modellerle sağlayabilmektedir.

8.4. P4 DESTEKLİ SİBER GÜVENLİK ÇÖZÜMLERİ

Yazılım tanımlı ağlar ile çeşitli siber güvenlik mimarileri ve çözümleri geliştirilebilmektedir [8], [10]. Veri katmanı programlama ile de ağ trafiği izleme, ağ yönetimi ve tıkanıklık kontrolü, yönlendirme, yeni ağ teknolojilerin desteklenmesi, ağ güvenliği gibi konularda performanslı çözümler geliştirilebilmektedir [18]. Bu mimariler ve çözümler kullanılarak veri katmanı programlama ile siber güvenlik alanında yeni çözümlerin geliştirilebileceği açıktır. Aşağıdaki alt bölümlerde veri katmanı programlamanın siber güvenliğe katkıları, veri katmanı programı kullanılarak geliştirilen ağ fonksiyonları ve çözümleri sunulmaktadır.

8.4.1. Ağ Veri Katmanı Programlamanın Siber Güvenlik Açısından Önemi

Veri katmanı programlanın sağladığı en önemli özellikler arasında hız, esneklik ve ağ protokollerinden bağımsız olması yer almaktadır. Bu özellikler ile yeni nesil ağlarda; ağ izleme, trafik ve tıkanıklık yönetimi, yönlendirme ve ağ güvenliği gibi alanlarda çok çeşitli çözümler geliştirilebilmektedir [18]. Veri katmanı programla dili ile SDN ve NFV mimarileri daha etkin kullanılabilmektedir. Veri katmanı programlama, NFV mimarisinde yer alan ağ fonksiyonlarının SDN mimarisindeki veri katmanına taşınabilmesine olanak sağlamaktadır. Ayrıca veri katmanı programlama ile geliştirilen uygulamalar NFV mimarilerine entegre edilerek daha etkin ağ fonksiyonu yönetimi ve orkestrasyonu sağlanabilmektedir [19]. Yazılım tanımlı ağların dinamik trafik kontrolü sağlaması, merkezi kontrol ve programlanabilir mekanizmaları sunması gibi özellikleri ile siber güvenliğe önemli katkılar sunmaktadır [6]. Veri katmanı programlamanın bu konuda sağladığı ek katkılar Tablo 8.2'de özetlenmiştir.

Tablo 8.2. Veri katmanı programlamanın siber güvenliğe katkısı

Katkı	Açıklama
Hat hızında paket işleme	Programlanabilir donanımlarla paketler çoğu zaman kontrol katmanına ihtiyaç duymadan ağ trafiği ile aynı hızda işlenebilmektedir.
Ağ durumsal bilgilerini anahtarda yönetebilme	Ağ trafiği ile ilgili bilgilerin saklanabilmesi ve bu bilgilerin kontrol bloklarında kullanılması için yazmaçlar, değişkenler, sayaçlar ve ölçüler yönetilebilmektedir.
Yeni ağ protokolleri tanımlayabilme	Paketler tanımlanan durum makinelerine uygun istenilen seviyede ayrıştırılabilmekte ve çıkış paketlerinin başlıkları istenilen şekilde oluşturulabilmektedir.
Paketleri dinamik işleme hatlarına dahil edebilme	Paketler dinamik olarak paket işleme hatlarına dahil edilebilmekte, belirli değişkenlere ve ağ durum bilgilerine göre kararlar verilerek paketlere uygulanacak tablolar ve işlemler seçilebilmektedir.
Ağ fonksiyonları geliştirebilme	Ağ durum bilgileri de kullanılarak paketler üzerinde iş mantığına göre işlemleri gerçekleştirecek ağ fonksiyonları geliştirilebilmekte ve ağ fonksiyonlarının anahtarlara taşınması sağlanabilmektedir.
Ağ trafiği izleme	Ağ trafiğinin izlenmesi için dinamik tanımlamalar yapılabilmekte, ağ trafiğinin izlenmesini sağlayan protokoller geliştirilebilmekte veya desteklenebilmektedir.

8.4.2. Programlanabilir Veri Katmanı ile Güvenlik Çözümleri Geliştirme

Programlanabilir veri katmanı ile gerçekleştirilebilecek güvenlik duvarı, saldırı tespit ve önleme sistemi, DDoS saldırı önleme ağ fonksiyonu önerileri aşağıda özetlenmiştir.

8.4.2.1. Güvenlik Duvarı Ağ Fonksiyonları

Veri katmanı programlama ile istenilen paket başlıkları ayrıştırılabildiği ve istenilen ağ protokolleri ile işlem yapılabildiği için geniş kapsama sahip güvenlik duvarları geliştirilebilmektedir [20]. Ayrıca veri katmanı programlama ile hat hızında işlem kabiliyeti kazanıldığı için yeni teknolojileri destekleyecek güvenlik duvarlarının geliştirilmesi kolaylaşmaktadır. Özellikle 5G gibi yeni teknolojilerin ihtiyaçlarının karşılanabilmesi veri katmanı programlama ile sağlanabilecek çözümler geliştirilebilmektedir. 5G mobil ağlar için NetFPGA kartı ve P4 programlama dili ile geliştirilen iki güvenlik duvarı uygulamasında [21], [22] ağ trafiğindeki paketlerin istenilen başlıkları ayrıştırılarak paketlerin düşürülüp düşürülmeyeceğine hızlı şekilde karar verilebilmektedir. Bu uygulamaların ilkinde pakette bulunan Ethernet, IP, TCP/UDP ve GTP protokol başlıkları ayrıştırılmaktadır. İkinci uygulamada ise bu protokollerin yanında 5G mobiliteyi ve çoklu kullanımı desteklemek için VxLAN paketleri de ayrıştırılmaktadır. Tanımlanan eşleme-işlem tablosunda paketlerin kaynak IP, hedef IP, hedef port, kaynak port, taşıyıcı protokol tipi ve GTP tünel numarası eşleme anahtarları olarak kullanılmaktadır. Tablo ile eşleşen paketler düşürülmekte, herhangi bir eşleşme olmadığı durumlarda paket tekrar aynı başlıklarla oluşturularak normal şekilde yönlendirmektedir.

NFV mimarisinde ağ fonksiyonları ile güvenlik duvarı fonksiyonları karşılanabilmektedir. Bunun yanında NFV mimarilerinde bu fonksiyonlar veri katmanında uygulanabilmek üzere dinamik olarak tanımlanabilir. NFV mimarisinde kullanılmak üzere önerilen bir güvenlik duvarı [23], veri katmanında bulunan sayaçlar kullanılarak güvenlik duvarı fonksiyonunu dinamik olarak aktive edilebilmekte ve dinamik olarak güvenlik duvarı kuralları yüklenebilmektedir. Ayrıca ölçüler kullanılarak ağ trafik hızı kontrol edilebilmektedir.

Veri katmanı programlama ile akışların ağ durum bilgileri yazmaçlarda saklanarak akışların durumlarına göre güvenlik duvarı kuralları uygulanabilmek-

tedir. Akışlar için saklanabilecek veri boyutunun kısıtlı olmasından dolayı akışların özet değerleri anahtar olarak kullanılarak akış bilgileri yazmaçlara kaydedilebilmektedir [24]. Ağ durum bilgilerini kullanarak (örneğin TCP başlatma bayraklarının takibi) bir bağlantının kurulabilmesine karar verecek ağ fonksiyonları kolaylıkla veri katmanına taşınabilmektedir. Ayrıca istemci tarafında uygulanabilecek özel güvenlik duvarı fonksiyonları da veri katmanına taşınarak ağ güvenliği artırılabilmektedir. Örneğin, bir istemci servisine erişmek için önceden belirli sıra ile belirli portlara paket gönderme (port knocking) işlemleri P4 anahtarlarda bulunan yazmaçlarda takip edilerek sadece doğru sırada yapılan port yoklamalarını yapan akışın ilgili servise yönlendirilmesine izin veren ağ fonksiyonu geliştirilebilmektedir [25].

Klasik ağların tümünün yazılım tanımlı ağlara dönüştürülmesi kolay değildir [26]. Güvenlik duvarlarının yer aldığı klasik ağların hibrit SDN ağlarına dönüştürülebilmesi için veri katmanı programlama ile desteklenen anahtarların kullanılması ve güvenlik duvarı fonksiyonlarının veri katmanına taşınmasının maliyet etkin olabileceği ifade edilmiş ve örnek bir çalışma sunulmuştur [26].

8.4.2.2. Saldırı Tespit ve Önleme Çözümleri

Zararlı trafiğin tespit edilebilmesi için çoğunlukla trafiğin bir sunucuya gönderilmesi ve sunucu tarafından ilgili paketlerin sınıflandırılarak zararlı olup olmadığının tespit edilmesi gerekmektedir. Bu durum ağ trafiğinde performans kaybına ve zararlı trafiğin tespitinde gecikmelere sebep olabilmektedir. Bunun için bu işlemlerin tümünün veya bir kısmının veri katmanında gerçekleştirilmesi daha etkin sonuçlar elde edilmesine yardımcı olmaktadır.

Saldırı tespit ve önleme için kullanılan ağ fonksiyonları veri katmanına taşınabilmesi için saldırı tespiti amacıyla kullanılan kuralların anahtarlarda tanımlanabilmesi gerekmektedir. Yapılan bir çalışmada [27] Snort kural formatındaki veriler P4 destekli anahtarlarda tanımlanan tablo kayıtlarına dönüştürülmektedir. P4 anahtarda öncelikle durum bilgisi gerektirmeyen kurallar için filtreleme tablosu tanımlanmaktadır. Bu filtre kullanılarak istenilen paketler düşürülebilmekte, saldırı tespit sistemine yönlendirilebilmekte veya trafiğin normal akışı sağlanabilmektedir. Bu filtrenin sonrasında çok kullanılan akışlar için durumsal filtre uygulanmaktadır. Oluşturulan bu filtre ile çok kullanılan trafiğin ilk paketleri saldırı tespit sistemine yönlendirilmektedir. Saldırı tespit sistemine yönlendirilecek paket sayısı dinamik belirlenebilmekte ve de-

ğiştirilebilmektedir. Bu işlemin gerçekleştirilebilmesi için üç tablo ve iki yazmaç kullanılmaktadır. İlk iki tablo kontrol katmanı tarafından takip edilecek portların tanımlanabilmesi için kullanılmaktadır. Bu iki tabloda eşleşme olduğunda eşik değerlere göre şartlı yönlendirme yapılabilmesini sağlayan üçüncü bir tablo uygulanmaktadır. Hedef IP, kaynak IP, protokol tipi, kaynak port ve hedef port değerlerinin özeti yazmaçlarda anahtar olarak kullanılmakta, belirlenen sürede geçen paket sayısı ve en son görülme süreleri bu yazmaçlarda saklanmaktadır. Bu bilgilere göre akışların bir süre zarfında izlenebilmesi sağlanmaktadır.

Veri katmanı programlama ile belirli ağ protokollerine yönelik saldırı tespit sistemleri de geliştirebilmek mümkündür. Örneğin SCADA sistemlerinin çalıştığı ortamda siber güvenliğin artırılabilmesi için önerilen iki aşamalı saldırı tespit sistemi [28] önerilmiştir. İlk aşamada öncelikle paketin hedef IP, kaynak IP, protokol tipi, kaynak port ve hedef port değerleri kullanılarak beyaz liste kontrolü yapılmaktadır. Paketler bu tablo ile eşleşmediğinde Modbus protokolünün fonksiyon kodu ve mesaj uzunluğu alanlarının kontrolü için ikinci tabloya yönlendirilmektedir. İkinci tablo uygulandıktan sonra tablo kayıtları ile eşleşen paketler ilgili hedefe yönlendirilmektedir. Bu sayede ağdan sadece ilgili fonksiyon koduna sahip ve uzunluğu belli Modbus mesajlarının geçmesine izin verilmektedir. Hedefe yönlendirilmeyen paketler, incelemek üzere ikinci aşamaya geçirilmektedir. Bu işlem için gelen paketin IP ve TCP paketi arasına yeni bir başlık eklenmekte, gerçek hedef IP adresi ve protokol tipi bu başlıkta saklanarak paket Bro saldırı tespit sisteminin bulunduğu sunucuya yönlendirilmektedir. Paketler burada incelendikten sonra zararlı olarak belirlenmeyen tüm paketler tekrar gerçek hedeflerine yönlendirmektedir. Ayrıca bu aşamada 64 bit uzunluğunda bir etiket pakete eklenerek anahtarların analiz sonuçlarını görebilmeleri sağlanmaktadır.

Veri katmanında hat hızında makine öğrenmesi teknikleri ile ağ trafiği sınıflandırması gerçekleştirilebilmektedir. Qin ve diğ. [29] tarafından yapılan çalışmada uç ağlardaki trafiğin dağıtık öğrenme tekniklerinden faydalanılarak oluşturulan BNN sinir ağları ile sınıflandırılmasını sağlayan bir veri katmanı ağ fonksiyonu önerilmiştir. Bu öneride ağ trafiğinden öğrenilerek oluşturulan modeller veri katmanına yüklenmekte ve veri katmanında bu modeller kullanılarak paketler sınıflandırılabilmektedir. Bu işlem, ağ durum bilgilerinin yönetildiği bir yazmaç ve üç kontrol bloğu değişkeni kullanarak gerçekleştirilmektedir. Tanımlanan yazmaç, sinir ağlarındaki ağırlıkları saklamaktadır.

Değişkenler kontrol bloğundaki işlemlerin ara sonuçlarını yönetebilmek için kullanılmaktadır. Ayrıca BNN ile daha önceden sınıflandırılan paketlerin sınıflandırma sonuçları, paketin beş alanı (IP adresleri, protokol tipi ve portlar) ile elde edilen özet değerleri ile yazmaçlarda saklanmaktadır. Bu sayede aynı başlığa sahip paketlerin sınıfı, BNN sınıflandırma işleminden tekrar geçmeden hızlı şekilde tespit edilebilmektedir. Sınıflandırma sonucunda saldırı olarak ayrıştırılan paketler düşürülmektedir. Ayrıca veri katmanında sınıflandırma için kullanılan BNN ağırlıklarının güncellenebilmesi için yeni bir 4. seviye bir ağ protokolü tanımlanmıştır. Değişen model ağırlıkları için kontrol katmanında tanımlanan protokole uygun paketler oluşturularak anahtarlara gönderilmektedir. Bu paketleri alan anahtarlar veri katmanında model ağırlık değerlerini değiştirmektedir.

Veri katmanında paketlerin analizi için sadece paketlerin başlıklarını kullanan bu çalışmaların yanında paketlerin taşıdıkları yüklerin derin incelemesini yaparak belirli örüntülerin aranmasını sağlayacak ağ fonksiyonları da tanımlanabilmektedir. Bu kapsamda yapılan bir çalışmada [30] iki aşamalı olarak paketler filtrelenmektedir. İlk aşamada kaynak IP adresine göre filtreleme yapılmaktadır. Bu aşamada IP adresi eşleşen paketlere hiçbir işlem yapılmamakta veya içeriğinde örüntü aranmaktadır. Örüntü arama işlemi için Micro-C ile geliştirilmiş bir uygulama çevre birimi olarak programlanabilir veri katmanına P4 programlama dili ile kullanılabilecek şekilde eklenmiştir. Örüntü arama işlemi sonucunun değerlendirilmesi için bir sonraki aşamaya geçilmektedir. Bu aşamada eşleşen kural numarası, hedef IP adresi ve port bilgisi kullanılarak paketlerin hedefe yönlendirilmesi, düşürülmesi, hızlarının sınırlandırılması, bal küpüne gönderilmesi gibi işlemler tanımlanabilmektedir. Bu sayede veri katmanında derin paket inceleme ve sonucunda gerçekleştirilecek işlemler veri katmanında hat hızında gerçekleştirilebilmektedir.

8.4.2.3. DDoS Saldırı Tespit ve Önleme Çözümleri

Ağ seviyesi dağıtık hizmet engelleme saldırıları, en çok karşılaşılan ve engellenmesi çok zor olan problemlerden biridir. Bu saldırıların kaynağa en yakın noktada engellenmesi büyük önem taşımaktadır. Bu açıdan veri katmanında bu saldırıların tespit edilebilmesi için programlanabilir veri katmanı bazı kolaylıklar sunmaktadır. Örneğin en çok gerçekleştirilen DDoS saldırılarından olan TCP SYN sel saldırılarının tespiti için belirli zaman aralıklarında aynı

akıştaki TCP SYN paketleri sayılabilmekte ve bir akış için eşik değerine ulaşıldığında akışın paketleri düşürülebilmektedir [31]. DDoS saldırılarının tespiti için Lapolli ve diğ. [32] tarafından veri katmanı programlama ile belirli sayıdaki paketlerden IP adreslerinin entropisi hesaplanması önerilmiştir. Veri katmanı programlama ile ondalık ve karmaşık aritmetik işlemler yapılamadığı için entropi hesaplamasında kontrol katmanı tarafından güncellenebilen paket izleme aralığı tanımlanmakta, bu aralıktaki paketlerin IP adreslerinin frekansı tahmin edilerek entropi değerleri hesaplanmaktadır. Hesaplamalarda logaritmik işlemlerin sonuçları için hazır tablolar kullanılmaktadır. Hedef ve kaynak IP adreslerinin zaman serilerinden merkezi eğilim ve dağılım indekslerindeki değişim kullanılarak ilgili trafiğin anormal davranış olup olmadığı konusunda sınıflandırma yapılmaktadır. Diğer bir çalışmada [33] 0,25 saniyelik zaman aralıklarında kamaşma filtreleri (bloom filter) ile paket imzaları oluşturulup TCP SYN talep paketleri sayılmaktadır. Bunun için yazmaçlarda indeks olarak IP ve TCP paket başlığındaki alanlar kullanılmaktadır. Kontrol katmanında 10 saniyelik hareketli ortalamalar hesaplanarak veri katmanında bulunan DDoS saldırı imzası tablolarına hareketli ortalamanın iki standart sapma aralığı eşik değerler olarak yüklenmektedir. Eşik değerlerini aşan paketler anahtarlarda düşürülmektedir. Veri katmanındaki anahtarlara doğrudan sayaçlar bağlanarak istatistiki bilgiler toplanabilmektedir. Ayrıca aynı anda gerçekleştirilebilecek bağlantı sayısı için de kısıtlamaların uygulanabilmesi için çalışmada eşleme-işlem tabloları kullanılmaktadır. Aynı çalışmada TCP bağlantıları için basitleştirilmiş olasılık yoğunluk fonksiyonu ile bağlantının kullandığı bant genişliği hesaplanmaktadır. Bu bilgiler yazmaçlarda saklanmakta ve yavaş DDoS saldırılarının tespit edilebilmesi için kullanılmaktadır.

DDoS saldırılarının tespiti için belirli bir zaman aralığında gelen ve giden paket sayıları analiz edilebilir. Bu kapsamda yapılan bir çalışmada [34] aktif akış sayısının saklanması, her alt ağdaki akış istatistiklerinin yönetilmesi ve akışların takibi için yazmaçlar kullanılmıştır. Çalışmada paket ayrıştırmanın ardından beş aşamalı işleme hattından paketlerin geçirilerek DDoS saldırılarının tespit edilebileceği bir çözüm önerilmiştir. İlk aşamada paketin DDoS saldırı tespiti yapılabilecek ağda olup olmadığı belirlenmektedir. DDoS tespiti yapılacak ağlarda belirli zaman aralıklarında alınan ölçümler güncellenmektedir. Bir sonraki adımda yine kamaşma filtreleri (bloom filter) ile paketlerin IP ve UDP/TCP paketlerindeki beş başlığı kullanılarak akış sayıları hesaplanmaktadır. Bu değerler, geçmiş bilgiler kullanılarak TCP ve UDP paketleri için

ayrı ayrı belirlenen simetrik oranlarla karşılaştırılmaktadır. Eşik değerlerinin dışında kalan paketler tanımlanan kısıtlarının hangilerinin ihlal edildiğini belirtilerek işaretlenmektedir. Bu işlemler sonucunda saldırı olduğu değerlendirildiğinde ilgili alarmlar oluşturulmaktadır.

IP/MAC sahteciliğini tespit edilebilmesi için yapılan bir çalışmada [35] programlanabilir veri katmanı içeren anahtarlardaki portlara göre IP paketleri üzerinde ölçümler yapılmıştır. Önerilen bu yöntemde diğer anahtarlara bağlı olan portlara gelen trafik için normal yönlendirme yapılırken istemcilere bağlı olan portlardan saldırı yapılıp yapılmadığı tespit edilmeye çalışılmaktadır. Her port için port üzerinden saldırı olup olmadığı bilgisi ve son saldırı zamanı bilgisi yazmaçlarda saklanmaktadır. Bir port üzerinden saldırı gerçekleştirildiği bilgisi işaretlenmiş ve 1 saniyeden kısa sürede aynı paketler tekrar tespit edildiğinde bu paketler düşürülmektedir. Bu şekilde düşürülmeyen her paketin MAC ve IP kaynak adresleri kullanılarak akışın özet bilgisi hesaplanmakta ve paketin geldiği portla ilişkili olup olamadığı kontrol edilmektedir. Saldırı bilgisi işaretli değilken MAC ve IP çiftlerinin özet değerleri ilgili port ile eşleşmediğinde ve ilgili porttaki son saldırı zamanından 5 saniyeden kısa bir sürede alınan paketler yine düşürülmektedir. İlgili port üzerinden gerçekleşen son saldırı 5 saniyeden daha eski ise saldırının sonlandığı kabul edilmektedir. Aynı çalışmada ağ trafiğinin sınırlandırılması için P4 programlama ile paketlere ölçü tanımlanmıştır. Her bir akışın hızı ve miktarı ölçülerek tahsis edilen ve en yüksek kullanım oranlarına göre paketlerin sınıflandırılması sağlanmıştır. Tahsis edilen oranın altında kalan akış paketleri doğrudan hedeflerine yönlendirilmiştir. Tahsis edilen değeri aşan fakat en yüksek kullanım orana ulaşmayan akış paketleri hedefe yönlendirilirken aynı zamanda kontrol katmanına mesaj iletilmesi sağlanmıştır. En yüksek kullanım oranını aşan paketler düşürülmüş ve kontrol katmanına mesaj iletilmiştir.

8.5. SONUÇ VE DEĞERLENDİRMELER

Veri katmanı programlama, bu bölümde anlatılan siber güvenlik çözümlerinin yanında daha farklı güvenlik çözümlerinin geliştirilebilmesine de olarak sunmaktadır. Ağ yazılımlaştırma teknolojileri hızla gelişmekle birlikte veri katmanında programlama kabiliyetleri, ağlarda güvenlik ve hız gereksinimlerinin karşılanmasında çok büyük katkı sağlamaktadır. OpenFlow protokolü kullanılarak ağ katmanında kısıtlı da olsa programlama yapıla-

bilse de P4 gibi alana özel programlama dili ve bu dilleri destekleyen donanımlarla daha fazla ağ fonksiyonu veri katmanında gerçekleştirilebilmektedir. Özellikle ağda yer alan anahtarların iş birliği ile daha akıllı ve daha esnek güvenlik çözümlerinin veri katmanında geliştirilebilmesini kolaylaştırmaktadır. Siber güvenlik ile ağ fonksiyonları veri katmanında gerçeklenmesi ile hat hızında ve etkin çözümler üretilebilmektedir. P4 programlama dilini destekleyen donanımlar kısıtlı hafıza alanları sunmaktadır. Ayrıca bu donanımlar ondalık sayı işlemleri, karmaşık aritmetik işlemler ve döngüsel işlemleri desteklememektedir. Bu kısıtların giderilmesi için mevcut kabiliyetlerle yeni çözümlerin üretilmesi için çalışmalar yapılmaktadır. Makine öğrenmesi, örüntü arama gibi özelliklerin hat hızında gerçekleştirilebilmesi için programlanabilir veri katmanına çevre birim fonksiyonlarının eklenebilmesi imkânı bulunmaktadır. Bu çevre birim fonksiyonları kullanılarak veri katmanında daha karmaşık işlemler gerçekleştirilebilmektedir. Kriptografik işlemlerin de çevre birim fonksiyonu olarak sunulması durumunda bu alanda daha fazla güvenlik çözümlerinin uygulanabileceği değerlendirilmektedir.

KAYNAKLAR

[1] T. Bienkowski, “COVID-19 Network Traffic Patterns: A Worldwide Perspective from Our Customers”. https://www.netscout.com/blog/Network-Traffic-in-the-Age-of-COVID-19 (erişim Şub. 09, 2021).

[2] P. Bosshart vd., “P4: Programming protocol-independent packet processors. Computer Communication Review, 44(3)”, Computer Communication Review, c. 44, sayı 3, ss. 87–95, 2014.

[3] W. Cerroni, A. Galis, K. Shiomoto, ve M. F. Zhani, “Network Softwarization and Management”. https://www.comsoc.org/publications/magazines/ieee-communications-magazine/cfp/network-softwarization-and-management (erişim Şub. 09, 2021).

[4] S. Scott-Hayward, S. Natarajan, ve S. Sezer, “A survey of security in software defined networks”, IEEE Communications Surveys and Tutorials, c. 18, sayı 1, ss. 623–654, 2016, doi: 10.1109/COMST.2015.2474118.

[5] Y. Cui vd., “SD-anti-DDoS: Fast and efficient DDoS defense in software-defined networks”, Journal of Network and Computer Applications, c. 68, ss. 65–79, 2016, doi: 10.1016/j.jnca.2016.04.005.

[6] S. Demirci, Ö. Yürekten, ve M. Demirci, “Yazılım Tanımlı Ağlar ve Siber Güvenlik”, içinde Siber Güvenlik ve Savunma: Standartlar ve Uygulamalar, Şeref Sağıroğlu, Ed. 2019, ss. 121–152.

[7] ONF, "OpenFlow Switch Specification, v1.5.1", 2015. https://opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf (erişim Şub. 10, 2021).

[8] O. Yurekten ve M. Demirci, "SDN-Based Cyber Defense : A Survey", Future Generation Computer Systems, c. 115, ss. 126–149, 2021.

[9] "Network Functions Virtualisation (NFV) architectural framework". https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf (erişim Eyl. 11, 2020).

[10] Ö. Yürekten, "Yazılım Tanımlı Ağlar İçin Siber Tehdit İstihbaratı Destekli Savunma Sistemi Geliştirme", 2020.

[11] "IETF RFC8300 Network Service Header (NSH)". https://tools.ietf.org/html/rfc8300 (erişim Eyl. 06, 2020).

[12] "P4_16 Language Specification v 1.2.1", 2020. https://p4.org/p4-spec/docs/P4-16-v1.2.1.html.

[13] "P4Runtime Specification v1.3.0", 2020. https://p4.org/p4runtime/spec/v1.3.0/P4Runtime-Spec.html (erişim Şub. 14, 2021).

[14] "Behaviour Model (BMv2)". https://github.com/p4lang/behavioral-model (erişim Şub. 21, 2021).

[15] S. Kaur, K. Kumar, ve N. Aggarwal, "A review on P4-Programmable data planes: Architecture, research efforts, and future directions", Computer Communications, c. 170, ss. 109–129, 2021.

[16] "V1Model". https://github.com/p4lang/p4c/blob/master/p4include/v1model.p4 (erişim Şub. 14, 2020).

[17] "What is P4". https://plvision.eu/expertise/sdn-nfv/p4 (erişim Şub. 14, 2021).

[18] F. Hauser vd., "A Survey on Data Plane Programming with P4: Fundamentals, Advances, and Applied Research", 2021.

[19] M. He, A. Basta, A. Blenk, N. Deric, ve W. Kellerer, "P4NFV: An NFV Architecture with Flexible Data Plane Reconfiguration", içinde 14th International Conference on Network and Service Management, CNSM 2018, 2018, ss. 90–98.

[20] P. Vörös ve A. Kiss, "Security middleware programming using P4", içinde Lecture Notes in Computer Science, c. 9750, 2016, ss. 277–287.

[21] R. Ricart-Sanchez, P. Malagon, J. M. Alcaraz-Calero, ve Q. Wang, "Hardware-Accelerated Firewall for 5G Mobile Networks", içinde International Conference on Network Protocols, ICNP, 2018, ss. 446–447, doi: 10.1109/ICNP.2018.00066.

[22] R. Ricart-Sanchez, P. Malagon, J. M. Alcaraz-Calero, ve Q. Wang, "NetFPGA-Based Firewall Solution for 5G Multi-Tenant Architectures", içinde 2019 IEEE International Conference on Edge Computing (EDGE 2019), 2019, ss. 132–136.

[23] R. Datta, S. Choi, A. Chowdhary, ve Y. Park, "P4Guard: Designing P4 Based Firewall", içinde IEEE Military Communications Conference MILCOM, 2019, ss. 64–69.

[24] J. Cao, J. Bi, Y. Zhou, ve C. Zhang, "CoFilter: A high-performance switch-assisted stateful packet filter", içinde SIGCOMM 2018 - Proceedings of the 2018 Posters and Demos, Part of SIGCOMM 2018, 2018, ss. 9–11, doi: 10.1145/3234200.3234251.

[25] E. O. Zaballa, D. Franco, Z. Zhou, ve M. S. Berger, "P4Knocking: Offloading host-based firewall functionalities to the network", içinde 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN 2020), 2020, ss. 7–12.

[26] W. Feng, C. Liu, Z. L. Zhang, ve J. Chen, "CLÉ: Enhancing security with programmable dataplane enabled hybrid SDN", CoNEXT 2019 Companion - Proceedings of the 15th International Conference on Emerging Networking EXperiments and Technologies, Part of CoNEXT 2019, ss. 76–77, 2019.

[27] B. Lewis, M. Broadbent, ve N. Race, "P4ID: P4 Enhanced Intrusion Detection", içinde IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2019 - Proceedings, 2019, ss. 2019–2022.

[28] G. K. Ndonda ve R. Sadre, "A Two-level Intrusion Detection System for Industrial Control System Networks using P4", içinde International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR), 2018, ss. 31–40, doi: 10.14236/ewic/ics2018.4.

[29] Q. Qin, K. Poularakis, K. K. Leung, ve L. Tassiulas, "Line-Speed and Scalable Intrusion Detection at the Network Edge via Federated Learning", içinde IFIP Networking 2020 Conference and Workshops, Networking 2020, 2020, ss. 352–360.

[30] J. Hypolite, J. Sonchack, S. Hershkop, N. Dautenhahn, A. Dehon, ve J. M. Smith, "DeepMatch: Practical deep packet inspection in the data plane using network processors", içinde The 16th International Conference on Emerging Networking EXperiments and Technologies, CoNEXT 2020, 2020, ss. 336–350.

[31] F. Paolucci, F. Civerchia, A. Sgambelluri, A. Giorgetti, F. Cugini, ve P. Castoldi, "P4 edge node enabling stateful traffic engineering and cyber security", Journal of Optical Communications and Networking, c. 11, sayı 1, ss. A84–A95, 2019, doi: 10.1364/JOCN.11.000A84.

[32] A. C. Lapolli, J. Adilson Marques, ve L. P. Gaspary, "Offloading real-time DDoS attack detection to programmable data planes", içinde 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019), 2019, ss. 19–27.

[33] K. Friday, E. Kfoury, E. Bou-Harb, ve J. Crichigno, "Towards a unified in-network DDoS detection and mitigation strategy", Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridging the Gap Between AI and Network Softwarization, NetSoft 2020, ss. 218–226, 2020.

[34] M. Dimolianis, A. Pavlidis, ve V. Maglaris, "A Multi-Feature DDoS Detection Schema on P4 Network Hardware", 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops, ICIN 2020, sayı Mis 100815, ss. 1–6, 2020, doi: 10.1109/ICIN48450.2020.9059327.

[35] G. Simsek vd., “DroPPPP: A P4 Approach to Mitigating DoS Attacks in SDN”, içinde Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), c. 11897 LNCS, Springer International Publishing, 2020, ss. 55–66.

Bölüm 9

HAVACILIK SİSTEMLERİNDE SİBER GÜVENLİK

Nurşah Çevik - Sedat Akleylek

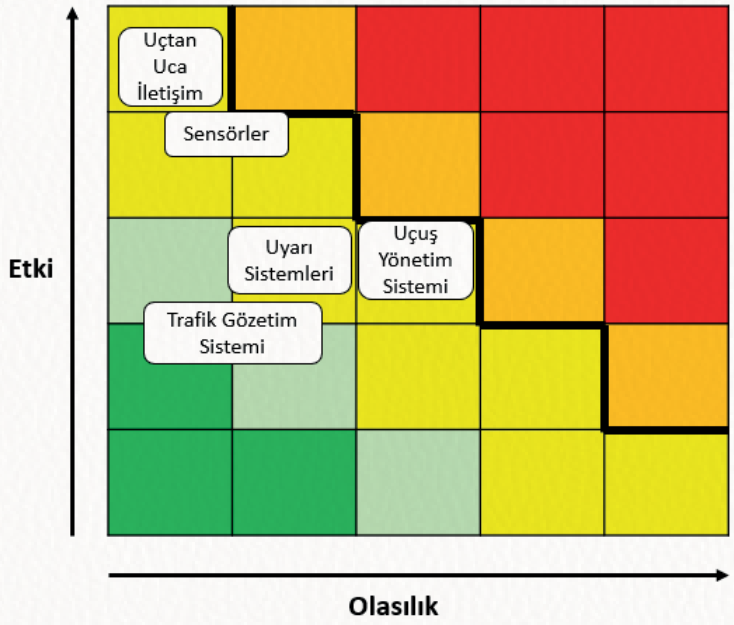
Son yıllarda havacılık sektörüne, askeri ve ticari alanlarda büyük yatırımlar yapılmış ve yatırımların sonucu olarak da önemli gelişmeler yaşanmıştır. Bu gelişmeler ve artan kullanım hacmi bu alandaki güvenlik problemlerini de beraberinde getirmiştir. Havacılık sistemlerinin, kritik altyapılardan oluştuğu bilinmektedir. Bu sistemlere karşı düzenlenen saldırıların, ülke ekonomisi, askeri güvenlik ve yolcu güvenliği gibi kritik alanlarda önemli hasarlara sebep olabileceği görülmektedir. Bu nedenle havacılık sistemleri sıkı güvenlik tedbirleri ile kapalı ve birbirinden bağımsız yapılar olarak tasarlanmaktadır. Fakat 2005 yılında Amerika'da başlatılan NextGen adlı proje ve bu projenin Avrupa'daki ayağı olan SESAR projesi ile beraber havacılık altyapısı modernize edilmeye başlanmıştır. Son 15 yılda bu alanda yapılan çalışmalar, birçok alt sistemdeki işlemleri otomatik hale getirmiş ve daha fazla birbirine bağımlı sistemler oluşturmuştur. Birbirine bağımlı sistemler daha verimli olsa da farklı güvenlik açıkları ortaya çıkarmaktadır. Ayrıca hava trafik kontrol bilgi sistemlerini ve havacılık sistemlerini korumak ve siber güvenlik rollerini ve sorumluluklarını netleştirmek gibi alanlarda zorluklarla karşı karşıya kalmıştır. Bu nedenle, havacılık sistemlerinin, güvenliği, güvenilirliği ve sürdürülebilirliğinin arttırılması için bu konular üzerine yapılan çalışmaların önemli olduğu görülmektedir. Bu çalışma kapsamında, havacılık altyapılarının güvenliği incelenmiş ve beş farklı alt sistem için saldırı senaryoları ve bu saldırılara karşı sunulan çözüm önerileri detaylı olarak paylaşılmıştır.

9.1. GİRİŞ

Kritik altyapıların güvenliğini sağlamak üzerine yapılan çalışmalar uzun süredir devam etmektedir. 1997'den beri bilgi güvenliği devletler seviyesinde yüksek riskli bir konu olarak belirlenmiş, 2003 yılında da aviyonik sistemler gibi kritik altyapıları destekleyen bilgi sistemlerinin güvenliği bu kapsam dahilinde öncelikli bir konu haline gelmiştir. Aviyonik sistemler üzerine düzenlenen bir saldırı kapsamında, bu sistemlerin düzgün çalışmaması halinde ülke ekonomisi ve muhtemelen yolcu güvenliği gibi kritik alanlarda zararlı etkileri olacağı görülmektedir. Bu nedenle, havacılık sistemleri sıkı güvenlik tedbirleri ile kapalı ve birbirinden bağımsız yapılar olarak oluşturulmuştur. Fakat 2005 yılında Amerika'da başlatılan NextGen (Next Generation Air Transportation System) adlı proje ve bu projenin Avrupa'daki ayağı olan SESAR (Single European Sky ATM Research) projesi [1] ile beraber havacılık altyapı sistemleri yeni sistemler ile değiştirilmeye başlanmıştır. Bu projelerde yüksek verimli, daha az maliyetli, güvenilir ve güvenli sistemler tasarlamak hedeflenmiştir. Son 15 yılda bu alanda yapılan çalışmalar ve sunulan sistemler ile beraber birçok alanda işlemler otomatik hale getirilmiş, bu nedenle de daha fazla birbirine bağımlı sistem kullanılmaya başlanmıştır. Birbirine bağımlı sistemler, daha verimli olsa da farklı güvenlik açıkları ortaya çıkarmaktadır. Ayrıca hava trafik kontrol bilgi sistemlerini korumak, aviyonik sistemleri korumak ve siber güvenlik rollerini/sorumluluklarını netleştirmek gibi alanlarda zorluklarla karşı karşıya kaldığı görülmektedir. Bu nedenle, aviyonik sistemlerin, güvenliği, güvenilirliği ve sürdürülebilirliğinin arttırılması için bu konular üzerine çalışmalar yapılmaya başlanmıştır.

Aviyonik sistemlerin saldırılara karşı güvenliği ve muhtemelen saldırıların önlenmesi oldukça önemli ve kritik bir çalışma alanıdır. Bir sistemin güvenli olarak adlandırılması için; sistemin, gizlilik, kimlik doğrulama, bütünlük ve inkâr edememe özelliklerini sağlaması gerekmektedir. Ancak, güvenlik ihlallerini tamamen önlemek gerçekçi bir yaklaşım değildir. Bu nedenle, izinsiz girişlerin tespit edilmesi, ardından hasarların onarılması için çeşitli önlemler alınmaktadır. Güvenli sistemler, muhtemel saldırıları tespit etmeli ve saldırıların risklerini belirlemelidir. Bu sayede, kabul edilebilir risk seviyesindeki olayları tanımlamak ve risk seviyesi yüksek olaylara karşı önlem almak çok daha kolay bir hale gelecektir. Burada farklı risk yönetim mekanizmaları kullanılmaktadır. Örneğin, Amerika Federal Havacılık İdaresi (Federal Aviation

Administration - FAA) uçuş güvenliğinde (safety) risk yönetimi için bir araç sunmuş ve yayınladığı raporda risk bileşenlerinden ve sonuçlarından bahsetmiştir [2]. Literatürde, aviyonik sistemlerde kullanılan teknolojilerin, uçuş yönetim sistemi, sensörler, uyarı sistemleri, trafik gözetim sistemi ve uçtan uca iletişimi sağlayan bağlantı sistemleri olmak üzere beş ana başlık altında incelendiği gözlemlenmiştir. DO-356 gibi bu alanda kabul edilmiş standartlarda da bu temel bileşenlerin kabul edilebilir risk sınırları Şekil 9.1'deki grafikte tanımlanmıştır. Grafik üzerinde baktığımızda uçtan uca sistemler gibi kritik bileşenlerde en düşük olasılıkta bile saldırının yüksek etkiye sahip olacağı görülmektedir [3].



Şekil 9.1. Risk kabul edilebilirlik grafiği [3]

Aviyonik sistemlerin için risk değerlendirilmesinde temel amaç: prosedürleri, riskleri belirleme, muhtemel riskleri öngörme ve bu riskleri yönetme sürecidir. Amerika Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology - NIST) yayınladığı risk değerlendirme raporunda tavsiye edildiği üzere, aviyonik sistemler için siber saldırılara karşı durumsal farkındalığının arttırılması, güvenlik zafiyetlerinin belirlenmesi ve periyodik güvenlik kontrollerinin gerçekleştirilmesi gerekmektedir [4].

Yıllar içerisinde uçuş sistemlerinin birbirine daha bağımlı yapılar haline gelmesi, internet kavramının hayatımıza girmesi ve erişilebilirlik kavramının kapsamının genişlemesi ile beraber birçok sektörde siber saldırılar artmıştır. Geçmişten günümüze havacılık sektörüne karşı yapılmış siber saldırılar göz önünde bulundurulduğunda, güvenlik riskinin arttığı en önemli ve kritik sektörlerden biri olduğu görülmektedir. Zuhijun Wu ve arkadaşları tarafından yapılan çalışmada paylaşılan Tablo 9.1'de, son yıllarda Hava Trafik Kontrol (Air Trafffic Control - ATC) sistemlerine yönelik siber saldırıları gösterilmektedir. Bu saldırıların yanı sıra Airbus Group tarafından yayınlanan raporda, şirketin her yıl yaklaşık 12 büyük siber saldırıya uğradığını belirtmiştir [5].

Tablo 9.1. Havacılık sektörüne yönelik yapılan başlıca saldırılar [5]

Yıl	Saldırı Açıklaması
2006	FAA'nın ATC sistemlerine bulaşan bir virüs, Alaska'daki ATC sistemlerinin bir kısmının kapanmasına sebep oldu.
2007	Taylan'da Elektronik Uçuş Çantasına (Electronic Flight Bag - EFB) bulaşan virüs hataya sebep oldu.
2008	Bu yıl içerisinde toplam 800 siber saldırı olayı raporlandı ve bu saldırılardan 150'den fazlası henüz çözülemedi.
2009	FAA sunucularına saldırı düzenlendi ve 48.000 çalışanın isimleri ve sosyal güvenlik numaraları çalındı.
2009	Küresel Konumlama Sistemi (Global Positioning System - GPS) bozucu taşıyan bir kamyon yanlışlıkla Newark Liberity Havaalanı'nın yer istasyonu sistemlerini bozdu.
2011	Yazılım mühendisleri tarafından, Uluslararası Hava Taşımacılığı Birliği (International Air Transport Association - IATA) havaalanı kodlarına yapılan saldırı nedeni ile 50 uçuş gecikti.
2014	Avrupa'da 13 uçak ATC radarından 25 dakikalığına kayboldu. Bu olayda ATC sistemlerinin ele geçirildiği şüphesi vardır.
2016	Havacılık endüstrisine karşı ayda 1000'den fazla saldırı düzenlendi.
2017	New York'ta bir havaalanından, cihazların şifrelerini ve çalışanların sosyal güvenlik numaralarını içeren 750 GB hassas veri sızdırıldı.
2019	Malezya Havayolları'ndan, yolcuların pasaport bilgileri, adresleri, telefon numaraları gibi detayları içeren milyonlarca veri sızdırıldı ve internet ortamında paylaşıldı.

Bu çalışma kapsamında, sivil havacılık sistemlerinin güvenliği ve bu sistemlerin alt bileşenlerine karşı yapılabilecek saldırılar detaylı olarak ele alınmıştır. Sivil havacılık altyapılarının bir kısmı askeri havacılık sistemlerinde de ortak olarak kullanılmaktadır ama protokol bazında özelleştirmeler içermektedir. Askeri bilgiler gizlilik nedeni ile paylaşılmamaktadır. Bu nedenle, bu çalışma kapsamında sivil havacılık sistemleri incelenmiş ve bu sistemler üzerine yapılabilecek muhtemelen saldırılar detaylı olarak paylaşılmıştır.

9.2. AVİYONİK SİSTEM ZAFİYETLERİ

Aviyonik mimariler, birbirinden neredeyse bağımsız analog bilgisayarlar ve ağır güç kaynaklarının yer işgal ettiği, noktadan noktaya hantal mimariler olarak tasarlanmıştı. Gelişen teknoloji ile beraber Uçuş Yönetim Sistemleri (Flight Management System - FMS), halen bağımsız olsa da verilerini bir yerde toplayarak uçuş ekibine daha global bir sunum yapabilen ilk merkezi mimari yaklaşım olmuştur. Uçak bilgi yönetimi sistemi ile bu bir adım daha ileri götürülerek veriler merkezi bir birimde toplanmaya ve buradan dağıtılmaya başlanmıştır. Entegre modüler aviyonik mimarisi ise bu sistemi daha da ileriye götürerek aviyonik sistemlere çok daha merkezi ve çok daha yazılıma dayalı bir mimariyi getirmiştir. Bu mimaride, bütünsel bir sistem sunulsa da yazılımlar ve kaynaklar birbirinden soyutlanarak hareket edildiği için, merkezi yapıdan gelen risk de minimize edilmiş olmaktadır. Bu şekilde, sistemin bir kısmına bulan zararlı yazılımın diğer kısımlara geçişi engellenmektedir [6].

Aviyonik sistemlerde kullanılmak üzere sunulacak herhangi bir yazılımın, güvenlik sistemleri de dahil, beş temel özelliği sağlaması gerekmektedir. Bu alanda kullanılacak herhangi bir sistem, Şekil 9.2'de görüldüğü üzere gerçek zamanlı çalışabilen, yüksek güvenlik seviyesine sahip, gömülü sistemlerde kullanılabilen, sürdürülebilir ve bu alandaki sertifikasyon süreçleri ile uyumlu bir sistem olmalıdır [7].

Şekil 9.2. Aviyonik sistem bileşenlerinin sağlaması gereken temel bileşenler

Entegre modüler aviyonik mimarisi ile beraber aviyonik sistemler daha merkezi ve yazılıma dayalı bir mimari haline gelmiştir. Bu nedenle, sistemlerin çeşitli siber saldırılara karşı savunmasız olabileceği öngörülmüş ve bu alandaki çalışmalar artmıştır. Sistem içerisinde, elektrik kesintisi, yazılım veya insan hatası gibi dahili tehditlerin yanı sıra, saldırganlar veya diğer sistemlerden kaynaklanan dış tehditler nedeni ile de sistemin güvenilirliğini belirlemek ve sistem zafiyetlerini değerlendirmek gerekmektedir. Sistem zafiyetleri tespit etmek ve siber farkındalık sağlamak için öncelikle tehdit alanları ve bu alanların kapsamları incelenmelidir [6].

1. **Ağlar:** İnternet Protokolü adresleriyle Hava Trafik Yönetimi (Air Traffic Management - ATM).
2. **Elektronik:** Pil gücü ve motor kontrolünü destekleyen sensörler.
3. **Yazılım:** Entegre Modüler Aviyonikler (Integrated Modular Avionics - IMA).
4. **Analitik:** GPS ve Otomatik Bağımlı Gözetim-Yayını (Automatic Dependent Surveillance–Broadcast - ADS-B) için uyumluluk ve yetkiler.
5. **İletişim:** Uçuşu koordine etmek için gereken navigasyon sinyalleri.
6. **Veri:** Çarpışmadan kaçınma için gerçek zamanlı destek için Sistem Çapında Bilgi Yönetimi (System Wide Information Management - SWIM) özelliği.

Ağlar, uçaktan, yerden ve uzaydan bilgi dağıtımını sağlayan sabit veya kablosuz yer ve hava yapılarıdır. Örneğin, hava trafik yönetiminde Internet Protokol (Internet Protocol - IP) adresleri kullanılabilmektedir. Elektronik sistemler, pil gücü ve motor kontrolünü sensörleri gibi elektronik altyapıları kapsamaktadır. Modern sistemler büyük verilerle çalıştığından, işlem verimliliği için karmaşık yöntemler kullanılmaktadır. Bu nedenle de yazılımların uygun şekilde çalışabilmesi için, entegre modüler aviyonikleri kullanılmaktadır. Aviyonik sistemlerin kullanılabilirliği, güvenilirliği gibi gerekliliklerin sağlanabilmesi için çeşitli standartlar tarafından belirlenen yapılar kullanılmaktadır. Bunlara örnek olarak, GPS ve ADS-B gibi teknolojiler verilebilir. Aviyonik sistemlerde iletişim, aktarılan sinyallerin koordinasyonu en kritik ve üzerine en çok çalışma olan alandır. Aviyonik sistemlerin güvenli bir şekilde çalışabilmesi için, uzay ve hava yollarından gelen kablosuz sinyallerin güvenilir şekilde sisteme ulaşması gerekir. Bu sistemlerdeki en önemli ve kritik yapılar da navigasyon sistemleridir. Son olarak fiziksel ağlarda ve iletişim yollarında,

veriler protokoller ile bütünlük ve tutarlılıkla iletilmelidir. Örneğin, uçaklarda çarpışmadan kaçınma için gerçek zamanlı destek için sistem çapında bilgi yönetimi özelliği bulunmaktadır. Veriler gerçek zamanlı olarak aktarılamazsa, çok büyük problemlere sebep olabilmektedir.

9.3. ELEKTRONİK UÇUŞ ÇANTASI (ELECTRONIC FLIGHT BAG - EFB)

Elektronik uçuş çantaları yenilenmiş ticari uçaklarda, pilotun yükünü azaltmak, raporlamaları otomatik hale getirmek, pilotun rotayı takip edebileceği bir kaynak sunmak gibi çeşitli amaçlarla kullanılmaktadır. Örneğin, modern Türk Hava Yolları (THY) uçaklarında Skorsky helikopterlerine de dağıtım yapan UHT şirketinin tabletleri EFB olarak kullanılmakta, eski AtlasJet uçaklarında Apple tabletler tercih edilirken, Pegasus uçaklarında Panasonic tabletler kullanılmaktadır. Normal tabletlere göre fiziksel dayanıklılık oranı arttırılmış bu tabletler ile uçuş rotası yüklenerek takip edilebilmektedir [8].

Şekil 9.3. Elektronik uçuş çantası

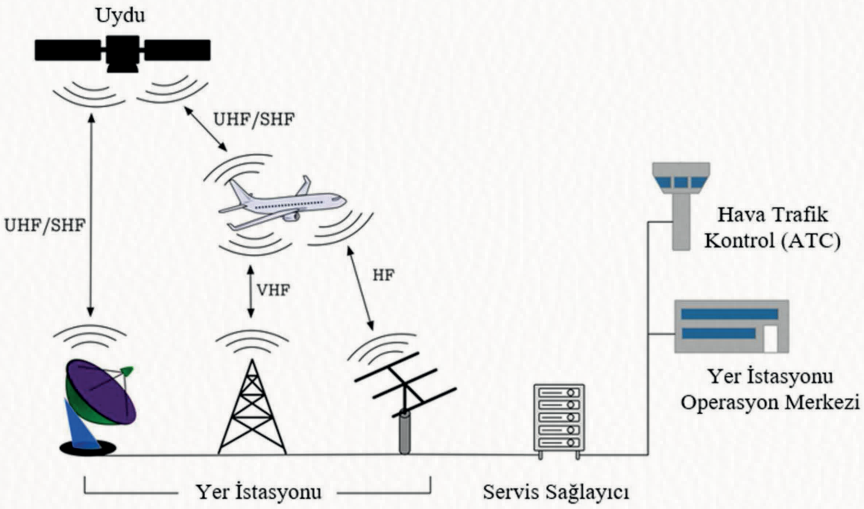
NextGen ve SESAR projeleri kapsamında bu tabletlerin kullanım alanları genişlemiş ve uçak sensör bilgileri, kapı açılış kapanış bilgileri gibi farklı altyapılara ulaşma yetkisi getirilerek pilotların raporlama yükleri azaltılmış ve hata oranları da düşürülmüştür. Fakat EFB'ler, uçağın kritik sistemleri ile bağlantılı olduğu zaman, bu cihaza bulaşan bir kötü amaçlı yazılım uçuş yönetim sistemleri gibi diğer kritik yerleşik sistemlere izinsiz girişlere neden olabilmekte ve uçuş rotasını değiştirerek pilotları yanıltabilmektedir. Ayrıca tedarikçi tarafından gelen bir siber saldırı ya da fiziksel erişimi olan saldırganlara karşı sistem zafiyeti oluşturabilmektedirler. EFB'ye yapılabilecek saldırılar beş farklı sistem sınıfında incelenmektedir [9]:

1. **Kod çalıştırma saldırısı:** Bu saldırıda, yetkisiz bir saldırgan uzaktan erişim sunucusu bileşeninde bulunan bir güvenlik açığından yararlanarak, sistemde kod yürütülmesine neden olmaktadır. Bir güvenlik açığından yararlanan bir saldırgan, sunucuda kötü amaçlı kod çalıştırabilmekte ve hatta kritik sisteme tam erişim elde edebilmektedir [9, 10].
2. **Yetki yükseltimi saldırısı:** Uzak erişim sunucusu genellikle yüksek yetkiye sahip, yönetici/kök yetkisi ile çalışan bir sistemdir. Bu nedenle, bu hizmetteki bir güvenlik açığından yararlanan bir saldırgan, sistemdeki yetkilerini standart bir kullanıcıdan yönetici/kök kullanıcısına yükseltebilmektedir [9].
3. **Kimlik doğrulama atlama saldırısı:** Uzak erişim protokolleri için bir kimlik doğrulama aşaması uygulansa da, bir saldırgan, istemci kimlik bilgilerini yanıltarak yetkisiz bir cihaz ile kritik sisteme bağlanmayı deneyebilmektedir. Ayrıca, kötü niyetli bir varlık çalınan kimlik bilgilerini kullanabilmektedir. Bu senaryolarda, saldırgan sisteme tam erişim elde edebilmektedir [9].
4. **Hizmet reddi saldırısı (Denial-of-Service - DoS):** Bu saldırıda, uzaktan erişim protokolünün sisteme bağlanmak için mevcut tek yol olduğu durumlarda, saldırgan bu yolu meşgul ederek gerçek kullanıcıların sistemle bağlantı kurmasını engelleyebilmektedir [9, 10].
5. **Yanıltma saldırısı:** Havacılık sistemleri kritik düzeyde güvenlik kısıtları göz önünde bulundurularak tasarlanmıştır fakat uzaktan erişim sağlayan cihaz bu sistemler kadar güvenli değildir. Bu durumda saldırgan bu cihazın açıklıklarını kullanarak sisteme saldırı düzenleyebilmektedir. Havacılık sistemi ile bağlantı kuran kullanıcı cihazında bulunan kötü amaçlı bir uygulama, kullanıcı adına yanlış komutlar gönderebilmekte veya kritik sistemde kullanıcı tarafından gerçekleştirilen komutları değiştirebilmektedir [9].

9.4. UÇAK İLETİŞİM ADRESLEME VE RAPORLAMA SİSTEMİ (AIRCRAFT COMMUNICATIONS ADDRESSING AND REPORTING SYSTEM - ACARS)

Uçak iletişim adresleme ve raporlama sistemi bir veri aktarma sistemidir. 1980'lerin başlarında ticari ve özel jet uçakları için geliştirilmiştir. Pilot ve mürettebatın iş yükünü oldukça azaltmış, rutin olarak alınıp gönderilen birçok mesaj ve raporun bilgisayar teknolojisi kullanılarak alınıp gönderilme-

sini sağlamıştır. Sistemin temel amacı; hava aracı ile yerde bulunan çeşitli servis sağlayıcılar arasındaki karakter tabanlı veri aktarımının sağlanmasıdır. ACARS sisteminde hava trafik kontrol ile uçak arasında Şekil 9.4'te görüldüğü üzere Ultra Yüksek Frekans (Ultra High Frequency - UHT), Çok Yüksek Frekans (Very High Frequency - VHF) veya Yüksek Frekans (High Frequency - HF) antenleri ile iletişim kurulabilmektedir.



Şekil 9.4. Uçak iletişim adresleme ve raporlama sistemi [11]

ACARS sistemleri niçin kullanılır sorusuna cevap aşağıda maddeler halinde verilmiştir.

1. Uçuş Planı
2. Durum Raporu
3. ATC Mesajları
4. Doğrudan İletişim

Örneğin, kalkıştan önce uçuş planı, uçuş sırasında durum raporları uçuş kontrol sistemine ACARS kullanılarak iletilmektedir. Daha önce uçak ile hava trafik kontrolü arasında sesli bir şekilde gerçekleştirilen iletişim ve komut aktarımı yanlış anlaşılmalara sebep olmaktaydı. Fakat bu ACARS sisteminde bilgiler yazılı olarak iletildiği için sözlü iletişim problemlerinden kaynaklanan hataları minimum seviyeye indirilmiştir.

ACARS sisteminde veri aktarımında kimlik doğrulama işlemi yapılmamaktadır. Askeri uçuşlar veya devletler için gizli bilgi içeren uçuşlarda trafiğin oldukça küçük bir kısmı şifrelense bile genel trafiğin %99'u şifrelenmeden, düz metin olarak iletilmektedir. Bu nedenle, saldırganlar veri üzerinde değişiklik ve işlem yapma ihtimaline sahiptir. Havacılık otoriteleri bu açıkları kesin bir sistem açığı olarak kabul etmese de teknolojik olarak bu saldırıların gerçekleşme ihtimali bulunmaktadır. Bu nedenle, ACARS sistemine karşı muhtemel saldırı senaryoları üzerine birçok çalışma yapılmıştır [12]. Örneğin, korumasız ACARS iletişimlerine bir saldırgan dahil olabilir ve bir uçağa yanlış konum bilgileri veya sahte uçuş planları gibi hatalı mesajlar gönderebilmektedir [12].

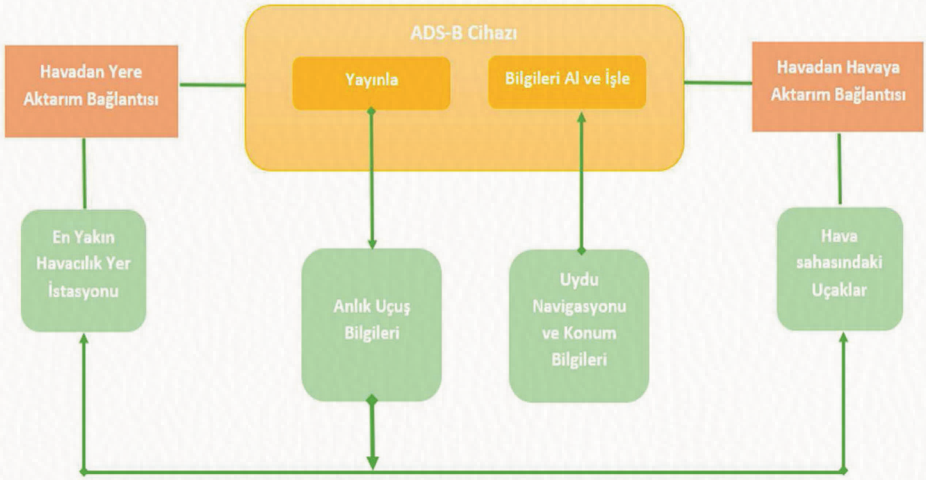
Jan Phipp ve arkadaşları tarafından yapılan çalışmada, ACARS sistemine karşı saldırı senaryoları uygulanmış ve sonuçları paylaşılmıştır. Bu çalışmada, saldırı gerçekleştirilen iki ekipten ikisi de, ACARS aracılığıyla iletilen uçuş planı güncellemelerinde bir problem olduğunu fark etmiş ve uçuş planının sıradışı olduğunu belirtmiş hava trafik kontrol kulesine belirtmişlerdir. Bugüne kadar ACARS uçuş planı güncelleme olayı ile ilgili herhangi bir (siber) saldırı raporlanmamıştır. Bu çalışmada, tek bir saldırının güvenlik açısından kritik olmadığı gösterilmiştir. Fakat aynı anda çok sayıda uçağın hedef olarak belirlendiği durumda, hava trafik kontrol kulesinin radyo kapasitesinin aşırı yüklenebileceği belirtilmektedir [13].

9.5. OTOMATİK BAĞIMLI GÖZETİM-YAYINI (AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST - ADS-B) SISTEMI

Günümüzde modern uçaklar, hava trafik kontrolü tarafından izlenebilmek için çeşitli bilgileri periyodik olarak yayınlayan ADS-B olarak bilinen bir sistemle donatılmıştır. Bu sistem, NextGen projesi kapsamında 2020 ocak ayı itibari ile sivil havacılıkta birçok uçuş sistemi için zorunlu hale gelmiştir. Bu bölümde, literatürde ADS-B cihazı üzerine yapılan saldırı çeşitleri detaylı olarak incelenmiştir. Amerika Federal Havacılık İdaresi tarafından 2010 yılında yayınlanan rapor kapsamında, çeşitli kuruluşlar saldırganların, uçaklara saldırmak için ADS-B yayınlarını dinleyebileceğini ve hatta araya girme saldırıları ile sinyallerin kesintiye uğrayabileceğini ifade etmiştir [2]. Fakat FAA, bu

cihazın yayınları ile açığa çıkan verilerin, bugünkü sistemlerin maruz kaldığı riskten daha yüksek bir riske sebep olmadığını belirtmiştir [2]. Günümüzde, gerçek hava sahasında uygulanmış başarılı bir ADS-B saldırısı raporlanmadığı için bu saldırıların uygulanabilirliği FAA açısından tartışmalıdır [5]. Fakat bu alanda yapılan güncel çalışmalar, ADS-B'ye cihazlarına düşük maliyetle önemli ve başarılı saldırılar yapılabileceğini ortaya koymaktadır [5].

ADS-B cihazları, Şekil 9.5'te görüldüğü üzere, uydu navigasyon sisteminden aldığı anlık uçuş ve konum bilgilerini, en yakın yer istasyonuna ve hava sahasındaki diğer uçaklara periyodik olarak yayın yapmaktadır. Bu şekilde diğer uçakların radarlarında görülebilmektedir.



Şekil 9.5. ADS-B cihazı mimarisi

ADS-B cihazı tarafından yayınlanan bilgiler şifreli olmadığı için ADS-B alıcısına sahip herkes tarafından alınabilmektedir. Örneğin, flightradar isimli sitede bu sistem vasıtasıyla bütün uçuşlar gözlemlenmektedir [14]. Bu cihazın yayınladığı bilgiler başta konum, irtifa, yön, hız gibi bilgilerdir. Bu bilgilerin yanı sıra bir saldırgan, havayolu şirketlerinin internet sitelerinden açık olarak yayınlanan uçuş numarası, başlangıç ve varış noktası, tahmin edilen varış zamanı ve uçak modeli gibi birçok bilgiye erişilebilmektedir [15]. ADS-B üzerine yapılabilecek siber saldırılara için elde edilebilecek açık bilgiler Tablo 9.2'de gösterilmektedir [15].

Tablo 9.2. Saldırganın elde edebileceği bilgiler [15]

ADS-B	Açık Veriler
Çağrı işareti	Uçuş numarası
ICAO numarası	Şirket
Ülke	Başlangıç noktası
Konum	Varış noktası
İrtifa	Tahmin edilen varış zamanı
Yön	Uçak modeli
Hız	Koltuk sayısı
Tırmanma hızı	Motor modeli

Tablo 9.2'de paylaşılan bilgiler herhangi bir uzmanlık gerektirmeden kolay bir şekilde elde edilebilmektedir. Bu nedenle literatürde, ADS-B cihazı üzerine birçok çalışma yapılmış, muhtemel saldırı senaryoları ve sonuçları detaylı olarak paylaşılmıştır. Bu saldırı senaryoları, yer sistemlerine ve uçak sistemlerine karşı yapılan saldırıları senaryoları olmak üzere iki temel grup altında incelenmektedir. Uçak sistemlerine yapılan saldırılar ise, pasif ve aktif olarak iki gruba ayrılmaktadır. Bu saldırı gruplarındaki saldırı senaryoları Şekil 9.6'da gösterilmiştir.

Şekil 9.6. Muhtemel saldırı senaryoları [5]

Pasif Saldırılar: Pasif saldırılarda, saldırgan yalnızca yayınlanan verileri dinlemekte ve veri üzerinde herhangi bir değişiklik yapmamaktadır. Bu saldırılarda saldırganın menzili, saldırıyı gerçekleştirmek için tüm hedef uçakların konumunu içermelidir. Menzil, saldırgandaki alınan sinyal gürültü oranına (SNR) bağlıdır. Engeller ve coğrafi koşullar, saldırganın menzili önemli ölçüde azaltmaktadır [5].

Aktif Saldırılar: Aktif saldırılarda ise hizmet aksatma ve hayalet uçak oluşturma gibi farklı senaryolar izlenebilmektedir. Bu saldırılarda, saldırgan mesaj ekleme, silme ve değiştirme özelliklerine sahiptir. Bu sayede, uçağın radarında olmayan hayalet uçaklar göstererek kokpitte zor anlar yaşanmasına sebep olabilmekte, uçuşun kalitesini ve güvenilirliğini etkileyebilmektedir. Aynı şekilde bu saldırılar yer sistemlerine de uygulanabilmektedir. Bu saldırıları gerçekleştirmek için temel bir saldırgan modeli tanımlanmaktadır. Aktif saldırılarda, saldırgan modeline göre, saldırganın kablosuz iletişim kanalı üzerinde tam bir kontrole sahip olduğunu ve herhangi bir ADS-B mesajını kanala ekleyebileceğini, silebileceğini ve değiştirebileceğini varsayıyoruz.

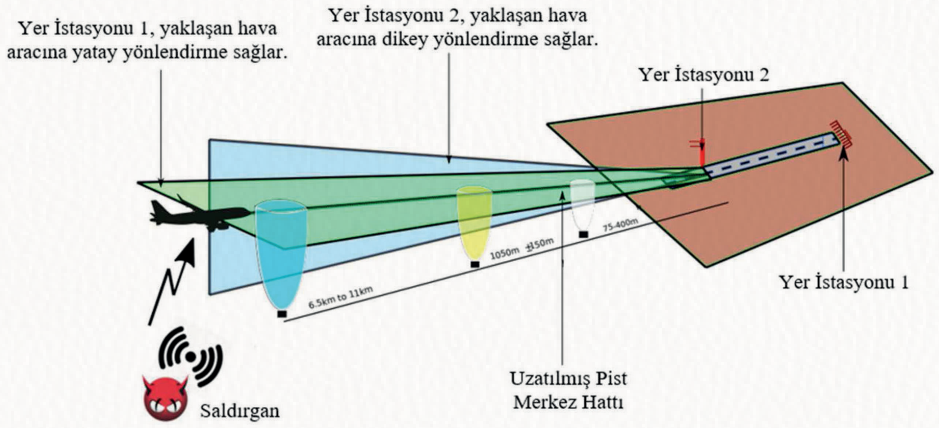
1. **Hayalet Uçak Ekleme:** Bu saldırıda, saldırgan sahte mesaj ekleme özelliğini kullanarak mevcut olmayan (hayalet) bir uçağı ADS-B mesajları aracılığı ile ADS-B iletişim kanalına eklenmektedir. Bu saldırı hem havadan havaya iletişimde hem de yerden havaya iletişimde uygulanabilmektedir. Havada, ADS-B tabanlı bir hayalet uçak ekleme saldırısında, çarpışma önleme sisteminin vereceği tepkiler pilotların dikkatini dağıtabilmektedir. Yerde, hava trafik kontrolörleri hayalet uçaklar ile gerçek uçakları ayırt etmede zorlanabilmektedir.
2. **Hayalet Uçak Baskını:** Hayalet uçak ekleme saldırısı ile aynı tekniklerine kullanan bu saldırıda saldırgan, aynı anda birden fazla uçak sisteme ekleyerek gözetim sistemlerinin hizmet reddini amaçlamaktadır.
3. **Yer İstasyonu Baskını:** Hayalet uçak baskını ile aynı teknik kullanılarak, yer istasyonu sistemlerine saldırı düzenlenmektedir. Bu saldırı sonucunda, ADS-B kullanan ATC sistemleri, fazla yüklenme nedeni ile iletişim arızası vermekte ve bu durum da hizmet aksamasına sebep olabilmektedir.
4. **Sanal Yörünge Değişikliği:** Bu saldırıda saldırgan, doğru ADS-B konum raporlarını yayınlayan bir uçağın yörüngesini değiştirmeyi amaçlamaktadır. Bu saldırı, mesaj silme ve ekleme yöntemleri birleştirerek veya doğru-

dan mesaj değiştirilerek uygulanmaktadır. Bu saldırının tespit edilemediği durumlarda, hava trafik kontrolörlerinin yanlış yönlendirmesi veya çarpışma önleme sistemlerinin gecikmiş tepkisi bir kazaya sebep olabilir.

5. **Uçağın Kaybolması:** Bu saldırıda saldırgan, hedef uçağın tüm mesajlarını ADS-B yayınlarından silmektedir. Bu şekilde, uçağın ADS-B yer istasyonları veya diğer uçaklar tarafından tespit edilmesini engellenmektedir. Bu saldırının tespit edilememesi ölümcül sonuçlara yol açabilmektedir.

9.6. ALETLİ İNİŞ SİSTEMİ (INSTRUMENT LANDING SYSTEM - ILS)

Bu sistemler sürekli olarak yatay ve dikey pozisyonda radyo sinyalleri yayınlamaktadır. Uçaklar piste yaklaşıp alçalmaya geçtiğinde uçak bu sinyallere tutulmakta ve otomatik olarak piste iniş yapmaktadır. Bu sinyallerin yanıltılması, uçağın yanlış noktadan yanlış açıyla sinyallere tutulmasına sebep olabilmekte bu da ölümcül kazalara sebep olabilmektedir. Bu nedenle bu sistemlerin güvenliği oldukça kritiktir.



Şekil 9.7. Muhtemel saldırı senaryosu [16]

Şekil 9.7'de görüldüğü üzere yer istasyonu 1 yatay yönde yönlendirme için sinyal üretirken, yer istasyonu iki dikey yönde yönlendirme sağlamaktadır. Bu sistemler pist başı, uzatılmış pist merkezi gibi bilgiler dahilinde piste en

güvenli inişi sağlayabilmek için uçakları kontrol etmektedir. Uçaklarda özellikle bazı hava koşullarında görüşsüz yani aletli uçuş gerçekleştirildiği için bu sistemlerin doğruluğu oldukça önemlidir. Saldırgan havaalanına yakın noktadan aynı frekans aralığında farklı sinyaller yayınlayarak sinyali bozabilir. Bu durum bir pilotun uçağın uçuş açısını veya alçalma hızını değiştirmesine ve dolayısıyla bir güvenlik tehlikesi oluşturmasına neden olabilmektedir.

2017'de Hong Kong'dan İstanbul'a gitmesi planlanan bir THY kargo uçağı Kırgızistan'daki duraklama noktasına inmeye çalışırken yanlış irtifada ILS sinyaline tutulmuş ve çok dik açı ile iniş gerçekleştirdiği için hızlanarak havaalanına yakın bir yerleşim bölgesine düşmüştür. Uçak bulut içerisinde olduğu için yüksek irtifada ILS'e tutulduğunu fark etmemiş ve bu kaza sonucunda 35 yerel sakinin ile 4 uçuş görevlisi hayatını kaybetmiştir. 2021 yılında 9 ocakta Mısır Havayolları uçağı Kahire havaalanına iniş yaparken yanlış tutulum gerçekleştirmiş ve hava trafik kontrolünün acil uyarısı ile pisti pas geçerek 15 dakika gecikmeli iniş gerçekleştirmiştir. Bu şekilde yanlış tutulmalar olmakta ve oldukça büyük tehlikeler oluşturmaktadır. O yüzden bu senaryolar dahilinde bu sinyalleri bozma ve yanıltma saldırıları gerçekleştirilebilmektedir. Bu saldırılar da oldukça yüksek etki oranına sahip saldırılar olmaktadır. Ayrıca, NASA'nın havacılık güvenliği raporlama sistemi [17], pilotların, ILS'nin kritik bileşenlerindeki düzensizliğin bildirildiği 300'den fazla olay bulunduğunu belirtmektedir.

Bu örnekler ILS sistemine yanlış bağlanma veya teknik bir problemden kaynaklanmaktadır. Fakat bu teknik düzensizliklerin yanı sıra ILS sistemlerine karşı yapılabilecek iki tür saldırı senaryosu bulunmaktadır:

1. **Gölgeleme saldırısı (Overshadow attack):** Bu saldırıda saldırgan, daha yüksek sinyal gücüne sahip, önceden hazırlanmış ILS sinyallerini, gerçek ILS sinyallerini bozmak için kullanmaktadır. Saldırgan, gerçek ILS sinyallerini gölgeleyerek kendi ürettiği sahte sinyaller ile pilotu yanlış yönlendirmektedir. Bu saldırı, hava durumunun gözle görüşe elverişli olmadığı zamanlarda tamamen aletli uçuş yapan pilotlar için oldukça büyük bir tehlike oluşturmaktadır. Gölgeleme saldırısı, saldırganın özel hazırlanmış ILS sinyallerini bir güç düzeyinde ilettiği ve gerçek sinyallerin saldırganın alıcıdaki sinyaline üstün geldiği bir saldırı yöntemidir. Böyle bir saldırının işe yaramasının ana nedeni, alıcıların yalnızca alınan en güçlü sinyali kilitlenmesi ve bu sinyali kullanarak inişi gerçekleştirmesi-

dir. Bu durum, özellikle düşük görüş koşullarında uçağın pistin kenarına yakın olduğu durumda hem hava trafik kontrolörleri hem de uçaktaki pilotlar tarafından potansiyel bir saldırı olarak algılanmamaktadır. Örneğin, uçağın kayma eğiminin, önerilen değer olan 3 yerine 0,1'lik bir hata ile 2,9 olarak alınması, uçağın pistin güvenli konma bölgesinin neredeyse 800 m ötesine inmesine neden olmaktadır [18]. Bu örnek, sinyallerdeki hassasiyeti ve olabilecek bir bozulmanın sebep olabileceği tehlikeyi açıkça göstermektedir.

2. **Tek tonlu saldırı (Single-tone attack):** Bu saldırı, saldırganın belirli bir sinyal gücünde (gerçek ILS sinyal gücünden daha düşük) tek bir frekans ton sinyali ileterek rota sapmalarını veya gösterge iğnesi sapmalarını kontrol ettiği özel bir saldırıdır. Gölgeleme saldırısının aksine, tek tonlu saldırı, yüksek güçlü yanıltıcı sinyaller gerektirmemektedir. Bir gölgeleme saldırısı durumunda, yanıltma sinyali, gerekli tüm frekans bileşenlerini kullanarak oluşturulurken; bu saldırıda saldırgan, iki yan bant frekansından sadece birine müdahale etmeyi amaçlamaktadır [18, 19].

Literatürde ILS sisteminin güvenliği üzerine yapılan çalışmalarda, ILS sinyallerinde kriptografik kimlik doğrulama uygulamalarının bulunmadığı bu nedenle sinyallerde bir saldırgan tarafından değişiklik yapılabileceği vurgulanmaktadır. Ayrıca bu sistemlerin güvenliği üzerine yapılan çalışmalar araştırıldığında, sistem güvenliği için tasarlanmış herhangi bir çözüm yöntemi bulunamamıştır. Bu nedenle, güvenli, ölçeklenebilir ve verimli uçak iniş sistemleri oluşturmaya yönelik bir açık olduğu görülmektedir [18].

9.7. KÜRESEL UYDU SEYRÜSEFER SİSTEMİ (GLOBAL NAVİGATİON SATELLİTE SYSTEMS - GNSS)

Uçakların coğrafi konumunu belirlemek ve navigasyon sisteminin doğruluk, güvenilirlik ve kullanılabilirlik gibi özelliklerini iyileştirmek için Küresel Uydu Seyrüsefer Sistemi kullanılmaktadır. Bu sistemleri Uydu Tabanlı İyileştirilmiş Sistemler (Satellite-based Augmentation Systems - SBAS) ve Yer Tabanlı İyileştirilmiş Sistemler (Ground-based Augmentation Systems - GBAS) olmak üzere farklı uygulama alanlarına sahiptir. SBAS sistemleri uydu bazlı olarak çalışır ve doğruluk ve bütünlüğün kritik olduğu uygulamalar için gereklidir. Özellikle, insanların hayatlarının tehlikede olduğu veya bir tür yasal veya ticari

garantinin gerekli olduğu ve GNSS'nin kullanıldığı durumlarda vazgeçilmezdir. Örneğin, havacılık sektöründe GPS, Uluslararası Sivil Havacılık Örgütü (International Civil Aviation Organization - ICAO) tarafından son yaklaşma gibi kritik uçuş aşamalarında kullanılmak üzere belirlenen katı gereksinimleri karşılamamaktadır. Ancak SBAS'ın eklenmesiyle bu standartlar karşılanmıştır. Büyük alanlara etki edebilir ve saat, atmosferik bilgiler ve coğrafi bilgileri yayınlar. GBAS'da GNSS'in kullanıldığı sistemlerde ILS sistemi kullanılmıyorsa uçakların piste inişi içi bütün ve doğru verileri sağlamaktan sorumludur.

Şekil 9.8. İnsansız hava araçları için GNSS saldırı senaryosu

Şekil 9.8'de görüldüğü üzere bu senaryo kapsamında GNSS üzerinden insansız hava araçlarının kontrolü gösterilmiştir. Burada saldırgan yine pasif olarak yayını dinlemenin yanı sıra, komut ve kontrol verilerini değiştirme ve bozma erişimine de sahiptir. Bu alanda kaydedilmiş birçok yanıltma ve ele geçirme saldırısı bulunmaktadır. Örneğin, 2011 yılında İran hava sahasındaki bir Amerikan insansız hava aracı ele geçirilmiş ve yok edilmeden kontrollü bir şekilde iniş yapabilmesi sağlanmıştır. 2015 yılında Amerika Meksika sınırında devriye gezen insansız hava araçları yanıltılarak uyuşturucu ticareti yapılmaya çalışıldığı fark edilmiştir. Philadelphia Kuzey Doğu Havaalanı (PNE) yakındaki bir otoparkta çalışan bir GPS karıştırıcısının, havaalanının GNSS sisteminin -karışmasına neden olduğu tespit edilmiştir. Özellikle günümüzde insansız

hava araçları kontrolsüz bir şekilde yaygınlaşmıştır. Gelecekte de daha yaygın bir teknoloji olarak birçok sektörde kullanılacağı öngörülmektedir. Bu nedenle bu alandaki çalışmalar oldukça önemlidir. Askeri ve sivil sistemler için GNSS sinyallerine karşı yapılabilecek muhtemel saldırılar Tablo 9.3'te tanımlanmaktadır.

Tablo 9.3. GNSS sinyallerine yapılabilecek muhtemel saldırılar [19]

<table>
<tr><th rowspan="2">GNSS Sinyal Türü</th><th rowspan="2">Sinyal Bozma Saldırısı</th><th colspan="2">Yanıltma Saldırısı</th></tr>
<tr><th>Yönlendirilmiş yanıltma saldırısı</th><th>Yanıltma saldırısı üretme</th></tr>
<tr><td>Askeri Sinyal</td><td rowspan="2">Bu saldırıların uygulaması daha kolaydır. Ayrıca uydu sinyalleri üzerinde güçlü bir etkiye sahiptir. Fakat bu saldırılar alıcı tarafından kolaylıkla tespit edilebilmektedir.</td><td rowspan="2">Bu saldırıda, eğer saldırgan bazı yanıltma yöntemlerini birleştirmezse, alıcı navigasyon mesajının bazı karakteristik bilgilerine dayanarak saldırıyı tespit etmektedir.</td><td>Askeri mesajlar sinyaller açıkça yayınlanmadığı için saldırganın askeri sinyallere yanıltma saldırısı yapması mümkün değildir.</td></tr>
<tr><td>Sivil Sinyal</td><td>Sivil havacılık sistemlerinin navigasyon mesaj içeriği, yapısı ve sinyal özellikleri açık olarak paylaşıldığı için saldırgan, açık verileri kullanarak sinyallere yanıltma saldırısı gerçekleştirebilir.</td></tr>
</table>

Tablo 9.3'te de tanımlandığı şekilde GNSS sistemlerine karşı iki farklı saldırı gerçekleştirilmektedir. Bu saldırılar aşağıda kısaca açıklanmıştır:

1. **Yanıltma saldırısı:** Bu saldırıda saldırgan gerçek sinyal bilgilerini engelleyip alıcıya sahte sinyal bilgilerini göndermektedir. Bu şekilde GNSS yanıltılmakta ve uçuş sistemi aldığı sahte sinyallerden dolayı yanlış hız ve konum bilgilerini göstermektedir. Bu şekilde uçuş rotası değiştirilebilmektedir. Bu saldırıyı gerçekleştirecek saldırgan navigasyon uydusunun bilgi formatı ve uydu sinyal yapısı hakkında detaylı bilgiye ve sahte uçuş sinyallerini otomatik olarak yayınlayacak bir cihaza sahip olmalıdır. Bu senaryo, genel yanıltma saldırısı üretme senaryosu olarak tanımlanmaktadır. Yönlendirilmiş

yanıltma saldırısında ise saldırgan, uydu tarafından alıcıya iletilen orijinal sinyali yakalar ve ardından yakalanan uydu sinyalini hedef alıcıya iletmeden önce geciktirir. Bu nedenle, saldırgan tarafından iletilen girişim sinyali, sinyalin gecikmesi ve genliğinin farklı olması dışında, gerçek navigasyon sinyali ile tamamen aynıdır. Bu gecikmeli bilgiyi alan GNSS, konum bilgisini belirlerken gecikmeden dolayı yanlış konumu hesaplamaktadır [19].

2. **Sinyal bozma saldırısı:** Bu saldırıda, verici yüksek güçlü girişim sinyallerini iletmek için kullanılmakta ve alıcının önündeki uydu sinyalleri bastırılmaktadır. Bu şekilde, GNSS alıcısı tarafından alınacak GNSS uydu sinyalleri perdelenmektedir. Ek olarak, karıştırma saldırısı, alınan sinyallerin sinyal-gürültü oranını önemli ölçüde azaltan GNSS alıcısının normal çalışma yeteneğinin de bozulmasına sebep olmaktadır [19]. Karıştırma saldırısına uğrayan GNSS alıcısı, rutin olarak izlenen uydu sinyallerini alamamaktadır [20]. Bu nedenle, yapılan saldırı uçuşu doğrudan etkilese de kolay bir şekilde tespit edilmektedir.

Jan Philipp ve arkadaşları [13] yaptıkları çalışmada GNSS sistemi üzerine yapılabilecek muhtemel saldırılardan bazılarını simülatör ortamı üzerinde gerçekleştirmiş ve pilotların saldırılara verdikleri tepkiler ve fark edip etmediklerini gözlemlemiştir. Bu çalışmada, saldırı olarak pilotların GNSS rotasına sızıp rotada değişiklik yapılmaktadır. Rotada yapılan değişiklikler pilotlar tarafından fark edilememiştir. Arada gerçekleşen kesinti de sistem gecikmesi olarak algılanmıştır. Saldırının sona ermesinden ve gerçek uçağın konumunun yeniden sistemde görülmesinden sonra tüm ekipler, haritadaki kaymayı tespit etmiş ve yeniden eski rotalarına geçiş yapmışlardır.

9.8. HAVACILIK ALANINDAKİ GÜVENLİK ÇÖZÜMLERİ

Bu bölümde, literatürdeki aviyonik sistem bileşenleri ve bu bileşenlerin güvenliği için tasarlanan güvenlik çözümleri detaylı olarak ele alınmaktadır.

9.8.1. Elektronik Uçuş Çantası için Güvenlik Çözümleri

Elektronik uçuş çantaları uçak içinde uzaktan yer sistemleri ile bağlantı ve veri aktarımı sağlayabilen, uçuş yönetim sistemi gibi kritik sistemlere erişimi olan bir aviyonik sistem bileşenidir. Bu nedenle, bu cihaz üzerinde

yapılabilecek muhtemel saldırılar uçuşun güvenliğini önemli ölçüde tehdit etmektedir.

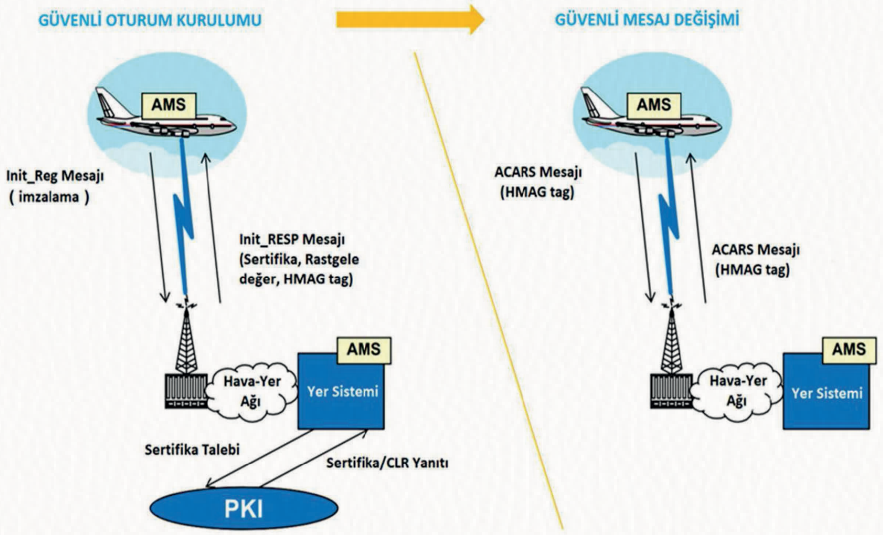
Bu saldırılara karşı bir güvenlik çözümü olarak farklı yaklaşımlar sunulmuştur. Temel olarak bu cihazlar havacılık alanında katı güvenlik kısıtları göz önünde bulundurularak geliştirilmektedir. Fakat dışarıdan gelebilecek tehditlere de açık bulunmaktadır. Bu nedenle, literatürde bu alandaki muhtemel saldırıları yöntemlerine karşı farklı güvenlik çözümleri sunulmuştur.

1. **Makine öğrenmesi:** EFB'lere bulaşan zararlı yazılımları tespit etmek için makine öğrenmesi tabanlı saldırı tespit yöntemleri kullanılmaktadır. Ron Bitton ve Asaf Shabtai tarafından yapılan çalışmada, saldırganın EFB'ye erişimini engellemek için ağ tabanlı bir saldırı tespit sistemi sunulmaktadır [10]. Bu sistem, EFB ile yer sistemi arasındaki veri aktarım işlemlerini ve EFB'nin sistem içerisindeki hareketlerini gözlemlemekte ve herhangi bir anomali tespit edildiğinde uyarı vermektedir. Önerilen çözümde, uzaktan erişim protokolünün ilettiği İletim Kontrol Protokolü (Transmission Control Protocol - /TCP) paketi ilk olarak daha önce eğitilmiş, sekiz farklı sınıfa sahip bir karar ağacı sınıflandırıcısı tarafından sınıflandırılmaktadır. Daha sonra, anormal paketlerin tespiti için bir anomali tespit modeli (k-ortalama ve CBLOF) uygulanmaktadır. Bu çalışmada sunulan saldırı tespit sistemi, 0,863 doğru pozitif oranına ve 0,0001 yanlış pozitif oranına sahip bulunmaktadır [10].
2. **Cihaz doğrulaması:** EFB'ye bağlı olan son kullanıcıyı doğrulamak için cihaz doğrulaması yöntemi kullanılmaktadır. Ayrı bir modül olarak tasarlanan bu güvenlik çözümü, son kullanıcı cihazı ile sistem arasındaki iletişimi sürekli olarak izlemekte ve sisteme yetkisiz cihazların bağlanmasını engellemektedir. Saldırgan MAC adresi gibi bilgileri değiştirebileceği için ek bir doğrulama aşamasına, alternatif bir yönteme ihtiyaç duyulmaktadır. Bu güvenlik çözümü, gerçek bir kullanıcının kimlik bilgilerini çalarak sisteme uzaktan yetkisiz erişim sağlayan bir saldırganı tespit etmek ve engellemek için kullanılmaktadır [9]. Saldırganın tespit edilmesinde davranışsal desene dayanan kimlik doğrulama yöntemleri gibi farklı yöntemler tercih edilebilmektedir.

3. **Kod ekleme saldırısı tespiti:** Bu güvenlik yönteminde zararlı kod parçalarını anlayabilmek için ilk olarak literatürdeki saldırı veri tabanları detaylı olarak incelenmektedir. Bu veri tabanlarındaki zararlı kod ekleme saldırıları gözden geçirilerek muhtemel saldırı senaryoları oluşturulmaktadır. Var olan uygulamaların normal hareketleri kaydedilmekte ve makine öğrenmesi tabanlı anomali tespit sistemlerinde kullanılmaktadır. Bu alanda yapılan çalışmalar ağ verileri ve cihaz uygulama hareketleri üzerindeki anomalilerin tespiti olarak ayrılmaktadır. İki durumda da en büyük zorluk normal hareketin belirlenmesi ve anomalilerin sınıflandırılmasıdır.
4. **Kullanıcı doğrulaması:** Sisteme bağlanan kullanıcının doğrulaması ve sistem üzerindeki yetkilerin doğrulanmış kullanıcıya göre belirlenmesi de farklı bir güvenlik çözümüdür. [10] numaralı çalışmada sunulan kullanıcı doğrulama modülü iki farklı bileşenden oluşmaktadır. Bu bileşenlerden birincisi kullanıcının gerçek bir insan mı yoksa bir bilgisayar mı olduğunu ayırt etmektedir. Diğer bileşen ise işlem süresince sürekli bir doğrulama sağlayarak sisteme bağlanan kullanıcının yetkilendirilmiş kullanıcı olup olmadığını kontrol etmektedir. Burada klavye deseni, mouse deseni gibi sürekli doğrulama yapılabilecek davranışsal kimlik doğrulama yöntemleri kullanılabilmektedir [9, 10].

9.8.2. Uçak İletişim Adresleme ve Raporlama Sistemi için Güvenlik Çözümleri

ACARS sisteminin orijinal standardında zorunlu kılınmış veya dahil edilmiş bir güvenlik sistemi olmamasına rağmen, literatürde güvenlik kısıtlarını karşılayan ek sistemler bulunmaktadır. ARINC 823 - ACARS Mesaj Güvenliği (ACARS Message Security - AMS) [21] raporunda ACARS sisteminde kullanılabilecek güvenlik çözümleri için gerekli standartlar verilmektedir. Bu raporda, şifreleme, mesaj doğrulama ve veri bütünlüğü algoritmaları dahil olmak üzere gerekli teknik güvenlik kontrolleri, AMS kullanılarak korunan ACARS mesajları için mesaj formatı ve içeriği, gönderim protokolleri gibi güvenlik çözümleri için gereksinimler tanımlanmaktadır. Sunulan sistemin genel şeması, güvenli mesaj değişimi için gereken güvenlik oturum kurulumu adımı ve mesaj değişim adımı Şekil 9.9'da tanımlanmaktadır.



Şekil 9.9. ACARS mesaj güvenliği

1. ACARS güvenlik sistemlerinden en çok öne çıkanı, Honeywell firması tarafından sunulan, Güvenli ACARS [22] sistemidir. Bu sistem, ACARS iletişimi için şifreleme algoritmalarını kullanarak güvenlik sağlamaktadır. AMS, modern şifreleme yöntemlerini kullanarak mesaj doğrulama, bütünlük ve gizlilik koruma mekanizmaları sağlamaktadır.
2. Ayrıca [23] numaralı çalışmada herhangi bir donanım değişikliği yapılmadan ve mesaj gecikmeleri ile sistemi zorlamadan uçağa eklenebilecek yeni bir çözüm sunulmaktadır. Korumalı ACAR (PACARS) uygulaması, uçtan uca mesaj koruması ve/veya kimlik doğrulaması sağlamak için bir veya daha fazla yer varlığıyla iletişim kurarak sistem güvenliğini sağlamaktadır. ARINC 823 standartlarına uygun bir özet fonksiyon kullanarak hem mesaj gecikmesi hem de genel mesaj boyutunu azaltmaktadır. Bu sistem eliptik eğri kriptografisine dayanmaktadır.

ARINC standartlarında şifreli ACARS kullanımı teşvik edilmektedir [22]. Fakat bu sistemleri kullanmak, ödenecek standart ACARS servis ücretine ek olarak bir ücret gerektirmektedir. Bu durum, koruma sistemlerinin alımını yavaşlatmış ve firmaların korumalı sistem kullanımında isteksiz olmasına neden olmuştur.

9.8.3. Otomatik Bağımlı Gözetim-Yayını Sistemi için Güvenlik Çözümleri

ADS-B sistemine karşı yapılabilecek muhtemel saldırılar göz önünde bulundurularak, sistemlerin güvenliğini sağlamak için çeşitli güvenlik çözümleri önerilmiştir. Literatürde önerilen güvenlik çözümleri, [5] numaralı çalışmada, güvenli konum doğrulama ve güvenli yayın doğrulama olmak üzere iki ana başlık altında incelenmektedir.

1. **Güvenli yayın doğrulaması:** Bu başlık altındaki yöntemler, şifreleme kullanan ve kullanmayan yöntemler olmak üzere iki bölüme ayrılmaktadır. Şifreleme kullanan yöntemler, kablosuz ağlarda da ağın güvenliğini sağlayan en önemli koruma yöntemleri arasındadır. Bu nedenle, ADS-B ağının güvenliğinde de dikkate alınmaktadır. Şifreleme kullanmayan yöntemler ise, temel olarak parmak izi teknolojisi ve yayılım spektrum teknolojisi başlıkları altında incelenmektedir. Bu yöntemler, şifrelemeli yöntemlerin aksine anahtar dağıtım ve yönetim sorunları bulunmamaktadır.
2. **Güvenli konum doğrulaması:** Bu başlık altındaki yöntemler, güvenli yayın doğrulamasından farklı olarak, uçağın pozisyonunun gerçekliğini, diğer katılımcıların konum bilgileri ile çapraz kontrol ederek doğrulamaktadır.

Bu başlıklar kapsamında literatürde, ADS-B sistemlerinin güvenliği için sunulan güvenlik çözümlerine bakacak olursak:

1. **Açık anahtarlı şifreleme:** Literatürde yapılan çalışmalara göre, açık anahtarlı şifreleme yöntemleri arasından Eliptik Eğri Dijital İmza Algoritması (Elliptic Curve Digital Signature Algorithm/ECDSA) yönteminin bu sistemlerde kullanıma en uygun sistem olduğu ve en küçük boyutlu imza uzunluğuna sahip olduğu görülmüştür [24]. Eliptik eğri kriptografisine dayanan farklı veri doğrulama şemaları önerilmiştir [25]. Açık anahtarlı şifreleme yöntemleri kullanıldığından, iletişim taraflarının anahtarı önceden paylaşmasına gerek yoktur. Ancak, açık anahtar şifrelemesinin temel zorluğu, dijital imzalar için açık anahtar altyapısının (PKI) ölçeklenebilirliğini ve maliyetini çözmektir [5].
2. **MAC:** Bu yöntemde, ADS-B'nin mesaj içeriğini korumak için Mesaj Doğrulama Kodu (Message Authentication Code/MAC) ve şifreleme teknolojisi kullanılmaktadır [26]. Kimlik doğrulama şemasında, tüm katılımcılar mesajları açık metin olarak göndermekte ve kimlik doğrulama sağlamak için MAC değeri, normal ADS-B mesajına eklenmektedir.

3. **TESLA:** Zamanlanmış Verimli Akış Kaybına Toleranslı Kimlik Doğrulama (Timed Efficient Flow Loss Tolerant Authentication - TESLA) protokolü geleneksel açık anahtarlı şifreleme yöntemlerinden biridir ve ADS-B ağlarında kimlik doğrulama için kullanılmaktadır [5]. TESLA protokolünün en önemli özelliği, açık anahtarlı bir algoritma değil, gizli anahtarlı bir algoritma kullanmasıdır.
4. **Multilaterasyon:** Bu yöntemde, sistem farklı (en az üç) yer istasyonundan aldığı konum bilgilerinin sinyal varış zamanları arasındaki farkı hesaplayarak uçağın konumunu belirlemek için hiperbolik bir denklem oluşturmaktadır. Bu yöntem, birden fazla sistemin haberleşmesini ve işbirliğini gerektirir ve havadan havaya iletişim senaryoları için uygun değildir.
5. **Kalman Filtresi:** Bu yöntem, sistemin durumunu en iyi şekilde tahmin edebilmek ve sistem giriş-çıkış verilerini gözlemlemek için doğrusal sistem durum denklemini kullanan bir algoritma olarak tanımlanmaktadır. Sivil havacılıkta, uçağın belirlenen rotayı takip edip etmediğinin kontrolünde kullanılmaktadır. Bu yönteme karşı yapılan saldırılarda, saldırgan araya girerek gerçek düğümün sinyalini bozabilir ve yanlış konum bilgisini yavaş bir hızda araya ekleyebilir. Bu şekilde, Kalman Filtresi sinyalin değişimini fark etmez. Ayrıca, bu yöntemde, veri işleme süresi uzun olduğu için karmaşıklık arttıkça hizmet reddi saldırısına (DOS) maruz kalma olasılığı daha da artmaktadır.
6. **Veri Birleştirme:** Bu yöntemde, farklı kaynaklardan edilen veriler aralarındaki ilişki göz önünde bulundurularak birleştirilmektedir. Bu şekilde, tek kaynaklı verilere göre daha doğru ve güvenilir sonuçlar elde edilmektedir. Bu yöntemde, olasılıklı modelleme ve analiz, makine öğrenimi ve bulanık mantık gibi farklı yöntemler kullanılmaktadır [5].
7. **Mesafe Sınırı:** İki uçak arasındaki mesafe verinin iletim süresine göre hesaplanabilmektedir. Araya giren saldırgan bu veri iletimi süresini bozmakta ve bu şekilde saldırı tespit edilebilmektedir. Fakat bu yöntem yüksek hızla giden uçaklar için uygun bir sonuç vermemektedir.
8. **Trafik Modelleme:** Alınan sinyal gücü ile mesafe arasındaki ters orantı kullanılarak, uçağın gerçek konum bilgisine erişilebilir. Bunun yanı sıra, sinyal varış açısı ile sinyal gücü birleştirilerek geçmiş konum bilgileri de kontrol edilebilir.

9. **Parmak izi:** Bu yöntemin üç farklı uygulaması bulunmaktadır. İlk olarak yazılım tabanlı uygulamasında, kablosuz cihaz üzerinde çalışan yazılımlar farklı modları veya davranışlarına göre sınıflandırılmaktadır. Fakat günümüzde çoğu hava yolu şirketi birbirine çok benzeyen yapılar kullanmaktadır. Bu nedenle, farklı sistemleri ayırt etmek zorlaşmaktadır. İkinci olarak donanım tabanlı uygulamasında, donanım farklılıkları aracılığı ile ağ aygıtları sınıflandırılmaktadır. Fakat uzun mesafeli ağlarda sinyallerde bozulmalar olabileceği için uygulaması zorlaşmaktadır. Son olarak kanal tabanlı yöntemde, iletişim kanalının özellikleri kullanılarak bir sınıflandırma gerçekleştirilir.
10. **Yayılma spektrumu:** Bu yöntemde, kanallar arasında rastgele bir geçiş ve rastgele belirlenen bir yayılma kodu kullanılmaktadır. Bu şekilde, saldırganın kanalı dinlemesi ve tıkaması engellenmektedir. Bu yöntemde, taraflar aynı kanalda olmadığı için bant genişliği boşa kullanılmaktadır.

Bu bölümde anlatılan güvenlik çözümleri özellikleri, sağladıkları güvenlik seviyesi, uygulanabilirliği ve engellediği saldırılar göz önünde bulundurularak karşılaştırılmış ve bu karşılaştırma Tablo 9.4'te detaylı olarak paylaşılmıştır.

Tablo 9.4. Sunulan güvenlik çözümlerinin özellikleri [5]

Yöntem	Engellediği Saldırılar	Sağladığı Özellikler	Uygulama	Güvenlik
PKI	Dinleme, Mesaj Ekleme/Silme	Veri ve Konum Bütünlüğü, Güvenilirlik, Kimlik Doğrulama	Zor	Yüksek
MAC	Mesaj Ekleme/Silme	Kimlik Doğrulama	Kolay	Düşük
TESLA	Mesaj Ekleme/Silme	Kimlik Doğrulama	Orta	Orta
Multilaterasyon	Mesaj Ekleme/Silme	Konum Bütünlüğü	Kolay	Düşük
Parmak İzi	Mesaj Ekleme/Silme, DOS Saldırısı	Kimlik Doğrulama, Erişilebilirlik	Orta	Orta
Yayılım Spektrumu	Dinleme, Parazit Oluşturma, DOS Saldırısı	Güvenilirlik, Erişilebilirlik	Çok Zor	Yüksek
Uzaklık Sınırlama	Mesaj Ekleme/Silme	Konum Bütünlüğü	Zor	Düşük
Kalman Filtresi	Mesaj Ekleme/Silme	Veri ve Konum Bütünlüğü, Kimlik Doğrulama	Kolay	Orta
Veri Birleştirme (Füzyon)	Mesaj Ekleme/Silme, DOS Saldırısı	Konum Bütünlüğü, Kimlik Doğrulama, Erişilebilirlik	Kolay	Orta
Trafik Modelleme	Mesaj Ekleme/Silme	Konum Bütünlüğü	Orta	Düşük

9.8.4. Küresel Uydu Seyrüsefer Sistemi için Güvenlik Çözümleri

GNSS sinyalinin bilinmeyen değişikliklere karşı korunması için farklı güvenlik yöntemleri kullanılmaktadır. Bu yöntemler, kimlik doğrulama ve bütünlük özelliklerini sağlamaktadır. Bu şekilde, sisteme karşı yapılan bir sinyal yanıltma saldırısı tespit edilebilmektedir. Literatürde yapılan çalışmalar incelendiğinde, bu alanda farklı yaklaşımların izlendiği gözlemlenmiştir. Bu alanda yapılan çalışmalar temelde iki sınıf altında incelenmektedir [27]:

1. **Kriptografik olmayan yöntemler:** Navigasyon veri erişim kontrol mekanizmaları olarak da adlandırılan bu yöntemler, herhangi bir kriptografik algoritma kullanmadan sinyal gücündeki değişiklikleri tespit etmek veya varış açısını tahmin etmek gibi sinyalin belirli bir özelliğine dayanmaktadır.
2. **Kriptografik yöntemler:** Bu yöntemler, alıcı ile gönderici arasındaki güveni sağlayabilmek, alıcının göndericinin kimliğinden emin olabilmesi veya mesajın gizliliğinin korunması gibi özellikleri sağlamak için kriptografik sistemleri kullanmaktadır. Bu yöntemler, veri bağlantı katmanında veya fiziksel katmanda çalışmaktadır. Bu yöntemleri sisteme entegre edebilmek için protokollerde değişiklik yapmak gerekmektedir. Ayrıca kriptografik sistemler sistemlerde gecikmelere sebep olabilmektedir. Bu da gerçek zamanlı çalışan uygulamalar için bir problem oluşturmaktadır.

GNSS uydu konum belirleme sistemlerini doğrulamak için yukarıda da belirtildiği üzere farklı yaklaşımlar izlenmektedir. İlk olarak sinyallerin saldırıdan bağımsız olarak hava durumu, saat hatası gibi etkenlerle bozulması olasılığına karşı çözüm yöntemleri aramıştır. Bu problemlere çözüm olarak kriptografik olmayan bir yöntem olan Alıcı Otonom Bütünlük İzleme (Receiver Autonomous Integrity Monitoring/RAIM) sistemi sunulmuştur. RAIM, GPS'ten gelen verilerin doğruluğunu belirlemek için kullanılan bir algoritma olarak da tanımlanmaktadır. RAIM algoritması, farklı uydu sistemlerinden elde edilen konum verilerinin tutarlı olduğundan emin olmak için elde edilen verileri kendi aralarında karşılaştırmaktadır. Sinyallerin herhangi birinden elde edilen konum ile diğer sinyallerden hesaplanan konumdan farklı olabilmektedir. Bu durum, o sinyalin alındığı uydudaki saat hatası gibi bir arızadan veya beklenmeyen bir hava durumu değişikliğinden kaynaklanmaktadır. RAIM, birkaç uydunun mesafe ölçümlerini karşı-

laştırarak uydudaki bir arızayı tespit ederek GNSS alıcısının kullanıcısını uyarmaktadır. RAIM kullanmayan bir sistemin GPS konumunun doğruluğu konusunda hiçbir güvencesi bulunmamaktadır [28].

Literatürde yanıltma (spoofing) ve tekrarlama (replay) saldırılarına karşı bir güvenlik önlemi olarak RAIM ve kümeleme algoritmalarını birleştiren bir yaklaşım sunulmuştur [28]. Yapılan çalışmada, DBSCAN algoritması ile RAIM'den elde edilen çoklu uydu verileri kümelenmiştir. Kümeleme algoritmasından elde edilen sonuçlara göre farklı sinyaller aynı anda tespit edilerek yanlış olan bir sinyalin tespit edilebildiği gözlemlenmiştir. Bu çalışmada en az altı uydu sinyalinin bulunduğu durumda aykırı uydu sinyalleri tespit edilebilmektedir. Fakat saldırgan, aynı anda birden fazla uydu sinyalini manipüle edebiliyorsa, RAIM algoritması ile çalışan sistemler bu saldırganın tespitinde problem yaşamaktadır. 2019 yılında sunulan farklı bir çalışmada birden fazla sunucudan doğrulama alan GNSS sinyallerinin, birden fazla sunucuya erişimi ve etkisi olan bir saldırgan tarafından değiştirilme durumu ele alınmış ve buna yönelik çoklu doğrulama çözümü sunulmuştur [29]. Yazarlar sundukları çözümün, algılama olasılığı ve yanlış alarm olasılığı gereksinimleri göz önüne alarak saldırganın, alıcının erişebildiği uydudan daha az uydu sinyalini manipüle ettiği durum için alıcının performansını değerlendirmişlerdir. Ayrıca, saldırgan mevcut tüm uydu sinyallerini manipüle edemediğinde, rastgele ölçüm aralıklarına küçük hatalar eklense bile, sunulan çözüm yönteminin hatalı sinyalleri algılayabildiğini iddia etmektedirler [29].

Kriptografik olmayan yöntemlerin yanı sıra GNSS sistemlerinin güvenliğini sağlayabilmek için farklı kriptografik yöntemlerde sunulmuştur. GNSS'de açık sinyaller için bir kimlik doğrulama mekanizması entegre etmeye yönelik ilk girişim Logan Scott tarafından, Yayılmış Spektrum Güvenlik Kodları (Spread Spectrum Security Codes - SSSC) adı verilen gizli yayılma dizileri ile başlamıştır [30]. Bu yöntem, navigasyon verilerinin kimliği doğrulayarak yanıltma saldırılarına karşı güvenlik sağlarken, tekrarlama saldırılarına karşı bir güvenlik sağlamamaktadır. Navigasyon mesajı doğrulama (Navigation Message Authentication - NMA) şeması bu yöntemler arasında üzerine en çok çalışma yapılan yöntemlerden biri olmaktadır. NMA, navigasyon mesaj akışına doğrulama mesajları ekleyerek hem verinin kaynağı doğrulamakta hem de navigasyon verilerinin kriptografik bütünlüğünün korunmasını sağlamak-

tadır. Bu sayede güvenilir bir şekilde iletişim kurulabilmektedir. Bu sistemlerde kriptografik şifreleme yöntemi olarak açık anahtarlı şifreleme altyapısı kullanılmaktadır. Bu nedenle, anahtar dağıtım mekanizması ve güvenilir bir kurum gereksinimi bulunmaktadır. Örneğin, [31] çalışmasında, açık anahtar altyapısı olarak küçük anahtar ve elektronik imza boyutu nedeni ile ECDSA algoritması uygulanmış ve sistemin performans kısıtları ve gereksinimleri detaylı olarak paylaşılmıştır.

9.9. SONUÇ VE DEĞERLENDİRMELER

Bu kitap bölümünde beş temel sivil havacılık sistem bileşeni ve bu bileşenler özelinde muhtemel siber saldırı senaryoları anlatılmıştır. Ardından bu senaryolara karşı sunulan güvenlik çözümleri incelenmiştir. Havacılık altyapılarındaki yenileme süreci ile beraber birbirine bağımlı hale gelen havacılık bileşenleri daha fazla güvenlik açığına sahip bulunmaktadır. Bu nedenle, bu sistemler üzerindeki çalışmalar artmıştır. Fakat sunulan güvenlik çözümleri havacılık alanındaki katı kısıtlamalar nedeni ile henüz kullanılmamaktadır.

Elektronik uçuş çantası uçuş ekibinin iş gücünü oldukça azaltan bir cihazdır. Fakat dışarıdan tedarik edilmesi üretici tarafından gelebilecek saldırılara açık olduğunu göstermektedir. Ayrıca havaalanında gerçekleştirilen veri aktarımı sırasında yerel ağa bağlanması da sistemin içerisine dışarıdan erişim olanağı sunmaktadır. Bu nedenle, bu alanda saldırıların tespitinde anomali tabanlı sistemler kullanılmaktadır. Ayrıca sistem yazılımları da detaylı olarak test edilmektedir.

Uçak iletişim adresleme ve raporlama sistemi orijinal yapısında herhangi bir şifreleme altyapısı bulunmamaktadır. Daha önceki yıllarda havacılık sistemlerinin daha az birbirine bağımlı olması, sistemler hakkında bilgi edinmenin zor olması ve teknolojik olarak bu sistemlere karşı saldırı düzenleme olasılığının düşük ve maliyetinin yüksek olması nedeni ile bir tehdit alanı olarak görülmemiştir. Fakat son yıllarda internet ortamında havacılık ile ilgili verilere kolayca erişilebilmesi ucuz Yazılım Tanımlı Radyoların (Software Defined Radio - SDR) çıkması bu alandaki tehdit olasılığını arttırmıştır. İnternetten indirilebilen yazılımlar ve düşük maliyetli donanımlar ile ACARS sistemini dinlemek oldukça kolay bir hale gelmiştir. Bu nedenle, bu alanda farklı güvenlik çözümleri sunulmuştur. Fakat ek güvenlik sistemlerinin aynı zamanda ek maliyete sebep olması bu alandaki uygulanabilirliği düşürmektedir.

Aletli iniş sistemine karşı yapılabilecek saldırı senaryoları detaylı olarak araştırılmış ve araştırma sonuçları paylaşılmıştır. Literatürdeki çalışmalara bakıldığında bu alanda çok fazla çalışma olmadığı gözlemlenmiştir. Ayrıca muhtemel saldırı senaryolarına çözüm olarak sunulan bir çalışmaya rastlanmamıştır. Uçuşun en tehlikeli aşamalarından biri olan iniş aşamasında kullanılan kritik bir bileşen olan ILS sistemi daha detaylı olarak araştırılmalı ve muhtemel saldırı senaryolarına karşı yeni güvenlik çözümleri geliştirilmelidir.

Otomatik bağımlı gözetim-yayını sisteminde dışarıdan gelebilecek müdahaleleri kontrol etmek için kullanılan bir güvenlik çözümü bulunmamaktadır. Literatürde sunulan güvenlik yöntemleri incelendiğinde, bir uçağın muhtemel saldırıları tespit edebilmesi için ek sensörler taşıması gerekmektedir. Bu da ek bir maliyet gerektirdiği için genellikle kullanımı tercih edilmemektedir. Bir diğer çözüm yolu ise kriptografik algoritmalar kullanarak iletişim güvenliğinin sağlanmasıdır. Bu tarz güvenlik çözümlerini kullanan sistemlerde, iletişimde şifreleme/şifre çözme gecikmesinden kaynaklanan aksamalar olabilmektedir. Ayrıca protokol tasarımında ve standart ADS-B mesaj formatında bir değişiklik gerektirdiği için uygulaması bulunmamaktadır.

Küresel uydu seyrüsefer sistemi üzerine yapılabilecek muhtemel saldırı senaryoları ve bu senaryolara karşı sunulan güvenlik çözümleri incelendiğinde GNSS sistemine olan güvenin bir zayıflık oluşturabileceğini göstermektedir. Literatürde yapılan bir çalışmada simülasyon testlerinde, GNSS sistemine karşı gerçekleştirilen saldırıların tespit edilemediğini raporlamıştır. Tüm ekipler, GNSS tabanlı navigasyon sisteminin son derece güvenilir olduğunu ve uçuş kariyerlerinde kayda değer herhangi bir arıza ile karşılaşmadıklarını belirtmişlerdir. Bazı pilotlar GNSS sisteminde bir bozulma olabileceği olasılığını bilse de sisteme karşı yapılabilecek saldırılar hakkında bilgi sahibi değillerdir [13]. Bu nedenle, bu alanda havacılık sektörü çalışanlarının muhtemel saldırı senaryolarına karşı eğitilmesi bu alanda önemli bir farkındalık sağlayacaktır. Günümüzde kritik uygulamalarda GNSS'nin kullanımı gittikçe artmaktadır. Bu nedenle, sağlam ve güvenilir GNSS sistemine ihtiyaç duyulmaktadır.

Bu alanda yapılan çalışmalar değerlendirildiğinde, havacılık alanındaki çalışanların muhtemel siber saldırı senaryoları hakkında detaylı olarak bilgilendirilmesi gerektiği görülmüştür. Pilotlara uygulanan periyodik testlerde muhtemel siber saldırı senaryoları da göz önünde bulundurulmalı ve simülasyon testlerinde pilotların siber saldırılara karşı verdikleri tepkiler dikkatle incelen-

melidir. Bu tepkilere göre muhtemel zayıflıklar çıkarılmalı ve bu alanlarda güvenlik zafiyetlerini giderecek yeni çözüm yöntemleri araştırılmalıdır.

Teşekkür

Yazarlardan Nurşah Çevik YÖK 100/2000 Öncelikli Alan Doktora Bursu ile desteklenmektedir.

KAYNAKLAR

[1]. FAA-SESAR, "Nextgen – sesar state of harmonisation report," Single European Sky ATM Research Joint Undertaking-Federal Aviation Administration, Tech. Rep., 2019.

[2]. FAA, "Automatic dependent surveillance-broadcast (ads-b) out performance requirements to support air traffic control (atc) service - final rule," Federal Aviation Administration, ABD, Tech. Rep. 2010-12645, 2010.

[3]. RTCA, "Airworthiness security methods and considerations," Radio Technical Commission for Aeronautics, Tech. Rep. DO-356, 2014.

[4]. NIST, "Guide for conducting risk assessments," National Institute of Standards and Technology, ABD, Tech. Rep. SP 800-30, 2012.

[5]. Z. Wu, T. Shang, ve A. Guo, "Security issues in automatic dependent surveillance - broadcast (ads-b): A survey," IEEE Access, vol. 8, pp. 122 147–122 167, 2020.

[6]. A. Uncu, S. Üzümcü, ve A. A. Mert, "Cyber security concerns regarding federated, partly ima and full ima implementations," in 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), pp. 1–5, 2019.

[7]. A. Damien, M. Fumey, E. Alata, M. Kaaniche, ve V. Nicomette, "Anomaly based intrusion detection for an avionic embedded system," in Aerospace Systems and Technology Conference, 2018.

[8]. EASA, "Best practices for the evaluation and approval of efb applications for aircraft performance calculations and mass and balance," European Union Aviation Safety Agency, Tech. Rep., 2015.

[9]. M. Smith, M. Strohmeier, V. Lenders, ve I. Martinovic, "On the security and privacy of acars," in 2016 Integrated Communications Navigation and Surveillance (ICNS), pp. 1–27, 2016.

[10]. "Internet: Flightradar," https://www.flightradar24.com/41.02,28.99/6, son Erişim Tarihi: 2021-06-11.

[11]. M. Schäfer, V. Lenders, ve I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in Applied Cryptography and Network Security, M. Jacobson, M. Locasto, P. Mohassel, and R. Safavi-Naini, Eds., Berlin, Heidelberg, pp. 253–271, 2013.

[12]. K. D. Wesson, T. Humphreys, ve B. Evans, "Can cryptography secure next generation air traffic surveillance?" IEEE Security and Privacy, 2014.

[13]. F. Ziliang, P. Weijun, ve W. Yang, "A data authentication solution of ads-b system based on x.509 certificate," in 27TH INTERNATIONAL CONGRESS OF THE AERONAUTICAL SCIENCES, pp. 51–55, 2012.

[14]. K. Samuelson, E. Valovage, ve D. Hall, "Enhanced ads-b research," in 2006 IEEE Aerospace Conference, pp. 1–7, 2006.

[15]. R. Bitton, C. Feher, Y. Elovici, A. Shabtai, G. Shugol, R. Tikochinski, ve S. Kur, "A proxy-based solution for securiting remote desktop connections in mission-critical systems," in 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 153–156, 2017.

[16]. R. Bitton ve A. Shabtai, "A machine learning-based intrusion detection system for securing remote desktop connections to electronic flight bag servers," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1164–1181, 2021.

[17]. GAO, "Aviation cybersecurity faa should fully implement key practices to strengthen its oversight of avionics risks," United States Government Accountability Office, Tech. Rep., 2020.

[18]. J. P. Buch, R. Geister, L. Canzian, G. Gamba, ve O. Pozzobon, What the Hack Happened to the Flight Deck: Analyzing the Impact of Cyber Attacks on Commercial Flight Crews. American Institute of Aeronautics and Astronautics, 2019.

[19]. B. A. Hamilton, "Asrs - aviation safety reporting system," BAH, Tech. Rep., 2020.

[20]. H. Sathaye, D. Schepers, A. Ranganathan, ve G. Noubir, "Wireless attacks on aircraft instrument landing systems," in 28th USENIX Security Symposium (USENIX Security 19). Santa Clara, CA: USENIX Association, pp. 357–372, 2019.

[21]. H. Sathaye, D. Schepers, A. Ranganathan, ve G. Noubir, "Wireless attacks on aircraft landing systems: Demo," in Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. Association for Computing Machinery, p. 295–297, 2019.

[22]. Z. Wu, Y. Zhang, Y. Yang, C. Liang, ve R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," IEEE Access, vol. 8, pp. 165, 2020.

[23]. L. Wang, R. Wu, W. Wang, D. Lu, ve Q. Jia, "Joint gnss interference mitigation approach for jamming and spoofing based on multi-antenna array," Journal of Electronics & Information Technology, vol. 38, pp. 2344–2350, 2016.

[24]. A. Roy, "Secure aircraft communications addressing and reporting system (acars)," in 20th DASC. 20th Digital Avionics Systems Conference (Cat. No.01CH37219), vol. 2, pp. 7A2/1–7A2/11, 2001.

[25]. P. E. Storck, "Benefits of commercial data link security," in 2013 Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1–6, 2013.

[26]. ARINC, "Datalink security part 1 – acars message security," Aeronautical Radio Inc, Tech. Rep. 823P1, 2007.

[27]. K. Zhang ve P. Papadimitratos, "Secure multi-constellation gnss receivers with clustering-based solution separation algorithm," in 2019 IEEE Aerospace Conference, pp. 1–9, 2019.

[28]. G. Caparra, N. Laurenti, R. Ioannides, ve C. Massimo, "Improving secure code estimate-replay attacks and their detection on gnss signals," in Navitec 2014, 2014.

[29]. L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003), pp. 1543–1552, 2003.

[30]. Z. Wu, R. Liu, ve H. Cao, "Ecdsa-based message authentication scheme for beidou-ii navigation satellite system," IEEE Transactions on Aerospace and Electronic Systems, vol. 55, no. 4, pp. 1666–1682, 2019.

[31]. K. Zhang, R. A. Tuhin, ve P. Papadimitratos, "Detection and exclusion raim algorithm against spoofing/replaying attacks," in International Symposium on GNSS, 2015.

Bölüm 10

KLAVYE DESENİ İLE KİMLİK DOĞRULAMA

Nurşah Çevik - Sedat Akleylek - Halil İbrahim Çelenli

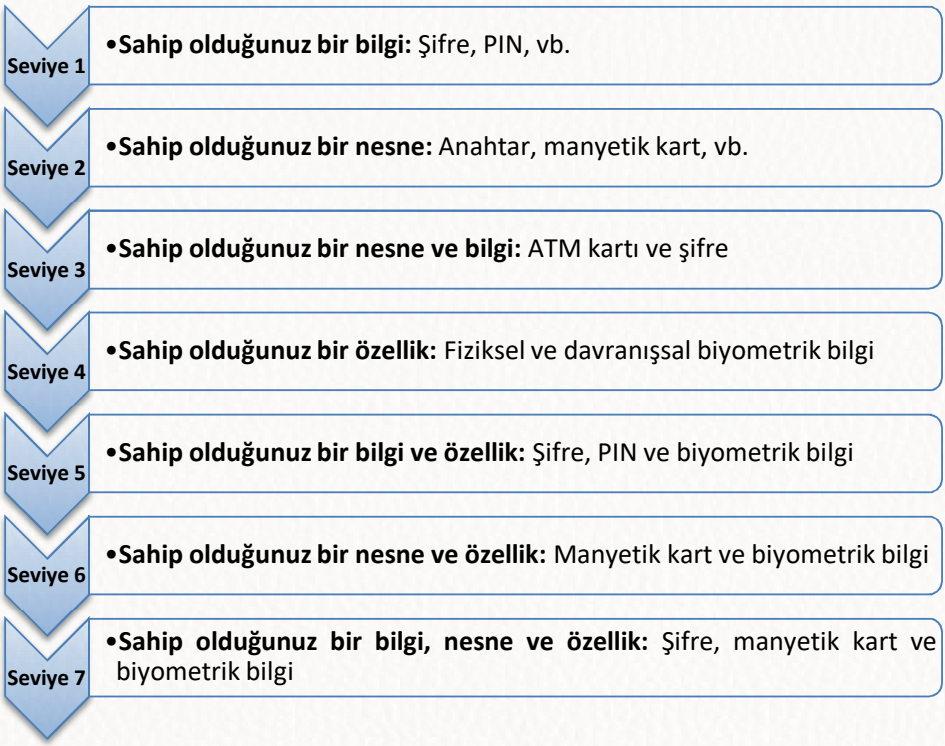
İnternetin hızla yayılması ve birçok işlemin sanal ortama aktarılmasıyla beraber güvenlik problemleri ortaya çıkmış ve bu problemlere karşı farklı güvenlik çözümleri sunulmuştur. Bu güvenlik problemlerinden birisi de haberleşen tarafların birbirlerinin kimliklerini doğrulayabilmesidir. Literatürde, bu probleme çözüm olarak farklı kimlik doğrulama yöntemleri önerilmiştir. Bu yöntemler arasında, biyometrik özelliklere dayanan kimlik doğrulama sistemleri, en çok tercih edilen yöntemler arasında yer almaktadır. Bu yöntem, fiziksel ve davranışsal biyometrik olmak üzere iki gruba ayrılmıştır. Fiziksel biyometrik yöntemler, parmak izi, yüz şekli gibi sabit özelliklerimize dayanırken; davranışsal biyometrik yöntemler, yürüme deseni, klavye deseni gibi zamanla değişebilen özelliklerimize dayanmaktadır. Son on yılda makine öğrenmesi alanındaki gelişmeler, davranışsal yöntemlerin doğruluk oranını arttırmış ve insanların dikkatini bu alana yöneltmiştir. Davranışsal yöntemler arasında, klavye deseni ile doğrulama yöntemi, iki aşamalı doğrulamada, "Kullanıcı adı ve Şifre" yönteminin yanında herhangi bir ek işlem gerektirmeden ikinci aşama kullanılabilmektedir. Bu nedenle, iki aşamalı doğrulamanın kritik olduğu alanlarda klavye desenine dayanan sistemlerin kullanımı artmıştır. Askeri sistemler, bankacılık hizmetleri gibi kimlik doğrulamanın kritik olduğu alanlarda iki aşamalı doğrulama için düşük maliyetli ve uygulaması kolay bir yöntem olarak öne çıkmıştır. Bu kitap bölümü kapsamında, klavye desenine dayanan kimlik doğrulama sistemleri, bu sistemlerde kullanılan algoritmalar ve farklı yaklaşımlar detaylı olarak açıklanmıştır.

10.1. GİRİŞ

Kimlik doğrulama kavramı temelde haberleşen tarafların birbirlerinin kimliklerini doğrulayabilmesi anlamına gelmektedir. Kimlik doğrulama işlemini sağlamak için sahip olunan bir bilgi, eşya veya özellik kullanılmaktadır [1]. Günümüzde birçok sistemde kimlik doğrulama için sahip olunan bir bilgiye dayanan, "Kullanıcı Adı-Şifre" yöntemi tercih edilmektedir. Yalnızca "Kullanıcı Adı-Şifre" kullanan sistemler, tek aşamalı bir kimlik doğrulama işlemi gerçekleştirmektedir. Bu durumda şifrenin basit seçilmesi, başkası ile paylaşılması, başkası tarafından ele geçirilmesi veya farklı sistemlerde benzer şifrelerin kullanılması gibi çeşitli kullanıcı hatalarından dolayı kabul edilebilir bir güvenlik seviyesi sağlanamamaktadır [2]. Kritik sistemlere olan yetkisiz girişlerin verdiği zararlar ve itibar kayıpları göz önüne alındığında; kimlik doğrulama sistemleri üzerine yapılan çalışmaların değerli olduğu görülmektedir. Bu nedenle, gereken güvenlik seviyesini sağlayabilmek ve yetkisiz erişim ihtimalini düşürmek için ek kimlik doğrulama aşamalarına ihtiyaç duyulmaktadır. Şekil 10.1'de gösterildiği üzere, "Kullanıcı Adı-Şifre" gibi sahip olunan bir bilginin yanı sıra parmak izi gibi sahip olunan bir özellik ve/veya akıllı kart gibi sahip olunan bir eşyanın beraber kullanıldığı çok aşamalı yöntemlerin kullanılması önerilmektedir.

Şekil 10.1. Kimlik doğrulama aşamaları

Çok aşamalı kimlik doğrulama işlemi kritik sistemlerde zorunlu olmasının yanı sıra günümüzde kritik olarak adlandırılmayan birçok alanda da kişisel verilerin güvenliği için kullanımı oldukça önemlidir. Çok faktörlü kimlik doğrulama yöntemlerinin kullanıldığı sistemler, kullanılan yöntemlere göre farklı güvenlik seviyelerine ayrılmaktadır. Şekil 10.2'de, güvenlik seviyeleri gösterilmektedir.



Şekil 10.2. Çok faktörlü kimlik doğrulamada güvenlik seviyesi

Şekil 10.2'de tanımlanan seviyelere bakıldığında, güvenlik seviyesi arttıkça sistemin kullanımının zorlaştığı, kullanıcının fazladan işlem gerçekleştirdiği, kullanıcı dostu olmayan bir sistem tasarımı oluştuğu gözlemlenmiştir. Bu nedenle, sistemin sağlaması gereken güvenlik seviyesi, sistemin kullanım sıklığı ve kullanıcı profili gibi özellikler göz önünde bulundurularak kimlik doğrulama yöntemlerinin belirlenmesi en uygun seçenek olacaktır. Günümüzde çok faktörlü kimlik doğrulama için "SMS" ile doğrulama yönteminin hala kullanılan yöntemlerden biri olduğu görülmüştür. Son yayınlanan BDDK mevzuatı [3] gereğince ikincil doğrulama için uygun olmaması, kullanıcı için ekstra bir işlem gerektirmesi ve atılan mesaj başına bir maliyet içermesi bu sistemin gelecekte kullanılmayacağını göstermektedir. Bu nedenle bu alanda farklı yaklaşımlara gerek duyulduğu bilinmektedir. Bu alanda yapılan çalışmalar incelendiğinde, biyometrik özelliklerimizin çok aşamalı doğrulama için en çok tercih edilen yöntemlerden biri olduğu görülmüştür.

Literatürde, biyometrik özelliklerimiz, fiziksel ve davranışsal biyometrik özellikler olmak üzere iki temel gruba ayrılmaktadır. Fiziksel biyometrik özelliklerimiz, göz, yüz, parmak izi gibi sabit fiziksel özelliklerimize dayanırken; davranışsal biyometrik özelliklerimiz klavye deseni, fare deseni gibi kişilerin fark etmeden birbirinden farklı olarak gerçekleştirdiği davranışlar üzerine kurulmuştur. Fiziksel biyometrik özellikleri kullanan kimlik doğrulama sistemlerinde ek sensor kullanımı gerekmekte, ayrıca kullanıcıdan ek bir işlem talep edilmektedir. Fakat davranışsal biyometrik özellikleri kullanan sistemlerde kullanıcı deneyimini etkilemeden ikincil bir kimlik doğrulama faktörü sağlamaktadır. Bunun yanı sıra ek sensor kullanımı gerekmektedir.

Klavye, fare kullanımı ve yürüme deseni gibi özellikleri içinde barındıran davranışsal biyometrik sistemler günümüzde kamu ve özel sektörde kritik sistemlerin güvenliğinde kullanılmaktadır. Bu yöntemler arasında klavye desenine dayanan kimlik doğrulama sistemleri makine öğrenmesi alanındaki ilerlemeler sayesinde yüksek bir doğruluk ile yapılmaya başlanmıştır [4]-[7]. Bu nedenle, diğer biyometrik özellikler arasında uygun bir alternatif haline gelmiştir. Yeni yayınlanan BDDK mevzuatındaki çok aşamalı doğrulama sistemleri için gerekli kısıtlara uyumlu bir sistem olduğu için Finans ve Bankacılık gibi güvenliğin kritik olduğu alanlarda tercih edilebilir bir alternatif haline gelmiştir [3].

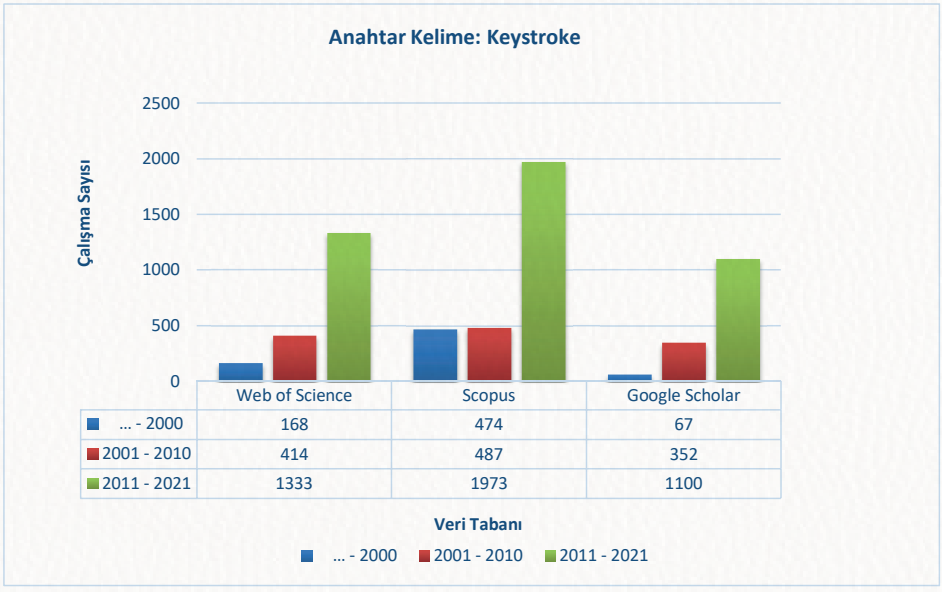
Bu kitap serisinin daha önce yayınlanan 3. Cilt 13. Bölümde biyometrik sistemlerin genel bir güvenlik analizi verilmiş ve kimlik doğrulama uygulamalarında kullanımı ve güvenlik tehditleri detaylandırılmıştır [8]. Ardından 4. Cilt 5. Bölümde, davranışsal biyometrik sistemler üzerine bir çalışma paylaşılmıştır [9]. Bu kitap bölümlerinde de kısaca bahsedilen tuş vuruş dinamikleri, başka bir ifade ile klavye desenine dayanan kimlik doğrulama işlemi burada detaylı olarak paylaşılmaktadır. Diğer bölümlerden farklı olarak bu çalışmada yalnızca klavye desenine dayanan kimlik doğrulama sistemleri üzerine odaklanılmış ve bu alanda kapsamlı bir değerlendirme sunulmuştur. İlk olarak literatür özeti ve bu alandaki yayın sayılarına odaklanılmıştır. Ardından sistemin uygulanışı, kayıt ve doğrulama aşamaları analiz edilmiş ve sistem değerlendirilmesinde tercih edilen metrikler paylaşılmıştır. Son olarak, sonuç ve gelecek çalışmalar verilerek çalışma sonlandırılmıştır.

10.2. LİTERATÜR ÖZETİ

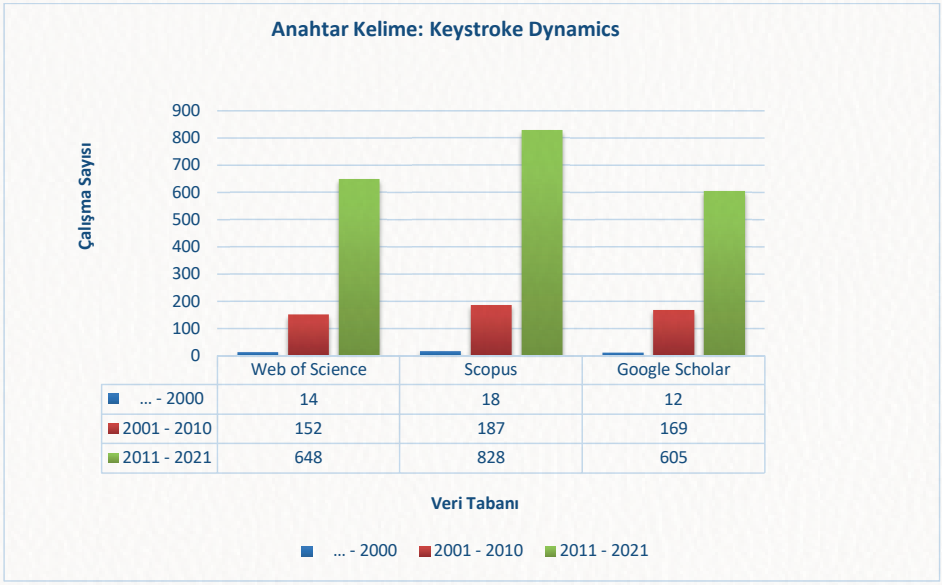
Klavye desenine dayanan kimlik doğrulama yöntemi yeni bir yöntem değildir. Fakat son on yıl içerisinde makine öğrenmesi alanındaki gelişim ve makine öğrenmesi algoritmalarının kullanıcı deseni tanımlanırken kullanılması alandaki başarım oranını yükseltmiş ve bu yöntem kullanılabilir bir seçenek haline getirmiştir. Bu sistemlerin doğruluk oranının hızla artması akademik çevrelerin de ilgisini çekmiş ve bu alandaki çalışmaların ortalama %70'i son on yıl içerisinde yapılmıştır.

10.2.1. Yapılan Yayın Sayıları

Güncel veri tabanlarında, klavye dinamikleri üzerine yapılan çalışmalar aratıldığında son on yıldaki artış araştırılmıştır. En sık kullanılan Web of Science, Scopus ve Google Scholar bilimsel atıf veri tabanlarında "Keystroke" ve "Keystroke Dynamics" anahtar kelimeleri aratılmış ve sonuçları sırasıyla Şekil 10.3 ve Şekil 10.4'te paylaşılmıştır.



Şekil 10.3. Keystroke – literatürdeki çalışmaların yıllara göre dağılımı



Şekil 10.4. Keystroke Dynamics – Literatürdeki çalışmaların yıllara göre dağılımı

10.2.2. Önceki Çalışmalar

Klavye dinamikleri ile kullanıcı tanımlama alanındaki ilk yaklaşım 1800'lerin ortalarında telgrafçılar tarafından ortaya getirilen bir konudur. Bir telgraf üzerinde çalışan operatörlerin birbirinden farklı dokunma özellikleri olduğu ve bu özelliklere bakılarak hangi operatörün telgrafı göndermiş olduğuna dair tahminlerde bulunulabildiği fikri ortaya çıkmıştır [10]. Literatürde 1970'lerden itibaren, klavye dinamikleri kullanılarak kullanıcıları tanımak ve doğrulamak için çalışmalar yapılmaya başlanmıştır [11, 12]. 1980'lerde kullanıcılardan toplanan sabit metinler üzerinden kullanıcıları tanımak ve doğrulamak için farklı istatistiksel yöntemler kullanılmıştır [13, 14]. İstatistiksel yöntemler kullanıcının klavye dinamikleri ile yeni giriş arasındaki mesafeyi hesaplayarak, girişin bir anomali/saldırı olup olmadığını tespit etmektedir [28]. Bunun için klasik Öklit uzaklığı veya Manhattan algoritması gibi yöntemler kullanılmaktadır. Günümüzde, bu alandaki en büyük problem, paylaşılan bir veri tabanı bulunmadığı için, sunulan yöntemlerin başarımlarının karşılaştırılamaması olmuştur. Bu probleme çözüm olarak, Killourhy ve arkadaşları, sabit bir şifre üzerinden 51 farklı kullanıcıdan toplamda 20400 klavye girişi

toplamış ve topladıkları klavye verilerini açık olarak paylaşmıştır. Bu veri tabanı (CMU) literatürde karşılaştırma veri tabanı olarak kullanılmaya başlanmıştır [4]. Bu veri tabanı oluşturulurken, kullanıcılar daha önce tanımlanan şifre bilgisini 8 farklı oturumda her oturumda 50 defa olmak üzere toplamda 400 kere yazmış ve toplamda 20400 veri elde edilmiştir.

2010 yılına kadar, bu sistemlerin doğruluk oranlarının fiziksel biyometrik özelliklere göre oldukça düşük olması ve bilgisayar kullanımının ve internetin günümüzdeki kadar yaygın olmaması nedeni ile bu alandaki çalışma sayısında yavaş bir artış görülmüştür. 2010 yılından sonra, klavye dinamikleri ile kimlik doğrulama sistemlerinde makine öğrenmesi yöntemlerinin kullanılmaya başlanmıştır. Makine öğrenmesi yöntemleri, sistemlerin doğruluk oranlarını yükselttiği için bu alandaki çalışma sayısını da arttırmıştır [4-7]. 2011 yılında Giot tarafından yayınlanan çalışmada, bu alandaki çalışmalar, klavye dinamiklerinin topolojisi ve o zamana kadar yapılan çalışmaların sonuçları detaylı olarak paylaşılmıştır [15]. Literatürdeki çalışmalar, uzun metin/kısa metin, sabit metin/değişken metin ve sürekli rastgele metin/tek seferlik sabit metin doğrulaması gibi farklı alt başlıklar altında incelenmiştir. Fakat makine öğrenmesi yöntemleri günümüzdeki kadar başarılı olmadığı için, çalışmada bu yöntemler üzerine detaylı uygulamalar paylaşılamamıştır. 2012 yılında Zhong ve arkadaşları tekrar eden kısa şifre dizilerini içeren CMU veri tabanında, yeni mesafe metriklerini değerlendirmiştir. Bu metriklerin geleneksel mesafe algoritmalardan daha iyi sonuçlar verdiğini ve hata oranı ERR'yi %8.40'a düşürdüğünü göstermiştir [16]. Monaco ve arkadaşları, üniversitede öğrencilerin ödev yaptıkları çevrim içi bir sistem üzerinden uzun ve serbest metinlerin klavye sürelerini toplamış ve bu metinler üzerinden %91,5 doğruluk oranı ile kullanıcı desenlerini tanımlamıştır [17]. Teh ve arkadaşları 2013 yılında yaptıkları çalışmada [2], 1980-2012 yılları arasında klavye dinamiklerinin çıkış noktası ve günümüzdeki sistemlere ve makine öğrenmesi yöntemlerine geçiş aşamalarını detaylı olarak anlatmıştır. Yapılan çalışmalardaki veri toplama yöntemleri, kullandıkları sınıflandırma algoritmaları, özellik çıkarımları ve kullandıkları protokollere göre sistemleri karşılaştırmış ve sistemlerin başarım ölçütlerini vermiştir. Başarım ölçütü olarak doğruluk oranının yanı sıra verimlilik, değişime uyumluluk ve kullanıma uygunluk gibi kriterlerin göz önünde bulundurulması gerektiğini belirtmiştir. Ayrıca, klavye dinamiklerinin, düşük uygulama bedeli, kullanıcı deneyimini etkilememesi ve kolaylıkla sistemlere entegre edilebilmesi gibi özellikleri nedeni ile iki aşamalı doğrulamada kullanıma uygun olduğunu belirtmiştir [18]. Literatürdeki diğer çalış-

malardan farklı olarak, Deng ve arkadaşları, eğitim aşmasında saldırgan hareketlerine ihtiyaç duymadan çalışan Gaussian Mixture Model (GMM-UBM) ve Deep Belief Nets (DBN) modellerini geliştirmiştir. Yazarlar, önerdikleri modellerin eğitim ve test aşamalarında diğer yaklaşımlara oranla daha hızlı çalıştığını ve sürekli doğrulamanın kullanıldığı sistemlerde yüksek başarımla çalışacağını belirtmişlerdir. Ayrıca, modeller bu alandaki karşılaştırma veri tabanı olan CMU veri tabanına uygulandığında, hata oranında bir azalma olduğunu göstermişlerdir [19]. Tappert ve arkadaşları tarafından yapılan çalışmada uzun metinler üzerinden kimlik doğrulama yapılmış ve devamlı ve tekrar eden metinlerin kimlik doğrulama sistemlerinde verdiği sonuçlar karşılaştırılmıştır [20]. Klavye dinamiklerinin kullanıcının biyometrik bilgilerini barındırması nedeni ile farklı güvenlik problemleri konuşulmaya başlanmıştır. Bu probleme bir çözüm olarak, Wesolowski ve Porwik yaptıkları çalışmada, kullanıcılardan sürekli olarak serbest metinler üzerinden veri toplamış ve kullanıcıların verilerinin korunması için, şifrelenmiş klavye dinamiklerine dayalı bir kullanıcı deseni oluşturma yöntemi tanımlamıştır [21]. 2015 yılında Ali ve arkadaşları sundukları çalışmada,1980 ve 2014 yılları arasındaki çalışmaları analiz etmiş ve veri toplama cihazlarının algoritmaların başarım oranları üzerindeki etkisini göstermiştir [22]. Bunun yanı sıra, literatürdeki çalışmalarda sistemlerin çalışma zamanına (verimliliklerine) yeteri kadar ilgi gösterilmediğini belirtmiştir. Kimlik doğrulama işleminin gerçek zamanlı bir işlem olması ve sistemin uygulanabilir olması için verimliliğin oldukça önemli bir kısıt olduğuna dikkat çekmiştir [22]. Pahuja ve Nagabhushan tarafından sunulan çalışmada, klavye dinamiklerine dayanan kimlik doğrulama sistemlerinin iki ana problemine değinilmiştir [5]. Birincisi, zaman içinde insan davranışlarının değişkenlik göstermesi; ikincisi, doğru sonuçların değerlendirmesi için standartlaştırılmış bir protokolün bulunmamasıdır [4]. Aynı şekilde, Raul ve arkadaşları da bu alandaki sistemlerin performanslarının hala geliştirmeye açık olduğu söylemiş ve bu alandaki en büyük problemin, yeterli elemana ve gerekli özelliklerin hepsine sahip kapsamlı bir veri kümesinin bulunamaması olduğu belirtmiştir [23]. 2009 yılında sunulan CMU veri tabanı eskimesine rağmen, literatürdeki en kapsamlı veri tabanı olduğu için günümüzdeki çalışmalarda hala kullanılmaktadır. Singh ve arkadaşları, 2020 yılında sundukları çalışmada CMU veri tabanında XGBoost algoritmasını kullanarak kurdukları modelin literatürdeki diğer algoritmalar ile karşılaştırıldığında %93,59 ile en yüksek doğruluk oranını verdiğini göstermişlerdir [24]. Son zamanlarda yayınlanan çalışmalarda, klavye dinamiklerine dayanan sistemlerde farklı öz-

niteliklerin çıkarılması üzerine çalışmalar yapılmaya başlanmıştır. Boz tarafından yapılan çalışmada, serbest metin üzerinde tuşların bölgesel dağılımları da öznitelik olarak alınmış ve klavye deseni ile kimlik doğrulama işlemi gerçekleştirilmiştir. Farklı öznitelik kümeleri üzerinde çalışmalar yapılmış ve en verimli sonucu elde etmek için çok katmanlı bir yapay sinir ağı kullanılmıştır [25]. Porwik tarafından yapılan çalışmada, herhangi bir metne bağımlı olmadan arka planda sürekli bir doğrulama gerçekleştiren bir yöntem sunulmaktadır. Bu çalışmada sınıflandırıcıların dinamik seçimi kullanılarak biyometrik verilerin analizini yapan bir yöntem önerilmiş ve deneyin sonuçları Wilcoxon ve Bayes istatistiksel testleri ile kontrol edilmiştir [26].

Son yıllarda derin öğrenme algoritmalarının ses analizi, yüz tanıma gibi alanlarda sağladığı yüksek başarım oranları nedeni ile klavye dinamiklerine dayanan sistemlerde de bir alternatif olarak görülmeye başlanmıştır [27]. Altwaijry sunduğu çalışmada, CMU veri tabanı üzerinde Konvansiyonel Sinir Ağlarını kullanmış ve ortalama hata oranını düşürdüğünü göstermiştir [28]. Fakat CMU veri tabanı gibi yalnızca sabit bir şifreden elde edilen bir veri üzerinde derin öğrenme yöntemlerinin kullanılmasındansa, oturum süresince toplanan kullanıcı klavye verilerinden oluşan bir veri tabanı üzerinde derin öğrenme algoritmalarının daha başarılı sonuçlar vereceği öngörülmektedir [29].

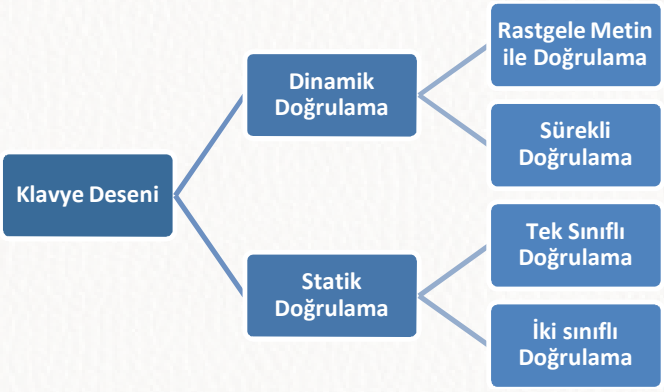
Teknolojinin ve internetin hızlı gelişimi ile mobil cihazların hayatımızdaki yeri oldukça artmıştır. Mobil cihazların kullanımındaki artış, bu alandaki güvenlik gereksinimlerini de beraberinde getirmiştir [30]. Bu gereksinim dahilinde, klavye dinamikleri kimlik doğrulama alanında kullanılabilir bir seçenek olarak öne çıkmış ve bu alanda yapılan çalışmalar artmıştır. Mobil cihazlar üzerinde, klavye desenine dayanan kimlik doğrulama yöntemlerini uygulamak için farklı çalışmalar yapılmaya başlanmıştır [30-32]. Burada klavyeler sanal olduğu ve ekran üzerinden dokunma ile anlaşıldığı için farklı yazılımsal altyapıların kurulması gerekmektedir. Klavye deseni ile benzer şekilde mobil klavyelerde de tuşa dokunma ile tuşu bırakma zamanı ve tuş kodu sisteme kaydedilmektedir. Normal klavyelerde olduğu gibi mobil cihazlarda da zaman hassasiyeti klavye deseninin performansını büyük oranda etkilemektedir. Bunların yanı sıra, geleneksel bilgisayar klavyelerinden farklı olarak, birçok gömülü sensör içermektedir [31]. Modern mobil cihazlar dokunmatik ekran, ivmeölçer, jiroskop, manyetometre, kamera, parmak tarayıcı, mikrofon, GPS, yakınlık sensörü, duyma oranı sensörü, hareket sensörü, barometre gibi özellikleri içerebilmektedir. Bunların arasında, dokunmatik ekran sen-

sörleri, ivmeölçer ve jiroskop özelliklerinin mobil cihazlarda kullanıcı kimliğinin doğrulamasında kullanılabileceği gösterilmiştir [26,33]. Zhong yaptığı çalışmada, bu özelliklerin yanı sıra dokunma sensörünün farklı özelliklerinden yararlanmak için uygun teknolojiler geliştirilirse, mobil cihazlar yüksek güvenlik elde etme konusunda büyük potansiyele sahip olduğunu belirmiştir.

Literatürdeki çalışmalar incelendiğinde gelecekte iki aşamalı doğrulamanın birçok sistem için zorunlu hale geleceği görülmüştür. Klavye dinamiği kullanılarak yapılan kimlik doğrulama sistemlerinin kullanım kolaylığı, makine öğrenmesi yöntemleri ile doğruluk oranlarının yükselmesi ve kullanıcıyı rahatsız etmemesinden dolayı iki aşamalı doğrulama sistemleri için güçlü bir alternatif olduğu gözlemlenmiştir.

10.3. KLAVYE DESENİNE DAYANAN KİMLİK DOĞRULAMA SİSTEMLERİ

Klavye desenine dayanan kimlik doğrulama sistemlerinin farklı uygulama alanları ve yöntemleri bulunmaktadır. Bu bölüm kapsamında, klavye desenine dayanan kimlik doğrulama sistemlerinde kullanılan farklı yöntemler tanımlanmaktadır. Yapılan çalışmalar incelendiğinde klavye yöntemine dayanan sistemlerin, doğrulama yöntemine göre dinamik ve statik olmak üzere iki temel gruba ayrıldığı gözlemlenmiştir [15]. Klavye desenine dayanan kimlik doğrulama sistemlerinin doğrulama yöntemine göre sınıflandırılmış hali Şekil 10.5'te gösterilmektedir.



Şekil 10.5. Klavye deseni topolojisi [15]

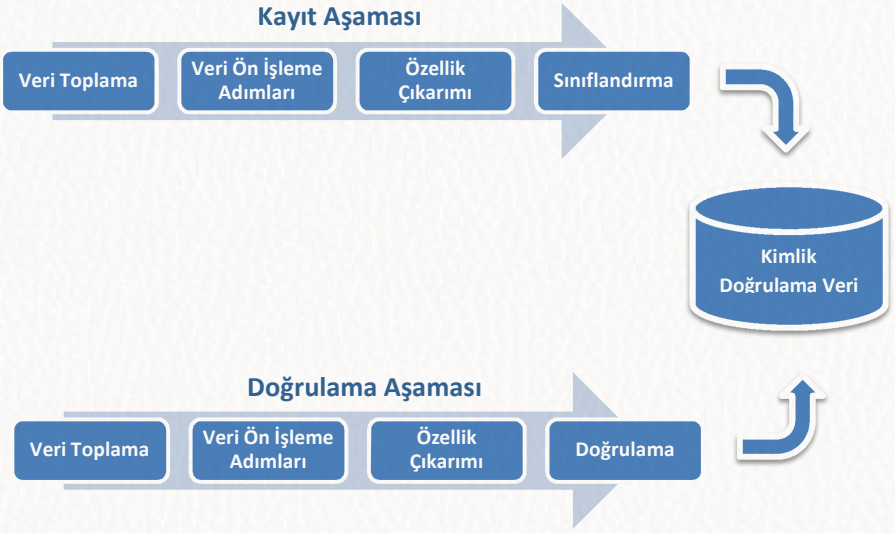
Dinamik kimlik doğrulama yöntemlerinde, kullanıcı sistemde aktif olduğu sürede kullanıcının klavye deseni kaydedilmekte ve eş zamanlı bir kimlik doğrulama sağlanmaktadır. Bu yöntem özellikle, uzaktan eğitim, uzaktan sınav gibi bütün aşamalarda tek kullanıcının aktif olması beklenen durumlarda kullanılmaktadır. Dinamik doğrulama sistemlerinde iki farklı yaklaşım kullanılmaktadır. İlk yaklaşımda, kullanıcıdan oturumu süresince belirli aralıklarla rastgele metin/şifre girmesi talep edilerek dinamik doğrulama işlemi gerçekleştirilmektir. Bu yöntem periyodik doğrulama olarak da adlandırılmaktadır. Bu yöntem sabit bir metne bağlı değildir. Birden çok girdi ile uygulanabilir ve herhangi bir girdi için doğrulama gerçekleştirebilir. İkinci yaklaşımda ise, sürekli bir şifre yazma gibi ek görevler gerçekleştirmeye gerek kalmadan kullanıcı kimliği doğrulanabilmektedir. Bu yaklaşımda, kullanıcı klavye hareketleri oturum süresince kaydedilmekte ve bu veriler kullanılarak kullanıcı klavye deseni oluşturulmaktadır. Bu sayede herhangi bir saldırgan, periyodik doğrulama yöntemine göre daha hızlı tespit edilebilmektedir. Kullanıcı klavye deseni bütün oturum boyunca kaydedilmekte ve anomaliler tespit edilmektedir. Bu sistemler, günümüzde de yaygın bir şekilde kullanılan uzaktan eğitim ve uzaktan çalışma gibi alanlarda, kimlik doğrulama gereksiniminin bulunduğu durumlarda kimlik doğrulama için kullanılmaktadır. Fakat bu yöntemde yüksek miktarda veri depolama alanına ve işlem gücüne ihtiyaç duyulmaktadır [15].

Statik kimlik doğrulama yöntemlerinde, Klasik olarak kullanılan, literatürde de üzerine en çok çalışma yapılan alan kısa metne/şifreye dayalı bir yöntem ile kullanıcı kimliğinin tespit edilmesidir. Bu çalışmalarda, kullanıcılar tarafından birçok kez tekrarlanan tek bir sözcük veya şifre gibi karakter dizileri analiz edilmektedir [26]. Burada girilen metin genellikle 8 ile 20 karakter arasında sınırlıdır. Diğer yöntemlerde ise kimlik doğrulama aşamasında uzun metinler kullanılmaktadır. Statik yöntemlerde tek sınıflı ve iki sınıflı doğrulama olmak üzere iki farklı doğrulama yöntemi kullanılmaktadır. Tek sınıflı doğrulama yöntemlerinde, bir kullanıcı deseni belirlenmekte ve anomaliler, aykırı değerler tespit edilmektedir. İki sınıflı doğrulama yöntemlerinde ise tek sınıflı yöntemlerin aksine geçerli kullanıcı klavye girdilerinin yanı sıra kullanıcıya ait olmayan klavye girdilerine de ihtiyaç duyulmaktadır. Bu nedenle, tek sınıflı yöntemlere göre daha az tercih edilmektedir [34]. Obaidat ve arkadaşları, kişiler veriler üzerinden statik doğrulama ile ilgili kapsamlı bir değerlendirme sunmuştur [35].

Uzun metin kullanan statik kimlik doğrulama yöntemlerinde, kullanıcı kimliği analiz edilirken, daha önce hazırlanmış sabit bir metin veya kullanıcının tercih ettiği uzun bir metin kullanılmaktadır. Uzun metinlerde aynı paragrafı kullanarak kullanıcı tespiti yapma yaklaşımı, gerçek yaşam durumlarından oldukça uzaktır. Bu nedenle, dinamik doğrulama yöntemlerinden rastgele metin yöntemi tercih edilmeye başlanmıştır. Bu yöntemin dezavantajı ise verileri yönetmek için daha fazla çaba gerektirmesidir [36].

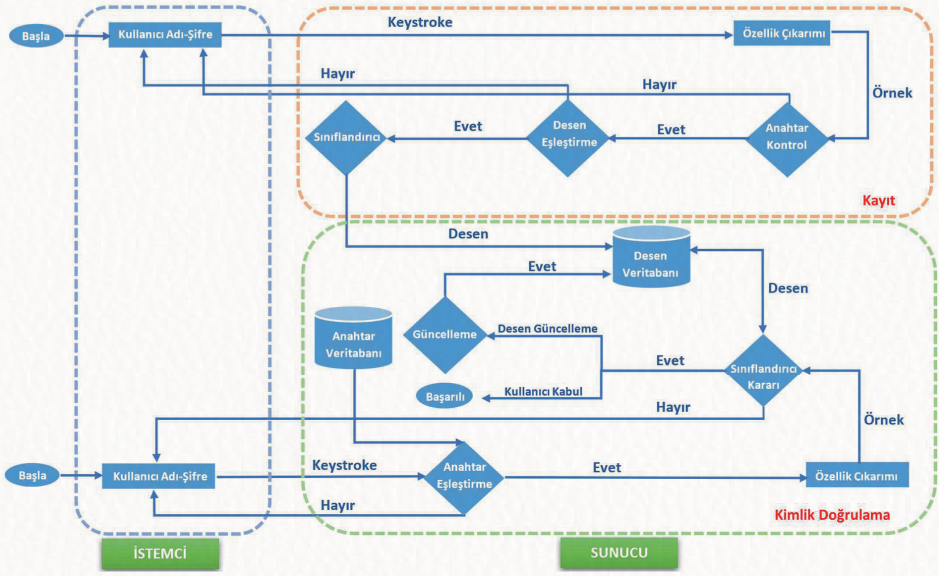
10.3.1. İşlem Akışı

Bir kimlik doğrulama sistemi, kayıt ve doğrulama olmak üzere iki ana bölümden oluşmaktadır. Kayıt ve doğrulama aşamaları ise 4 adımdan meydana gelmektedir. Bu dört adımın ilk üçünde benzer işlemler gerçekleştirilmektedir. İlk adımda, kullanıcının klavye verileri toplanmaktadır. İkinci adımda, veri içerisindeki gürültüler ve sapmalar temizlenmekte, veri ön işleme adımları gerçekleştirilmektedir. Üçüncü adımda, özellik çıkarımı yapılmaktadır. Kayıt aşamasının son adımında veriler sınıflandırılarak kimlik doğrulama veri tabanına kaydedilirken; doğrulama aşamasında kullanıcıdan toplanan klavye verilerinin, kimlik doğrulama veri kümesindeki ilgili kayıt ile eşleşip eşleşmediği kontrol edilmektedir. Sistemin kayıt ve doğrulama aşamalarındaki işlem akışı Şekil 10.6'da paylaşılmaktadır.



Şekil 10.6. Klavye deseni ile kimlik doğrulama aşamaları

Literatürde klavye deseni ile kimlik doğrulama yöntemi en çok, kullanıcı kayıt ve giriş ekranlarında şifre bilgisinin yanı sıra ikincil bir doğrulama ya da risk değerlendirmesi sunmak için kullanılmaktadır. Şekil 10.7'de "Kullanıcı Adı-Şifre (Parola)" bilgisine dayanan, kayıt ve doğrulama aşamalarını kapsayan örnek bir sistem şeması sunulmaktadır.



Şekil 10.7. Örnek-Klavye deseni ile kimlik doğrulama şeması

Şekil 10.7'de bakıldığında anahtar ve desen veri tabanının sunucuda tutulduğu bir sistem şeması sunulmaktadır. Bu sistemde, kayıt ve doğrulama girişi olmak üzere iki farklı başlama noktası bulunmaktadır.

1. İlk adımda, sistemde bulunmayan bir kullanıcı sisteme kaydolmaktadır.
   a. Bu aşamada sistem kullanıcının klavye bilgilerini toplayarak bir kullanıcı deseni oluşturmaktadır.
   b. Kullanıcı deseni, kullanıcı kayıt ekranında kullanıcı adı ve şifre bilgisini girerken bastığı tuşları ve tuşlar arası geçiş zamanlarını göz önünde bulundurarak oluşturulmaktadır.
   c. Kullanıcının kayıt aşamasında iki kere girdiği şifre (Anahtar/Parola) bilgisi eşleşmiyorsa kullanıcıdan yeniden giriş talep edilmektedir.

d. Ardından bu iki girişin klavye desenleri karşılaştırılmaktadır. Bu iki desen arasında büyük bir farklılık varsa kullanıcıdan yeniden giriş talep edilecektir. İlk aşamada kullanıcı hakkında kısıtlı veriye sahip olduğumuz için kullanıcının ilk iki girişi kullanıcı deseninin tanımlanmasında kritik öneme sahip bulunmaktadır.
e. Desenler eşleştikten sonra kullanıcı modeli eğitilmekte ve kullanıcı deseni desen veri tabanına kaydedilmektedir.

2. İkinci adımda, sistemde kayıtlı bir kullanıcı sisteme giriş yapmak istemektedir.
   a. İlk adımda klasik şifre doğrulama işlemi gerçekleştirilmektedir.
   b. Ardından şifrenin doğru olduğu durumda kullanıcının klavye bilgileri alınarak özellik çıkarımı yapılmaktadır.
   c. Özellik çıkarımının ardından elde edilen veri sınıflandırıcıya iletilmekte ve sınıflandırıcı, yeni girilen kullanıcı deseni ile veri tabanındaki kullanıcı desenini karşılaştırarak bir karar vermektedir.
   d. Şekil 10.7'de sunulan örnekte, kimlik doğrulama aşamasında iki ihtimal bulunmaktadır. İlk ihtimalde, kullanıcı sınıflandırıcının sonucuna göre kabul edilmekte ve kullanıcının son girişi veri tabanına eklenerek desen güncellenmektedir. İkinci ihtimalde ise, kullanıcı deseni eşleşmediği için kullanıcı sisteme kabul edilmemektedir. Fakat kullanıcı deseninde zaman içinde değişiklik olabilmesi, klavye değişiminin olması veya yorgunluk, heyecan, stres gibi durumların kullanıcının yazma desenini etkileyebilmektedir. Bu nedenle, kullanıcıyı reddetme seçeneği genellikle tercih edilmemektedir. Burada farklı risk değerlendirme metrikleri kullanılmakta ve kullanıcının erişim alanlarının ve hareketlerinin kısıtlanması gibi yaklaşımlar uygulanmaktadır.

10.3.2. Kayıt Aşaması

Bir kimlik doğrulama sisteminin kayıt aşamasında, kullanıcı sisteme kaydedilmekte ve kullanıcının yazma deseni veri tabanına eklenmektedir. Örneğin, kısa metin üzerinden doğrulama işlemi gerçekleştiren sistemlerde, kullanıcı sisteme kaydolurken kullanıcıdan "Kullanıcı Adı-Şifre (Parola)" bilgisi talep edilmektedir. Kullanıcı, "Kullanıcı Adı-Şifre" bilgilerini girerken kullanıcının

klavye verileri toplanmakta ve veri ön işleme adımlarından geçirilerek özellik çıkarımı yapılmaktadır. Ardından kayıt aşamasında girilen şifre bilgilerinin eşleşip eşleşmediği kontrol edilmekte, bilgiler eşleşiyorsa kullanıcı deseni çıkarılarak kullanıcı veri tabanına kaydedilmektedir. Kimlik doğrulama aşamasında, ilk olarak anahtar veri tabanındaki anahtar ile kullanıcı anahtarının eşleşme durumu kontrol edilmektedir. Ardından kullanıcı deseni verileri üzerinde özellik çıkarımı gerçekleştirilmekte ve sınıflandırıcı veri tabanındaki örnek şablonlar ile karşılaştırma yapılmaktadır. Kullanıcı veri tabanında değişime uyum sağlanabilmesi ve sınıflandırıcının doğruluk oranının arttırılması için en az son 20 kayıt tutulmalıdır. Ayrıca kullanıcı karakterindeki değişimlere göre oluşturulan desen düzenli olarak güncellenmelidir. Bu alanda yapılan farklı çalışmalarda, profil güncelleme mekanizmaları önerilmiştir [37, 38].

10.3.2.1. Veri Toplama

Veri toplama adımı, yüksek doğruluk oranına sahip bir kimlik doğrulama sistemi tasarlamak için en önemli adımdır. Kayıt ve doğrulama aşamalarında kullanıcı klavye desenleri toplanmakta ve veri tabanına kaydedilmektedir. İlk olarak kayıt aşamasında kullanıcının klavye desenini kullanarak kullanıcı kimliğini tanımlayabilmek için kişinin klavye verileri toplanmaktadır. Burada toplanan veri miktarı sistemin hassasiyeti, kullanım alanı ve kullanım amacı gibi faktörlere göre değişkenlik göstermektedir. Literatürde, beş girdiden [15] yüzden fazla girdiye kadar [35] farklı miktarda veri toplanan çalışmalar bulunmaktadır. Doğrulama aşamasında ise toplanan veriler, kayıt aşamasında kullanıcıdan alınan klavye verileri kullanılarak oluşturulmuş örnek model ile karşılaştırılmaktadır [15].

Veri toplama adımında, verinin kalitesini etkileyen farklı etkenler bulunmaktadır. Bu etkenlerden en önemlisi daha önce de belirttiğimiz üzere farklı çeşit klavyelerin kullanımıdır. Günümüzde kullanıma özel mekanik klavye, laptop klavyesi, ergonomik klavye gibi farklı çeşit klavyeler bulunmaktadır. Bunların yanı sıra F ve Q tipi klavyelerde değişen tuş konumu, farklı markaların farklı tuş kombinasyonlarını kullanması veya mekanik klavyelerdeki tuş hassasiyetinin farklılığı toplanan verinin kalitesini etkilemektedir. Klavyelerdeki bu donanımsal farklılıklar, kullanıcının kayıt ve doğrulama aşamasındaki veri girişinin tutarlılığını engellemektedir. Bu arayüz farklı bir klavye kullanımı, klavye deseninin tanınma performansını etkilemektedir [39].

Klavye deseni oluşturulurken temelde kullanıcının bir tuşa dokunma zamanı ve tuşu bırakma zamanı kaydedilmektedir. Daha sonra bu zaman veriler kullanılarak farklı özellikler çıkarılmaktadır. Bunun yanı sıra tuş kodu da sisteme kaydedilmektedir. Tuş kodu, klavyede aynı karakteri veren farklı tuşların ayırt edilmesinde kullanılmaktadır. Bu nedenle, kullanıcı desenini oluştururken kullanıcılar arası ayrıcı bir bilgi verebilmektedir [40]. Toplanan veriler içerisinden zaman değerlerinin doğruluğu hassasiyeti oldukça önemlidir. Fakat cihazın zamanlayıcısı, cihazın çözünürlüğüne, seçilen programlama diline veya işletim sistemine bağlı olarak farklılık gösterebilmektedir. Bu nedenle, daha yüksek doğruluk oranına sahip bir zamanlayıcı kullanımının daha iyi performans verdiği bilinmektedir [41]. Kullanıcılar aynı makineyi kullansalar bile, zamanlayıcının doğruluğu kullanılan farklı diller arasında değişiklik gösterebilmektedir. Bu nedenle, bu alanda basınç sensörü kullanımı, tuş vuruşlarında çıkan sesi kaydedilmesi gibi farklı yaklaşımlar denenmiş ve bu yaklaşımlar ile kullanıcı deseni oluşturulmaya çalışılmıştır [15]. Bu yöntemler arasında, tuş vuruşu sırasında üretilen ses verilerinin işlenmesi ile elde edilen veriler ve tuş vuruş zaman verileri beraber kullanıldığında doğrulama sistemi en iyi sonucu vermektedir [42]. Literatürde yapılan bazı çalışmalarda, klavye deseni ile kimlik doğrulama gerçekleştirirken kişinin kimliğinin belirlenmesinde klavye tuşlarından elde edilen süre bilgilerinin yanı sıra konum, IP adresi gibi çevresel faktörler ve kullanıcıya özel yaş, sağ-sol el kullanımı, meslek gibi özel faktörler de kullanılmaktadır [43].

10.3.2.2. Veri Ön İşleme

Modelin doğruluk oranını arttırmak için verilerin normalize edilmesi, veri içerisindeki gürültülerin temizlenmesi, eksik verilerin tamamlanması vb. veri ön işleme adımlarının detaylı olarak gerçekleştirilmesi gerekmektedir [15]. Ayrıca toplanan verinin miktarının da modelin başarım oranında önemli bir kriter olduğu bilinmektedir.

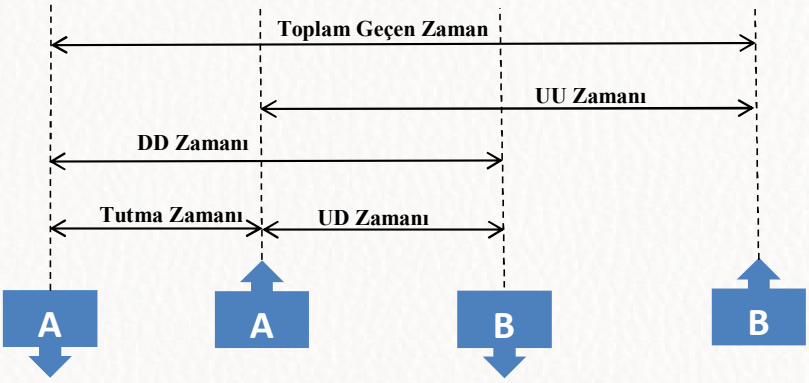
10.3.2.3. Özellik Çıkarımı

Klavye desenine dayanan kimlik doğrulama sistemlerinde, veri toplama aşamasından sonra en önemli adım özellik çıkarımı adımıdır. Bu adımda kullanıcı deseni çıkarılırken kullanılacak özellikler belirlenmektedir. Literatürdeki çalışmalar incelendiğinde, tuşlar arası gecikme ve tuş tutma süreleri gibi

benzer özelliklerin tercih edildiği gözlemlenmiştir. Bunların yanı sıra sıklıkla tercih edilmese de IP adresi, kullanıcı kişisel bilgileri gibi farklı kavramsal özellikler de kullanılabilmektedir.

1. **Tutma zamanı:** Bir tuşa basılma zamanı ile o tuşu bırakma zamanı arasındaki fark ile ifade edilmektedir.
2. **Gecikme zamanı:** İki tuş arasındaki geçişteki gecikme zamanını temsil etmektedir.
   a. **DD Zamanı:** Bir tuşa dokunma ve bir sonraki tuşa dokunma arasında geçen zaman.
   b. **UD Zamanı:** Bir tuşu bırakma ve bir sonraki tuşa dokunma arasında geçen zaman.
   c. **UU Zamanı:** Bir tuşu bırakma ve bir sonraki tuşu bırakma arasında geçen zaman.

Bu özellikler, sırasıyla peş peşe basılan A ve B tuşları üzerinden Şekil 10.8'de detaylı olarak gösterilmiştir.



Şekil 10.8. Klavye dinamikleri zaman özellikleri

Literatürde yapılan çalışmalar incelendiğinde, temelde Şekil 10.8'de gösterilen özelliklerin yanı sıra farklı özelliklerin çıkarıldığı görülmektedir. Bu ikincil özelikler, temel özellikler ve ham veri kullanılarak elde edilmektedir [15].

- **Toplam Geçen Zaman:** Bir metni yazmak için gereken toplam süre olarak tanımlanmaktadır [44].

- **Orta Zaman:** Kısa metinlerde, örneğin "Kullanıcı Adı-Şifre" bilgisinde kullanıcının şifresinin ortasındaki karakteri yazdığı zaman ile ilk karakteri yazdığı zaman arasındaki farkı ifade etmektedir [44].
- **Hata Oranı**: Kullanıcıya yazım hataları yapma yetkisi verildiğinde, geri al tuşuna kaç kez basıldığını sayılmaktadır. Bu özellik, sürekli kimlik doğrulama yapılan sistemlerde kullanılmaktadır, ancak sabit kimlik doğrulamada kullanımı oldukça nadirdir [44].
- **Digraph:** Bir digraf, bir tuşa bastıktan sonra iki tuş sonrasındaki tuşa basmak için gereken süreyi temsil eder. Bu kavram, n farklı değer için de hesaplanabilmektedir, ngraf olarak adlandırılmaktadır [45].
- **Yazım Zorluğu:** Belirli tuş kombinasyonlarının diğerlerinden daha zor yazılması gerçeğine dayanmaktadır. Yazma zorluğu, iki ardışık karakter arasındaki klavye mesafesine ve bir karakter oluşturmak için hangi tuşların gerektiğine göre değişlik göstermektedir [46].
- **Ortalama/Standart Sapma:** Gecikme ve tutma zamanındaki ortalama ve standart sapma değerini ifade etmektedir [15].

Toplanan veriler ve bu verilerden çıkarılan özellikler, modelin üzerindeki başarım oranları dikkat alınarak değerlendirilmektedir. Daha sonra modelin başarımı arttırmak için hangi özelliklerin kullanılacağına karar verilmektedir. Riot yaptığı çalışmada [47], özellik çıkarma işlemini iki farklı alt alana ayırmıştır:

- **Filtre yaklaşımı:** Filtre yaklaşımında amaç, diğer özellikler ile arasında ilişki bulundurmayan, sistemin sonuçlarını etkilemeyen ilgisiz özellikleri kaldırmaktır (varyans) [47].
- **Sarmalayıcı yaklaşımı:** Bu yaklaşımda, ilk olarak farklı özelliklerden alt kümeler oluşturulmakta, ardından oluşturulan alt kümelerin değerlendirilmesi sonucunda elde edilen en iyi alt küme veri tabanında saklanmaktadır [47].

Bu yaklaşımlar ile kullanıcıdan toplanan temel veriler değerlendirilmekte ve sistemde yeni özellikler çıkarılmakta ya da özellik azaltımı yapılmaktadır. Literatürde en sık kullanılanlar özellikler daha önce de belirtildiği üzere tuş tutma zamanı ve tuşlar arası gecikme zamanıdır.

10.3.2.4. Sınıflandırma

Kimlik doğrulama sistemlerinde, doğrulama modülü bir karşılaştırma puanı geri döndürmektedir. Bu puan daha önce tanımlanan sınır değerinin altındaysa, kullanıcının kimliği doğrulanmakta, aksi takdirde kullanıcı reddedilmektedir. Bu aşamada karşılaştırma puanı hesaplanırken farklı sınıflandırma yöntemleri kullanılmaktadır.

Klavye desenine dayanan kimlik doğrulama teknikleri kullandıkları yönteme göre istatistiksel yöntemler ve makine öğrenmesi yöntemleri olmak üzere iki ana başlık altında incelenmektedir. İstatistiksel yöntemler, makine öğrenmesi yöntemlerinden önce yoğun olarak kullanılmıştır. Fakat doğruluk oranı istenilen seviyeye erişemediği için yerini makine öğrenmesi yöntemlerine bırakmıştır. Makine öğrenmesi yöntemlerindeki gelişimle beraber davranışsal biyometrik sistemlerin doğruluk oranı da hızla artmıştır. Bu nedenle, son yıllarda bu alanda yapılan çalışma sayısında da büyük bir artış olmuştur.

Literatürdeki çalışmalara bakıldığında, Rassal Orman (Random Forester) ve Karar Ağacı (Decision Tree) algoritmalarının en yüksek doğruluk oranına sahip algoritmalar olduğu gözlemlenmiştir. Bu algoritmaların ardından Destek Vektör Makineleri (Support Vector Machine - SVM), K-En Yakın Komşu (K-Nearest Neighbor – K-NN) ve XGBoost algoritmalarının sık kullanılan makine öğrenmesi algoritmaları olduğu görülmüştür. Fakat yayınlanan sonuçlara bakarak, bu alanda en iyi sonucu veren algoritmayı belirlemek kolay değildir. Sistem ve veri yapısındaki farklılıklar algoritmanın başarım oranını oldukça yüksek oranda etkilemektedir. Bu nedenle, birçok farklı algoritmanın denenmesi ve veri için en uygun olanının seçilmesi gerekmektedir. Makine öğrenmesi algoritmalarının yanı sıra yeterli veri miktarının ve işlem gücünün sağlanması durumunda derin öğrenme algoritmaları da kullanılmaktadır.

10.3.3. Doğrulama Aşaması

Bir kimlik doğrulama sisteminin doğrulama aşamasında, ilk olarak anahtar veri tabanındaki şifre bilgisi ile kullanıcının girdiği şifre bilgisinin eşleşme durumu kontrol edilmektedir. Şifre bilgileri eşleşiyorsa, sistem kullanıcının klavye girdilerini analiz etmektedir. İlk olarak kayıt aşaması ile benzer şekilde kullanıcı klavye verileri üzerinde özellik çıkarım işlemi gerçekleştirilmekte ve bir kullanıcı deseni çıkarılmaktadır. Ardından sınıflandırıcı veri tabanındaki desen ile kullanıcının giriş deseni karşılaştırılmaktadır.

Klavye deseni ile kimlik doğrulama işlemi gerçekleştirirken karşılaşılan en büyük problem kullanıcının klavye deseninin değişikliğe uğrayabilmesidir. Parmak izi, yüz şekli gibi fiziksel biyometrik özelliklerimiz genel olarak sabit kalmakta ve kaza gibi etkenler olmadığı sürece bu özelliklerde bir değişim beklenmemektedir. Fakat davranışsal biyometrik özelliklerimiz, kullanıcının ruh hali, dikkati, kullandığı klavye, uzaktan erişim sağlaması veya sağlamaması gibi özelliklere göre değişkenlik gösterebilmektedir. Bu nedenle, sistemlerde bir sınır değeri belirlenmekte ve sistemin değişimi öğrenebilmesi için en az son 20 gerçek giriş deseni veri tabanında saklanmaktadır [43]. Ayrıca davranışsal deseni kullanarak oluşturulan kimlik doğrulama uygulamalarında, kullanıcı kabulü için belirlenen sınır değeri, uygulama özelinde, uygulamanın hassasiyetine göre belirlenmelidir. Sınır çok sıkı tutulduğunda, gerçek kullanıcının sisteme giriş yapamama ihtimali artarken, serbest bırakıldığında da kullanıcı şifresine erişim sağlayabilen bir saldırganın sisteme giriş yapabilme ihtimali artmaktadır. Bu nedenle, hatalı girişi en düşük seviyede tutabilmek için, uygulama özelinde bir sınır değeri belirlenmelidir. Bu sınır değerine göre desenler eşleşiyorsa kullanıcının sisteme giriş onaylanmaktadır. Desenlerin büyük oranla eşlemediği, başka bir ifade ile kullanıcı deseninin belirlenen sınırın altında kalarak anomali veya saldırgan olarak sınıflandırıldığı durumlarda, sistem risk değerlendirme yöntemlerini kullanarak kullanıcı girişini kısıtlamakta veya engellemektedir. Kullanıcı deseninde ihmal edilebilir olasılıkta bir değişim varsa, kullanıcı deseni güncellenmektedir. Bu alanda yapılan çalışmalarda, farklı profil güncelleme mekanizmaları önerilmiştir [37, 38].

10.4. KİMLİK DOĞRULAMA SİSTEMİNİN DEĞERLENDİRİLMESİ

Klavye desenine dayanan kimlik doğrulama sistemlerinde, doğruluk oranını etkileyen farklı bileşenler bulunmaktadır. Bu bileşenler, sistemin doğruluk oranının yanı sıra sistemin etkinliğini ve performansını değerlendirmek için de kullanılmaktadır. Sistemler değerlendirilirken aşağıdaki bileşenler dikkate alınmalı ve sistem kullanım alanına göre ağırlıklandırılmalıdır [36].

- **Etkinlik:** Sistemin, sahtekâr ve gerçek kullanıcıyı doğru bir şekilde tanımlama yeteneğini ifade etmektedir. Literatürde en çok FRR, FAR, EER performans metrikleri kullanılmaktadır. Sistemin kullanılacağı alana göre performans metriklerinin alması gereken değerlerde de-

ğişiklik olabilmektedir. Bu nedenle, sistemin iyi analiz edilmesi ve uygun performans metrikleri ile değerlendirilmesi gerekmektedir.

- **Verimlilik:** Kullanıcı kimliğinin tanımlaması için kullanılan sınıflandırma yöntemlerinin karmaşıklığı, sistemin verimliliği belirlemektedir.
- **Uyarlanabilirlik:** Sistemin, kullanıcı klavye desenindeki değişimleri algılayabilme ve kurulan modelde değişime göre güncelleme yapabilme oranını temsil etmektedir.
- **Sağlamlık:** Bir sistemin, sahtekâr kullanıcıyı tespit etmede gösterdiği performansı ifade etmektedir.
- **Kolaylık:** Bir sistemin kullanıcı açısından kullanım kolaylığını ifade etmektedir.

Klavye dinamiklerine dayanan kimlik doğrulama yöntemlerini değerlendirmek için en iyi çözüm aynı veri tabanı için literatürde kullanılan değerlendirme yöntemleri ile aynı yöntemi seçmektir. Fakat bu alanda iki farklı problemle karşılaşılmaktadır. Bunlardan birincisi, yapılan çalışmalarda genellikle veri tabanı paylaşılmamasıdır. Veri tabanı ve çıkarılan özellikler modellerinin başarımını doğrudan etkilemektedir. Bu nedenle, sonuçlar üzerinde bir iyileştirme olduğunu iddia edebilmek için öncelikle aynı veri tabanının kullanılmış olması gerekmektedir. Bu alanda en çok kullanılan açık veri tabanı Kilbory ve arkadaşlarının [4] çalışmasında paylaştığı veri tabanıdır. Fakat bu veri tabanı 2009 yılında toplandığı için günümüz donanım sistemlerinden farklıdır. Bir diğer problem ise, çalışmalarda farklı değerlendirme metriklerinin kullanılmasıdır. Yazarlar çalışmalarında en iyi sonucu veren değerlendirme metriklerini paylaşmaktadır. Bu nedenle, bu çalışmaları karşılaştırmak zorlaşmaktadır.

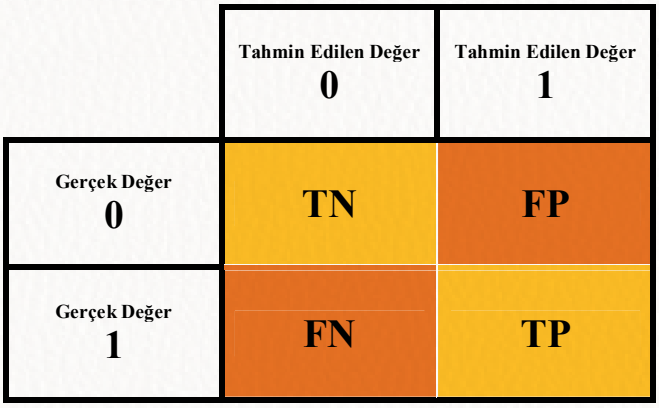
10.4.1 Performans Metrikleri (veya Değerlendirme Metrikleri)

Modeller değerlendirilirken farklı performans metrikleri kullanılarak modelin başarım oranı ve hata oranı gibi değerler hesaplanmaktadır. Bu değerler kullanılarak aynı veri kümesindeki modeller birbiri ile karşılaştırılabilmektedir. Modelleri değerlendirmede kullanılan bu metrikler kimlik doğrulama sisteminin kullanılacağı alana göre değişiklik gösterebilmektedir. Bazı değerlendirme metrikleri birbiri ile ters orantılıdır. Bu nedenle, sistemin kullanım alanı hangi metriğin daha önemli olduğunu belirlemektedir. Bu bölümde literatürde sıklıkla kullanılan performans metrikleri detaylı olarak paylaşılmaktadır.

Karışıklık Matrisi (Confusion Matrix): Sınıflandırma modellerinin başarımını değerlendirmek için kullanılan matristir. Matris içerisinde TN, TP, FN ve FP olmak üzere dört farklı değer tanımlanmaktadır.

- **TN:** Doğru sınıflandırılan negatif örneklerin sayısını ifade etmektedir.
- **TP:** Doğru sınıflandırılan pozitif örneklerin sayısını ifade etmektedir.
- **FN:** Yanlış sınıflandırılan pozitif örneklerin sayısını, başka bir ifade ile aslında pozitifken, negatif olarak sınıflandırılan örneklerin sayısını ifade etmektedir.
- **FP:** Yanlış sınıflandırılan negatif örneklerin sayısını ifade etmektedir, başka bir ifade ile aslında negatifken, pozitif olarak sınıflandırılan örneklerin sayısını ifade etmektedir.

Bu tanımlar kapsamında modellerin yaptığı hatalardan FP değeri Tip 1 Hatası ve FN değeri Tip 2 Hatası olarak adlandırılmaktadır. Bu değerler, Şekil 10.9'da tanımlı karışıklık matrisi oluşturularak görselleştirilmektedir.



Şekil 10.9. Karışıklık matrisi

Bu tanımlar kapsamında modellerin yaptığı hatalardan FP değeri Tip 1 Hatası ve FN değeri Tip 2 Hatası olarak adlandırılmaktadır. Bu değerler, Şekil 10.9'da tanımlı karışıklık matrisi oluşturularak görselleştirilmektedir.

- **Doğruluk (Accuracy - ACC):** Modelin doğru yanıtlarının sayısının, toplam örnek sayısına bölümünden elde edilmektedir. Basit olarak verilen veri kümesi için modelin doğruluk oranı vermektedir. Mo-

dellerin başarımını değerlendirirken en sık kullanılan değerlendirme metriklerinden biridir. Doğruluk metriği aşağıdaki denklemde gösterildiği şekilde hesaplanmaktadır.

$$ACC = \frac{TN + TP}{TN + TP + FP + FN}$$

– **Yanlış Kabul Oranı (False Acceptance Rate - FAR):** Yanlış sınıflandırılan negatif örneklerin sayısının, toplam negatif örnek sayısına oranını ifade etmektedir. Kimlik doğrulama sistemleri için bu oran, yetkisi olmayan bir kullanıcının yanlışlıkla sisteme kabul edilme oranını göstermektedir. Aşağıdaki denklemde tanımlanan FAR değeri düştükçe sistemin başarım oranı artmaktadır. Bu oranı düşürmek için sistemde tanımlı kabul eşik değerinin arttırılması gerekmektedir.

$$FAR = \frac{FP}{FP + TN}$$

– **Yanlış Ret Oranı (False Rejection Rate - FRR):** Yanlış sınıflandırılan pozitif örneklerin sayısının, toplam pozitif örnek sayısına oranını ifade etmektedir. Kimlik doğrulama sistemleri için bu oran, yetkisi olan bir kullanıcının yanlışlıkla sisteme kabul edilmeme oranını göstermektedir. Aşağıdaki denklemde tanımlanan FRR değeri düştükçe sistemin başarım oranı artmaktadır. Bu oranı düşürmek için sistemde tanımlı kabul eşik değerinin düşürülmesi gerekmektedir.

$$FRR = \frac{FN}{TP + FN}$$

– **Eşit Hata Oranı (Equal Error Rate - ERR):** FAR ve FRR oranları arasında ters bir orantı olduğu görülmektedir. Örneğin, FAR değerini düşürmek için eşik değeri arttırıldığında FRR değeri yükselmekte, FRR değerini düşürmek için eşik değeri düşürüldüğünde FAR değeri artmaktadır. Modeller karşılaştırılırken, iki oran arasındaki ilişki tek bir değer ile tanımlanmak istendiğinde ERR metriği kullanılmaktadır. ERR değeri, FAR ve FRR değerlerinin birbirine eşit olduğu en düşük noktayı ifade etmektedir. ERR değerinin düşük olması, modelde tanımlanan eşik değerinin, sınıflar arasındaki ayrımı yüksek başarılı olarak gerçekleştirdiğini göstermektedir.

– **Hatırlama (Recall):** Doğru sınıflandırılan pozitif örneklerin sayısının, toplam pozitif örnek sayısına oranını ifade etmektedir. Kimlik doğrulama sistemleri için bu oran, yetkisi olan bir kullanıcının sisteme kabul edilme oranını göstermektedir. Aşağıdaki denklemde tanımlanan Recall değeri yükseldikçe sistemin başarım oranı artmaktadır.

$$Recall = \frac{TP}{TP + FN}$$

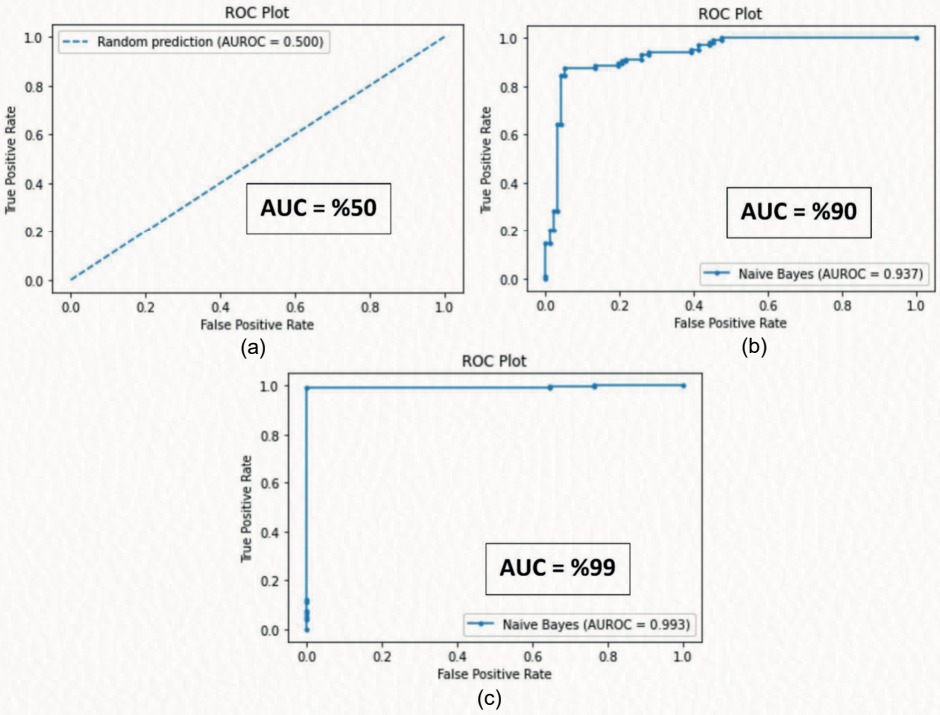
– **Kesinlik (Precision):** Doğru sınıflandırılan pozitif örneklerin sayısının, pozitif olarak sınıflandırılan örnek sayısına oranını ifade etmektedir. Kimlik doğrulama sistemleri için bu oran, sisteme kabul edilen kullanıcıların ne kadarının yetkisi olan bir kullanıcı olduğunu göstermektedir. Aşağıdaki denklemde tanımlanan Precision değeri yükseldikçe sistemin başarım oranı artmaktadır.

$$Precision = \frac{TP}{TP + FP}$$

– **F-Puanı (F-Score):** Düşük kesinlik ve yüksek hatırlama veya yüksek kesinlik ve düşük hatırlama değerine sahip iki farklı modeli karşılaştırmak için F-Puanı kullanılmaktadır. F-Puanı, bu iki metrik göz önünde bulundurularak modelin başarımı değerlendirmekte ve aşağıdaki denklemde gösterildiği şekilde hesaplanmaktadır.

$$F - Score = 2\,\frac{Precision \times Recall}{Precision + Recall}$$

– **ROC Eğrisi:** X ekseninde FAR oranını, Y ekseninde FRR oranını bulunduran bir olasılık eğrisidir. Farklı sınıflardan oluşan modellerin karşılaştırmasında sıklıkla kullanılmaktadır. Bu eğrinin altında kalan alan AUC-ROC olarak adlandırılmakta ve modelin performansının belirlenmesinde önemli bir kısıt olarak göz önünde bulundurulmaktadır. Eğrinin altında kalan alan ne kadar büyükse, modeller o kadar az hata oranına sahip bulunmaktadır. ROC eğrisinin altında kalan alan en ideal 1 değerini almaktadır. Fakat pratikte biri artarken diğeri azaldığı için bu sonucu elde etmek pek mümkün değildir. Şekil 10.10'da farklı eğri örnekleri verilmektedir.



Şekil 10.10. ROC eğrisinin altında kalan AUC alanı

Şekil 10.10'da 2000 rastgele üretilen örnekli iki sınıflı bir problem için ROC eğrileri verilmektedir. Şekil 10.10'daki (a) ve (c) numaralı grafiklerde veri içerisine gürültü eklenmemiştir. (a) numaralı grafik, rastgele tahmin değerlerinin sonucunu ifade ederken; (c) numaralı grafik, Naive Bayes algoritmasının sonucunu göstermektedir. (b) numaralı grafik de ise veriye gürültü değeri eklenmiş ve Naive Bayes algoritmasının sonucu paylaşılmıştır.

10.4.2. Veri Tabanı Değerlendirme Kriterleri

Klavye desenine dayanan kimlik doğrulama sistemleri için, kullanılabilir sınırlı sayıda kıyaslama veri tabanı bulunmaktadır. Veri tabanları kullanıcıların kimlik desenlerini içermektedir. Bu nedenle, araştırmacılar, veri tabanlarını paylaşmamayı tercih etmektedir. Kişisel veri tabanları birkaç araştırmacı tarafından paylaşılmış olsa da yine de araştırmacıların çoğu kendi veri kümelerini oluşturmaktadır. Bu nedenle, bu alanda büyük ve yeni veri tabanlarına ihtiyaç

duyulduğu görülmektedir [36]. Kullanılan veri tabanlarının önemli özelliklerine bakacak olursak:

- **Veri Boyutu:** Veri tabanında kullanıcı sayısı arttıkça çalışmanın ölçeklenebilirliği daha iyi gösterilmektedir. Ancak birçok durumda, kişilerin kimlik bilgilerinin bulunması, veri toplama aşamasının zor olması gibi farklı sebeplerden dolayı çalışmaların çoğunda 50'den az kullanıcı bulunmaktadır [36].
- **Veri Tipi:** Girişler genellikle kullanıcılar tarafından karakter bazlı metin veya sayı şeklinde sağlanmaktadır. Girişin karakter tabanlı metin biçiminde olduğu araştırmalar daha önce de belirtildiği üzere kısa ve uzun metin olarak adlandırılmaktadır. Kısa metinde, veriler "Kullanıcı Adı-Şifre" şeklinde olurken, uzun metinde belirli uzunluklar arasında daha önce belirlenmiş veya kullanıcı tarafından belirlenen bir paragraf kullanılmaktadır. Kullanıcının belirlediği bir metin üzerinden kimlik doğrulaması yapılacaksa veri tabanını yönetmek biraz daha zor olmaktadır. Sabit bir metin kullanan kimlik doğrulama sistemlerinde, farklı kullanıcılar aynı girdi üzerinde çalıştığı için veri tabanını yönetmesi çok kolay olmaktadır [36].

10.5. SONUÇ VE DEĞERLENDİRMELER

Günümüzde kritik sistemlere olan yetkisiz girişlerin verdiği zararlar ve itibar kayıpları göz önüne alındığında; kimlik doğrulama sistemleri üzerine yapılan çalışmaların değerli olduğu görülmektedir. Bankacılık uygulamalarından, kurum içi ağlara kadar birçok farklı sektörde kimlik doğrulama sistemleri kullanılmaktadır. Bu sistemler içerisinde, biyometrik teknolojilere dayanan kimlik doğrulama sistemleri sıklıkla tercih edilmektedir. Bu sistemler içerisinde, davranışsal kimlik doğrulama yöntemlerinden biri olan klavye deseni ile doğrulama yönteminin yeri ve önemi bu kitap bölümünde detaylı olarak ele alınmıştır. Bu yöntem, yapay zekâdaki ilerlemeler sayesinde çok yüksek bir doğruluk ile yapılabilmektedir. Bu nedenle, birçok firma, iki faktörlü kimlik doğrulamanın ikinci aşamasında, klavye desenini kullanmaktadır.

Konu güvenlik olduğunda devletler ve özel şirketler için, yurt dışı kaynaklı ürünler kullanılarak kullanıcı kimliğinin doğrulanması tavsiye edilmeyen bir yöntemdir. Müşteri bilgilerinin gizliliği ve güvenliği için bu alanda yer-

li tasarımlara ve ürünlere ihtiyaç olduğu görülmektedir. Ulusal pazarda bir ürün haline gelen sistemlere bakıldığında, yalnızca SecurifyID firmasının iki aşamalı kimlik doğrulama için klavye desenine dayanan bir çözüm sunduğu gözlemlenmiştir. Bu ürün, makine öğrenmesi algoritmalarını kullanılarak kullanıcı klavye verileri işlenmekte ve iki faktörlü bir kimlik doğrulama gerçekleştirmektedir. Bunun dışında ulusal pazarda DVA Telekomünikasyon firması, uluslararası hizmet veren Behaviosec firması ile iş birliği içinde bu hizmeti sunmaktadır. Bu alanda yapılan çalışmalara bakıldığında, davranışsal biyometrik sistemler üzerine yerli ve milli yazılımlara ihtiyaç duyulduğu, var olan yazılımların kapsamlarının genişletilmesi ve geliştirilmesi gerektiği açıkça görülmektedir. BDDK mevzuatıyla bankacılık sektörü için zorunlu hale getirilen iki faktörlü doğrulamanın, önümüzdeki 5 yıl içerisinde birçok kurum ve kuruluş için zorunlu hale geleceği öngörülmektedir. Bu bilgiler ışığında bu alanda yapılacak çalışmaların, yerli sistemlerin geliştirilmesine ve ülkemizin küresel kimlik doğrulama sektöründen bir pay almasına katkı sağlayacağı düşünülmektedir.

Klavye desenine dayanan kimlik doğrulama sistemlerinin kullanımı yaygınlaştırmak için bu alandaki yaygın problemlerin çözmesi gerekmektedir. Literatürdeki çalışmalar incelendiğinde bu alandaki en büyük problemin, kullanıcıların kayıt ve doğrulama aşamalarında farklı cihazları kullanması olduğu gözlemlenmiştir. Kullanıcıların farklı cihaz veya klavye kullanıldığı durumlarda, zamanlama metriklerinde değişiklikler oluşmaktadır. Bu nedenle, klavye desenine dayanan kimlik doğrulama sistemlerinin kullanımının artması için farklı donanımlardaki zamanlama değişimlerine uyum sağlayabilen sistemler tasarlanmalıdır. Bu değişimin, sistemin kullanıcı tanıma performansı üzerindeki etkisi en düşük seviyeye indirgenmeli, mümkünse bu etki sıfırlanmalıdır.

Biyometrik verilerdeki değişim, bu alandaki bir diğer problemdir. Fiziksel biyometrik özelliklerimiz genel olarak sabit kalmakta ve büyük bir etken olmadığı sürece bu özelliklerde bir değişim beklenmemektedir. Ancak davranışsal biyometrik özelliklerimizde zamanla bir değişim gerçekleşebilmektedir. Örneğin, kullanıcı zamanla şifreye alışmakta ve şifreyi daha hızlı girebilmektedir. Farklı bir klavyeye geçtiğinde mekanik gecikmelerden bağımsız olarak kullanıcı deseninde de değişiklikler oluşabilmektedir. Bu nedenle, kullanıcının tanımlanmasındaki doğruluk oranı azalabilmektedir. Klavye değişimi ve uzaktan erişim gibi problemler ile başa çıkabilmek için

hafıza kısıtının olmadığı uygulamalarda dinamik doğrulama yöntemleri tercih edilebilir.

Günümüzde mobil cihazların, internet bankacılığı, internet alışverişi gibi alanlarda sıklıkla kullanılması sebebi ile bu cihazların güvenilirliği tartışılmaya başlanmıştır. Bu güvelik gereksinimleri kapsamında, klavye dinamikleri mobil cihazlar için de kimlik doğrulama alanında kullanılabilir bir seçenek olarak öne çıkmış ve bu alanda yapılan çalışmalar artmıştır. Mobil cihazlar, bazıları bilgisayarlarda bulunmayan dokunmatik ekran, ivmeölçer, jiroskop, kamera, parmak tarayıcı, mikrofon, GPS, yakınlık sensörü, duyma oranı sensörü, hareket sensörü, barometre vb. birçok sensöre sahip bulunmaktadır. Literatürdeki çalışmalarda, dokunmatik ekran, ivmeölçer ve jiroskop sensörleri klavye deseni ile kimlik doğrulama sistemlerinde sıklıkla kullanılmaktadır. Dokunma sensörü yalnızca dokunma olayını değil, aynı zamanda dokunmanın boyutunu ve basıncını da algılamaktadır. Dokunmatik ekranlar üzerinde elin şeklinin ve konumunun sistemlerin doğruluk oranını etkilediği görülmektedir. Mobil cihazlarda bilgisayarlara oranla daha fazla davranışsal veri toplanabildiği için, yüksek doğruluk oranı ile kimlik doğrulama işleminin gerçekleştirilebileceği ön görülmektedir. Mobil cihazlar klavye deseni ile kimlik doğrulama gerçekleştirilirken bazı problemlerle karşılaşılmaktadır. Örneğin, kullanıcılar sıklıkla cihazlarını değiştirmektedir. Bu nedenle, çevrim içi bir kimlik doğrulama sisteminde desenler bir sunucuda saklanıyorsa, kullanıcının yeni cep telefonu ile yeniden kaydolması sistemin performansını artırmaktadır. Fakat bu durumda, kullanıcıdan ek bir işlem talep edilmektedir. Ayrıca bu cihazlarda sensör verilerinin anlamlandırılması ve özellik çıkarım aşaması bilgisayarlara göre daha karmaşıktır.

Literatürde farklı algoritmaların farklı veri kümeleri üzerindeki sonuçları paylaşılmıştır ama veri kümeleri farklı olduğu için bu çalışmalar üzerinde karşılaştırma gerçekleştirmek mümkün değildir. Bu konuya çözüm olarak Killourhy ve Maxion karşılaştırma için büyük bir veri kümesi toplamış ve bu veri kümesi üzerinde 14 farklı makine öğrenmesi algoritmasını denemiştir. Algoritmaların sonuçları ve veri kümesi açık olarak paylaşılmıştır. Fakat bu veri tabanı eski kalmıştır. Ayrıca yapılan çalışmalarda farklı veri tabanları kullanıldığı için sınıflandırma algoritmalarını karşılaştırmak, sistemi analiz etmek ve net bir bilgi vermek mümkün değildir. Bu nedenle, yeni ve kapsamlı veri tabanlarına ihtiyaç duyulmaktadır. Bu alanda, ulusal veri tabanı oluşturulmalıdır.

Teşekkür

Bu çalışma, TÜBİTAK tarafından 7201256 proje numarası ile desteklenmektedir.Yazarlardan Nurşah Çevik YÖK 100/2000 Öncelikli Alan Doktora Bursu kapsamında desteklenmektedir.

KAYNAKLAR

[1]. P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines," NIST Special Publication 800-63-3, 2017, Last Updates 2020, DOI: 10.6028/NIST.SP.800-63-3.

[2]. A. Ometov et al., "Multi-factor authentication: A survey," Cryptography, vol. 2, 2018, DOI: 10.3390/cryptography2010001.

[3]. BDDK, "Bankaların bilgi sistemleri ve elektronik bankacılık hizmetleri hakkında yönetmelik," Bankacılık Düzenleme ve Denetleme Kurumu, 2020.

[4]. K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in 2009 IEEE/IFIP International conference on Dependable Systems Networks, Lisbon, Portugal, 2009, pp. 125–134, DOI:10.1109/DSN.2009.5270346.

[5]. S. Boonkrong, "Multi-factor authentication," in Authentication and Access Control, Apress, Berkeley, CA, 2021, DOI: 10.1007/978-1-4842-6570-3_6.

[6]. R. P. Jover, "Security analysis of sms as a second factor of authentication: The challenges of multifactor authentication based on sms, including cellular security deficiencies, ss7 exploits, and sim swapping," Queue, vol. 18, no. 4, pp. 37–60, 2020, DOI: 10.1145/3424302.3425909.

[7]. S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," in Expert Systems with Applications, vol. 143, p. 113114, 2020, DOI: 10.1016/j.eswa.2019.113114.

[8]. B. Arslan and Ş. Sağıroğlu, "Biyometrik sistemlerde güvenlik ve mahremiyet," BGD Siber Güvenlik ve Savunma: Standartlar ve Uygulamalar, Turkey: Grafiker Yayınları, 2019, ch. 3, sec. 13, pp. 347-385.

[9]. H. Tutumluer and R. Samet, "Davranışsal biyometrik sistemler, teknolojiler ve güvenlik," BGD Siber Güvenlik ve Savunma: Biyometrik ve Kriptografik Uygulamalar, Turkey: Nobel Akademik Yayıncılık, 2020, ch. 4, sec. 5, pp. 163-204.

[10]. W. L. Bryan and N. Harter, "Studies in the physiology and psychology of the telegraphic language," in Psychological Review, vol. 4, no. 1, pp. 27–53, 1897, DOI: 10.1037/h0073806.

[11]. R. Spillane, "Keyboard apparatus for personal identification," IBM Technical Disclosure Bulletin, vol. 17, no. 3346, 1975.

[12]. G. Forsen, M. Nelson, and R. J. Staron, "Personal attributes authentication techniques," Tech. Rep. RADC-TR-77-333, Pattern Analysis and Recognation Corporation Rome N Y, ADA047645, 1977. Available: https://apps.dtic.mil/sti/citations/ADA047645

[13]. R. S. Gaines, W. Lisowski, S. Press, and N. Shapiro, "Authentication by keystroke timing: some preliminary results," CA: RAND Corporation, Santa Monica, R-2560-NSF, 1980. Available: https://www.rand.org/pubs/reports/R2526.html

[14]. D. Umphress and G. Williams, "Identity verification through keyboard characteristics," in International Journal of Man-Machine Studies, vol. 23, no. 3, pp. 263–273, 1985, DOI: 10.1016/S0020-7373(85)80036-5.

[15]. R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics authentication," Ed. Intech, chapter 8, 2011, DOI: 10.5772/17064.

[16]. Y. Zhong, Y. Deng and A. K. Jain, "Keystroke dynamics for user authentication," in IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, Providence, RI, USA, 2012, pp. 117-123, DOI: 10.1109/CVPRW.2012.6239225.

[17]. J. V. Monaco, J. C. Stewart, S. Cha, and C. C. Tappert, "Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works," in IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1-8, DOI: 10.1109/BTAS.2013.6712743.

[18]. NIST, "Security and privacy controls for information systems and organizations," National Institute of Standards and Technology, Gaithersburg, Maryland, USA, Tech. Rep. NISTIR 800-53 Revision 5, 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[19]. Y. Deng and Y. Zhong, "Keystroke dynamics user authentication based on gaussian mixture model and deep belief nets," in ISRN Signal Processing, 2013, DOI: 10.1155/2013/565183.

[20]. C. C. Tappert, M. Villani, and S. Cha, "Keystroke biometric identification and authentication on long-text input," in Behavioral Biometrics for Human Identification: Intelligent Applications, IGI Global, 2010, pp. 342-367, DOI:10.4018/978-1-60566-725-6.ch016.

[21]. T. E. Wesołowsk and P. Porwik, "Computer user profiling based on keystroke analysis," Advanced Computing and Systems for Security, Advances in Intelligent Systems and Computing book series, Springer, New Delhi, 2015, vol. 395, pp. 3-13. Available: https://doi.org/10.1007/978-81-322-2650-5_1.

[22]. P. A. Grassi et al., "Digital identity guidelines authentication and lifecycle management," National Institute of Standards and Technology, Gaithersburg, Maryland, USA, Tech. Rep. NISTIR 800-63B, 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[23]. N. Raul, R. Shankarmani and P. Joshi, "A comprehensive review of keystroke dynamics-based authentication mechanism," in International Conference on Innovative Computing and Communications, Singapore, 2020, DOI:10.1007/978-981-15-0324-5_13.

[24]. S. Singh, A. Inamdar, A. Kore and A. Pawar, "Analysis of algorithms for user authentication using keystroke dynamics," in International Conference on Communication and Signal Processing, Chennai, India, 2020, pp. 0337-0341, DOI: 10.1109/ICCSP48568.2020.9182115.

[25]. H. A. Boz, M. Gürkan and B. Yanıkoğlu, "Keystroke dynamics based biometric identification," in Signal Processing and Communications Applications Conference, Gaziantep, Turkey, 2020, pp. 1-4, DOI: 10.1109/SIU49456.2020.9302273.

[26]. P. Porwik, R. Doroz, and T. E. Wesolowski, "Dynamic keystroke pattern analysis and classifiers with competence for user recognition," in Applied Soft Computing, vol. 99, pp. 106902, 2021, DOI: 10.1016/j.asoc.2020.106902.

[27]. Y. Deng and Y. Zhong, "Keystroke dynamics advances for mobile devices using deep neural network", in Recent Advances in User Authentication Using Keystroke Dynamics, vol. 2, pp. 59–70, 2015, DOI: 10.15579/gcsr.vol2.ch4.

[28]. Najwa Altwaijry, "Keystroke Dynamics Analysis for User Authentication Using a Deep Learning Approach," in International Journal of Computer Science and Network Security, vol. 20, no. 12, pp. 209-216, 2020, DOI: 10.15579/gcsr.vol2.ch2.

[29]. M. L. Bernardi, M. Cimitile, F. Martinelli and F. Mercaldo, "Keystroke analysis for user identification using deep neural networks," in International Joint Conference on Neural Networks, Budapest, Hungary, 2019, pp. 1-8, DOI: 10.1109/IJCNN.2019.8852068.

[30]. F. Alshanketi, I. Traore, and A. A. Ahmed, "Improving Performance and Usability in Mobile Keystroke Dynamic Biometric Authentication," 2016 IEEE Security and Privacy Workshops (SPW), pp. 66-73, 2016, DOI: 10.1109/SPW.2016.12.

[31]. E. Maiorana, H. Kalita, and P. Campisi, "Mobile keystroke dynamics for biometric recognition: An overview," in IET Biometrics, vol. 10, no. 1, pp. 1-23, 2021, DOI: 10.1049/bme2.12003.

[32]. P. Kobojek and K. Saeed, "Application of recurrent neural networks for user verification based on keystroke dynamics," in Journal of Telecommunications and Information Technology, vol. nr 3, pp. 80-90, 2016.

[33]. C. Giuffrida et al., "I sensed it was you: Authenticating mobile users with sensor-enhanced keystroke dynamics," in Detection of Intrusions and Malware, and Vulnerability Assessment, S. Dietrich, Lecture Notes in Computer Science, vol. 8550, pp. 92–111, 2014, DOI: 10.07/978/3-319-08509-86.

[34]. M. Antal and L. Z. Szabó, "An Evaluation of One-Class and Two-Class Classification Algorithms for Keystroke Dynamics Authentication on Mobile Devices," 2015 20th International Conference on Control Systems and Computer Science, Bucharest, Romania, 2015, pp. 343-350, DOI: 10.1109/CSCS.2015.16.

[35]. M. S. Obaidat and B. Sadoun, "Verification of computer users using keystroke dynamics," in IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 27, no. 2, pp. 261-269, April 1997, DOI: 10.1109/3477.558812.

[36]. S. J. Quraishi and S. S. Bedi, "Keystroke dynamics biometrics, a tool for user authentication–review," in International Conference on System Modeling & Advancement in Research Trends, Moradabad, India, 2018, pp. 248-254, DOI: 10.1109/SYSMART.2018.8746932.

[37]. D. Hosseinzadeh and S. Krishnan, "Gaussian Mixture Modeling of Keystroke Patterns for Biometric Applications," in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 38, no. 6, pp. 816-826, Nov. 2008, DOI: 10.1109/TSMCC.2008.2001696.

[38]. J. W. Lee, S. S. Choi, and B. R. Moon, "An evolutionary keystroke authentication based on ellipsoidal hypothesis space," in Proceedings of the 9th Annual Genetic and Evolutionary Computation Conference, London, UK, 2007, pp. 2090—2097, DOI: 10.1145/1276958.1277365.

[39]. A. Ross, K. Nandakumar, and A. Jain, "Handbook of Multibiometrics", Springer, 2006.

[40]. L. C. F. Araujo et al., "User authentication through typing biometrics features," in IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 851-855, Feb. 2005, DOI: 10.1109/TSP.2004.839903.

[41]. K. Killourhy and R. Maxion, "The effect of clock resolution on keystroke dynamics," in Recent Advances in Intrusion Detection, Lecture Notes in Computer Science, vol. 5230, Springer, Berlin, Heidelberg, 2008, DOI: 10.1007/978-3-540-87403-4_18.

[42]. H. Dozono, S. Itou, and M. S. Nakakuni, "Comparison of the adaptive authentication systems for behavior biometrics using the variations of self organizing maps," in International Journal of Computers and Communications, vol. 1, no. 4, pp. 108–116, 2007.

[43]. K. Bicakci, O. Salman, Y. Uzunay and M. Tan, "Analysis and evaluation of keystroke dynamics as a feature of contextual authentication," in International Conference on Information Security and Cryptology, Ankara, Turkey, 2020, pp. 11-17, DOI: 10.1109/ISCTURKEY51113.2020.9307967.

[44]. J. Ilonen, "Keystroke dynamics", Advanced Topics in Information Processing–Lecture, 2002.

[45]. F. Bergadano, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," in ACM Transactions on Information System Security, vol. 5, no. 4, pp. 367–397, Nov. 2002, DOI: 10.1145/581271.581272.

[46]. W. G. De Ru and J. H. P. Eloff, "Enhanced password authentication through fuzzy logic," in IEEE Expert, vol. 12, no. 6, pp. 38-45, Nov.-Dec. 1997, DOI: 10.1109/64.642960.

[47]. G. Pahuja and T. N. Nagabhushan, "Biometric authentication identification through behavioral biometrics: A survey," in 2015 International Conference on Cognitive Computing and Information Processing, Noida, India, 2015, pp. 1–7, DOI: 0.1109/CCIP.2015.7100681.

Bölüm 11

NESNELERİN İNTERNETİ AYGITLARININ GÜVENLİĞİ İÇİN HAFİF SİKLET KRİPTOGRAFİK ALGORİTMALARA GENEL BAKIŞ

İhsan Çiçek

Transistörün icadı ve ardından tümleşik devre teknolojilerinin gelişimiyle ortaya çıkan mikroişlemcilerin ve programlanabilir mantık devrelerinin yaygın etkisiyle ile 20.yy'ın ilk yarısında analog nitelikte olan pek çok mühendislik ürünü ikinci yarıda hızla dijitalleşmeye başlamıştır. 90'ların ardından ortaya çıkan internet sadece insanları değil makineleri de birbirine bağlayarak sınırları ortadan kaldıran çok boyutlu bir fırsat ve tehdit yüzeyi yaratmıştır. Bu tehditler 2010'lu yılların sonlarında özellikle Nesnelerin İnterneti aygıtları üzerinden düzenlenen siber saldırıların ortaya çıkmasıyla gündelik hayatı doğrudan etkiler hale gelmiştir. Genellikle düşük maliyetli mikroişlemci tabanlı gömülü sistemler olarak tasarlanan Nesnelerin İnterneti aygıtlarında gerek pazara erken çıkma baskısı gerekse geliştirme maliyetleri nedeniyle güvenlik konusu üreticiler tarafından genellikle ihmal edilmektedir. Herhangi bir ağa bağlandıklarında en zayıf halkayı oluşturan bu aygıtlar günümüzde siber saldırganların olağan hedefi haline gelmiş bulunmaktadır. Bilgi güvenliğinin sağlanması kriptografi ile mümkündür ancak modern algoritmaların, düşük performanslı ve maliyetli mikroişlemcilerde gerçeklenmesi önemli bir mühendislik problemidir. Hafif siklet kriptografik algoritmalar Nesnelerin İnterneti aygıtlarının güvenliğini performans darboğazı yaratmadan sağlamak amacıyla geliştirilmiş özel kriptografik algoritmalardır. Bu bölümde düşük maliyetli ve performanslı gömülü sistemlerde kullanılabilecek hafif siklet kriptografik algoritmaların ve özetleme fonksiyonlarının temel özellikleri tanıtılacak ve bu konuda dünyadaki standartlaşma faaliyetleri hakkında güncel bilgiler sunulacaktır.

11.1. GİRİŞ

Niteliği aslen analog olan pek çok elektronik ürün, 70'lerde maliyet etkin CMOS tümleşik devre üretim teknolojisinin gelişmesi sonucu ortaya çıkan mikroişlemcilerin ve programlanabilir mantık devrelerinin yaygın etkisi ile, 80'li yıllardan itibaren hızla dijitalleşmeye başlamıştır. Bu tarihsel gelişim süreci boyunca, birçok farklı mikroişlemci ve komut seti mimarileri pazara girerek sahada ticari elektronik ürünlerden otomotive, biyomedikalden savunma sanayiine pek çok alanda kendine yer buldu. Ne yazık ki 80'lerden günümüze mikroişlemci çeşitliliği, telif hakkı lisansı gerektiren tescilli komut seti mimarilerine sahip işlemcilerin egemenliğiyle sürekli olarak azalmış ve erozyona uğramıştır.

Bugün ARM işlemcileri, mobil cihazlardan giyilebilir cihazlara, ağ ekipmanlarından otomotiv parçalarına ve Nesnelerin İnterneti aygıtlarına kadar elektroniğin neredeyse her alanında vazgeçilmez bir dayanak noktası haline geldi. ARM ve MIPS benzeri işlemciler, esas olarak, komut ve veri için ayrı belleklerle birlikte daha küçük bir komut seti ile gelen Azaltılmış Komut Seti (Reduced Instruction Set Computer - RISC) mimarisine dayanmaktadır. RISC tabanlı işlemciler, geleneksel olarak çok sayıda komut, adresleme modu ve doğrudan bellek üzerinde çalışabilen komutlarla gelen Karmaşık Komut Seti (Complex Instruction Set Computer - CISC) işlemci mimarisine dayanan konvansiyonel masaüstü bilgisayar pazarına da girmeye başladı [1]. Günümüzde komut seti lisanslama maliyetleri nedeniyle endüstride ARM işlemcilerinden, açık kaynak komut seti ve RISC mimarisine sahip olan RISC-V işlemci çekirdeğine doğru bir yönelimin olduğu gözlemlenmektedir. Sonuç olarak gömülü sistem aygıtlarında, çalışma zamanında çeviklik, verimlilik ve esneklik sağlarken aynı zamanda siber güvenlik özelliklerini de karşılayabilen işlemcilerin kullanılması gerekmektedir [2]. Güncel ve sürekli gelişen mimarisi ve açık kaynak lisanslı genişletilebilir komut seti sayesinde RISC-V işlemcisi, mevcut ve gelecekteki güvenli gömülü sistem uygulamaları için doğal bir aday platform olarak öne çıkmakta ve pek çok teknoloji devi tarafından desteklenmektedir [3].

Gömülü sistemlerin yaygın etkisi nedeniyle günümüz uygulamalarında siber güvenlik en önemli konu haline gelmiştir. Gömülü sistem geliştirmede siber güvenlik gereksinimlerinin belirlenmesi ve ölçülmesi zor bir problemdir. Gömülü sistemlerin siber güvenliği için gizlilik, veri bütünlüğü ve kimlik

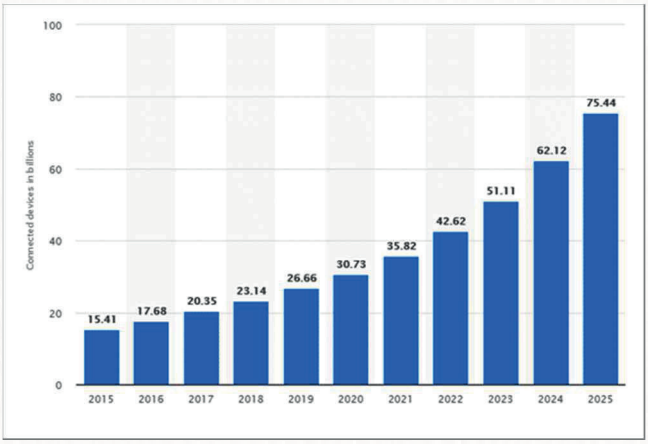
doğrulama gibi gereksinimlerin karşılanması gerekmektedir, ancak tasarım süreçlerinde gömülü bir sistemi değerlendirmek için gereken ölçülebilir siber güvenlik metrikleri, global standartlaşma eforuna rağmen, halen yeterli olgunluğa ulaşamamıştır. Her geçen gün daha da önemli hale gelen siber güvenliği sağlamada en güvenilir çözüm, hedef uygulama için en uygun kriptografik algoritmaların seçilerek kullanılmasıdır. Tasarımcılar için hangi algoritmanın en uygun olduğunu seçmek önemli bir problem teşkil etmektedir. Özellikle hafif siklet gömülü sistemlerdeki kısıtlı işlemsel kaynaklar nedeniyle modern kriptografik algoritmalar bu platformlarda yüksek başarımla kullanılamamaktadır. Nesnelerin İnterneti aygıtları gibi bu tür kısıtlı kaynağa sahip sistemlerin güvenliğini sağlayabilmek amacıyla geliştirilen hafif siklet kriptografi bu önemli darboğazın aşılabilmesi için fırsatlar sunmaktadır [4].

11.2. NESNELERİN İNTERNETİ KAVRAMINA GENEL BAKIŞ

İnternet, dünya çapındaki ağın yayına girmesinden bu yana insanları birbirine bağlamak için kullanılıyor, ancak günümüzde iletişim teknolojisindeki ilerlemelerin bir sonucu olarak, internet, insanlardan çok daha fazla cihazı birbirine bağlar hale gelmiştir. Nesnelerin İnterneti (Internet of Things - IoT) terimi, bu bağlı cihazları tanımlamak için kullanılmaktadır. Bunlardan bazıları masaüstü bilgisayarlar veya tabletler gibi güçlü bilgi işlem yeteneklerine sahip olsa da, Nesnelerin İnterneti ekosisteminde kablosuz sensör düğümleri, giyilebilir biyomedikal telemetri aygıtları, uzaktan alarm monitörleri ve radyo frekansıyla tanımlama (RFID) cihazları gibi sınırlı bilgi işlem kaynaklarına sahip cihazlar ve sistemler popülasyonun çoğunluğunu oluşturmaktadır [5].

İnternete ya da bir ağa bağlanabilme kabiliyeti olan herhangi bir gömülü sistem aygıtı üzerine entegre algılayıcı ve/veya eyleyiciler de bulunuyorsa kolaylıkla bir Nesnelerin İnterneti aygıtı haline getirilebilmektedir. Nesnelerin İnterneti aygıtlarının sahaya dağıtım, uzaktan izleme ve servis sağlama, uzaktan yönetim ve sonrasında düzenli güncellemeler ile hizmet ömrünün sonunda hizmetten çıkarma şeklinde çok basit bir geliştirme yaşam döngüsü bulunmaktadır. Bilinen ilk Nesnelerin İnterneti aygıtı 1982 yılında Carnegie-Mellon Üniversitesi Bilgisayar Bilimleri Bölümü'ndeki bazı lisansüstü öğrencilerin bir içecek otomatını hobi amaçlı internete bağlamasıyla ortaya çıkmıştır [6]. Basit bir arayüze sahip olan bu proje kullanıcıların makinenin içecek stok durumunu ve mevcut sıcaklığını uzaktan gözlemleyebilmelerine

olanak sağlıyordu. Bu milattan sonra Nesnelerin İnterneti paradigması sürekli gelişerek ve yaygınlaşarak günümüze kadar ulaşmıştır. Bugün, bir dizi Nesnelerin İnterneti ürününün dünyada bulunan insan sayısını geride bıraktığı kaydadeğer bir gerçektir. Şekil 11.1'de gösterilen gelecek projeksiyonuna göre 2025'li yıllarda 75 milyar Nesnelerin İnterneti aygıtının globalde var olacağı öngörülmektedir [7].



Şekil 11.1. Nesnelerin interneti aygıtları için gelecek projeksiyonu [7]

Grafikten de görüldüğü üzere, Nesnelerin İnterneti pazarında eksponansiyel bir genişleme beklenmektedir ve bu beklentilere uygun şekilde günümüzde Nesnelerin İnterneti aygıtlarının pazarı her geçen gün hızla genişlemekte ve bunları günlük olarak kullanan kullanıcı sayısındaki ciddi artışla birlikte daha popüler hale gelmektedir.

11.3. NESNELERİN İNTERNETİNDE GÜVENLİK PROBLEMİ

Nesnelerin İnterneti aygıtlarının sunmuş oldukları çeşitli avantajlar vardır ve bunlar gerek uzaktan gözlem, gerek uzaktan kontrol imkanları sunarak gündelik hayatı pek çok alanda daha verimli kılmakta ve yaşam kalitesini artırmaktadır. Nesnelerin İnterneti teknolojisi, makineler arası etkileşimi artırarak cihazlar arasındaki bağlantıları teşvik etmektedir ve bunun sonucunda daha iyi çalışan bir kontrol döngüsü elde edilmekte ve sistemlerin otomasyonu kolaylaşmaktadır. Nesnelerin İnterneti aygıtları çevresel parametrelerin

çok daha iyi, detaylı uzun vadeli olarak gözlemlenmelerine olanak sağlar ve böylece pek çok iş alanında zamandan tasarruf sağlayarak verimliliği artırır. Sağlamış olduğu pek çok avantaja rağmen Nesnelerin İnterneti teknolojisinin bazı dezavantajları da bulunmaktadır. Öncelikle Nesnelerin İnterneti aygıtları için üzerinde uzlaşılmış olan herhangi bir uluslararası standart bulunmamaktadır. Kompleks yapıları nedeniyle sistemlerin arızalanmasını daha kolay hale getirebilmektedirler. Ancak en önemli dezavantaj siber güvenlik sorunu olarak karşımıza çıkmaktadır. Nesnelerin İnterneti aygıtları gizlilik ve güvenlik ihlalleri için siber saldırganlara çeşitli fırsatlar sunmaktadır.

Nesnelerin İnterneti, dünyayı kapsayan devasa bir saldırı yüzeyi oluşturarak birçok fırsatın yanı sıra birçok tehdidi de beraberinde getirmektedir. Nesnelerin İnterneti aygıtları aracılığıyla gerçekleştirilen siber saldırıların ortaya çıkması ve son yıllardaki gözlemlenen artış, günlük hayatımızın bağlı olduğu hizmetler için artık engelleyici bir tehdit haline gelmiştir [8]. Nesnelerin interneti aygıtlarında bilgi güvenliği özellikleri, hem pazara hızlı çıkma baskısı hem de maliyeti azaltma kaygıları nedeniyle üreticiler tarafından tasarım sürecinde genellikle ihmal edilmektedir. Prematüre tasarlanmış bu Nesnelerin İnterneti aygıtları, herhangi bir ağa bağlandıklarında doğal olarak siber güvenlik açısından zincirin en zayıf halkasını oluşturmakta ve en az eforla en fazla karı elde etmeyi hedefleyen siber suçlular için olağan hedefler haline gelmektedirler. Modern kriptografi mühendisliği sayesinde siber güvenliğin sağlanması mümkündür, ancak kısıtlı kaynaklara sahip bu düşük maliyetli Nesnelerin İnterneti aygıtlarında modern kriptografik algoritmaların çalıştırılması önemli bir problem olarak karşımıza çıkmaktadır.

Hafif siklet kriptografik (HSK) şifreleme algoritmaları, performanstan ödün vermeden Nesnelerin İnterneti aygıtları, RFID kartları gibi hafif siklet gömülü sistemlerin siber güvenliğini sağlamak için geliştirilmişlerdir. Hafif siklet kriptografi, performans darboğazları veya ek maliyetler yaratmadan gömülü sistemlerin güvenliğini sağlamayı hedeflediği için endüstrinin ilgisini çekmektedir. Örneğin, RFID teknolojisindeki ilerlemeler, dün hayal olan birçok uygulamayı günümüzde mümkün kılmıştır ve RFID etiketleri, mühendisliğin kimlik doğrulama, uzaktan takip, depo otomasyonu gibi birçok farklı alanında yaygın olarak kullanılmaktadır. Ancak, ortaya çıkan RFID aygıtlarının sunduğu fırsatlar, güvenlik açıklarından kaynaklanan meydan okumalarla maliyet-fayda terazisini dengelemektedir. Düşük maliyetli temel RFID etiketlerinin genellikle 1-10 bin lojik kapıyla sınırlı bir donanım kaynağı bütçesi

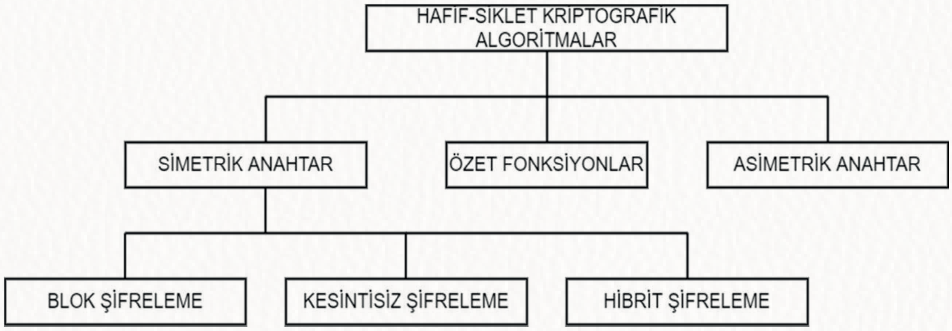
vardır ve bunların yalnızca sınırlı bir kısmı güvenlik işlevleri için kullanılabilmektedir [9]. Bu nedenle, hafif siklet kriptografi çözümlerinin çok verimli bir nitelikte olmaları, en az kaynak kullanarak en fazla güvenliği sağlamaları başarı hedeflerine ulaşabilmek için hayati önem taşımaktadır. Literatürde her biri kendi özel avantajlarına sahip çok sayıda hafif siklet kriptografik algoritma bulunmaktadır, ancak günümüzde bu algoritmalar için ortaya konmuş ve üzerinde anlaşılmış uluslararası bir norm bulunmamaktadır. Bununla birlikte, halihazırda devam etmekte olan bazı standardizasyon çalışmaları vardır [10]. Hafif siklet kriptografik algoritmalar, tipik olarak gerçek zamanlı uygulamaların ihtiyaçlarını karşılamak için minimum gecikmeyle çalışacak şekilde ve aynı zamanda maliyete duyarlı uygulamaların ihtiyaçlarını da karşılayabilmek için düşük karmaşıklık düzeyinde tasarlanırlar [11]. Bu algoritmaların kabul edilebilir bir kriptografik güvenlik düzeyi sağlamaları için genellikle yeterli tur sayısında çalıştırılmaları gereklidir.

Bu çalışmada, Nesnelerin İnterneti uygulamalarında kullanıma uygun olan hafif siklet kriptografik algoritmaların bir derlemesi gerçekleştirilmiştir. Bölüm 11.2'de Nesnelerin İnterneti hakkında tarihsel gelişim, ortaya çıkan fırsatlar ve tehditler tanıtılmış, Bölüm 11.3'te ise Nesnelerin İnterneti paradigmasının en önemli probleminin siber güvenlik olduğu anlatılmıştır. Bölüm 11.4'te Nesnelerin İnterneti aygıtlarında siber güvenlik problemini çözmek için kullanılabilecek hafif siklet kriptografik algoritmaların ve özetleme fonksiyonlarının bir taksonomisi sunulmuştur. Bölüm 11.4.1'de simetrik, Bölüm 11.5'te ise asimetrik anahtar kullanan hafif siklet kriptografik algoritmalar ve her algoritmanın göze çarpan temel özellikleri tanıtılmıştır. Bölüm 11.6'da hafif siklet özetleme algoritmaları hakkında bilgiler paylaşılmış ve Bölüm 11.7'de ise hafif siklet kriptografi konusunda günümüzdeki standartlaşma çalışmalarının durumu hakkında genel bilgiler sunulmuş ve son olarak, Bölüm 11.8'de ise genel bir değerlendirme ve gelecek öngörüleri paylaşılmıştır.

11.4. HAFİF SİKLET KRİPTOGRAFİK ALGORİTMALAR

Modern kriptografik algoritmalar, hızlı bilgi işleme kabiliyetine sahip cihazlarda yüksek performansla çalışabilirler, ancak bunları kaynakları ve işlem gücü sınırlı olan Nesnelerin İnterneti aygıtlarında verimli şekilde çalıştırmak zor bir problemdir. Buna teşebbüs edildiğinde Nesnelerin İnterneti aygıtların-

daki kısıtlı kaynaklar nedeniyle ciddi bir performans darboğazı ile karşılaşılacağı açıktır. Ayrıca, bu cihazlardan bazıları batarya ile çalışabilir niteliktedir ve sahaya bir kez yerleştirildikten sonra batarya değişimi mümkün olmayabilir. Cihazdaki yazılımın neden olduğu güç tüketimi çok yüksek ise cihazın planlanan ömrü çok kısa olacaktır. Bu nedenle Nesnelerin İnterneti aygıtları için tasarlanmış özel kriptografik algoritmalara ihtiyaç bulunmaktadır. Bu sınırlamalar göz önünde bulundurularak tasarlanan kriptografik algoritmalar hafif siklet algoritmalar olarak sınıflandırılmaktadır [12]. Hafif siklet kriptografik şifreleme algoritmaları, mimari yapılarına göre Şekil 11.2'de gösterildiği şekilde sınıflandırılabilir [13].



Şekil 11.2. Hafif siklet kriptografik algoritmaların sınıflandırılması

11.4.1. Simetrik Anahtar Hafif Siklet Kriptografik Algoritmalar

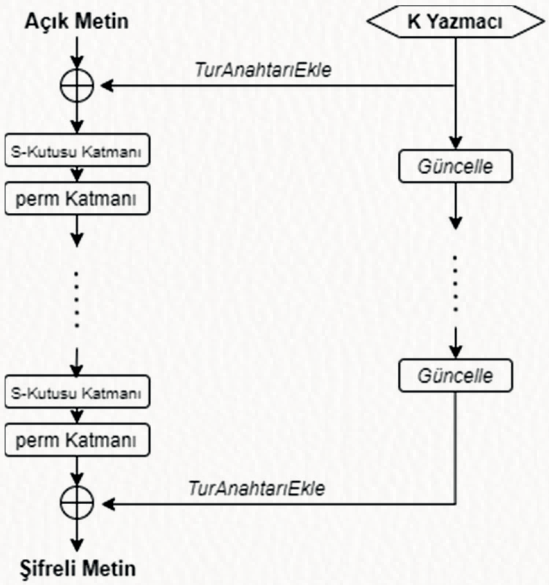
Simetrik anahtar hafif siklet kriptografik (SA-HSK) algoritmalarında şifreleme ve şifre çözme işlemleri için aynı mimari ve tek anahtar kullanılır. Bu anahtarın gizli olması ve saldırganlara karşı haberleşme yapanlar tarafından korunması gerekmektedir. SA-HSK algoritmalar asimetrik anahtar kullanan hafif siklet kriptografik algoritmalara (AA-HSK) göre çok daha yüksek hızlarda çalışırlar. PRESENT, PRINCE, SIMON, IDEA gibi algoritmalar hafif siklet simetrik anahtar kriptografik algoritmalara örnek olarak verilebilirler [14-16]. Günümüzde özellikle veri şifreleme ve veri bütünlüğü uygulamalarında simetrik anahtar kriptografik algoritmalar çok yaygın bir şekilde kullanılmaktadır. Simetrik anahtar kriptografik algoritmalar blok şifreleme, kesintisiz şifreleme ve hibrit şifreleme şeklinde sınıflandırılabilirler.

11.4.2. Blok Şifreleme Yapısındaki SA-HSK Algoritmalar

Simetrik anahtar altyapısı kullanan blok şifreleme mimarisine dayanan hafif siklet kriptografik algoritmalar, veri akışındaki tek tek bitler yerine veri bloklarına bir anahtar ve algoritma şeklinde uygulanırlar. Geleneksel simetrik anahtar kriptografik algoritmalara göre çok daha az kaynak harcayan ve pek çok gömülü sistem uygulamasının ihtiyaç duyduğu güvenliği performanstan ödün vermeden sunan blok yapıdaki bu algoritmalar aşağıdaki şekilde temel özellikleri verilerek tanıtılmıştır.

11.4.2.1. PRESENT

Simetrik anahtar blok şifreleme mimarisine sahip olan geleneksel AES algoritması, kaynakların çok kısıtlı olduğu RFID etiketleri ya da algılayıcı ağ uygulamaları için uygun olmamasından yola çıkılarak geliştirilen PRESENT algoritması yer değiştirme – permütasyon ağlarına dayanan blok yapıda bir SA-HSK olarak geliştirilmiştir ve AES'e göre 2.5 kat daha küçüktür [14]. 31 turda tamamlanan algoritma 64 bitlik veri bloklarını 80 bitlik ya da 128 bitlik iki farklı anahtar boyu kullanarak işleyebilmektedir. PRESENT SA-HSK algoritmasının genel yapısı Şekil 11.3'te gösterildiği gibidir [14].



Şekil 11.3. PRESENT SA-HSK algoritmasının mimarisi

Her tur, bir tur anahtarı, doğrusal bit bazında bir permütasyon ve doğrusal olmayan bir yer değiştirme katmanı işlemek için bir XOR işleminden oluşur. Doğrusal olmayan katman, her tura paralel olarak 16 kez uygulanan 4 bitlik bir S-kutusu kullanır [14]. PRESENT algoritması 80 veya 128 bitlik anahtarlar kullanabilmektedir. 80 bitlik anahtar programlama senaryosunda, kullanıcı tarafından sağlanan ve $k_{79}k_{78}k_{77}...k_0$ ile temsil edilen anahtar bir K anahtar yazmacında saklanır. Çalışma esnasında i. turundaki 64 bitlik tur anahtarı $K_i=k_{63}k_{62}...k_0$, K yazmaç içeriğinin en soldaki bitlerinden oluşturulur. Tur anahtarı oluşturma yöntemi Şekil 11.4'te gösterildiği şekilde gerçekleşir.

Algoritma 1: PRESENT Tur Anahtarı

```
1 TurAnahtarlarıÜret()
2 for i = 0 to 31 do
3 |   TurAnahtarlarıEkle(DURUM, K_i)
4 |   sKutuKatmanı(DURUM)
5 |   permKatmanı(DURUM)
6 end
7     TurAnahtarıEkle(DURUM, K_32)
```

Şekil 11.4. PRESENT SA-HSK algoritmasında tur anahtarı üretimi

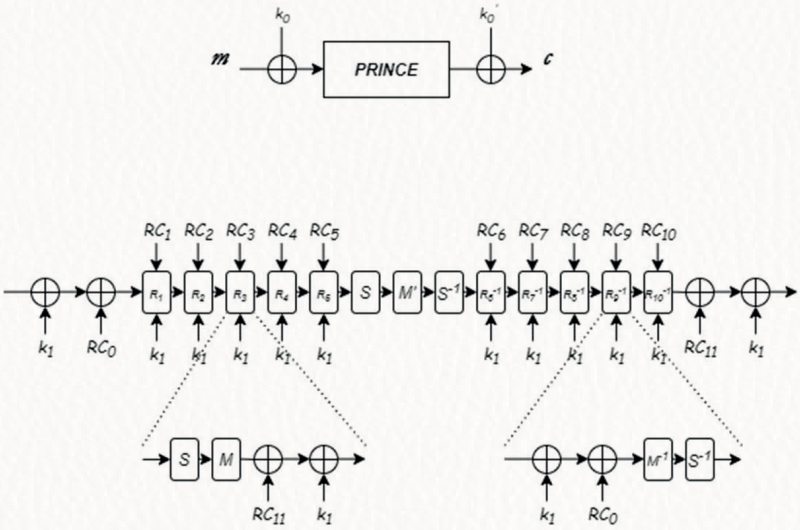
11.4.2.2. PRINCE

Düşük maliyetli ve yerdeğiştirme – permütasyon ağları tabanlı blok yapıdaki SA-HSK algoritmalarından biri de PRINCE algoritmasıdır. PRINCE, anlık şifreleme gerçekleştirebilir, düşük gecikme sağlayan tek bir saat döngüsü içinde şifreli metin hesaplanır. PRINCE, 128 bit anahtarlı 64 bitlik bloklar kullanan bir SA-HSK algoritmasıdır. Anahtar 64 bitlik $K = K_0 \,||\, K_1$ şeklinde iki gruba bölünerek ve Denklem 11.1 uyarınca 192 bite genişletilerek kullanılır [15].

$$[K_0 \,||\, K_1] \rightarrow (K_0 \,||\, K'_0 \,||\, K_1) = (K_0 \,||\, (K_0 >>> 1)) \text{ xor } (K_0 >>> 63) \,||\, K_1 \qquad (11.1)$$

K_0 ve K'_0, eş dağıtımlama anahtarı olarak kullanılır, öte yandan K_1 anahtarı, PRINCE algoritmasındaki 12 turluk blok şifreleme için kullanılacak olan 64 bitlik anahtarı temsil eder [15]. PRINCE algoritmasının her turu, bir anahtar

ekleme, bir S-kutusu katmanı, bir doğrusal katman ve bir tur sabitinin eklenmesinden oluşmaktadır. PRINCE algoritmasının uygulanması Şekil 11.5'te gösterildiği gibi özetlenebilir [15].



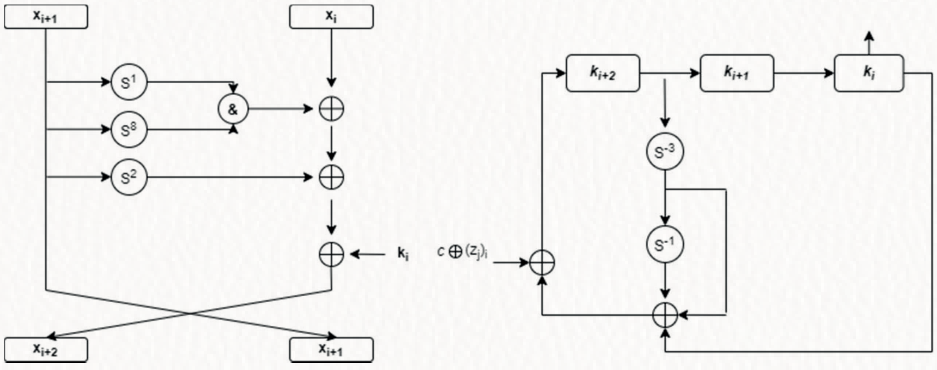
Şekil 11.5. PRINCE SA-HSK algoritmasında şifreleme işlem akışı

11.4.2.3. SIMON

SIMON, ABD Ulusal Güvenlik Ajansı NSA tarafından son derece kısıtlı kaynaklara sahip aygıtlar için tasarlanmış Feistel ağlarına dayanan ve blok yapıda olan bir SA-HSK algoritmasıdır [16]. SIMON ailesi blok boyutları ve anahtar boyutları için Tablo 11.1'de gösterildiği gibi çeşitli seçenekler sunmaktadır. Şekil 11.6a'da da gösterildiği gibi SIMON tur fonksiyonu AND-RX yapısındaki bir Feistel ağ mimarisine sahiptir ve matematiksel olarak bit düzeyinde XOR, bit düzeyinde AND, bit düzeyinde sola rotasyon $S^a(b)$ (a: rotasyon sayacı) işlemlerine dayanır [16]. Simon anahtar üretim zamanlaması, tüm tur anahtarlarının asıl bir anahtardan üretilmesini sağlayarak algoritmaya anahtar genişletme kabiliyeti sunmaktadır. Anahtar genişletme işlemi Şekil 11.6b'de gösterildiği gibi bit düzeyinde XOR ve bit düzeyinde sağa rotasyon işlemleri ile sağlanmaktadır [16].

Tablo 11.1. SIMON SA-HSK algoritma ailesinin parametreleri

Blok Boyutu (2n)	Anahtar Boyutu (mxn)	Veri boyutu (n)	Tur Anahtar Sayısı (m)	Sabitler	Tur Sayısı (T)
32	64	16	4	Z_0	32
48	72	24	3	Z_0	36
48	96	24	4	Z_1	36
64	96	32	3	Z_2	42
64	128	32	4	Z_3	44
96	96	48	2	Z_2	52
96	144	48	3	Z_3	54
128	128	64	2	Z_2	68
128	192	64	3	Z_3	69
128	256	64	4	Z_4	72

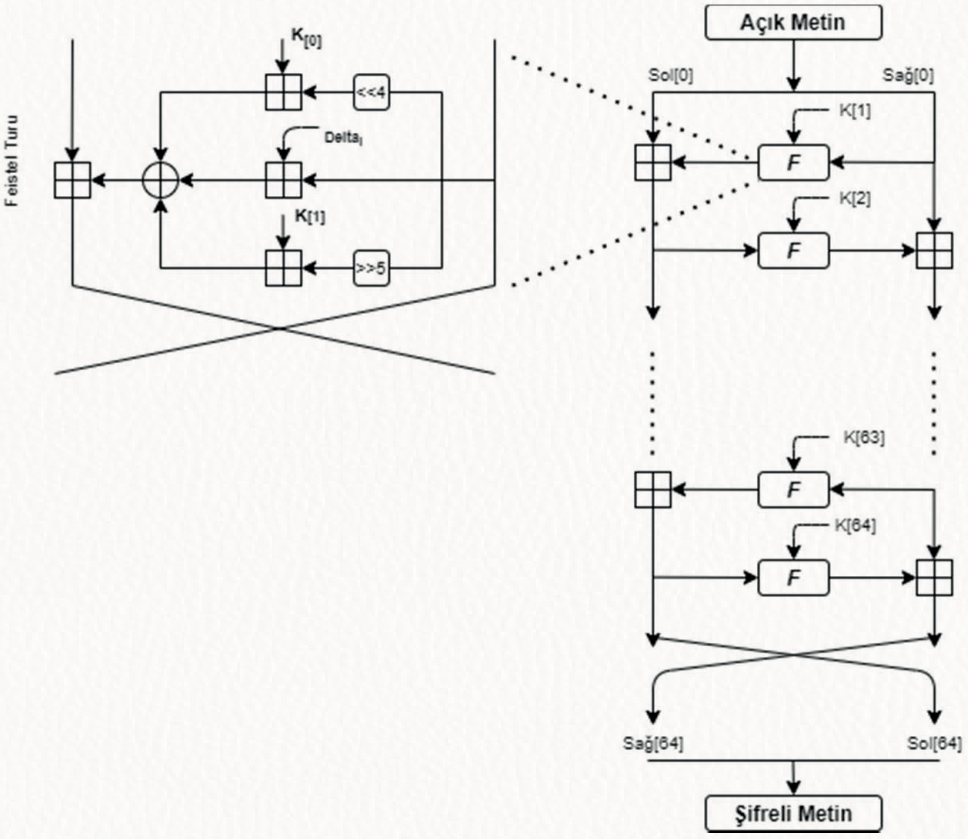


Şekil 11.6. SIMON SA-HSK algoritmasının (a) Tur fonkisyonu ve (b) Anahtar genişletme işlemi

11.4.2.4. Tiny Encryption Algorithm - TEA

TEA, Wheeler ve Needham tarafından 1994'de tasarlanan Feistel blok şifreleme yapılı bir SA-HSK algoritmasıdır [17]. Bellek alanını en aza indirmek ve hızı en üst düzeye çıkarmak için tasarlanmıştır. TEA, karışık cebirsel grup

işlemleri kullanan bir Feistel tipi şifreleme algoritmasıdır. Çift kaydırma, verilerin ve anahtarların ardışıl olarak karşılaştırılmasını sağlar. Anahtar üretim algoritmasında, 128 bitlik K anahtarı 32 bitlik dört bloğa bölünür. Şifreleme algoritmasının giriş verileri 64 bitlik açık metin bloğu ve 128 bitlik K anahtarından oluşur. Açık metin bloğu sol[0] ve sağ[0] olarak iki parçaya bölünür ve her blok diğer bloğu 64 turda şifreleyerek işlem sonunda 64 bitlik şifreli bir metin bloğu üretilir. 64 adet Feistel döngüsünden oluştuğu bilinen TEA SA-HSK algoritmasının genel yapısı Şekil 11.7'de verilmiştir [17]. TEA her döngüde anahtar ve delta[i] sabiti ile toplama, XOR ve mantıksal kaydırma işlemlerinden oluştuğu gözlemlenebilir.



Şekil 11.7. TEA SA-HSK algoritmasının mimarisi ve feistel tur fonksiyonu

11.4.2.5. HIGHT

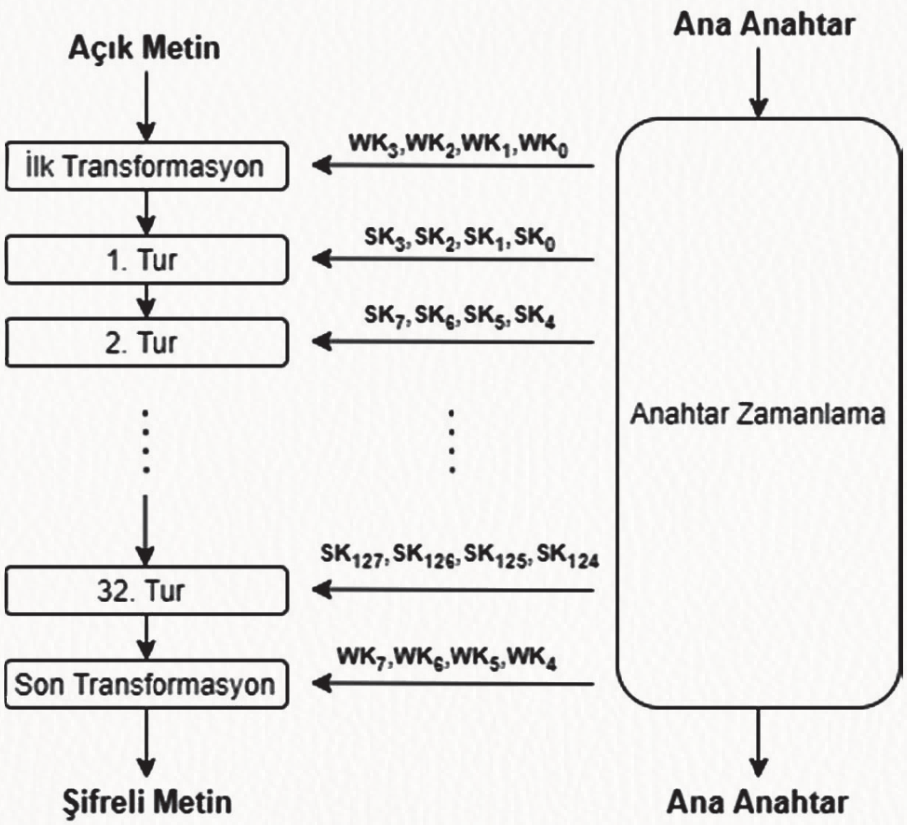
HIGHT, 64 bit blok uzunluğuna ve 128 bit anahtar uzunluğuna sahip hafif siklet bir blok şifreleme algoritmasıdır. Algoritma, düşük maliyetli, düşük güçlü ve ultra hafif uygulamalar için uygundur. XOR, ek mod (2^8) ve sol bit yönünde döndürme gibi basit işlemlerden oluşan 32 tur yinelemeli bir yapıya sahiptir [18]. HIGHT şifreleme algoritması Şekil 11.8'de açıklandığı gibi çalışır:

Algoritma 2: HIGHT SA-HSK Algoritması

Girdi: P, M K, açık metin, anahtar
Çıktı: C, M K
Sonuç: C, Şifreli metin
1 HIGHT Şifrele(P, M K)
2 Anahtar Zamanla (M K, W K, S K)
3 HIGHT Şifrele(P, W K, S K)
4 İlkTransformasyon (P,X_0, W K_3, W K_2, W K_1, W K_0);
5 **for** i = 0 to 31 **do**
6 TurFonksiyonu (X_i, X_{i+1}, S K_{4i+3}, S K_{4i+2}, S K_{4i+1}, S K_{4i});
7 **end**
8 SonTransformasyon (X_{32}, C, W K_7, W K_6, W K_5, W K_4);

Şekil 11.8. HIGHT SA-HSK algoritması

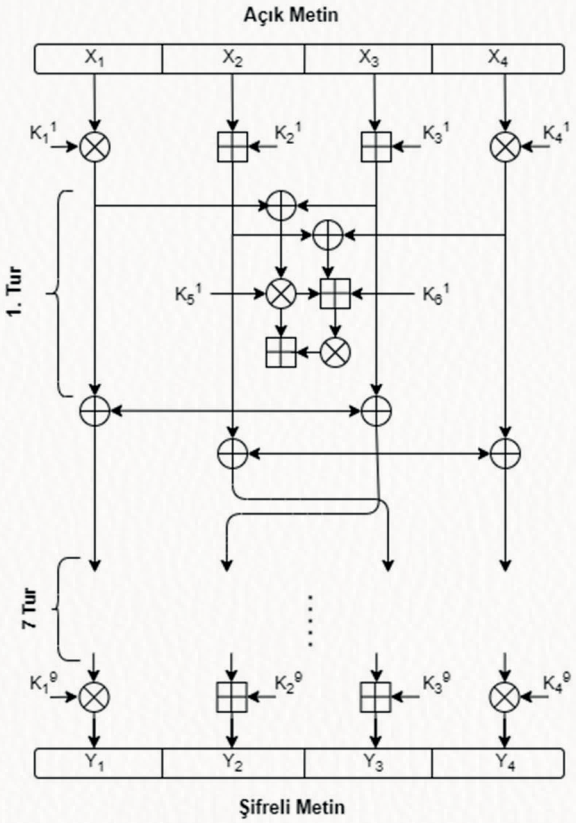
HIGHT algoritması yazılım değil donanım odaklı bir SA-HSK algoritmasıdır. HIGHT'ın anahtar zamanlama algoritması, tüm genişletme anahtarlarını ve tüm alt anahtarları oluşturduktan sonra ana anahtarın orjinal değerini koruyacak şekilde tasarlanmıştır. HIGHT algoritmasının şifreleme işlemi Şekil 11.9'da gösterilmektedir. 64 bitlik açık metin ve şifreli metin, 8 baytlık bağlantılar olarak kabul edilir ve 128 bitlik ana anahtar, 16 baytlık bir bağlantı olarak kabul edilir. HIGHT'ın şifreleme işlemi, anahtar zamanlama, ilk transformasyon, tur fonksiyonu ve son transformasyondan oluşan şifre çözme işlemiyle aynıdır [18].



Şekil 11.9. HIGHT SA-HSK algoritmasının işlem akışı

11.4.2.6. International Data Encryption Algorithm (IDEA)

Uluslararası Veri Şifreleme Algoritması (IDEA), 64 bit blok boyutu ve 128 bit anahtar uzunluğu üzerinde çalışan bir SA-HSK blok şifreleme algoritmasıdır [19]. Aynı anahtarı kullanarak hem şifreleme hem de şifre çözme işlemleri gerçekleştirilir. Algoritma, şifrelemede karıştırma ve difüzyon yöntemlerini kullanır ve matematiksel olarak bit düzeyi XOR, mod (2^{16}) toplama ve mod (2^{16}+1) çarpma cebirsel işlemlerine dayanır [19]. IDEA SA-HSK algoritmasının bir turu, sekiz özdeş transformasyondan oluşur. Algoritma bu transformasyonlara ek olarak, yarım turda tamamlanan bir çıktı transformasyonundan oluşur. Algoritmanın şifreleme işlemi Şekil 11.10'da gösterilmiştir [19].



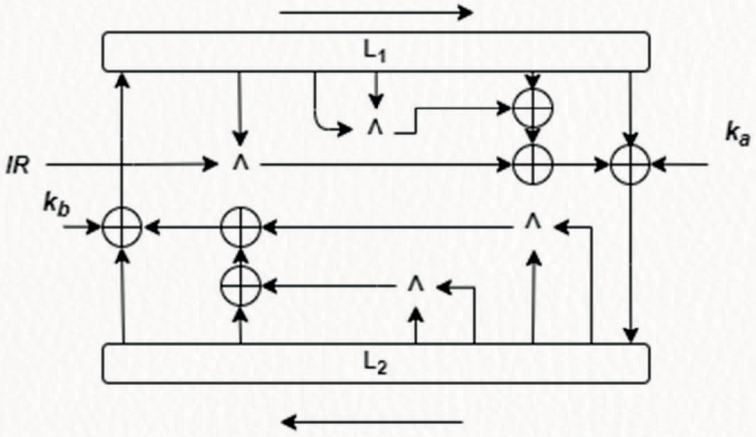
Şekil 11.10. IDEA SA-HSK algoritmasının işlem akışı

11.4.2.6. KATAN / KTANTAN

KATAN / KTANTAN SA-HSK blok şifreleme algoritma ailesi donanım odaklı ve lineer olmayan kaydırma yazmaçlarına dayalı bir şifreleme algoritmasıdır [20]. Her iki blok şifreleme algoritması aynı boyutlu anahtara sahip olmasına karşın blok boyutları farklı olabilmektedir. Bu ailedeki algoritmaların isimlendirilmeleri Tablo 11.2'deki parametrelere göre yapılır. KATAN / KTANTAN ailesinin bir turunun genel yapısı Şekil 11.11'de gösterildiği gibidir [20]. Açık metin, L_1 ve L_2 olmak üzere iki yazmaça yüklenir. Her turda, L_1 ve L_2, sola kaydırılır ve hesaplanan yeni bitler L_1 ve L_2 nin en az anlamlı olan konumlarına yüklenir. Şifreleme algoritmasının 254 turundan sonra, yazmaçların içeriği şifreli metin olarak dışa aktarılır.

Tablo 11.2. KATAN/KTANTAN SA-HSK Algoritma Ailesinin Parametreleri

Algoritma Varyantı	Blok Boyutu (bit)	Anahtar Boyutu (bit)
KATAN32	32	80
KATAN48	48	80
KATAN64	64	80
KTANTAN32	32	80
KTANTAN48	48	80
KTANTAN64	64	80



Şekil 11.11 KATAN/KTANTAN SA-HSK algoritmasının yapısı

11.4.3. Kesintisiz Şifreleme Yapısındaki SA-HSK Algoritmalar

Blok şifrelemeye alternatif olarak geliştirilmiş olan kesintisiz şifreleme, bir veri akışındaki her bir ikilik tabandaki basamağa, her seferinde bir bit olmak üzere bir şifreleme anahtarının ve algoritmanın uygulandığı bir şifreleme yöntemidir. Kesintisiz şifreleme yöntemlerini özellikle benzersiz yapan şey, verileri bir seferde bir bit veya bayt olarak şifrelemeleridir. Bu, hızlı ve blok şifrelemeye göre nispeten daha kolay bir şifreleme işlemi sağlar. Simetrik anahtar altyapısı kullanan kesintisiz şifreleme mimarisine dayalı SA-HSK algoritmaları temel özellikleriyle tanıtılacaktır.

11.4.3.1. MICKEY

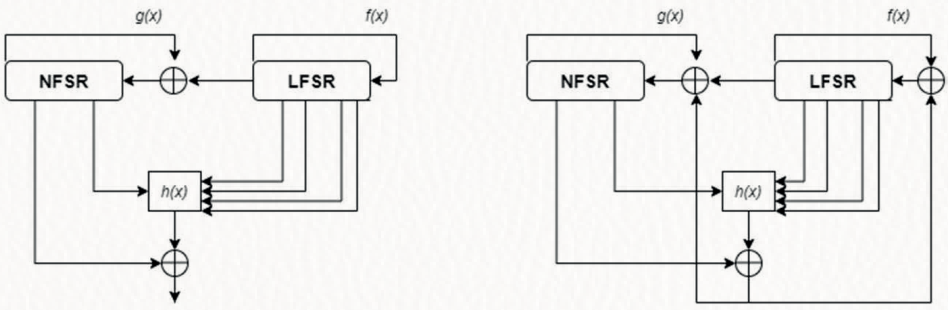
MICKEY (Mutual Irregular Clocking KEY stream generator), Babbage ve Dodd tarafından kısıtlı kaynaklara sahip donanım platformları için geliştirilmiş bir kesintisiz SA-HSK algoritmasıdır [21]. Karşılıklı düzensiz saatle çalışan anahtar akış üreteci yapısına sahip olan MICKEY SA-HSK algoritmasında kesintisiz şifreleme iki yazmacı temel alır: Bir doğrusal geri besleme kaydırmalı yazmaç (LFSR) ve bir doğrusal olmayan geri besleme kaydırmalı yazmaç (NLFSR). Bu iki yazmacın arasındaki temel fark güncelleme fonksiyonudur. İlk olarak eSTREAM projesine sunulan MICKEY v1.0, tespit edilen güvenlik açıklarını gidermek için MICKEY v2.0 olarak güncellenmiş bir sürüm olarak literatüre sunulmuştur [21]. MICKEY 2.0 kesintisiz SA-HSK algoritması, R (Doğrusal yazmaç) ve S (Doğrusal olmayan yazmaç) olarak adlandırılan, her biri düzensiz saat işaretleriyle sürülen ve her biri diğeri tarafından kontrol edilen iki adet 100 bitlik kaydırma yazmacına sahiptir. Şifre spesifikasyonları, her anahtarın aynı uzunluktaki 2^{40} 'a kadar farklı ilk değerlerle kullanılabileceğini ve her anahtar-ilkdeğer çiftinden 2^{40} 'a kadar kesintisiz anahtar akışı bitlerinin üretilebileceğini rapor etmektedir [21].

11.4.3.2. GRAIN

GRAIN, toplam lojik kapı sayısı, güç tüketimi ve belleğin sınırlı olduğu Nesnelerin İnterneti gibi hafif siklet donanım platformları için geliştirilmiş bir kesintisiz akış SA-HSK şifreleme algoritma ailesidir [22]. GRAIN, doğrusal bir geri besleme kaydırma yazmacı (LFSR), doğrusal olmayan bir geri besleme kaydırma yazmacı (NLFSR) ve bir Boole filtre fonksiyonu olarak üç yapıtaşına dayanmaktadır. GRAIN v1, 80 bit anahtar boyutuna ve 64 bit ilkdeğer vektörüne sahiptir. GRAIN algoritmasının genel yapısı Şekil 11.12a'da gösterilmektedir [22].

LFSR'nin içeriği $[s_i,s_{i+1},...s_{i+79}]$ ile ifade edilmiştir ve NLFSR'nin içeriği de $[b_i,b_{i+1},...b_{i+79}]$ ile temsil edilmektedir. LFSR'ı güncellemek için sonlu alan aritmetiğinde bir geri besleme polinomu olarak yazılabilen farklı düğümler ya da düğümlerdeki tek değerleri XOR'layarak kaydırma yazmacının nasıl güncelleneceğini belirleyen özel fonksiyonlar kullanılabilir. GRAIN algoritmasının çalışması bir anahtar ilklendirme aşaması ve bir kesintisiz anahtar akışı üretme aşaması olarak toplam iki aşamadan oluşur [22]. Şekil 11.12b'de gösterilen anahtar ilklendirme işlemi şifreleme sürecinin ilk aşamasında yapılır. Her bir biti $k_i \in [0, 79]$ ile gösterilen k anahtarı, NLFSR'ye yüklenir.

Bundan sonra, LFSR'nin ilk 64-biti, IV_i ile gösterilen bir ilkdeğer vektörüne (IV) yüklenir, burada i ϵ [0, 79] şeklindedir ve her $s_i = IV_i$ için de i ϵ [0, 63] şeklindedir. LFSR'nin geri kalan 16 bitine lojik 1 değeri yazılır. Son olarak, algoritma, 160 saat döngüsünde herhangi bir çıkış biti üretmeden boşta çalıştırılır. Bu süreçte z_i çıkış fonksiyonundan elde edilen bitler geri beslemede kullanılarak LFSR'nin yanı sıra NLFSR'nin girişi ile XOR işlemi yapmak için kullanılır. Bu işlem Şekil 11.12b'de gösterilmiştir [22].

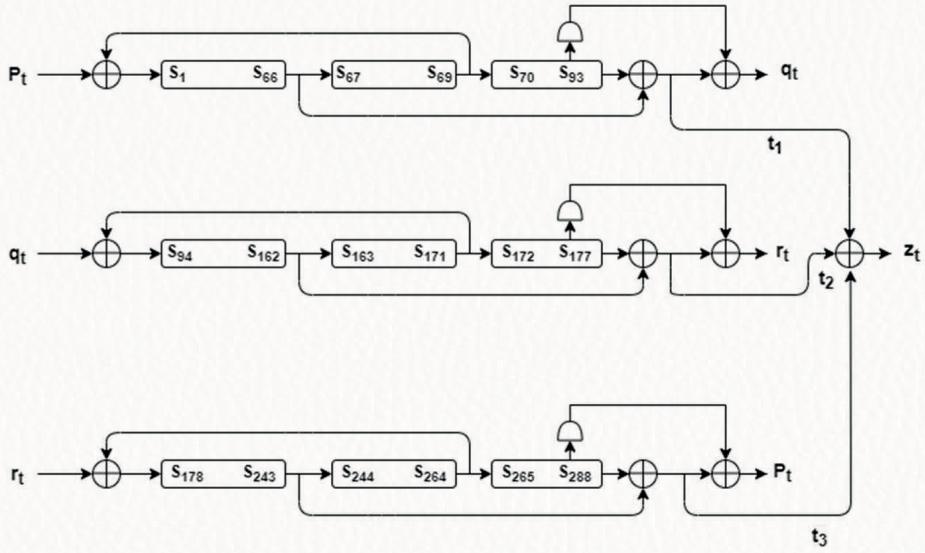


(a) (b)

Şekil 11.12. GRAIN Hibrit SA-HSK algoritmasının (a) Yapısı ve (b) Anahtar ilklendirme işlemi

11.4.3.3. TRIVIUM

TRIVIUM, Cristophe De Camiére ve Bert Preneel tarafından, yüksek performans gereksinimleri olan kısıtlı kaynaklara sahip aygıtlar için geliştirilmiş eşzamanlı çalışan bir kesintisiz SA-HSK algoritmasıdır [23]. TRIVIUM, kurulum ve kesintisiz anahtar akışı oluşturma aşamalarından oluşur. Tüm süreç, maksimum 2^{64} bit uzunluğunda bir anahtar akışı oluşturur. Kurulum aşamasında, şifrenin gizli durum değişkeni S, farklı kapasitelerde (93, 84, 111) olan üç lineer olmayan geri beslemeli kaydırma yazmacı (NLFSR) kullanılarak tanımlanır ve saklanır [23]. 80 bitlik ilkdeğer vektörü (IV), gizli durum değişkeninin ikinci bileşeni olarak kullanılır. Başlatmadan sonra, gizli durum değişkeni birkaç AND, XOR ve bit kaydırma işlemi yürütülerek daha da işlenir. Kesintisiz anahtar akışı oluşturma aşamasında, halihazırdaki gizli durum değişkeni S'in değerine dayanan ve ardışıl olarak gelen komutları N defa tekrar çalıştırarak N bit uzunluğunda bir anahtar akışı oluşturur. Trivium SA-HSK algoritmasının genel yapısı Şekil 11.13'te gösterilmektedir [23].



Şekil 11.13. TRIVIUM Kesintisiz SA-HSK algoritmasının yapısı

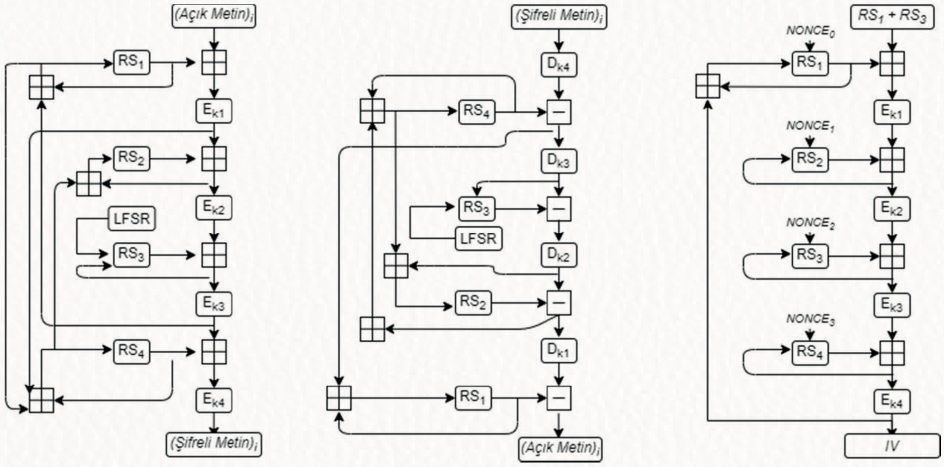
11.4.4. Hibrit Yapıdaki SA-HSK Algoritmalar

Blok ve kesintisiz yapılara sahip olan SA-HSK algoritmalarına ek olarak, bunlardan türetilmiş ve her iki sınıfın da en yararlı özelliklerini kullanmayı hedefleyen hibrit yapıdaki algoritmalar da literatürde bulunmaktadır ve temel özellikleri bu bölümde tanıtılmıştır.

11.4.4.1. HUMMINGBIRD

HUMMINGBIRD, blok ve kesintisiz akış şifrelerine dayalı hibrit bir yapıda bir SA-HSK algoritmasıdır. Özellikle RFID etiketleri ve kablosuz sensör düğümleri gibi kaynakları kısıtlı gömülü cihazlar için tasarlanmıştır [24]. Hibrit yapı, küçük blok boyutunda güvenlik sağlamaktadır. Bu nedenle, çok çeşitli hafif siklet gömülü sistem uygulamaları için düşük yanıt süresi ve güç tüketimi gereksinimlerini karşılamaktadır. Hummingbird, 16 bit blok boyutu, 256 bit anahtar boyutu ve 80 bit dahili durum değişkeni ile blok ve kesintisiz akış yapısının optimum birleşimine dayanmaktadır. Hummingbird algoritmasının genel yapısı Şekil 11.14'te gösterilmektedir ve aşağıdaki notasyon ve işlemlerden oluşmaktadır [24]:

- Dört adet 16 bitlik blok şifre E_{k1}, E_{k2}, E_{k3}, E_{k4}
- Dört adet 16 bit dahili durum kaydı RS_1, RS_2, RS_3, RS_4
- Bir adet 16 aşamalı Lineer Geri Besleme Kaydırma Yazmacı (LFSR),
- Modulo 2^{16} toplama operatörü,
- Modulo 2^{16} çıkarma operatörü,
- Bit düzeyi XOR operatörü.



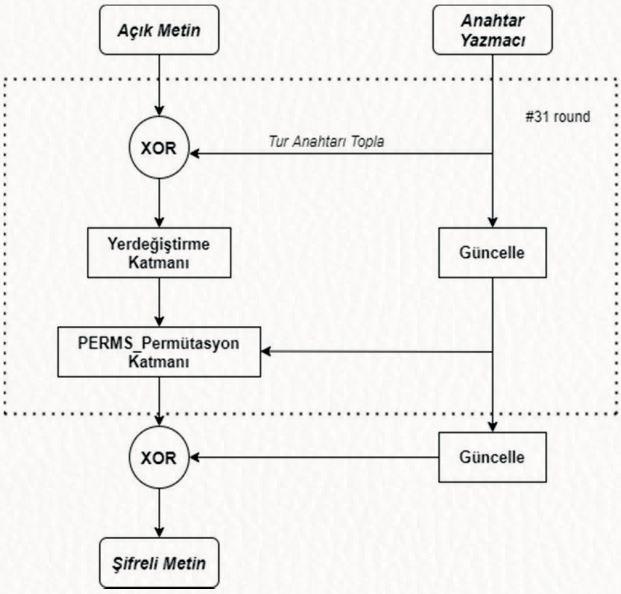
(a) (b) (c)

Şekil 11.14. HUMMINGBIRD Hibrit SA-HSK algoritma yapısı (a) Şifreleme ve (b) Şifre çözme (c) İlklendirme

11.4.4.2. PRESENT-PERMS Hibrit

PRESENT blok şifresi, taşınabilir ve güvenli yazılımların yanı sıra donanım uygulamalarını destekleyen birçok hafif şifreleme algoritmasının ilham kaynağı olmaya devam etmektedir. PRESENT blok şifresinin bir permütasyon katmanı, performansını iyileştirmek için PERMS bit permütasyon işlemi ile değiştirilir ve uygulanır [25]. Diğer bit permütasyon komutlarıyla karşılaştırıldığında, PERMS kriptografik özellikler açısından verimli bir bit permütasyon işlemi sağlar, daha kısa CPU döngüleri gerektirir ve silikon üzerinde az sayıda mantık kapısına ihtiyaç duyar. Bu avantajlar ve özelliklerin bir sonucu olarak, kısıtlı kaynaklara sahip hafif siklet gömülü aygıtlar için yeni

bir hibrit şifreleme algoritması olarak önerilmiştir [25]. PRESENT-PERMS hibrit şifreleme algoritmasının yapısı Şekil 11.15'te gösterilmektedir. PRESENT-PERMS algoritması 128 bit anahtar uzunluğuna sahiptir, 64 bit veya 128 bit olarak iki farklı blok boyutu kullanabilir ve hesaplanması 31 turda tamamlanmaktadır [25].

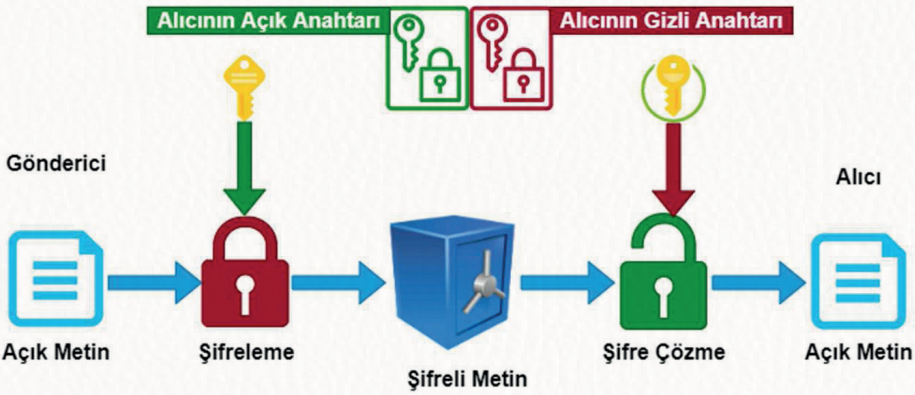


Şekil 11.15. PRESENT-PERMS Hibrit SA-HSK algoritma yapısı

11.5. ASİMETRİK ANAHTAR HAFİF SİKLET KRİPTOGRAFİK ALGORİTMALAR

Asimetrik kriptografi, biri gizli ve diğeri herkese açık olmak üzere iki ayrı anahtar gerektiren özel bir kriptografik algoritma sınıfıdır. Asimetrik ya da diğer bilinen adıyla açık anahtar şifreleme algoritmaları, mesajları şifrelemek ve şifresini çözmek için gizli ve açık anahtar çiftini kullanır. Asimetrik şifreleme kullanıcıları, açık ve gizli anahtar çiftlerini güvenilir bir sertifika yetkilisinden alır. Şekil 11.16'da gösterildiği gibi gönderen kullanıcı iletişim kurmak istediğinde, mesajını şifrelemek ve alıcı tarafa göndermek için alıcının herkese açık olan anahtarını ortak bir dizinden alarak şifreleyip alıcıya gönderir. Şifreli mesaj ulaştığı anda alıcı, asla başkalarının elinde olmaması gereken

ve her zaman saklaması gereken gizli anahtarını kullanarak mesajın şifresini çözer. Bu şekilde asimetrik kriptografi, simetrik kriptografik algoritmaların anahtar dağıtım problemini çözmektedir, ancak bu yeni durumda açık anahtarları saklamak ve paylaşabilmek için güvenilir bir otoriteye ihtiyaç duyulur.



Şekil 11.16. Asimetrik kriptografik algoritma kullanarak güvenli haberleşme

Açık anahtar şifrelemesinin ardındaki ana fikir, yalnızca birinin algoritmasını herkese açık hale getirebilmesi değil, aynı zamanda onun anahtarını da herkese açık hale getirebilmesidir [26]. Açık anahtar şifrelemesi ayrıca reddedilemeyecek dijital imzalar da sağlar. Açık anahtar şifrelemesi, her kullanıcının kendi özel anahtarını korumaktan sorumlu olmasını gerektirirken, simetrik gizli anahtar sistemleri, kullanıcıların gizli anahtarları paylaşmasını ve hatta iletim için üçüncü taraflara güvenmesini gerektirir ki; uygulamada simetrik anahtar dağıtımı önemli bir sorundur. Ayrıca, simetrik gizli anahtar sisteminde, göndericilerin paylaşılan gizli anahtarın iletişimde yer alan taraflardan biri tarafından ele geçirildiğini iddia etmeleri de mümkün olabilmektedir.

Açık anahtar kriptografik algoritmaların sağladığı ana avantajı ileri seviye veri güvenliği olsa da, açık anahtar kriptografik algoritmalarıyla ilgili en yaygın zorluk düşük işlem hızı olarak karşımıza çıkmaktadır. AES ve DES gibi simetrik gizli anahtar şifreleme algoritmaları, mevcut açık anahtar şifreleme yöntemlerinden çok daha hızlıdır. Açık anahtarlı şifreleme ile bu zorluğun üstesinden gelmenin bir yolu, açık anahtar sisteminin güvenlik avantajlarını ve simetrik gizli anahtar sisteminin hızını kullanacak olan hibrit şifreleme yöntemleri geliştirmek olabilir. Açık anahtar kriptografik algoritmalarla ilgili

diğer bir zorluk da, sahte veya güvenliği ihlal edilmiş sertifika yetkilileri aracılığıyla saldırılara açık olmaları durumudur. Bu saldırılar gerçekleştiğinde, siber suçlular, güvenliği ihlal edilen yetkiliden bir ortak anahtar sertifikası seçerek neredeyse herkesin kimliğine bürünebilmektedirler. Bu, siber suçluların başka bir kullanıcının adına ortak bir anahtar bağlamasına olanak tanır.

Açık anahtar şifrelemesinin simetrik gizli anahtar şifrelemesinin yerini alması amaçlanmamıştır; gizli anahtar sistemlerine ek olarak tamamlayıcı nitelikte kullanılmaları hedeflenmiştir. Bununla birlikte, simetrik gizli anahtar şifrelemesinin ideal olmadığı ve özellikle çok sayıda kullanıcının olduğu durumlarda açık anahtar şifrelemesinin cazip olduğu bazı senaryolar vardır. Tipik olarak, açık anahtar şifreleme, çok kullanıcılı bir ortam olduğunda tercih edilen şifreleme yöntemidir ve kullanıcı kimliklerini doğrulamak için anahtar dağıtımı ve dijital imzalar yoluyla gizliliğin sağlanması gerekir.

Açık anahtar şifrelemesi, simetrik gizli anahtar şifreleme sistemlerine göre bir avantaja sahiptir, çünkü gizlice takas edilen anahtarların doğasında bulunan lojistik ve risk sorunlarını azaltmaktadırlar. Simetrik gizli anahtar kriptografisine kıyasla ölçeklenebilirliği ve yüksek güvenliği nedeniyle, açık anahtar kriptografisi uygulamada oldukça popülerdir ve günümüzde kurumsal ortamlarda yaygın olarak kullanılmaktadır. Uygulamada kullanılan açık anahtarlı şifreleme algoritmalarının bazıları RSA, eliptik eğri kriptografisi, ve ELGAMAL algoritması olarak sıralanabilir [27, 29, 32].

11.5.1. RSA Algoritması

RSA algoritması, Ronald Rivest, Adi Shamir ve Leonard Adleman tarafından 1978'de yayınlanan modüler üs tabanlı asimetrik anahtar algoritmasıdır [27]. Algoritma, verileri hem şifrelemek hem de şifresini çözmek için kullanılan gizli bir anahtara sahiptir. Simetrik algoritmalardan farklı olarak, genel anahtar algoritmaları hem açık ($K_{açık}$) hem de gizli (K_{gizli}) anahtarların matematik kullanılarak hesaplanmasını gerektirir. Tam sayıları çarpanlara ayırmanın hesaplama zorluğu, bir tür açık anahtar şifreleme yöntemi olan RSA'yı güvence altına almak için kullanılır. Bir RSA kullanıcısı, iki büyük asal tamsayının çarpımını hesaplar ve bunu, kendi seçtiği başka bir değerle birlikte bir ortak anahtar olarak bildirir. Seçilen asal faktörleri ise gizli anahtarı olarak saklar ve kaydeder. Belli bir kullanıcının açık anahtarına erişimi olan herkes ona herhangi bir mesajı şifreleyerek gönderebilir.

RSA algoritması anahtar oluşturma, şifreleme ve şifre çözme şeklinde üç temel kriptografik işleme dayanmaktadır [27]. Bunlardan RSA algoritmasının anahtar oluşturma kısmı, beş adımdan oluşan en önemli aşamadır ve şu şekilde gerçekleşir [27]:

1. P ve Q olarak iki büyük asal sayı seçin,
2. N = PxQ değerini hesaplayın,
3. T(N) = (P-1)(Q-1) değerini hesaplayın,
4. E ϵ [1, T(N)] ve E, T(N) aralarında asal olacak şekilde bir E tamsayısını seçin,
5. D = E^{-1} mod (T(N)) olacak şekilde bir D tamsayısını hesaplayın.

Bu hesaplamalara göre (N,E) kullanıcının açık anahtarını (N,D) ise kullanıcının gizli anahtarını oluşturur [27]. RSA algoritmasının güvenlik gereksinimlerini karşılayabilmek için P ve Q asal sayılarının en az 1024 bit boyutunda olmaları gerekmektedir. Açık ve gizli anahtar çiftleri oluşturulduktan sonra M açık metin, C şifreli metin, (N,E) açık anahtar ve (N,D) gizli anahtar olmak üzere şifreleme ve şifre çözme işlemleri aşağıdaki şekilde Denklem 11.2 ve Denklem 11.3'e göre gerçekleştirilir [27].

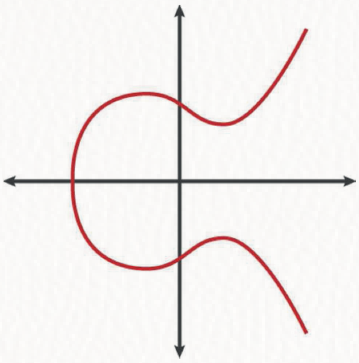
Şifreleme İşlemi : $C = M^E \bmod N$, (11.2)

Şifre Çözme İşlemi : $M = C^D \bmod N$. (11.3)

11.5.2. Eliptik Eğri Kriptografi Algoritması

Bir eliptik eğri aslında belirli bir matematiksel denklemi sağlayan noktalar kümesidir. Örnek bir eliptik eğrinin denklemi şu şekilde olabilir: $y^2=x^3+ax+b$ ve bu denklem Şekil 11.17'deki gibi gösterilebilir. Eğri üzerindeki bir noktayı bir sayı ile çarpmak eğri üzerinde başka bir nokta üretecektir, ancak orijinal noktayı ve sonucu bilseniz bile hangi sayının kullanıldığını bulmak çok zordur. Eliptik eğrilere dayalı denklemler, kriptografik amaçlar için çok değerli bir özelliğe sahiptir: hesaplanmaları nispeten kolay ve tersine çözümleri son derece zordur. Eliptik eğri kriptografisi (EEK), açık anahtarlı bir kriptografik sistem oluşturmak için eliptik eğrilerin matematiksel özelliklerini kullanır [28]. EEK, bir yönde hesaplanması kolay olan, ancak ters yönde çözülmesi çok zor olan matematiksel tuzak fonksiyonlarına dayanmaktadır [29]. Hesap-

lama karmaşıklığı veya zorluğu, genel olarak bilinen bir taban noktasına veya eliptik eğri ayrık logaritma problemine (EEALP) göre rastsal bir eliptik eğri öğesinin ayrık logaritmasının hesaplanamamasına dayanmaktadır [30].



Şekil 11.17. Tipik bir eliptik eğri

NIST tarafından aynı güvenlik seviyesini sağlayan kriptografik algoritmalar için için tavsiye edilen anahtar boyutları Tablo 11.3'te verilmiştir [31]. Eliptik eğri kriptografik algoritması, Tablo 11.3'te görüldüğü üzere RSA ile eşdeğer güvenlik seviyesini sağlamak için RSA'e kıyasla daha küçük anahtar boyutlarını kullanmaktadır.

Tablo 11.3. Eşdeğer güvenlik seviyesi için kullanılması gereken anahtar boyutları

Simetrik Anahtar Boyutu (bit)	RSA Anahtar Boyutu (bit)	EEK Anahtar Boyutu (bit)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

EEK, RSA ile aynı güvenlik seviyesini sağlamak için uygulamada daha az bellek alanı kullanır. Bu özelliği nedeniyle eliptik eğri kriptografik algoritması, asimetrik anahtar kriptografik algoritmaları kullanmak için sınırlı hesaplama kapasitesine sahip olan gömülü sistemlerin performans ve güvenlik gereksinimleri arasındaki boşluğu doldurmaktadır.

Eliptik eğri kriptografisi günümüzde pek çok uygulamada kullanılmaktadır. Devletler EEK'yi yerel iletişim ağlarını korumada kullanmaktadırlar. Ayrıca Bitcoin'lerin sahipliğini kanıtlamak için de EEK kullanılmaktadır. Haberleşme uygulamalarında güvenlik amaçlı dijital imzalarda da EEK kullanılmaktadır. İnternet haberleşmesinde DNS bilgilerinin DNSCurve ile şifrelemesinde ve SSL/TLS üzerinden güvenli web taraması için tercih edilen kimlik doğrulama yöntemi de EEK'ye dayanmaktadır. EEK'yi uygularken, imzaları gerçekleştiren bilgisayarda iyi bir rastsal sayı kaynağının kullanılması gibi bazı gereksinimler olmasına rağmen, eliptik eğri şifrelemesinin geleneksel RSA'ye göre avantajları daha fazladır.

11.5.3. ELGAMAL Algoritması

ElGamal, literatüre ilk kez 1984'te Taher El-Gamal tarafından sunulan asimetrik bir kriptografik algoritma olarak sınıflandırılır [32]. Ayrık logaritma işlemlerinin hesaplama zorluğu ElGamal algoritmasının temelini oluşturur. ElGamal algoritması hem veri şifreleme hem de dijital imzalama için kullanılabilir. ElGamal algoritmasının anahtar uzunluğu 256 bitten rastgele seçilen bir bit boyutuna kadar genişletilebilir. ElGamal şifrelemesi anahtar üreteci, şifreleme algoritması ve şifre çözme algoritması olmak üzere üç bileşenden oluşur.

$y=g^x \bmod(p)$ sayısal değeri, p, k, g ve x değişkenleri kullanılarak hesaplanır. k, y, g ve p, güvenli olmayan kanal üzerinden mesaj gönderecek tüm verici taraflara açık anahtarlar olarak iletilebilir [30]. Gizli anahtar olarak kullanılacak x değişkeni alıcı tarafından korunarak saklanır. Verici M mesajını şifrelemek istediğinde, C_1, C_2 'in değerleri Denklem 11.4 ve Denklem 11.5 yardımıyla hesaplanır [32].

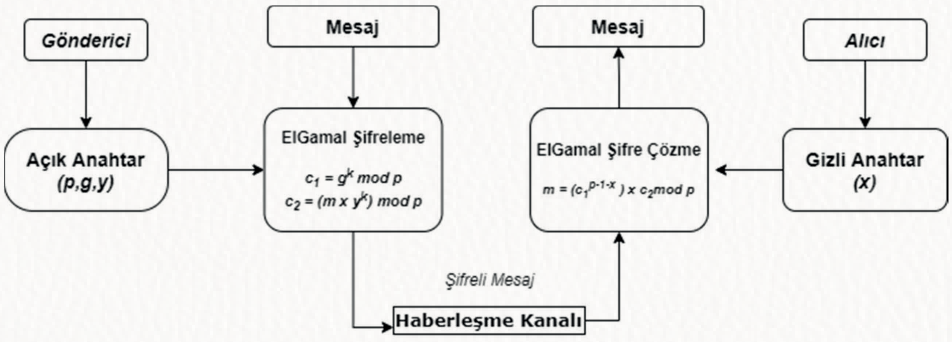
$$C_1 = g^k \bmod(p) \tag{11.4}$$

$$C_2 = M \times y^k \bmod(p) \tag{11.5}$$

Şifrelenmiş metin, bu işlemlerin yan ürünleri olarak elde edilen C_1 ve C_2 değerlerinden oluşmaktadır. Alıcıya teslim edilen şifreli metnin şifresini çözmek için C_1 ve C_2 değerleri kullanılarak Denklem 11.6 yardımıyla hesaplama yapılarak açık metin elde edilir [32].

$$M = C_2 / C_1^x \bmod(p) \quad (11.6)$$

Asimetrik anahtar yöntemleri hem RSA hem de ElGamal tarafından kullanılır ve bu algoritmanın gücü kullanılan bit uzunluğuna göre belirlenir. RSA'nın en zorlu kısmı büyük asal sayıların çarpanlara ayrılmasıyken, ElGamal'in en zor kısmıysa ayrık logaritmaların hesaplanmasıdır [27, 32]. İki algoritma arasındaki temel ayrım, kullanılan değişkenlerin miktarıdır. RSA iki değişken kullanarak şifrelerken ElGamal üç değişkenle şifreler [27, 32]. RSA, verileri şifrelemede ElGamal'den daha hızlıdır. ElGamal ise şifre çözmede RSA'dan daha hızlıdır. RSA algoritması, farklı saldırılara, özellikle kaba kuvvet saldırılarına karşı bir savunma mekanizması sağlama avantajına sahiptir. Öte yandan, büyük bir gizli anahtar, özellikle büyük mesaj boyutları için oldukça uzun bir şifre çözme prosedürü ile sonuçlanmaktadır. Sonuç olarak, RSA, parolalar ve PIN numaraları gibi küçük boyutlu verileri şifrelemek için sıklıkla kullanılır. ElGamal algoritmasını güvenli kılan, büyük asal modulo üzerinde ayrık logaritma hesaplamanın zorluğudur. ElGamal algoritması, ayrı logaritmalar kullanarak anahtarlar üretme avantajına sahiptir. Şifreleme ve şifre çözme teknikleri, orjinalinden iki kat daha büyük şifreleme çıktıları ile sonuçlanan büyük bir hesaplama çabası gerektirir. Bu tekniğin dezavantajı, şifreli metnin açık metinden iki kat daha uzun olması ve bu nedenle büyük logaritmik hesaplamaları yürütebilen bir işlemci gerektirmesi nedeniyle çok fazla kaynak tüketmesidir ElGamal algoritmasının genel şifreleme ve şifre çözme akışı Şekil 11.18'de gösterilmiştir [32].



Şekil 11.18. ElGamal algoritması kullanarak güvenli haberleşme senaryosu

11.6. HAFİF SİKLET KRİPTOGRAFİK ÖZETLEME ALGORİTMALARI

Özetleme fonksiyonları sonlu boyuta sahip olan giriş verisini tek yönlü olarak işleyerek daha küçük ve sabit boyutlu çıkış verisi üreten özel kriptografik fonksiyonlardır. Özet çıktı verisinin boyutu girdi verisinin boyutundan bağımsız ve belirli bir boyutta sabitlenmiştir. Özet çıktısı uygulanan girdiye göre hesaplanır. Aynı girdi verisi her zaman aynı özet çıktı verisinin elde edilmesine neden olur. İki ayrı veri girdisinin aynı özet değeri üretmesi ideal şartlarda mümkün değildir. Ayrıca özetleme fonksiyonlarının tek yönlü çalışan doğası nedeniyle özet çıktı verisinden girdi verisinin elde edilmesi de mümkün değildir. Özet fonksiyonları sonlu boyuta sahip dijital verileri tekil olarak tanımlayacak parmak izlerinin üretilmesinde kullanılırlar. Girdi verisindeki bir bitlik değişiklik bile tamamen farklı bir özet çıktısı ürettiğinden veri bütünlüğü uygulamalarında yaygın olarak kullanılırlar.

Özetleme fonksiyonlarında iki farklı veri girdisinin aynı veri çıktısını oluşturma durumuna çakışma adı verilir. Bu durumun oluşması halinde özet fonksiyonu kriptografik açıdan güvenilmez olarak sınıflandırılır ve kullanımı sınırlandırılır. Örneğin 2017 yılında SHA-1 için bir çakışma durumu tespit edilmiştir [33]. MD5 özetleme algoritmasının da çakışmalara sahip olduğu 2005 yılından beri bilinmektedir ve bu nedenle bahsi geçen özetleme algoritmaları günümüzde kriptografik açıdan güvenli kabul edilmemektedirler [34].

Özetleme fonksiyonlarının en iyi bilinen uygulamalarından biri de web uygulamalarında kullanıcı şifrelerini saklamak yerine, bunların özetlerinin veritabanında saklanmasıdır. Kullanıcı şifresini girdiğinde girilen verinin özeti hesaplanarak veritabanındakiyle karşılaştırılarak kimlik doğrulama işlemi gerçekleştirilmektedir. Böylece kullanıcıların şifrelerinin siber saldırılarla ele geçirilmesi engellenmektedir. Kriptografik özetleme fonksiyonlarının diğer bir uygulaması da dosya içeriklerinin karşılaştırılmasında eğer veri boyutu çok büyükse bunların özet değerlerinin karşılaştırılmasıdır. Örneğin, bilgisayardaki çoğullanmış resim ve video dosyalarını, özetlerini hesaplayarak hızlı bir şekilde karşılaştırma yapmak mümkündür. Bu bölümde hafif siklet kriptografik özetleme fonksiyonları olan PHOTON, QUARK ve SPONGENT algoritmaları tanıtılacaktır [9, 35, 36].

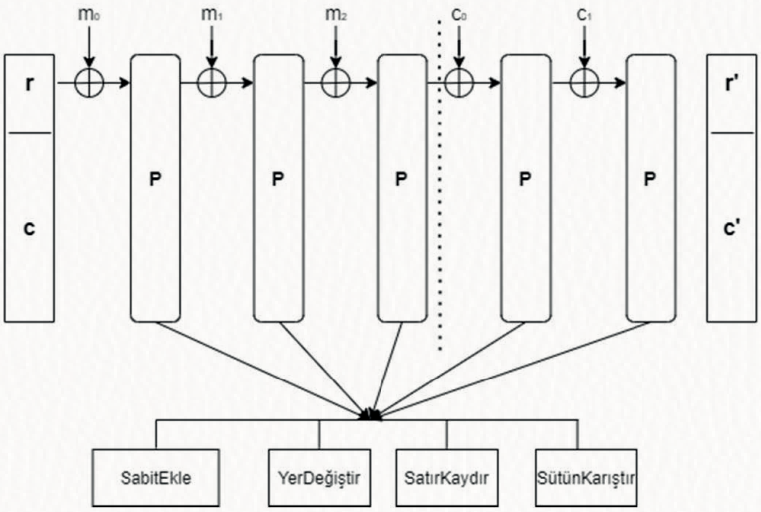
11.6.1. PHOTON

PHOTON donanım odaklı tasarlanmış olan bir hafif siklet kriptografik özetleme fonksiyon ailesidir [9]. Her varyantı özet çıktı boyutu N, 64 bit ile 256 bit arası değerler alır. Veri giriş hız oranı R ve veri çıkış hız oranı R' olarak belirlendiğinde PHOTON ailesindeki her bir özetleme fonksiyonu N/R/R' şeklinde etiketlenerek sınıflandırılırlar. C kapasite olmak üzere özetleme fonksiyonun iç durum değişkeni T = (C+R) özet çıkış veri boyutuna bağlı olarak 100, 144, 196, 256 veya 288 bit şeklinde beş ayrı değeri alabilir ve buna göre her bir iç durum değişkeni için bir tane olmak üzere beş iç permütasyon P_t tanımlanır [9]. Tablo 11.4'te PHOTON-N/R/R' varyantları için veri giriş-çıkış ve özet boyutları listelenmiştir.

Tablo 11.4. PHOTON HSK özetleme fonksiyon ailesinin varyantları

Varyant	N	R	R'
PHOTON-80/20/16	80	20	16
PHOTON-128/16/16	128	16	16
PHOTON-160/36/36	160	36	36
PHOTON-224/32/32	224	32	32
PHOTON-256/32/32	256	32	32

PHOTON HSK özetleme algoritması, büyük ölçüde Şekil 2.19'da gösterilen sünger fonksiyonlarından esinlenilerek tasarlanmıştır [9]. T-bit dahili durum değişkeni, C-bit kapasite ve R-bit veri hızı parametreleri mimaride belirleyicidir. Hesaplama İlk olarak, bir başlangıç değerinden ile başlatılır ve özetlenecek dolgulanmış mesaj R-bit veri bloklarına bölünür. Daha sonra, soğurma aşaması sırasında, bu mesaj bloklarının her biri, bir dahili permütasyon P uygulanmadan önce arka arkaya iç durum değişkeni T'ye dahil edilir. Tüm mesaj blokları işlendikten sonra, sıkıştırma aşaması sırasında dahili permütasyon P uygulanmadan önce dahili durumun R' bitleri doğru miktar olan N bit'e ulaşılana kadar art arda dışa aktarılır.



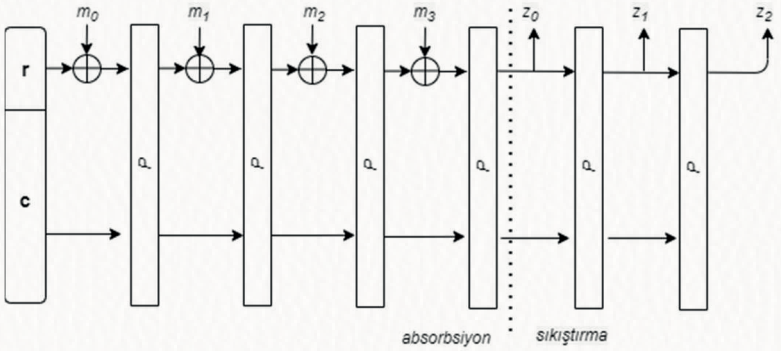
Şekil 2.19. PHOTON HSK özetleme algoritmasının bir turu için sünger yapısı

PHOTON'un dahili permütasyonu büyük ölçüde Advanced Encryption Standard (AES) yapısından esinlenmiştir. Başka bir ifadeyle, dahili durum değişkenine s-bit hücrelerin (d x d) boyutlu bir matrisi olarak bakılabilir. PHOTON bir hesaplama turunda sırayla aşağıdaki dört işlemi uygular [9]:

1. Sabitlerin toplaması
2. Hücrelerin yerdeğiştirilmesi
3. Satırların kaydırılması
4. Sütünların karıştırılması

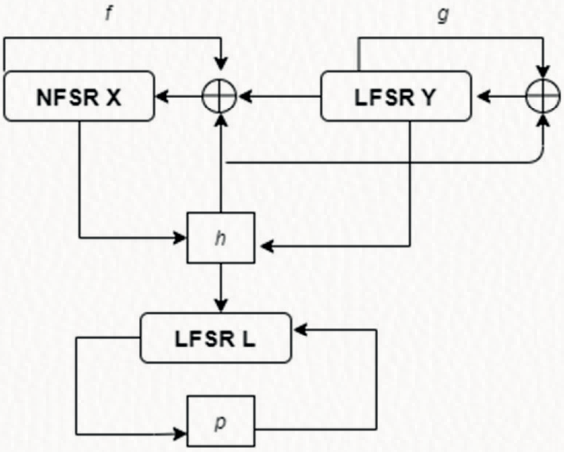
11.6.2. QUARK

Sünger yapılı hafif siklet bir kriptografik özetleme fonksiyon ailesi olan QUARK, genellikle bellek gereksinimlerini en aza indirmek için RFID teknolojisi ürünlerinde kullanılmaktadır [35]. Q-QUARK, D-QUARK ve S-QUARK olmak üzere üç tipten oluşan QUARK hafif siklet kriptografik özetleme fonksiyon ailesi, mesaj doğrulama, akış şifreleme veya kimlik doğrulamalı şifreleme için kullanılabilir. QUARK, Şekil 11.20'de gösterildiği gibi sünger yapısını ve 6 bitlik bir P permütasyonunu kullanır [35].



Şekil 11.20. QUARK HSK özetleme algoritmasının bir turu için sünger yapısı

Herhangi bir QUARK fonksiyonu veri giriş hız oranı (veya blok uzunluğu) R, bir kapasite C ve özet çıktı boyutu N parametreleriyle karakterize edilir. Sünger yapısının B = (R+C) veri genişliği, dahili durum değişkeninin boyutuna eşittir. Sünger yapılı özetleme süreci bir M mesajını sırasıyla ilklendirme, absorbe etme ve sıkıştırma olarak üç aşamada işler. QUARK Şekil 11.21'de görüldüğü üzere P ile temsil edilen bir permütasyon kullanır [35]. P'nin dahili durum değişkeni her biri B/2 bitlik iki doğrusal olmayan geri besleme kaydırma yazmacı ve log(4B) bitlik bir doğrusal geri besleme kaydırma yazmacından oluşur.



Şekil 11.21. PHOTON HSK özetleme algoritmasının permütasyon katmanı

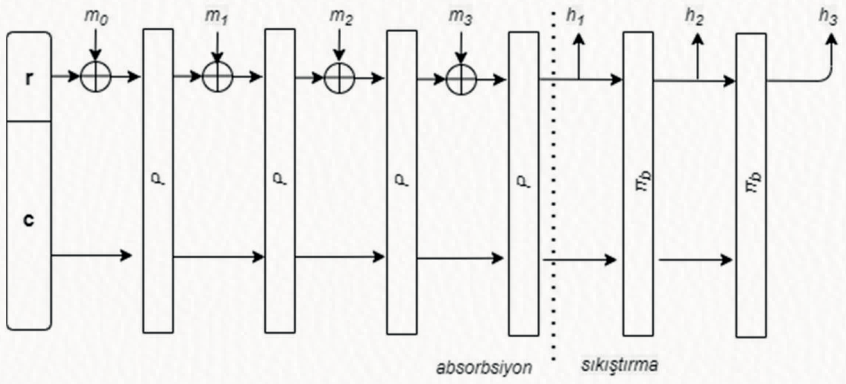
11.6.3. SPONGENT

SPONGENT, 88, 128, 224 veya 256 bit özet çıktısı boyutlarına ve PRESENT tipi bir permütasyon fonksiyonuna sahip olan sünger yapılı bir hafif siklet kriptografik özetleme ailesidir [36]. SPONGENT ailesinin farklı güvenlik seviyelerine sahip beş farklı türü Tablo 11.5'te listelenmiştir.

Tablo 11.5. SPONGENT HSK özetleme fonksiyon ailesinin varyantları

Varyant	N (bit)	B (bit)	C (bit)	R (bit)	Tur Sayısı
SPONGENT-88	88	88	80	8	45
SPONGENT-128	128	136	128	8	70
SPONGENT-160	160	176	160	16	90
SPONGENT-224	224	240	224	16	120
SPONGENT-256	256	272	256	16	140

Sünger yapısı, değişken uzunlukta bir veri girdisi alan ve sabit boyutlu B-bitlik bir dahili durum değişkeniyle çalışan SPONGENT bir hafif siklet kriptografik özetleme fonksiyon ailesidir ve değişken uzunlukta veri çıktısı sağlayabilen kendini yineleyen basit bir yapıya sahiptir. SPONGENT algoritmasının dahili durum değişkeninin boyutu $B = (R+C) \geq N$ şeklindedir [36]. R, veri giriş hız oranını, C kapasiteyi ve N ise özet çıktı boyutunu gösteren parametreleridir. SPONGENT hafif siklet kriptografik özet fonksiyonları Şekil 11.22'de gösterildiği gibi sünger yapılı ve sırasıyla ilklendirme, emilme ve sıkıştırma işlemlerinden oluşan üç aşamada çalışır [36].



Şekil 11.22. SPONGENT HSK özetleme algoritmasının bir turu için sünger yapısı

Şekil 11.22'deki $\pi_b:2^b \rightarrow \pi_b:2^b$ permütasyonu B-bitlik giriş dahili durumunun bir R-turundaki transformudur ve algoritmanın akışı Şekil 11.23'te gösterildiği gibidir [36].

Algoritma 3: SPONGENT HSK Özetleme

```
1 for i = 0 to R do
2 |   DURUM ←
  |   LSayaç*_b(i) ⊕ DURUM ⊕ LSayaç_b(i)
3 |   DURUM ← sKutuKatman_b(DURUM)
4 |   DURUM ← permKatman_b(DURUM)
5 end
```

Şekil 11.23. SPONGENT HSK özetleme algoritması

Şekil 11.23'teki algoritmada $sKutuKatman_b$ ve $permKatman_b$ dahili durum değişkeninin nasıl evrildiğini göstermektedir. Tur sayısı R, blok boyutu B ile ilintilidir ve $LSayac_b(i)$ bir LFSR'ın tur sabitini ürettiği i. andaki B parametresine dayalı durumunu gösterir ve durum değişkeninin en sağındaki bitlere eklenir. $LSayaç^*_b(i)$ ise $LSayaç_b(i)$ değerinin bit sırası evrilmiş halidir ve durum değişkeninin en solundaki bitlere eklenir [36].

11.7. HAFİF SİKLET KRİPTOGRAFİDE STANDARTLAŞMA ÇALIŞMALARI

2013 yılında ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından gerçekleştirilen CAESAR çağrısı kapsamında kuruma teslim edilen pek çok kriptografik algoritmanın kısıtlı kaynaklara sahip nesnelerin interneti gibi gömülü sistemler için uygun olmadığının farkedilmesinin ardından kurum tarafından hafif siklet kriptografi standartlaştırma faaliyetleri başlatılmıştır. Bu kapsamda NIST, Nesnelerin İnterneti gibi kısıtlı ortamlarda kullanıma uygun İlişkili Veri ile Doğrulanmış Şifreleme (Authenticated Encryption with Associated Data - AEAD) ve hafif siklet özetleme algoritmalarını seçmek için bir genel standardizasyon süreci başlattı. 2019 yılında başlatılan bu çağrı ile özellikle nesnelerin interneti uygulamalarını hedefleyen şifreleme ve özet he-

saplama algoritmalarının standartlaştırılması hedeflenmektedir. Çağrının ilk aşamasına 56 algoritma başvurusu yapılmıştır ve bunların 32'si 2019 yılında çağrının ikinci aşamasına geçmeye hak kazanmışlardır. 2021 yılı Temmuz ayı itibariyle çağrının durumunu belirten son güncel rapora göre aday algoritmaların sayısı Mart 2021'deki son değerlendirme turunda 10'a kadar indirilmiştir ve değerledirmelerin yıl içinde sonuçlandırılması beklenmektedir [10].

Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunication Standards Institute - ETSI) ticari nesnelerin interneti ürünlerin siber güvenliğine yönelik olarak ETSI EN 303 645 standardını 2020 yılında yürürlüğe sokmuştur [37]. ETSI siber güvenlik teknik komitesi tarafından açıklanan standart, internete bağlı tüketici ürünleri için bir güvenlik dayanağı oluşturarak gelecekteki Nesnelerin İnterneti sistemlerinin sertifikasyon işlemleri için bir temel oluşturacaktır. Evlerden, işyerleri ve fabrikalardan daha fazla cihaz internete bağlandıkça, nesnelerin interneti'nin siber güvenliği büyüyen bir endişe haline gelmiştir. ETSI tarafından geliştirilen EN 303 645 standardı, siber güvenlik uzmanlarının her gün karşılaştıkları akıllı cihazlara yönelik büyük ölçekli, yaygın saldırıları önlemek için tasarlanmıştır [37]. Bu yeni standart, siber saldırıların ardından üreticilerin güvenlik önlemlerini özensiz bir şekilde yamalamaları yerine, aygıtların tasarım süreçlerinden itibaren nesnelerin interneti ürünlerini güvenli hale getirmenin prensiplerini oluşturmayı hedeflemektedir. Standarda uygunluğun, saldırganların dünya genelinde bot-netler olarak bilinen cihazları kontrol etme, DDoS saldırıları başlatma, kripto para madenciliği yapma ve kendi evlerinde kullanıcıları gözetleme yeteneklerini kısıtlayacağı öngörülmektedir.

ETSI EN 303 645, internete bağlı tüketici ürünleri için sağlam bir güvenlik temelini ortaya koymaktadır: Standarda göre Nesnelerin İnterneti aygıtlarında varsayılan parola bulundurulmamalı, bir güvenlik açığı ifşa politikası uygulanmalı ve gömülü yazılımın güncel tutulması şarttır ve tüketici sınıfı Nesnelerin İnterneti cihazları için özel veri koruma hükümleri de bulunmaktadır [37]. ETSI EN 303 645 standardı kapsamına giren Nesnelerin İnterneti ürünleri arasında İnternet bağlantılı çocuk oyuncakları ve bebek monitörleri, duman dedektörleri ve kapı kilitleri gibi İnternet bağlantılı güvenlikle ilgili ürünler, akıllı kameralar, TV'ler ve hoparlörler, kişisel giyilebilir sağlık telemetri cihazları, internet bağlantılı ev otomasyon ve alarm sistemleri, internete bağlı beyaz eşyalar ve akıllı ev asistanları bulunmaktadır [37]. ETSI EN 303

645 standardı içeriği dolayısıyla, nesnelerin interneti aygıtlarına yönelik saldırıları önleyerek, temel güvenlik ve gizlilikte önemli bir güncel ilerlemeyi temsil etmektedir.

11.8. SONUÇ VE DEĞERLENDİRMELER

Nesnelerin İnterneti aygıtları saha uygulamalarında daha fazla dağıtıldıkça ve küresel ağa bağlanarak saldırılara maruz kaldıkça Nesnelerin İnternetine yönelik güvenlik ihtiyaçları günümüzün gelişen telekomünikasyon teknolojisinin yaygın etkisi ile en önemli sorun haline gelmiştir. Hafif siklet kriptografik algoritmalar, hafif işlem yüklerine, düşük kaynak ve enerji tüketim değerlerine sahip oldukları için özellikle sınırlı kaynaklara sahip cihazlarda güvenli iletişim ve Nesnelerin İnterneti aygıtları ve ortamları için önemli bir güvenlik sağlayıcı olarak öne çıkmaktadır. Bu çalışmada, farklı yapılarda yaygın olarak kullanılan hafif siklet kriptografik algoritmaların ve özetleme fonksiyonlarının bir sınıflandırması yapılarak temel özellikleriyle algoritmaları tanıtan bir derleme gerçekleştirilmiştir. Hafif siklet kriptografik algoritmalara yönelik uluslararası standartlaşma çalışmaları hakkında da güncel bilgiler paylaşılarak globalde hafif siklet kriptografinin bilinen son durumuna ilişkin gelişmeler hakkında güncel bilgiler paylaşılmıştır.

Halihazırda sahada işlemci mimarilerindeki RISC-V gibi ortaya çıkan yeni gelişmeler, literatürde önerilen yeni algoritmalar ve kriptanaliz teknikleri ile araştırmalar devam etmektedir. Nesnelerin İnternetine geçişi ve entegrasyonu güvence altına almak için sınırlı kaynaklara ve farklı işlemci mimarilerine sahip gömülü sistemler üzerinde kriptografik algoritmaların gerçekleştirilmesi ve optimizasyonu çalışmalarının, günümüzün ve geleceğin araştırmalarına yön vermeye devam edeceği öngörülmektedir.

KAYNAKLAR

[1] G. S. Nicholas, Y. Gui, and F. Saqib. “A survey and analysis on SoC platform security in ARM, Intel and RISC-V architecture.” In 2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS), IEEE, 2020, pp. 718–721.

[2] E. Tehrani, T. Graba, A. S. Merabet, and J. Danger. “RISC-V extension for lightweight cryptography.” In 2020 23rd Euromicro Conference on Digital System Design (DSD), IEEE, 2020, pp. 222–228.

[3] K. Stoffelen. “Efficient cryptography on the RISC-V architecture.” In International Conference on Cryptology and Information Security in Latin America, Springer, 2019, pp. 323–340.

[4] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas. “A review of lightweight block ciphers.” In Journal of Cryptographic Engineering, Springer, 2018, 8(2):141–184.

[5] S. S. Dhanda, B.it Singh, and Poonam Jindal. “Lightweight cryptography: A solution to secure IoT.” In WirelessPersonal Communications, 2020, 112(3):1947–1980.

[6] S. Madakam, R. Ramaswamy, S. Tripathi, (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 2015, Vol. 3, No.5, pp. 164-173. doi: 10.4236/jcc.2015.35021.

[7] Statistica, “Internet of Things (IoT) connected devices installed base worldwide from 2015-2025”, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, erişim tarihi, 25 Haziran 2021.

[8] H. Sinanović and S. Mrdovic, “Analysis of Mirai malicious software,” In 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2017, pp. 1-5. doi: 10.23919/SOFTCOM.2017.8115504

[9] J. Guo, T. Peyrin, and A. Poschmann. “The photon family of lightweight hash functions.” In Annual Cryptology Conference, Springer, 2011, pp. 222–239.

[10] M. T. Sönmez et. al. “Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process”, 21 July 2021, NIST Internal Report 8369. https://doi.org/10.6028/NIST.IR.8369

[11] L. Auer, C. Skubich, and M. Hiller. “A security architecture for RISC-V based IoT devices.” In 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE, 2019, pp. 1154–1159.

[12] A. Biryukov and L. P. Perrin. “State of the art in lightweight symmetric cryptography”. In in IACR Cryptology ePrint Archive, 2017, pages 1-40. https://eprint.iacr.org/2017/511.pdf

[13] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park. “Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions.” In Journal of Ambient Intelligence and Humanized Computing, 2017, pp. 1–18.

[14] A. Bogdanov et. al., L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J.B. Robshaw, Y. Seurin, and C. Vikkelsoe. “Present: An ultra-lightweight block cipher”. In International workshop on cryptographic hardware and embedded systems, Springer, 2007, pp. 450–466.

[15] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, et al. “Prince–a low-latency block cipher for pervasive computing applications”. In International conference on the theory and application of cryptology and information security, Springer, 2012, pages 208–225.

[16] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith and L. Wingers, "The SIMON and SPECK lightweight block ciphers,", In 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015, pp. 1-6, doi: 10.1145/2744769.2747946.

[17] D. J. Wheeler and R. M. Needham. "TEA, a tiny encryption algorithm. In International workshop on fast software encryption", Springer, 1994, pp. 363–366.

[18] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, et al. "HIGHT: A new block cipher suitable for low-resource device". In International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2006, pp. 46–59.

[19] X. L. and J. L Massey. "A proposal for a new block encryption standard." In Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1990, pp. 389–404.

[20] C. De Canniere, O. Dunkelman, and M. Knežević. "KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers". In International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2009, pp. 272–288.

[21] S. Babbage , M. Dodd. "The MICKEY Stream Ciphers." In: Robshaw M., Billet O. (eds) New Stream Cipher Designs. Lecture Notes in Computer Science, Springer, 2008 vol. 4986, pp. 1-5. https://doi.org/10.1007/978-3-540-68351-3_15

[22] M. Hell, T. Johansson, and W. Meier. "GRAIN: a stream cipher for constrained environments". In International journal of wireless and mobile computing, 2007, 2(1):86–93.

[23] C. De Canniere and B. Preneel. "TRIVIUM." In New stream cipher designs, Springer, 2008, pp. 244–266.

[24] D. Engels, X. Fan, G. Gong, H. Hu, and E. M. Smith. "HUMMINGBIRD: ultra-lightweight cryptography for resource-constrained devices". In International conference on financial cryptography and data security, Springer, 2010, pp. 3–18.

[25] C.G. Thorat and V.S. Inamdar. "Implementation of new hybrid lightweight cryptosystem". In Applied Computing and Informatics, 2020, Vol. 16 No. 1/2, pp. 195-206.

[26] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, November 1976, vol. 22, no. 6, pp. 644-654. doi: 10.1109/TIT.1976.1055638.

[27] R. L Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In Communications of the ACM, 1978, 21(2):120–126.

[28] M. Kashif, İ. Çiçek, "Field-programmable gate array (FPGA) hardware design and implementation of a new area efficient elliptic curve crypto-processor", In Turkish Journal of Electrical Engineering & Computer Sciences, 2021, Vol. 29, pp. 2127-2139.

[29] N. Koblitz. “Elliptic Curve Cryptosystems”, In Mathematics of computation. 1987, 48n, 1(77):l.

[30] S. D. Galbraith and P. Gaudry. Recent progress on the elliptic curve discrete logarithm problem. Designs, Codes and Cryptography, 78(1):51–72, 2016.

[31] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. “Recommendation for key management part 1: General (revision 3)”. In NIST special publication, 2012, 800(57), pp.1-147.

[32] T. Elgamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” In IEEE Transactions on Information Theory, July 1985, vol. 31, no. 4, pp. 469-472. doi: 10.1109/TIT.1985.1057074.

[33] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov. “The First Collision for Full SHA-1”. In: Katz J., Shacham H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10401. Springer, Cham. https://doi.org/10.1007/978-3-319-63688-7_19

[34] X. Wang , H. Yu. “How to Break MD5 and Other Hash Functions”. In: Cramer R. (eds) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11426639_2

[35] J. P. Aumasson, L. Henzen, W. Meier, and M. N.-Plasencia. “QUARK: A lightweight hash”. In International work- shop on cryptographic hardware and embedded systems, Springer, 2010, pp. 1–15.

[36] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varıcı, and I. Verbauwhede. “SPONGENT: A lightweight hash function”. In International workshop on cryptographic hardware and embedded systems, Springer, 2011, pp. 312–325.

[37] ETSI, 2020, “CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements” In ETSI EN 303 645 v2.1.1 (2020-06).

Bölüm 12

KUANTUM ÖNCESİNDEN KUANTUM SONRASINA ELİPTİK EĞRİ KRİPTOGRAFİ VE UYGULAMALARI

Murat Cenk - Burcu Ecem Karakaş - N. Gamze Orhon Kılıç

Eliptik eğriler kriptografide uzun süredir kullanılmaktadır. Açık anahtarlı bir kriptosistem olan eliptik eğri kriptografi, kullandığı küçük anahtar boyutları sayesinde diğer açık anahtarlı sistemlere göre büyük avantaj sağlamaktadır. Bu bölümde eliptik eğriler ile ilgili temel bilgi verildikten sonra eliptik eğrilerin kriptografide nasıl kullanıldığı üzerinde durulmuştur. Ardından, eliptik eğrilerin uygulama alanlarından bahsedilmiş ve blokzincirdeki kullanım alanları detaylı bir şekilde incelenmiştir. Son olarak eliptik eğri kriptografinin bilgi güvenliğindeki önemi ve bu alandaki açık problemler sunulmuştur.

12.1. GİRİŞ

Bilgisayar kullanımının yaygınlaşmasıyla birlikte bilgi güvenliğine duyulan gereksinim artmış, bu konuda birçok çalışma yapılmış ve önemli buluşlara imza atılmıştır. Bilgi güvenliğinin sağlanmasında kullanılan en önemli araçlardan biri de kriptografidir. Kriptografinin binlerce yıllık bir geçmişi olmasına karşılık, bilgisayarın icadı kriptografinin 20. ve 21. yüzyıllardaki gelişimini bir hayli hızlandırmıştır. Açık anahtarlı kriptografi kavramının Diffie ve Hellman [1] tarafından 1976 yılında önerilmesi ise kriptografide yepyeni bir dönem açılma-

sını sağlamıştır. Bu döneme kadar kullanılan tüm kriptosistemler şifreleme ve deşifreleme işlemleri için aynı anahtarları kullanmaktaydı. Fakat şifreli iletişim sağlamak isteyen taraflar arasında anahtarların paylaşılması durumu büyük bir sorun oluşturmaktaydı. Diffie ve Hellman'ın önerdiği sistemde ise şifreleme ve deşifreleme işlemleri için iki ayrı anahtar kullanılmaktadır.

Ayşe ve Barış'ın herkese açık olan bir kanal üzerinden açık anahtarlı bir kriptosistem kullanarak şifreli haberleşmek istediklerini düşünelim. Barış bir adet açık ve bir adet gizli anahtardan oluşan bir anahtar çifti oluşturur. Açık anahtarı herkese açık bir ortamda yayınlar. Ayşe, Barış'ın yayınladığı bu açık anahtarı kullanarak mesajını şifreler ve yine açık bir kanal üzerinden şifreli mesajı Barış'a iletir. Barış, gizli anahtarını kullanarak şifreyi açar. Bu sistemde kullanılan açık ve gizli anahtarlar üretilirken kullanılan matematik sistemi sayesinde, birbiriyle bağlantılıdır. Bu nedenle açık anahtar ile şifrelenen metnin şifresi gizli anahtarla çözülür. Ayrıca açık anahtar üzerinden gizli anahtarın bulunması da mümkün değildir. Barış gizli anahtarını kimseyle paylaşmadığı için, şifreli metin ve açık anahtarı elde etmiş olan kötü niyetli biri şifreyi çözemez. Bu sistem, önceden kullanılan simetrik kriptosistemlerde yaşanan anahtar paylaşım problemini ortadan kaldırmıştır. Ne var ki açık anahtarlı kriptosistemler simetrik kriptosistemlere göre daha yavaş çalışmaktadır. Bu nedenle bu iki sistem bir arada kullanıldığında güvenli ve hızlı bir uygulama elde edilir.

Eliptik eğrilerin açık anahtarlı kriptografide kullanılmasını Victor Miller [2] ve Neal Koblitz [3] yaptıkları bağımsız çalışmalarla önermişlerdir. Eliptik eğri kriptografi (*Elliptic Curve Cryptography – ECC*) eliptik eğrilerin sağladığı matematiksel altyapı sayesinde diğer açık anahtarlı kriptosistemlerden daha iyi bir performans sergilemektedir. Bu durum eliptik eğri kriptografinin, yaygın olarak kullanılan birçok uygulamada tercih edilmesine neden olmaktadır.

Günlük hayatta, belki de hiç fark etmeden kullanılan birçok uygulamanın arka planında eliptik eğri kriptosistemler barındıran protokoller çalışır. ECC, şifreleme, anahtar paylaşımı, kimlik doğrulama, kimlik belirleme, sayısal imza gibi birçok uygulama alanına sahiptir. Ayrıca 21. yüzyılın en önemli buluşlarından biri olan blokzincir teknolojisinin kullandığı mekanizmalardan biridir.

Açık anahtarlı kriptosistemler bugün kullandığımız bilgisayarlar ile yapılan saldırılara karşı güvenlidir. Ancak, gelecekte üretilmesi ve yaygınlaşması beklenen büyük ölçekli kuantum bilgisayarlar açık anahtarlı kriptosistemleri kolayca kırabilir. Bu nedenle bilim insanları büyük ölçekli kuantum bilgisayarlarda bile güvenli çalışabilecek açık anahtarlı kriptosistemler (kuantum

sonrası kriptografi) geliştirmeye başlamıştır. Kuantum güvenli çözümler sunan kriptosistemlerden birinin matematiksel zorluğu süpersingüler eliptik eğriler arasında izojen bulma problemine dayanır. Bu problemi kullanan sisteme süpersingüler izojen tabanlı kriptografi adı verilir. Eliptik eğrileri kullanan bu kriptosistem, kuantum sonrası kriptografide (*post-quantum cryptography*) gelecek vaat eden bir alandır.

Bu bölümde eliptik eğrilerin, kuantum öncesinde ve sonrasında, kriptografideki kullanım alanları anlatılmıştır. Bölüm 12.2'de eliptik eğrilerin matematiksel altyapısı ve kriptografide kullanılan özellikleri verilmiştir. Bölüm 12.3'te eliptik eğrileri kullanan kriptosistemler ve kuantum sonrası kriptografide eliptik eğrilerin kullanılması anlatılmıştır. ECC'nin haberleşme güvenliğinin ve nesnelerin interneti güvenliğinin sağlanmasındaki rolü Bölüm 12.4'te incelenmiştir. Sonraki bölümde eliptik eğrilerin blokzincir güvenliği, blokzincirde kimlik belirleme ve mahremiyetin sağlanması işlemlerindeki kullanımı açıklanmıştır. Son olarak Bölüm 12.6'da sonuç ve değerlendirmeler sunulmuştur. Bu bölümde anlatılan konular genel bilgilendirme amaçlı olup, daha detaylı bilgiler için bölümlerde verilen referanslara başvurulmalıdır.

12.2. ELİPTİK EĞRİLER

Eliptik eğrilerin kriptografi dünyasına girmesinin ardından matematiksel altyapısı eliptik eğrilere dayanan kriptosistemler, günden güne kullandığımız uygulamalarda yer almaya başlamıştır. Eliptik eğri kriptografi, internet ve haberleşme güvenliğinden nesnelerin internetine, veri güvenliğinden blokzincirlere kadar birçok alanda kullanılmaktadır.

Bu derece geniş çaplı bir uygulama alanına sahip olan bu açık anahtarlı kriptografi alanını anlamak için, güvenliğinin dayandığı matematiksel altyapıya hakim olmak büyük önem taşımaktadır. Bu nedenle bu bölümde eliptik eğri kriptografinin kullandığı matematiksel yapılar incelenmiştir. Bölüm 12.2.1'de temel matematik ve Weierstrass denklemleri, Bölüm 12.2.2'de eliptik eğrilerde grup kuralları, Bölüm 12.2.3'te eliptik eğri kriptografinin zorluğunun dayandığı işlem olan nokta çarpım işlemi, Bölüm 12.2.4'te sonlu cisimler üzerinde tanımlanan eliptik eğriler ve son olarak Bölüm 12.2.5'te, verimli gerçekleştirme başlığı altında, eliptik eğri aritmetiği hızlandırma işlemleri ve sonlu cisim aritmetiği hızlandırma işlemleri açıklanmıştır.

12.2.1. Temel Matematik ve Weierstrass Denklemleri

$\mathbb{K}$ bir cisim, $a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6, b_8, \Delta \in \mathbb{K}$ ve

$$b_2 = a_1^2 + 4a_2,$$

$$b_4 = 2a_4 + a_1a_3,$$

$$b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2,$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

$$\mathrm{j}(E) = (b_2^2 - 24b_4)^3/\Delta,$$

olsun. $\Delta \neq 0$ olmak üzere $\mathbb{K}$ üzerinde tanımlanan, genel Weierstrass formlu E eliptik eğrisi,

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{12.1}$$

şeklinde tanımlanır. Burada Δ'ya E eğrisinin diskriminantı, $\mathrm{j}(E)$'ye de j-değişmezi denir.

E_1 ve E_2, $\mathbb{K}$ cismi üzerinde

$$E_1: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

$$E_2: y^2 + \widehat{a_1}\mathrm{x}\mathrm{y} + \widehat{a_3}\mathrm{y} = x^3 + \widehat{a_2}x^2 + \widehat{a_4}\mathrm{x} + \widehat{a_6},$$

denklemleriyle tanımlanan iki eliptik eğri olsun. E_1 ve E_2 eğrileri,

$$\widehat{a_1} = (a_1 + 2s)/u,$$

$$\widehat{a_2} = (a_2 - sa_1 + 3r - s^2)/u^2,$$

$$\widehat{a_3} = (a_3 + ra_1 + 2t)/u^3,$$

$$\widehat{a_4} = (a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)/u^4,$$

$$\widehat{a_6} = (a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1)/u^6,$$

eşitliklerini sağlayacak $u \in \mathbb{K} - \{0\},\ r, s, t \in \mathbb{K}$ sayıları mevcut ise birbirine izomorftur [4], [5]. İzomorfizma fonksiyonları aşağıdaki gibi tanımlanır:

$$\phi: E_1 \to E_2, (x, y) \mapsto \left(\frac{x - r}{u^2}, \frac{y - s(x - r) - t}{u^3}\right), \tag{12.2}$$

$$\widehat{\phi}: E_2 \to E_1, (x', y') \mapsto (u^2 x' + r, u^3 y' + u^2 s x' + t). \tag{12.3}$$

Denklem 12.2 ve 12.3'te gösterilen dönüşümler, kabul edilebilir değişken değişikliği (*admissible changes of variables*) olarak adlandırılır.

Denklem 12.1'de tanımlanan Weierstrass eğrisi E, kabul edilebilir değişken değişikliği yapılarak daha basit eğri formlarına dönüştürülebilir. Eğrilerin tanımlı olduğu cismin özelliğine göre kullanılacak değişken değişiklikleri ve elde edilen eğri formları değişkenlik göstermektedir. Ancak kitabın bu bölümünde, yalnızca $\mathbb{K}$ cisminin karakteristiğinin 2 veya 3 olmadığı durum incelenecektir.

12.2.1.1. Kısa Weierstrass Denklemi

$\mathbb{K}$, karakteristiği 2 veya 3 olmayan bir cisim ve

$$E_G: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

$\mathbb{K}$ üzerinde tanımlı bir genel Weierstrass eğrisi olsun. E_G eğrisine,

$$(x, y) \to \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1 x}{216} - \frac{a_1^3 + 4a_1 a_2 - 12a_3}{24}\right),$$

kabul edilebilir değişken değişikliğinin uygulanması ile

$$E_K: y^2 = x^3 + ax + b$$

eğrisi elde edilir ve bu eğri kısa Weierstrass denklemi olarak adlandırılır. Kısa Weierstrass eğrisinin diskriminant ve j-değişmezi değerleri genel Weierstrass denklemindekilerden farklı olmak üzere,

$$\Delta E_K = -16(4a^3 + 27b^2),$$

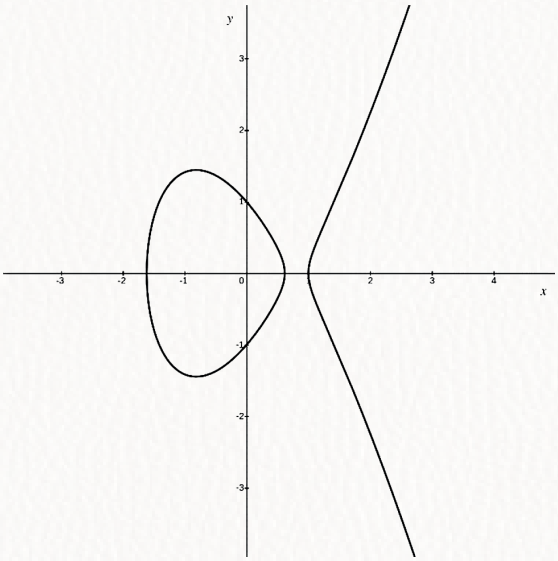
$$j(E_K) = -1728(4a^3)/\Delta,$$

şeklinde tanımlanır.

Eliptik eğrinin diskriminant değerinin sıfır olmaması durumu eğri denkleminin tekrarlayan kökünün olmaması anlamına gelir. Durumu gözlemleyebilmek için eğri denklemini çarpanlarına ayıralım:

$$x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3).$$

e_1, e_2, e_3 sayılarının karmaşık sayı olmasının da mümkün olduğu durumda, $(4a^3 + 27b^2) \neq 0$ koşulu ancak ve ancak e_1, e_2, e_3 sayıları birbirinden farklı olursa sağlanmaktadır. Şekil 12.1'de reel sayılar üzerinde tanımlanmış bir kısa Weierstrass eğrisi örnek olarak verilmiştir.



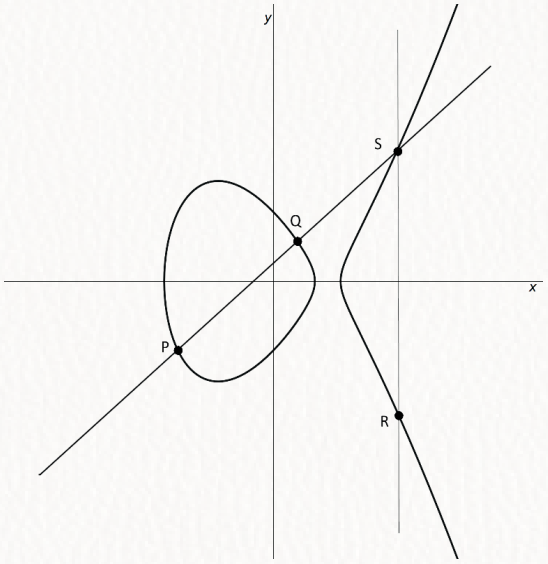
Şekil 12.1. $\mathbb{R}$ üzerinde tanımlanmış $\boldsymbol{E: y^2 = x^3 - 2x + 1}$ eliptik eğrisi

12.2.2. Grup Kuralları

P ve Q, E eliptik eğrisinde iki nokta olsun. Bu iki noktayı birbiriyle toplamak için her iki noktayı da kesen bir D doğrusu çizilir. Bu doğru E eğrisini P ve Q noktalarının dışında başka bir noktada daha keser. D doğrusunun, E eğrisini kestiği bu üçüncü noktanın x-eksenine göre simetriği, P ve Q noktalarının toplamını verir.

Şekil 12.2'de görüldüğü üzere, P ve Q noktalarını kesen doğru, eğriyi S noktasında da kesmektedir. S noktasının x-eksenine göre simetriği olan R noktası ise P ve Q noktalarının toplamını verir.

P noktasını kendisiyle toplamak için P noktasından eğriye teğet geçen bir doğru çizilir. Bu teğet doğrusu eğriyi başka bir noktada daha keser ve bu noktanın x-eksenine göre simetriği P noktasının kendisiyle toplamını verir. Başka bir deyişle $2P$ bu yöntemle hesaplanır.



Şekil 12.2. Eliptik eğri nokta toplama işlemi

P noktasını, x-eksenine göre simetriği olan P' ile toplamak istediğimizde, normal toplama işleminde çizdiğimiz, bu iki noktayı kesen doğru, y-eksenine paralel olduğu için eğriyi üçüncü bir noktada kesmez. Bu durumda, eğrinin birim elemanı olarak adlandırılan $\mathcal{O}$ noktasının, bu doğrunun eğriyi kestiği üçüncü nokta olduğu kabul edilir. Bu noktaya sonsuzdaki nokta (point at infinity) da denmektedir. Bir noktanın x-eksenine göre simetriği ile toplamı eğrinin birim elemanını verir ve $P + P' = \mathcal{O}$ şeklinde gösterilir.

Özetle, E eğrisi üzerinde tanımlanan toplama işlemi aşağıdaki özellikleri sağlamaktadır.

- **Birim eleman:** Her $P \in E$ için, $P + \mathcal{O} = \mathcal{O} + P = P$.

- **Ters eleman:** Her $P \in E$ için, $P + (-P) = \mathcal{O}$. Bu durumda, bir noktanın eğri üzerindeki tersi o noktanın x-eksenine göre simetriğidir. $P = (x, y)$ ise $-P = (x, -y)$ olarak ifade edilir.
- **Birleşme özelliği:** Her $P, Q, R \in E$ için, $(P + Q) + R = P + (Q + R)$.
- **Değişme özelliği:** Her $P, Q \in E$ için, $P + Q = Q + P$.

Yukarıdaki tüm özellikler göz önüne alındığında $E: y^2 = x^3 + ax + b$ eğrisi üzerinde bulunan $P = (x_1, y_1)$ ve $Q = (x_2, y_2)$ noktaları için toplama işlemi aşağıdaki adımlar takip edilerek yapılır:

- Eğer $P = \mathcal{O}$ ise $P + Q = Q$, eğer $Q = \mathcal{O}$ ise $P + Q = P$'dir.
- Değilse ve eğer $x_1 = x_2$ ve $y_1 = -y_2$ ise $P + Q = \mathcal{O}$'dır.
- Yukarıdaki koşulların hiçbiri sağlanmıyorsa λ,

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, P = Q \end{cases}$$

şeklinde tanımlanır. $P + Q = (x_3, y_3)$, Denklem 12.4 ve 12.5 kullanılarak hesaplanır.

$$x_3 = \lambda^2 - x_1 - x_2, \tag{12.4}$$

$$y_3 = \lambda(x_1 - x_3) - y_1. \tag{12.5}$$

12.2.3. Nokta Çarpımı

Eliptik eğri kriptografide uygulama zamanının büyük bir bölümünü alan işlem nokta çarpımı işlemidir. *E,* $\mathbb{K}$ sonlu cismi üzerinde tanımlanmış bir eğri, *P, E* üzerinde bir nokta ve *n* bir tam sayı olsun. *P* noktasının *n* tam sayısıyla çarpılması işlemi,

$$[n]P = \underbrace{P + P + \cdots + P}_{\text{n defa}}$$

olarak tanımlanır [6]. Nokta çarpımı *nP* olarak da ifade edilir.

n sayısının büyük olduğu durumlarda $[n]P$ hesaplamasını P, $2P$, $3P$,…,nP olarak yapmak verimli olmadığından daha performanslı algoritmalar tercih edilir. Bunlardan en sık kullanılanı iki kat al-ve-topla (double-and-add) algoritmasıdır. $[n]P = Q$ olsun. Q noktasını hesaplamak için ilk önce n sayısı ikilik tabanda yazılır. n sayısının ikilik tabanda yazılmış hali, $n_0, \dots, n_t \in \{0,1\}$ olmak üzere

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 \cdots + n_t \cdot 2^t,$$

şeklindedir. Ardından

$$Q_0 = P$$
$$Q_1 = 2Q_0$$
$$Q_2 = 2Q_1$$
$$\vdots$$
$$Q_t = 2Q_{t-1}$$

hesaplamaları yapılır. Burada $Q_i = 2^i P$ olarak durumu genelleyebiliriz. n_i katsayılarının 1 olduğu durumlarda ise elde edilen Q_i noktasının toplama eklenmesi gerekir. Bu durumda, $[n]P$ noktasını hesaplamak için toplamda t tane iki kat alma ve n_i'lerin 1'e eşit olduğu durumlar kadar nokta toplama işlemi yapılması gerekir. Bu yönteme iki kat al-ve-topla algoritması denir ve Algoritma 12.1'de sunulmuştur.

Algoritma 12.1. İki Kat-Al-ve-Topla Algoritması

Girdi: E eliptik eğrisi üzerinde bulunan P noktası ve pozitif n tam sayısı.

Çıktı: Q = nP.

1. Q = P ve R = $\mathcal{O}$ atamalarını yap.
2. n > 0 **sağlandığı sürece**
3. n mod 2 ≡ 1 **ise**
4. R = R + Q
5. Q = 2Q
6. n = ⌊$n/2$⌋
7. **Sonuç** R

12.2.4. Sonlu Cisimler Üzerine Tanımlanan Eliptik Eğriler

Bölüm 12.2'de eliptik eğriler reel sayılar kümesi üzerinde gösterilmiştir. Geometrik olarak nokta işlemleri reel sayılar üzerinde tanımlanmış eğriler ile görsel olarak kolayca ifade edilebilmektedir. Bu nedenle eliptik eğrilere bu noktadan başlamak daha rahat anlaşılmasını sağlar. Ancak, kriptografide genellikle sonlu cisimler üzerinde tanımlanmış eliptik eğriler kullanılmaktadır.

$p \geq 3$ bir asal sayı, $\mathbb{F}_p$ bir sonlu cisim olsun. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlanan E eliptik eğrisi

$$E: y^2 = x^3 + ax + b,$$

şeklinde ifade edilir. a ve b, $\mathbb{F}_p$ cisminin elemanlarıdır ve $4a^3 + 27b^2 \neq 0$ koşulunu sağlamaları gerekir. E eğrisi üzerinde bulunan noktalar,

$$E(\mathbb{F}_p) = \{(x,y) \mid x,y \in \mathbb{F}_p, y^2 - (x^3 + ax + b) = 0\} \cup \{\mathcal{O}\}.$$

şeklinde ifade edilir. Bölüm 12.2.2'de gösterilen grup kuralları $\mathbb{F}_p$ sonlu cismi üzerinde tanımlanmış E eğrisi için de uygulanabilir. Bu durumda bu eğri üzerine tanımlanan iki noktanın toplamı yine aynı eğri üzerinde bir nokta verir.

Sonlu cisimler üzerinde tanımlanan eliptik eğrilerin yaklaşık nokta sayısı Hasse teoremiyle bulunur. $\mathbb{F}_p$ üzerinde tanımlanan bir E eliptik eğrisinin nokta sayısı N olsun. Denklem 12.6, E eğrisinin nokta sayısını (kardinalitesini) yaklaşık olarak vermektedir.

$$|N - (p+1)| \leq 2\sqrt{p}. \tag{12.6}$$

1985 yılında Schoof, sonlu cisimler üzerindeki nokta sayısını polinom zamanda ve deterministik olarak hesaplayabilen Schoof algoritmasını önermiştir [7]. Ardından 1991 yılında Elkies'in ve 1988 yılında Atkin'in Schoof algoritmasına yaptığı katkılarla, sonlu cisimler üzerinde bulunan nokta sayısını hesaplayan, polinom zamanda ve deterministik olarak çalışan SEA (*Schoof-Elkies-Atkin*) algoritması ortaya çıkmıştır [8].

12.2.5. Verimli Gerçekleştirme

Eliptik eğri kriptografi, verimlilik ve güvenlik seviyesi bakımından diğer açık anahtarlı kriptografi rakipleri arasında dikkate değer bir performans göstermektedir. Eliptik eğri kriptosistemler küçük anahtar boyutlarıyla yüksek güvenlik seviyeleri sağlamaktadır. Tablo 12.1'de görüldüğü üzere aynı seviye güvenlik için RSA'dan çok daha küçük anahtar boyutları ECC için yeterli olmaktadır [9].

Kriptografide güvenlik seviyesi kriptografik protokollerin ne kadar güvenlik sağladığını gösteren bir ölçü birimidir. Genellikle *n*-bit güvenlik olarak ifade edilir ve güvenlik seviyesi *n*-bit olan bir kriptosistemin bir saldıran tarafından kırılması için 2^n işlem gerçekleştirilmesi gerektiği anlamına gelir.

Tablo 12.1. NIST (*National Institute of Standards and Technology*) tarafından önerilen güvenlik seviyesi - anahtar boyutu değerleri [9]

Güvenlik Seviyesi	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Benzer şekilde, hesaplama zamanlarında da ECC, RSA'dan çok daha iyi performans sergilemektedir. Eliptik eğrilerin sağladığı avantajların yanı sıra, eliptik eğri kriptosistemleri hızlandırmak üzere yapılan çalışmaların da bu performans farkında büyük bir önemi vardır. Eliptik eğrilerin açık anahtarlı kriptosistemler arasında kullanımının başlamasıyla, verimli gerçekleştirme konusunda çeşitli çalışmalar yapılmaya başlanmıştır. Bu bölümde, eliptik eğri kriptografinin daha verimli çalışması için yapılan çalışmalar iki başlık altında toplanarak açıklanacaktır.

12.2.5.1. Eliptik Eğri Aritmetiği Hızlandırma İşlemleri

Bölüm 12.2.1, 12.2.2 ve 12.2.4'te eliptik eğriler açıklanırken kullanılan koordinat sistemi afin (*affine*) koordinat sistemi olarak adlandırılır. Bölüm 12.2.2'de de açıklandığı üzere, afin koordinat düzleminde *P* ve *Q* noktalarının toplamı (x_3, y_3), istisna durumlar dışında

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, P = Q \end{cases}$$

olmak üzere,

$$x_3 = \lambda^2 - x_1 - x_2, \tag{12.7}$$

$$y_3 = \lambda(x_1 - x_3) - y_1, \tag{12.8}$$

şeklinde hesaplanır.

Formüllerde görüldüğü gibi bu hesaplamaları yapabilmek için tanımlanan sonlu cisimde ters alma işlemi yapılması gerekmektedir. Modüler ters alma işlemi, uygulamada en çok CPU zamanı harcayan işlemdir. Kriptografik protokollerin yazılımsal uygulamalarında nokta toplama, noktaların iki katını alma işlemleri defalarca tekrar edilir. Bu bağlamda, defalarca tekrar eden bu işlemlerde CPU zamanını bu denli harcayan bir işlemi her döngüde gerçekleştirmek büyük bir verimlilik kaybına neden olur. Ancak, bu protokolleri gerçekleştirmek için yapılan işlemleri başka bir koordinat sistemine taşımak bu kaybın azaltılmasına yardımcı olmaktadır.

Homojen izdüşümsel (*homogeneous projective*) koordinat sistemi, yaygın kullanılan koordinat sistemlerindendir. İzdüşümsel koordinatlarda $\mathbb{F}_p$ üzerinde tanımlanan E eliptik eğrisinin denklemi,

$$E: Y^2Z = X^3 + a_4XZ^2 + a_6Z^3,$$

ile ifade edilir. İzdüşümsel düzlemde bir nokta $(X_1 : Y_1 : Z_1)$ şeklinde gösterilir. Bu nokta afin düzlemde $Z_1 \neq 0$ durumunda $(X_1/Z_1, Y_1/Z_1)$ noktasına denk gelir. Birim eleman ya da sonsuzdaki nokta $\mathcal{O} = (0:1:0)$ noktasıdır. $(X_1 : Y_1 : Z_1)$ noktasının tersi ise $(X_1 : -Y_1 : Z_1)$ noktasıdır. Denklem 12.7 ve 12.8'de verilen toplama formülleri, izdüşümsel koordinat sistemine şu şekilde taşınır:

$P = (X_1 : Y_1 : Z_1)$ ve $Q = (X_2 : Y_2 : Z_2)$, E eğrisi üzerinde iki nokta olsun. $P \neq Q$ koşulu sağlandığında $P + Q = (X_3 : Y_3 : Z_3)$,

$A = Y_2Z_1 - Y_1Z_2$, $B = X_2Z_1 - X_1Z_2$, $C = A^2Z_1Z_2 - B^3 - 2B^2Z_1Z_2$,
$X_3 = BC$, $Y_3 = A(B^2X_1Z_2 - C)B^3Y_1Z_2$, $Z_3 = B^3Z_1Z_2$,

eşitlikleri kullanılarak hesaplanır [10]. $[2]P = (X_3 : Y_3 : Z_3)$ ise

$A = a_4Z_1^2 + 3X_1^2$, $B = Y_1Z_1$, $C = X_1Y_1B$, $D = A^2 - 8C$,
$X_3 = 2BD$, $Y_3 = A(4C - D) - 8Y_1^2B^2$, $Z_3 = 8B^3$,

şeklinde hesaplanır [10].

İzdüşümsel koordinat sistemi için verilen toplama ve iki kat alma formüllerinde görüldüğü gibi modüler ters alma işlemi bulunmamaktadır. Ancak işlemlerin sonunda koordinat sistemi değiştirilirken ters alma işlemi yapılır.

Eliptik eğri aritmetiğini hızlandırmak adına Weierstrass eğrisine izomorf olan başka eğri modelleri de kullanılmaktadır. Weierstrass eğrisine izomorf olan, hız odaklı uygulamalarda tercih edilen eğri denklemlerinden bir bölümü aşağıda verilmiştir.

- Extended Jacobi Quartic Form: $E_Q : y^2 = dx^4 + 2ax^2 + 1$ [11],
- Extended Huff Form: $H_{a,c,d} : y(1 + ax^2) = cx(1 + dy^2)$ [12],
- Jacobi Intersection Form: $E_I : bu^2 + v^2 = 1, au^2 + w^2 = 1$ [5],
- Short Weierstrass Form: $E_W : y^2 = x^3 + ax + b$,
- Twisted Edwards Form: $E_E : ax^2 + y^2 = 1 + dx^2y^2$ [13],
- Twisted Hessian Form: $E_{He} : ax^3 + y^3 + 1 = dxy$ [5], [14].

Bu eğri denklemlerindeki eğri değişkenleri üzerinde küçük değişiklikler yapılarak ya da eğri değişkenlerine bazı küçük sabit değerlerin atanmasıyla toplamda en küçük dereceli toplama ve iki kat alma formülleri elde edilmeye çalışılır. Uygulama sırasında ise eğri denklemi ve işlevine göre en uygun koordinat düzlemi seçilir. Böylece verimli gerçekleştirme sağlanır.

Bu konular ile ilgili daha detaylı bilgi için okuyucunun [5], [11], [12], [13], [14] ve [15] kaynaklarına bakması önerilmektedir.

12.2.5.2. Sonlu Cisim Aritmetiğini Hızlandırma İşlemleri

ECC'de kullanılan eliptik eğrilerin genellikle $\mathbb{F}_p$ üzerinde tanımlandığından söz etmiştik. Bu nedenle bu tip protokollerde yapılan tüm işlemler $\mathbb{F}_p$ üzerinde yapılır. Bu da yapılan her işlemde *mod p* indirgemesi yapılması gerektiği anlamına gelir. Bu işlem uygulama açısından zahmetli olduğu için bu alanda yapılacak verimlileştirmeler ECC'nin verimli gerçekleştirilmesinde büyük rol oynar. İndirgeme işlemi kullanılan asal sayı p özel bir forma sahip olduğunda (NIST asalları gibi) görece hızlandırılabilir.

Yazılım uygulamalarında 8'in katı olan W −bit mimari kullanıldığını düşünelim. Kullandığımız bilgisayarlar kullanım amacına göre değişmekle beraber genellikle 64, 32, 16, 8 bit mimariye sahiptir. W −bit uzunluğundaki bir sözcüğün (*word*) bitleri 0'dan $p-1$'e kadar numaralandırılır. En sağdaki bit 0'dır. $\mathbb{F}_p$ cisminin elemanları 0'dan $p-1$'e kadar olan tam sayılardır. $m = \lceil \log_2 p \rceil$, sayısının bit uzunluğu olsun. Bu durumda bu sayının sözcük uzunluğu $t = \lceil m/W \rceil$ olur.

Örneğin, $X = (X[t-1], X[t-2], \ldots, X[1], X[0])$, bir $x \in \mathbb{F}_p$ sayısının X dizisinde gösterilişi ve $X[0]$, x sayısının en önemsiz biti olmak üzere, $x \in \mathbb{F}_p$ sayısının W-bit mimaride ikilik tabanda şu şekilde ifade edilebilir:

$$x = 2^{(t-1)W} X[t-1] + 2^{(t-2)W} X[t-2] + \cdots + 2X[1] + X[0].$$

Algoritma 12.2 Büyük Sayı Toplama Algoritması

Girdi: $a, b \in [0, 2^{W_\alpha})$ tam sayıları. **Çıktı**: $x = a + b \ mod \ 2^{W_\alpha}$ ve t kalan sayı olacak şekilde (x, t).
1. $(t, X[0]) \leftarrow (A[0] + B[0])$ 2. $i = 1$**'den** $i = \alpha - 1$**'e kadar** 3. $(t, X[i]) \leftarrow (A[i] + B[i])$ 4. **Sonuç** (x, t)

Çok-sözcüklü sayılarda toplama işlemi yaparken x sayısı $(t,k) \leftarrow x$ olarak temsil edilir, bu eğer $t \leftarrow x \; mod \; 2^W$ ve $x \in [0,2^W)$ ise $t \leftarrow 0$, değilse $t \leftarrow 1$ anlamına gelir. $a,b \in [0,2^W)$ ve $k' \in \{0,1\}$ olduğunu varsayalım. Eğer $x = a + b + t'$ olarak ifade edilen bir tek-sözcük toplama işlemi ise, $x = k2^W + z$ olarak yazılır, bu gösterimde toplama işleminde k kalan bit olarak ifade edilir (k ancak ve ancak $z < x + k'$ koşulunda 1 olur.). İşlemciler komut kümesinde bulunduğu için kalan bit işlemini herhangi bir ek işlem olmadan halledebilir.

Algoritma 12.2 çok-sözcüklü tam sayıların toplama işlemini göstermektedir. Tam sayıları toplayan bu algoritmanın $\mathbb{F}_p$'de tanımlı sayılar üzerinde çalışması için algoritmaya ek olarak $mod\ p$ indirgeme adımını eklemek yeterlidir.

$a,b \in \mathbb{F}_p$ sayılarıyla cisim çarpımı için a ve b sayıları önce çarpılır ardından çarpım mod p'de indirgenir. Algoritma 12.3, $\mathbb{F}_p$'de tanımlı iki sayının çarpımını vermektedir.

Algoritma 12.3'te verilen (UV), W-bit uzunluğundaki U ve V sözcüklerinin birleşmesiyle oluşan $2W$-bit uzunluğunda bir değeri ifade etmektedir.

Ancak bu yöntem n-sözcük (word) tam sayılar için $O(n^2)$ işlem yapılmasını gerektirir. Verimli gerçekleştirmeden söz ediliyorsa bu hesaplama karmaşıklığı çok yüksek kalır. Bu nedenle böl-yönet yöntemini kullanan ve hesaplama karmaşıklığı $O\left(n^{\log_2 3}\right)$ olan Karatsuba çarpımı [16] yoğun bir şekilde kullanılır.

Örneğin, $n = 2l$ ve $x = x_1 2^l + x_0$, $y = y_1 2^l + y_0$ şeklinde gösterilen $2l$ bitlik tam sayılar olsun. Bu durumda xy çarpımı,

$$\begin{aligned} xy &= (x_1 2^l + x_0)(y_1 2^l + y_0) \\ &= x_1 \cdot y_1 2^{2l} + [(x_0 + x_1) \cdot (y_0 + y_1) - x_1 \cdot y_1 - x_0 \cdot y_0]^{2l} + x_0 \cdot y_0. \end{aligned}$$

şeklinde gösterilir. Böylece xy hesaplanırken bir tane $2l$ bitlik çarpım yapmak yerine, üç tane l bitlik çarpım ve bazı toplama çıkarma işlemleri yapılabilir. l'nin büyük olduğu durumlarda toplama ve çıkarma işlemleri, çarpma

işlemine göre daha az masraflıdır. Diğer yandan daha küçük l değerleri için ise bu yöntemin ek masraflar yaratması olasıdır. Büyük sayılarda bu çarpım işlemi uygulanırken belli bir eşik değerine kadar Karatsuba yöntemi uygulayıp ardından geri kalan işlemler için klasik yönteme dönmek daha verimli bir gerçekleştirme sağlar. Kalan değer ve donanımsal kısıtlar darboğaza neden olabilir. Bu gibi durumlarda uygulama alanında çeşitli yöntemler ile bu darboğazlardan kaçınılabilir. Karatsuba benzeri algoritmaların detaylı incelemesi için [17], diğer verimli güncel yaklaşımlar için de [18], [19] ve [20] çalışmalarına bakılabilir.

Algoritma 12.3 Büyük Sayı Çarpım Algoritması

Girdi: $a, b \in [0, p-1)$ tam sayıları.

Çıktı: $c = a \cdot b$.

1. $i = 0$**'dan** $i = \mathrm{t} - 1$**'e kadar**
2. $C[i] \leftarrow 0$
3. $i = 0$**'dan** $i = \mathrm{t} - 1$**'e kadar**
4. $U \leftarrow 0$
5. $j = 0$**'dan** $j = \mathrm{t} - 1$**'e kadar**
6. $(UV) \leftarrow C[i+j] + A[i] \cdot B[j] + U$
7. $C[i+j] \leftarrow V$
8. $C[i+t] \leftarrow U$
9. **Sonuç** c.

Eliptik eğrilerin uygulamalarında verimliliği en çok etkileyen bir diğer cisim işlemi de modüler indirgeme işlemidir. Özellikle NIST asalları gibi özel bir yapıda olmayan asal sayılar kullanıldığında $x \bmod p$ indirgemesi çok masraflı bir işlem olabilir. Montgomery [21] ve Barrett [22] indirgeme yöntemleri bu işlemi verimlileştirmek adına kullanılan iki yöntemdir. Bu yöntemler modüler indirgeme işleminde bulunan masraflı bölümleri daha masrafsız işlemler-

le değiştirmektedir. Her iki yöntemin de avantajlı ve dezavantajlı özellikleri mevcuttur. Örneğin, Montgomery indirgemesinde veri aktarımı söz konusudur. Bu nedenle ara çarpım işlemlerinde sonuçların kaydedilmesi gerekir. Öte yandan Barrett indirgemesinde işlem yükü fazla olan modülüs bağımlı hesaplamalar gerekir. Bu da bu yöntemin yalnızca tek bir modülüsün kullanıldığı durumlarda verimli olduğu anlamına gelir. Buna rağmen büyük çaplı protokollerde Barrett indirgemesi daha sık olarak tercih edilir çünkü bu tip işlemlerde modülüs değişikliğine çok fazla gereksinim duyulmamaktadır.

Barrett indirgemesi z ve p pozitif tam sayıları için $z \; mod \; p$ değerini bulan bir yöntemdir. Algoritma 12.4 Barrett indirgemesi yöntemini göstermektedir. Bu yöntemde $\lfloor z/\, p \rfloor$ bölümü daha uygun tabanların seçilmesi ve bunların üslerinin alınması (Örneğin, verilen L sayısı için $b = 2^L$ değeri modülüse bağlıdır ancak z değerine bağlı değildir.) gibi daha az masraflı işlemler kullanılarak hesaplanır. Algoritmanın birçok indirgeme işlemini tek bir modülüs kullanarak yapmasını sağlamak için ise modülüse bağlı olan $\lfloor b^{2k}/p \rfloor$ hesaplamasının yapılması gereklidir.

Algoritma 12.4 Barrett İndirgeme Algoritması

Girdi: $p, b \geq 3,\ k = \lfloor log_b p \rfloor + 1,\ 0 \leq z \leq b^{2k}, \mu = \lfloor b^{2k}/p \rfloor$.

Çıktı: $z \; mod \; p$

1. $\hat{q} \leftarrow \left\lfloor \lfloor b^{k-1} \rfloor \cdot \mu / b^{k-1} \right\rfloor$
2. $r \leftarrow (\text{z mod } b^{k+1}) - (\hat{q} \cdot \text{p } mod \; b^{k+1})$
3. $r < 0$ **ise**
4. $r \leftarrow r + b^{k+1}$
5. $r \geq p$ **olduğu sürece**
6. $r \leftarrow r - p$
7. **Sonuç** r.

Daha önce de söz edildiği gibi eliptik eğriler için cisim aritmetiğini kolaylaştırmanın bir yolu da özel asallar seçmektir. Örneğin, FIPS 186-4 [23] standartının önerdiği asal sayıların hepsinde az sayıdaki 2'nin katlarının farklarının toplamı olarak ifade edilebilme özelliği bulunur.

Daha önce de söz edildiği gibi eliptik eğriler için cisim aritmetiğini kolaylaştırmanın bir yolu da özel asallar seçmektir. Örneğin, FIPS 186-4 [23] standartının önerdiği asal sayıların hepsinde az sayıdaki 2'nin katlarının farklarının toplamı olarak ifade edilebilme özelliği bulunur.

$$\left.\begin{aligned} p_{192} &= 2^{192} - 2^{64} - 1 \\ p_{256} &= 2^{256} - 2^{224} - 2^{192} - 2^{96} - 1 \\ p_{384} &= 2^{384} - 2^{128} - 2^{96} - 2^{32} - 1 \end{aligned}\right\} \quad 12.9$$

Denklem 12.9'da, FIPS 186-4'te önerilen asallardan birkaçı verilmiştir. Bu standartta önerilen asal sayıların birçoğunda 2'nin kuvvetleri aynı zamanda 32'nin de katıdır. Bu durum özellikle 32-bit mimarilerde modüler indirgeme işlemini kolaylaştırmaktadır.

FIPS 186-4 dışında ECC'yi standartlaştıran ANSI X9.62 [24], Brainpool [25], IEEE P1363 [26] gibi başka standartlar da bulunur. Ayrıca Bernstein'in önerdiği *Curve25519* eğrisi [27] hem güvenlik hem de verimlilik açısından oldukça iyi bir performans sergileyen, özellikle son yıllarda kriptografik uygulamalarda sıklıkla tercih edilen ve standartlara giren bir eğridir. Lange ve Bernstein tarafından yayınlanan *SafeCurves* [28] adlı internet sitesi, güvenli eğrilerin kullanılmasında yapılması gerekenler için iyi bir referanstır.

12.3. ELİPTİK EĞRİLERİN KRİPTOGRAFİDE KULLANILMASI

Günümüzde veri güvenliğini sağlayan birçok kriptografik araçta matematiksel altyapısı Bölüm 12.2'de açıklanan, eliptik eğri kriptografi protokolleri kullanılmaktadır. Bu bölümde bu protokollerin zorluğunun dayandığı matematik problemi (Bölüm 12.3.1) ve bu problemi kullanan protokoller (Bölüm 12.3.2) açıklanmıştır. Ayrıca eliptik eğriler kullanılarak oluşturulan ve kuan-

tum sonrası kriptografide gelecek vaat ettiği düşünülen süpersingüler izojen tabanlı kriptografi de (Bölüm 12.3.3) açıklanmıştır.

12.3.1 Eliptik Eğri Ayrık Logaritma Problemi

Eliptik eğri kriptosistemlerin güvenliği eliptik eğri ayrık logaritma probleminin zorluğuna dayanmaktadır. Ayşe ve Barış'ın açık bir kanal üzerinden eliptik eğri kriptografi kullanarak haberleştiğini ve Ece'nin de bu açık kanaldan aktarılan bilgiyi görebildiğini düşünelim. Ayşe'nin gizli anahtarı,

$$Q = nP,$$

eşitliğini sağlayan pozitif n tam sayısı olsun. Ayşe açık kanaldan $\mathbb{F}_p$ sonlu cisminde tanımlanan E eğrisi üzerinde bulunan P ve Q noktalarını gönderir. Ece elde ettiği Q ve P noktalarından Ayşe'nin gizli anahtarı n'yi elde etmeye çalışır. Diğer bir deyişle, Ece Q noktasını elde etmek için P noktasını kaç defa kendisiyle toplamak gerektiğini çözmelidir.

P ve Q, sonlu cisim $\mathbb{F}_p$ üzerinde tanımlanan E eliptik eğrisi üstünde birer nokta, n ise $Q = nP$ şartını sağlayan pozitif bir tam sayı olsun. *Eliptik eğri ayrık logaritma problemi* (*ECDLP*), P ve Q bilgisinden n sayısını bulma problemidir. Burada n sayısı

$$n = \log_P Q,$$

şeklinde gösterilir ve Q'nun P tabanında ayrık logaritması olarak ifade edilir.

Q ve P noktalarının bilinmesine rağmen n tam sayısının bulunması işleminin hesaplama bakımından zorlu olduğu varsayılır. n sayısını hesaplamak için var olan algoritmalar içinde bilinen en hızlı yöntem Pohling-Hellman ve Pollard Rho algoritmalarının kombinasyonudur. p sayısı n'nin en büyük asal çarpanı olmak üzere algoritmanın zaman karmaşıklığı (*time complexity*) $O(\sqrt{p})$'dir. Bu durumda, bilinen en iyi algoritma bile yarı üstel zamanda (*sub-exponential complexity*) çözüm üretmektedir. Bu nedenle, düzgün seçilmiş parametrelerle çalışan, güvenliği ECDLP'ye dayanan bir eliptik eğri kriptosistemini makul bir zamanda kırmak hesaplamalı olarak imkansız kabul edilir.

12.3.2. Eliptik Eğri Kriptosistemler

12.3.2.1. Eliptik Eğri Diffie-Hellman Anahtar Değişimi

Diffie-Hellman anahtar değişim (*Diffie-Hellman key exchange*) protokolü, 1976 yılında Whitfield Diffie ve Martin Hellman tarafından yayınlanmıştır. Bu protokol iki taraf arasında açık bir kanal üzerinden ortak bir anahtar paylaşılmasını hedefler. Eliptik eğri Diffie-Hellman (*Elliptic Curve Diffie-Hellman – ECDH*) anahtar değişimi ise bu protokolün eliptik eğri kriptografiyi kullanan bir versiyonudur. ECDH'nin güvenliği aşağıda açıklanmış olan eliptik eğri Diffie-Hellman problemine dayanmaktadır.

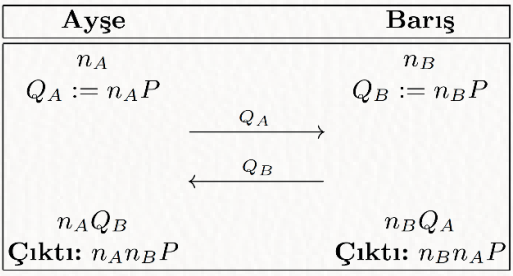
Bir sonlu cisim üzerindeki $E(\mathbb{F}_p)$ eliptik eğrisi ve $P \in E(\mathbb{F}_p)$ verilsin. $n_1, n_2 \in \mathbb{Z}^+$ olmak üzere, n_1P ve n_2P değerlerinden n_1n_2P değerini hesaplama problemine *Eliptik Eğri Diffie-Hellman* Problemi denir ve bu problem hesaplama bakımından zor kabul edilir.

Protokol şu şekilde çalışmaktadır: Ayşe ve Barış, $\mathbb{F}_p$ üzerinde E eliptik eğrisi ve bu eğri üzerinde bir P noktası kullanmayı kararlaştırır. Ayşe rastgele n_A gizli tam sayısını ve Barış rastgele n_B gizli tam sayısını seçer. Sonra Ayşe $Q_A = n_AP$ çarpımını hesaplayarak Barış'a, Barış da $Q_B = n_BP$ çarpımını hesaplayarak Ayşe'ye gönderir. Son olarak Ayşe n_A gizli çarpanını kullanarak n_AQ_B değerini, Barış n_B gizli çarpanını kullanarak n_BQ_A değerini hesaplar.

Ayşe ve Barış'ın paylaştığı ortak gizli anahtar,

$$n_AQ_B = n_An_BP = n_BQ_A,$$

olur ve bu anahtarı simetrik şifreleme yaparken kullanabilirler. Bu protokol Şekil 12.3'te açıklanmıştır.



Şekil 12.3. Eliptik eğri Diffie-Hellman anahtar değişimi

Örneğin, $\mathbb{F}_{227}$ üzerinde bir $E: y^2 = x^3 + 2x + 2$ eliptik eğrisi ve bu eğri üzerinde bir $P = (4,55)$ noktası verilsin.

Ayşe rastgele $n_A = 2$ gizli tam sayısını seçer ve $Q_A = n_A P = 2\mathrm{P}$ değerini hesaplar:

- $Q_A = 2P = P + P = (4,55) + (4,55)$,

$$\lambda \equiv \frac{3x_1^2 + a}{2y_1} \; mod\; p \equiv \frac{3 \cdot 4^2 + 2}{2 \cdot 55} \; mod\; 227 \equiv 50 \cdot 110^{-1} \; mod\; 227$$
$$\equiv 50 \cdot 97 \; mod\; 227 \equiv 83,$$
$$x_3 \equiv \lambda^2 - x_1 - x_2 \; mod\; p \equiv 83^2 - 4 - 4 \; mod\; 227 \equiv 71,$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \; mod\; p \equiv 83(4 - 71) - 55 \; mod\; 227 \equiv 59,$$
$$2P = (71,59). \qquad (12.10)$$

Ayşe $Q_A = (71,59)$ değerini Barış'a gönderir. Barış ise rastgele $n_B = 3$ gizli tam sayısını seçer ve $Q_B = n_B P = 3P$ çarpımını hesaplar. Bu işlemi yaparken iki kat al-ve-topla algoritması yardımıyla sırasıyla $P + P = 2P$ ve $2P + P = 3P$ toplamlarını hesaplar:

- $2P = P + P = (4,55) + (4,55) = (71,59)$,

olduğu Denklem 12.3.1'de görülebilir.

- $Q_B = 3P = 2P + P = (71,59) + (4,55)$,

$$\lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} \; mod\; p \equiv \frac{55 - 59}{4 - 71} \; mod\; 227 \equiv 223 \cdot 160^{-1} \; mod\; 227$$
$$\equiv 223 \cdot 166 \; mod\; 227 \equiv 17,$$
$$x_3 \equiv \lambda^2 - x_1 - x_2 \; mod\; p \equiv 17^2 - 71 - 4 \; mod\; 227 \equiv 214,$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \; mod\; p \equiv 17(71 - 214) - 59 \; mod\; 227 \equiv 7,$$
$$3\mathrm{P} = (214,7).$$

Barış da $Q_B = (214,7)$ değerini Ayşe'ye gönderir. Daha sonra Ayşe $n_A = 2$ gizli çarpanını kullanarak

$$n_A Q_B = 2Q_B$$

değerini hesaplar:

- $n_A Q_B = 2(214,7) = (214,7) + (214,7)$,

$$\lambda \equiv \frac{3x_1^2 + a}{2y_1} \; mod\; p \equiv \frac{3 \cdot 214^2 + 2}{2 \cdot 7} \; mod\; 227 \equiv 55 \cdot 14^{-1} \; mod\; 227$$
$$\equiv 55 \cdot 146 \; mod\; 227 \equiv 85,$$
$$x_3 \equiv \lambda^2 - x_1 - x_2 \; mod\; p \equiv 85^2 - 214 - 214 \; mod\; 227 \equiv 214,$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \; mod\; p \equiv 85(214 - 214) - 7 mod\; 227 \equiv 220,$$
$$n_A Q_B = 2Q_B = (214,220).$$

Son olarak, Barış $n_B = 3$ gizli çarpanını kullanarak

$$n_B Q_A = 3Q_A$$

değerini hesaplar:

- $2Q_A = 2(71,59) = (71,59) + (71,59)$,

$$\lambda \equiv \frac{3x_1^2 + a}{2y_1} \; mod\; p \equiv \frac{3 \cdot 71^2 + 2}{2 \cdot 59} \; mod\; 227 \equiv 143 \cdot 118^{-1} \; mod\; 227$$
$$\equiv 143 \cdot 202 \; mod\; 227 \equiv 57,$$
$$x_3 \equiv \lambda^2 - x_1 - x_2 \; mod\; p \equiv 57^2 - 71 - 71 \; mod\; 227 \equiv 156,$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \; mod\; p \equiv 57(71 - 156) - 59 \; mod\; 227 \equiv 90,$$
$$2Q_A = (156,90).$$

- $3Q_A = 2Q_A + Q_A = (156,90) + (71,59)$,

$$\lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} \; mod\; p \equiv \frac{59 - 90}{71 - 156} \; mod\; 227 \equiv 196 \cdot 142^{-1} \; mod\; 227$$
$$\equiv 196 \cdot 8 \; mod\; 227 \equiv 206,$$
$$x_3 \equiv \lambda^2 - x_1 - x_2 \; mod\; p \equiv 206^2 - 156 - 71 \; mod\; 227 \equiv 214,$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \; mod\; p \equiv 206(156 - 214) - 90 \; mod\; 227 \equiv 220,$$
$$n_B Q_A = 3Q_A = (214,220).$$

Ayşe ve Barış'ın paylaştığı ortak gizli anahtar,

$$n_A Q_B = n_A n_B P = n_B Q_A = (214,220),$$

şeklindedir.

Eliptik Eğri Diffie-Hellman anahtar değişiminde Ayşe ve Barış'ın eliptik eğri üzerindeki Q_A, Q_B noktalarını birbirlerine göndermeleri gerekmektedir. $x_Q, y_Q \in \mathbb{F}_p$ olmak üzere bir $Q = (x_Q, y_Q) \in E(\mathbb{F}_p)$ noktasının iki koordinatı vardır. Bu durumda, Ayşe ve Barış birbirlerine Q noktalarını gönderirken $\mathbb{F}_p$ cismi üzerindeki iki noktayı göndermeleri gerekir. Q noktası E eliptik eğrisi üzerinde olduğundan x_Q, y_Q değerleri arasında $y_Q^2 = x_Q^3 + ax_Q + b$ ilişkisi vardır. Ece a ve b değerlerini bildiğinden, eğer x_Q değerini doğru tahmin ederse y_Q için iki değer ihtimali vardır ve bu değerleri hesaplamak zor değildir. Ayşe Q_A noktasını Barış'a gönderirken sadece x_A değerini gönderirse, Barış buna karşılık iki adet y_A değeri hesaplar. Doğru y değerini seçerse Q_A noktasını, diğer y değerini seçerse de $-Q_A$ noktasını kullanarak $\pm n_A n_B P$ değerlerinden birine ulaşır. Ayşe de benzer şekilde bu değerlerden birini hesaplar. Her iki y değeri için x koordinatı aynı olduğundan, Ayşe ve Barış x koordinatını ortak paylaşılacak değer olarak kullanabilirler. Koordinat değerleri olan x ve y değerleri arasında denkleme bağlı bir ilişki olduğundan noktalar gönderilirken her iki koordinatı göndermek yerine çeşitli nokta sıkıştırma teknikleri kullanılarak neredeyse yarı boyutuna yakın büyüklükte veri gönderilerek haberleşme karmaşıklığında iyileştirmeler yapılabilir.

12.3.2.2. Eliptik Eğri Elgamal Açık Anahtarlı Kriptosistemi

Elgamal açık anahtarlı kriptosistemi, 1985 yılında Taher Elgamal tarafından yayınlanmıştır. Bu sistemin güvenliği ayrık logaritma problemine dayanmaktadır. Eliptik eğrileri kullanan versiyonu ise Eliptik Eğri Elgamal Açık Anahtarlı Kriptosistemi şeklinde isimlendirilmiştir. Bu kriptosistem şu şekilde çalışmaktadır:

Ayşe ve Barış bu açık anahtarlı kriptosistemde kullanmak üzere bir p asal sayısı, $\mathbb{F}_p$ üzerinde E eliptik eğrisi ve $E(\mathbb{F}_p)$ eğrisi üzerinde bir P noktası kararlaştırır. Ayşe n_A gizli çarpanını seçer ve $Q_A = n_A P$ noktasını açık anahtarı olarak yayınlar. Barış açık metni olan $M \in E(\mathbb{F}_p)$ noktasını şifrelemek için rastgele bir k tam sayısı seçer ve Ayşe'nin açık anahtarı Q_A noktasını kullanarak

$$C_1 = kP,$$

$$C_2 = M + kQ_A,$$

noktalarını hesaplar. Gizli metin olan (C_1, C_2) noktalarını Ayşe'ye gönderir.

Ayşe,

$$C_2 - n_A C_1 = M + kQ_A - n_A kP = M + kn_A P - n_A kP = M,$$

hesaplamasını yaparak açık metin M noktasına ulaşır. Tablo 12.2'de Eliptik Eğri Elgamal Açık Anahtarlı Kriptosistemi açıklanmıştır.

Tablo 12.2. Eliptik eğri Elgamal açık anahtarlı kriptosistemi

Anahtar üretimi: - Ayşe gizli anahtar n_A'yı seçer, - $Q_A = n_A P \in E(\mathbb{F}_p)$ noktasını hesaplar, - Açık anahtar olarak Q_A noktasını yayınlar.
Şifreleme: - Barış $M \in E(\mathbb{F}_p)$ açık metnini belirler, - Rastgele bir k tam sayısı seçer, - Ayşe'nin açık anahtarı Q_A noktasını kullanarak $C_1 = kP \in E(\mathbb{F}_p)$ ve $C_2 = M + kQ_A \in E(\mathbb{F}_p)$ noktalarını hesaplar, - (C_1, C_2) gizli metnini Ayşe'ye gönderir.
Şifre çözme: - Ayşe $C_2 - n_A C_1 \in E(\mathbb{F}_p)$ noktasını hesaplar, - Açık metin M noktasına ulaşır.

12.3.2.3. Eliptik Eğri Sayısal İmzalama

Sayısal İmzalama Algoritması (*Digital Signature Algorithm – DSA*) 1994 yılında NIST tarafından sayısal imzalama standartı olarak kabul edilmiştir. DSA'da eliptik eğrilerin kullanılmasıyla Eliptik Eğri Sayısal İmzalama Algoritması (*Elliptic Curve Digital Signature Algorithm – ECDSA*) elde edilir. ECDSA özellikle imza boyutunun önemli olduğu durumlarda yaygın

kullanıma sahiptir. Blokzincir [29], nesnelerin interneti gibi teknolojiler ECDSA kullanmaktadır. ECDSA algoritması aşağıdaki gibi çalışmaktadır:

Barış, Ayşe'ye sayısal imzalı bir mesaj göndermek istiyor olsun. Bu durumda, eliptik eğri sayısal imzalama algoritmasında kullanılmak üzere, güvenilir üçüncü taraf (*trusted third party*) bazı parametreler belirler. Bunlar p asal sayısı, $\mathbb{F}_p$ üzerinde E eliptik eğrisi ve bu eğri üzerinde mertebesi q (büyük bir asal sayı) olan bir P noktasıdır. Barış, $1 < s < q-1$ olacak şekilde gizli anahtarı $s \in \mathbb{F}_p$ değerini belirler ve açık anahtarını $Q = sP \in E(\mathbb{F}_p)$ şeklinde hesaplar.

ECDSA'nın imzalama adımında, Barış rastgele $d \bmod q$ sayısı seçerek,

$$s_1 \equiv x(dP) \bmod q,$$

değerini hesaplar. Burada $x(\cdot)$, parantez içindeki noktanın x koordinatını ifade etmektedir. Daha sonra Ayşe'ye göndereceği M mesajının özet fonksiyonu *(hash function) H(M)*'yi kullanarak,

$$s_2 \equiv d^{-1}(H(M) + ss_1) \bmod q,$$

ifadesini hesaplar ve (s_1, s_2) imzasını, mesajı ile birlikte Ayşe'ye gönderir.

ECDSA'nın imza doğrulama adımında, Ayşe (s_1, s_2) imza çifti ve M mesajı ile

$$v_1 \equiv s_2^{-1} H(M) \bmod q,$$

$$v_2 \equiv s_1 s_2^{-1} \bmod q,$$

değerlerini hesaplar. Daha sonra P noktasını ve Q açık anahtarını da kullanarak $v_1P + v_2Q$ değerini hesaplar ve Barış'ın imzasının doğruluğunu ölçer.

$$v_1P + v_2Q = s_2^{-1}H(M)P + s_1s_2^{-1}(sP) = (H(M) + ss_1)s_2^{-1}P$$
$$= (ds_2)s_2^{-1}P = dP \in E(\mathbb{F}_p),$$

işleminden de görülebileceği gibi dP sonucuna ulaşır.

$$x(v_1P + v_2Q) \bmod q \equiv x(dP) \bmod q \equiv s_1,$$

olduğundan imza geçerli kabul edilir.

Eliptik eğri sayısal imzalama algoritması Algoritma 12.5'te, eliptik eğri sayısal imza doğrulama algoritması ise Algoritma 12.6'da verilmiştir.

Algoritma 12.5 Eliptik Eğri Sayısal İmzalama Algoritması

Girdi: Mertebesi q olan $P \in E(\mathbb{F}_p)$ noktası, M mesajı, $1 < s < q - 1$ olacak şekilde s gizli imzalama anahtarı ve H özet fonksiyonu.

Çıktı: İmza (s_1, s_2).

1. Rastgele bir $d\ mod\ q$ tam sayısı seç.
2. $s_1 \equiv x(dP)\ mod\ q$ değerini hesapla.
3. $s_1 = 0$ **ise**
4. 1. adıma geri dön.
5. $s_2 \equiv d^{-1}(H(M) + ss_1)\ mod\ q$ değerini hesapla.
6. $s_2 = 0$ **ise**
7. 1. adıma geri dön.
8. **Sonuç** (s_1, s_2).

Algoritma 12.6 Eliptik Eğri Sayısal İmza Doğrulama Algoritması

Girdi: Mertebesi q olan $P \in E(\mathbb{F}_p)$ noktası, M mesajı, (s_1, s_2) imzası, $Q = sP \in E(\mathbb{F}_p)$ açık anahtar ve H özet fonksyonu.

Çıktı: r.

1. $r = Yanlış.$
2. $s_1, s_2 \in [1, q-1]$ **ise**
3. $v_1 \equiv s_2^{-1}H(M)\ mod\ q$, $v_2 \equiv s_1 s_2^{-1} mod\ q$ değerlerini hesapla.
4. $V = v_1P + v_2Q$ değerini hesapla.
5. $V \neq 0$ **ise**
6. $s_1 \equiv x(V) mod\ q$ **ise**
7. $r = Doğru.$
8. **Sonuç** r.

12.3.3. Kuantum Sonrası Kriptografide Eliptik Eğriler

Richard Feynman'ın kuantum mekaniği ile ilgili simülasyonların normal bilgisayarlar ile yapılamayacağını açıklaması üzerine, 1982 yılı itibariyle kuantum bilgisayarlar ile ilgili çalışmalar başlamıştır. Günümüzde yaygın olarak kullanılan normal bilgisayarlarda işlemler bitler ile yapılırken kuantum bilgisayarlarda kuantum mekaniğindeki süperpozisyon ve dolanıklık gibi kavramları temel alan kübitlerle işlem yapılmaktadır. Kuantum bilgisayarlarda ölçüm yapmak normal bilgisayarlara kıyasla daha zordur, fakat ölçüm işlemi düzgün yapılabildiğinde normal bilgisayarlarda zor hesaplanan bazı problemler kuantum bilgisayarlarda kolaylıkla hesaplanabilmektedir. Peter Shor'un 1994 yılında normal bilgisayarlarda yarı üstel çalışma zamanına sahip olan çarpanlara ayırma problemi için bulduğu algoritma [30] kriptografi biliminin yönünü değiştirmiştir. Çünkü bu algoritma kuantum-polinom zamanda çalışmaktadır. Bu ve bunun ardından gelen gelişmeler ile, yaygın olarak kullanılan RSA, sonlu cisim, eliptik eğri gibi açık anahtarlı kriptosistemlerin kuantum dünyasında güvenli sayılmayacağı ortaya çıkmıştır.

Günümüzde kuantum bilgisayarlar üzerine birçok gelişme olmuştur. Örneğin, IBM 50, Google ise 72-kübit işlemcili kuantum bilgisayarlar ürettiklerini açıkladılar. Bu işlemci kapasitesindeki bilgisayarlar günümüzde kullanılagelen açık anahtarlı kriptosistemleri etkisiz hale getirebilecek güçte değildir. Ancak önümüzdeki 15-20 yıl içerisinde geliştirilecek olan kuantum bilgisayarlar bu kriptosistemlerin güvenliğini tehdit edebilir. Simetrik kriptografiyi kuantum dayanıklı hale getirmek için var olan algoritmalarda anahtar boyutunu iki katına çıkarmak yeterli olurken, açık anahtarlı sistemler yeni algoritmaların tasarlanmasına gereksinim duymaktadır. Bu bağlamda, kuantum bilgisayarlar yaygınlaşmadan önce, bilim insanları kuantum dayanıklı açık anahtarlı kriptosistemler geliştirmek üzerine çalışmalar yapmaya başlamıştır. Kuantum sonrası kriptografi olarak adlandırılan bu çalışma dalı hem normal hem de kuantum bilgisayarlarla yapılan saldırılara karşı güvenliği sağlayabilen açık anahtarlı kriptosistemler tasarlamayı hedefler. Kod tabanlı (*code-based*), özet tabanlı (*hash-based*), kafes tabanlı (*lattice-based*), çok değişkenli polinom tabanlı (*multivariate polynomial-based*) ve süpersingüler izojen tabanlı (*supersingular isogeny-based*) olmak üzere 5 ayrı kuantum sonrası kriptografi alanı üzerinde çalışmalar yürütülmektedir.

Yukarıda söz edilen kuantum dayanıklı kriptografi örneklerinden dördü boyutu büyük olan açık anahtarlar kullanmaktadır. Ancak süpersingüler izojen

tabanlı kriptografi aynı güvenlik seviyesi için en kısa açık anahtar boyutunu sunmaktadır. Eliptik eğriler tam da bu noktada devreye girmektedir. Süpersingüler izojen tabanlı kriptografi eliptik eğrilerden yararlanır. Bu kriptosistem, süpersingüler eliptik eğriler arasında izojen bulunması zorluğuna dayanmaktadır. Bu bölümde süpersingüler izojen tabanlı kriptosistemlerin çalışma yapısı özetlenecektir.

12.3.3.1. Eliptik Eğri İzojenleri

E, $\mathbb{F}_q$ sonlu cismi üzerine tanımlanan, karakteristiği $p > 3$ ($q = p^n, n \in \mathbb{Z}$) olan bir eliptik eğri,

$$E: y^2 = x^3 + ax + b$$

olsun. E'nin j-değişmezi,

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

olarak tanımlanır. $j \neq 0$ ve $j \neq 1728$ eşitsizliklerini sağlayan herhangi bir $j \in \mathbb{F}_q$ değeri için, j-değişmezi değeri j olan

$$E': y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}$$

eliptik eğrisi mevcuttur. E ve E' eliptik eğrileri $\mathbb{F}_q$ üzerinde ancak ve arasındaki izomorfizma dönüşümleri cebirsel kapanış (*algebraic closure*) $\mathbb{F}_q$ üzerinde, tersinir cebirsel dönüşümlerdir ve verimli olarak hesaplanabilirler.

E'nin n-burulma (n-*torsion*) grubu, $E[n]$ ile gösterilir ve $E[n]$, $nP = \mathcal{O}_E$ koşulunu sağlayan $P \in E(\overline{\mathbb{F}}_q)$ noktalar kümesinden oluşur. Karakteristiği p olan cisim üzerinde tanımlanan eliptik eğriler p-burulma gruplarının yapısı ile sınıflandırılabilir. $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ durumunu sağlayan eliptik eğrilere sıradan (*ordinary*) eliptik eğriler denirken, $1.[p] \simeq \mathcal{O}$ özelliğine sahip eliptik eğrilere ise süpersingüler eliptik eğriler denir. Bölüm 12.2.1'de anlatılan kriptografik sistemlerde eğriler sıradan eğrilerken bu bölümde anlatılacak olan kriptosistem süpersingüler eğriler üzerinde çalışmaktadır. Bu nedenle güvenlikleri farklı problemlerin zorluğuna dayanmaktadır.

E eğrisinden E' eğrisine tanımlanan izojen $\varphi: E \to E'$ birim elemanı koruyan, sabit olmayan bir morfizmadır. Bu izojenin derecesi, morfizmadaki derecesine eşittir. φ ayrılabilen (*seperable*) bir izojen ise $deg\varphi = \#ker(\varphi)$ eşitliği vardır. Eğer E ve E' arasında ayrılabilir bir izojen tanımlanabiliyorsa bu iki eğri birbirine izojeniktir. Ayrıca Tate'nin teoremi, iki eğrinin ancak $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ koşulu sağlandığında birbirne izojenik olabileceğini söyler. İzojen φ, Vélu'nun formülleriyle hesaplanır. Derecesi d olan bir izojen d-izojen olarak adlandırılır. d pürüzsüz (*smooth*) derecesine sahip olan tüm izojenler $\overline{\mathbb{F}}_q$ üzerinde $d = \prod_{i=1}^{m} l_i^{e_i}$ asal dereceli izojenlerin bileşkesi olarak hesaplanabilir [31]. Aşağıda eliptik eğri izojenlerine ait bazı özellikler sıralanmıştır.

- İzojen bir grup homomorfizmasıdır ve çekirdeği (*kernel*) ile tek (*unique*) olarak belirlenebilir.
- Verilen $G \subseteq E$ için tek bir eliptik eğri E_G ve tek, ayrılabilir ve $ker(\varphi_G) = G$ olan bir izojen $\varphi_G: E \to E_G \cong E/G$ bulunur.
- Verilen ℓ asalı için, her biri birbirinden farklı, ℓ-izojenleri tanımlayan, ℓ mertebeli (*order*) $\ell + 1$ tane devirli altgrup vardır.
- $\Phi_\ell(x, y) \in \mathbb{Z}[x, y]$, hem x hem y değerleri için, $\ell + 1$ dereceli simetrik modüler bir polinomdur ve $\Phi_\ell(j_1, j_2) = 0$ eşitliği ancak ve ancak j_i-değişmezli iki eliptik eğri arasında ℓ-izojen varsa gerçekleşir.
- Verilen bir j değeri için, $\Phi_\ell(x, j) = 0$ ortak değişkenli denkleminin kökleri, j ile ℓ-izojenik olan eliptik eğrilerin j-değişmezleridir.
- $\varphi: E \to E'$ olarak ifade edilen tüm ℓ-izojenler için, $\hat{\varphi} o \varphi = \varphi o \hat{\varphi} = [\ell]$ durumunu sağlayan tek bir dual ℓ-izojen $\hat{\varphi}: E' \to E$ vardır ve bu iki izojenin bileşkesi ℓ ile çarpımı verir.
- E'den kendisine tanımlanan izojen, *endomorfizma* olarak adlandırılır. E eğrisinin endomorfizmalarından oluşan ve 0-izojenini de içeren küme $End(E)$ ile gösterilir. $End(E)$, noktasal çarpım ve bileşke operatörleri altında halka yapısı oluşturur.

Daha önce de söz ettiğimiz üzere süpersingüler izojen tabanlı kriptografinin güvenliği ECC'de olduğu gibi eliptik eğri ayrık logaritma problemine dayanmamaktadır. Süpersingüler izojen tabanlı kriptografi aşağıda sıralanan problemlerin zorluğuna dayanmaktadır. Bu problemler ile ilgili daha detaylı bilgi için okuyucunun [32] ve [33] kaynaklarını incelemesi önerilmektedir.

- Endomorfizma Halka Problemi,
- Hesaba Dayalı Süpersingüler İzojen Problemi (CSSI),
- Hesaba Dayalı Süpersingüler Diffie–Hellman Problemi (SSCDH),
- Süpersingüler Diffie–Hellman Karar Problemi (SSDDH),
- Modifiye Edilmiş Hesaba Dayalı Süpersingüler İzojen Problemi (MCSSI),
- Modifiye Edilmiş Süpersingüler Diffie–Hellman Karar Problemi (MSSDDH).

12.3.3.2. Süpersingüler İzojen Tabanlı Kriptografi

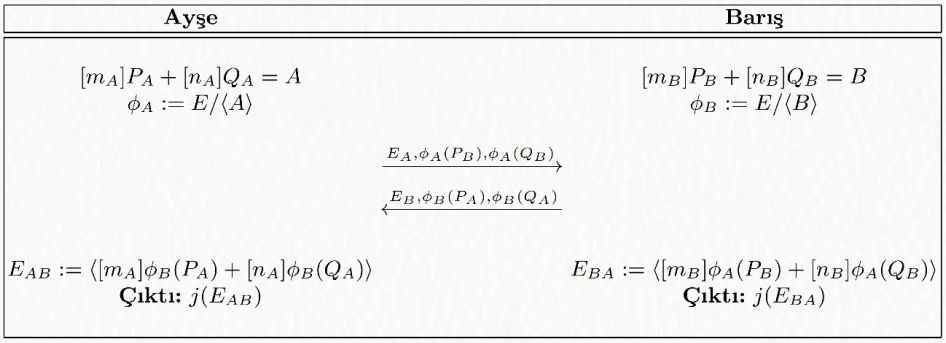
İlk kez 2006 yılında Rostovtev ve Stolbunov [34] izojen tabanlı kriptosistemleri tanıtmıştır. Bu çalışma, güvenliği sıradan eliptik eğriler arasında izojen bulma problemine dayanan açık anahtarlı bir kriptosistem sunmuştur. Klasik bilgisayarlarda yarı üstel zamanda kırılabilen bu kriptosistemlerin, kuantum bilgisayarlarda, sıradan eliptik eğrilerin endomorfizma halkalarının değişme özelliği nedeniyle, yarı üstel zamandan çok daha hızlı çözülebileceği [32]'deki referanslarda gösterilmiştir. Ardından, değişme özelliği olmayan endomorfizma halkalarına sahip olan süpersingüler eliptik eğriler arasındaki izojenlerin bulunması zorluğuna dayanan kriptosistemler 2011 yılında Jao ve De Feo [33] tarafından önerilmiştir. Kuantum bilgisayarlarda süpersingüler eliptik eğriler arasında izojenlerinin bulunması yarı üstel zamanlı bir işlemdir. Bu nedenle süpersingüler izojen tabanlı kriptografi kuantum dayanıklıdır.

- **Süpersingüler İzojen Diffie-Hellman Anahtar Değişimi *(SIDH)*:** [33]'te sunulan Süpersingüler İzojen Diffie-Hellman Anahtar Değişimi şu şekilde çalışmaktadır:

  Ayşe ve Barış'ın kuantum dayanıklı bir yöntemle ortak bir anahtar paylaşmak istediğini varsayalım.

- **Kurulum:** İlk olarak üzerinde çalışılacak asal sayı $p = \ell_A^{e_A}\ell_B^{e_B}f \pm 1$ oluşturulur. Burada, e_A ve e_B pozitif sayılar, ℓ_A ve ℓ_B 2, 3 gibi küçük asallar ve f, p sayısının asal olmasını sağlayacak küçük bir çarpandır. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlanan E eliptik eğrisiden (P_A, Q_A) ve (P_B, Q_B) noktaları seçilir.
- **Parametre üretimi:** Ayşe, ℓ_A ile bölünemeyen $m_A, n_A \in \mathbb{Z}$ şeklinde, rastgele iki sayı üretir. m_A, n_A ve (P_A, Q_A)'yı kullanarak $\phi_A: E \to E_A$ izojenini oluşturur. ϕ_A izojenini (P_B, Q_B) üzerinde hesaplayarak $\phi_A(P_B)$ ve $\phi_A(Q_B)$'yi hesaplar. Ayşe, elde ettiği E_A, $\phi_A(P_B)$ ve $\phi_A(Q_B)$'yi Barış'a gönderir. Benzer şekilde, Barış, ℓ_B ile bölünemeyen $m_B, n_B \in \mathbb{Z}$ şeklinde, rastgele iki sayı üretir. m_B, n_B ve (P_B, Q_B)'yi kullanarak $\phi_B: E \to E_B$ izojenini oluşturur. ϕ_B izojenini (P_A, Q_A) üzerinde hesaplayarak $\phi_B(P_A)$ ve $\phi_B(Q_A)$'yı hesaplar. Barış, elde ettiği E_B, $\phi_B(P_A)$ ve $\phi_B(Q_A)$'yı Ayşe'ye gönderir.
- **Anahtar hesaplama:** Ayşe, Barış'ın gönderdiği $\phi_B(P_A)$ ile m_A sayısını ve $\phi_B(Q_A)$ ile n_A sayısını çarpar ve bu çarpımları toplar. Elde ettiği toplam E_{AB} eğrisinin çekirdeğini oluşturur. Aynı şekilde Barış, Ayşe'nin gönderdiği $\phi_A(P_B)$ ile m_B sayısını ve $\phi_A(Q_B)$ ile n_B sayısını çarpar ve bu çarpımları toplar. Elde ettiği toplam E_{BA} eğrisinin çekirdeğini oluşturur. İşlemler sonucunda Ayşe'nin elde ettiği $1\,2_{AB}$ eğrisi ve Barış'ın elde ettiği E_{BA} eğrisi izomorftur. Bu nedenle bu eğrilerin j-değişmezleri birbiriyle aynıdır. Sonuç olarak, Ayşe ve Barış ortak anahtarı elde etmiş olur.

Şekil 12.4, süpersingüler izojen Diffie-Hellman anahtar değişim protokolünü özetlemektedir.



Şekil 12.4. Süpersingüler İzojen Diffie-Hellman Anahtar Değişimi

Güvenliği süpersingüler eliptik eğriler arasında izojen hesaplama zorluğuna dayanan bu protokol normal bilgisayarlarda $O\left(p^{\frac{1}{4}}\right)$ işlem, kuantum bilgisayarlarda ise $O\left(p^{\frac{1}{6}}\right)$ işlem gerektirmektedir.

SIDH protokolü için çeşitli performans arttırma çalışmaları yapılmaktadır. Örneğin, Costello, Longa ve Naehrig çalışmalarında [35], sonlu cisim aritmetiği, eliptik eğri aritmetiği ve izojen hesaplamalarında verimlileştirme yapmış ve SIDH için 128-bit kuantum güvenliği ve 256-bit klasik güvenlik elde etmiştir. Diğer yandan, zamanlama ve önbellek saldırılarını önlemek amacıyla protokolü sabit zamanda çalışan bir biçimde tasarlamışlardır. Bir diğer örnekte [36] ise verimli izojen hesaplamalarının yapılmasını sağlayan yeni asallar tanıtılmıştır. [37]'de ise yeni bir sonlu cisim gösterim yöntemi kullanılmıştır. Bu sonlu cisim gösterimi sayesinde verimli çarpma işlemleri elde edilmiş ve böylece performans artışı sağlanmıştır.

Güncel blokzincir gündemini yakından ilgilendiren önemli bir konu dijital imzalardır. Bölüm 12.5'te dijital imzalar ve blokzincir ilişkisi açıklanmıştır. Bu bölümde ise gelecekte blokzincir teknolojisinde yeni bir dönem açma potansiyeli barındıran kuantum sonrası dijital imza ve kimlik belirleme protokollerinden söz edilmiştir.

Birbirlerinden bağımsız olarak [38] ve [39]'da kuantum sonrası dijital imza protokolleri önerilmiştir. Bu protokoller [33]'te yer alan kimlik belirleme protokolünün sıfır bilgi ispatı (*zero-knowledge proof*) üzerine geliştirilmiştir. Taraflar arasında çalıştırılan protokoller etkileşimli (*interactive*) ve etkileşimsiz (*non-interactive*) olmak üzere iki farklı biçimde uygulanır. Etkileşimli proto-

kollerde mutabakat sağlanabilmesi için tarafların eşzamanlı olarak protokole katılım sağlaması gerekir. Etkileşimsiz protokollerde ise tarafların eşzamanlı katılım göstermesine gerek yoktur. Kuantum sonrası dijital imza protokolü öneren bu iki çalışma [33]'teki etkileşimli kimlik belirleme protokollerini etkileşimsiz hale getirerek dijital imza olarak kullanılmasını sağlamışlardır.

Kimlik belirleme protokolüne biraz daha yakından bakalım. Bu protokol kanıtlayan (*prover*) ve doğrulayan (*verifier*) olmak üzere iki taraf arasında etkileşimli olarak çalışır. Kanıtlayan taraf Pelin, doğrulayan taraf Veli olsun. Pelin, gizli bir bilgiye sahip olduğunu, o bilgi hakkında herhangi bir açık vermeden Veli'ye kanıtlamak ister. Pelin önce bir sayı belirler, Veli de Pelin'e zor bir matematiksel bilmece gönderir. Pelin belirlediği sayı, zorlu bilmece ve baştaki gizli bilgiyi kullanarak hesapladığı cevabı Veli'ye gönderir. Veli, Pelin'in cevabına göre gizli bilgiye sahip olup olmadığını tespit eder.

[33]'te önerilen süpersingüler izojen tabanlı sıfır-bilgi ispatı şu şekilde işler:

– Süpersingüler İzojen Tabanlı Sıfır-Bilgi İspatı: SIDH protokolünde olduğu gibi burada da işlemlerin üzerinde yürütüleceği asal sayı $p = \ell_A^{e_A}\ell_B^{e_B} f \pm 1$ olarak belirlenir. e_A ve e_B pozitif sayılar, ℓ_A ve ℓ_A 2,3 gibi küçük asallar ve f, p sayısının asal olmasını sağlayacak küçük bir çarpandır. $\mathbb{F}_{p^2}$ sonlu cismi üzerinde $\#E(\mathbb{F}_{p^2}) = \left(\ell_A^{e_A}\ell_B^{e_B} f\right)^2$ olacak şekilde (E eğrisinin kardinalitesi $\left(\ell_A^{e_A}\ell_B^{e_B} f\right)^2$ olacak şekilde) E eliptik eğrisi seçilir. Protokolde Pelin, devirli (*cyclic*) $\ell_A^{e_A}$ dereceli $\phi: E \rightarrow E/\langle S\rangle$ gizli izojenini ve açık bilgi olan E ve $E/\langle S\rangle$ eğrilerini bilmektedir. Pelin, Veli'ye gizli bilgi olan $\langle S\rangle$ üretecini bildiğini, açık vermeden kanıtlamak ister.

$\langle S\rangle$, $\ell_A^{e_A}$ dereceli gizli izojen ϕ'nin üreteci ve $\langle R\rangle$ de $\ell_B^{e_B}$ mertebeli devirli gruptur. Şekil 12.5. protokolün işleyişini gösterir.

$$\begin{array}{ccc} E & \xrightarrow{\ \phi\ } & E/\langle S\rangle \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi'} \\ E/\langle R\rangle & \xrightarrow{\ \phi'\ } & E/\langle S, R\rangle \end{array}$$

Şekil 12.5. Süpersingüler İzojen Tabanlı Sıfır-Bilgi İspatı

Pelin işlemleri şu sırayla yapar:

- Vélu'nun formüllerini kullanarak $\psi: E \to E/\langle R \rangle$ izojenini hesaplar.
- $R' = \phi(R)$'yi ve $\psi': E/\langle S \rangle \to E/\langle S, R \rangle$ izojenini hesaplar.
- $S' = \psi(S)$'yi ve $\phi': E/\langle R \rangle \to E/\langle S, R \rangle$ izojenini hesaplar.

$\mathbb{F}_{p^2}$ üzerinde tanımlanan süpersingüler eliptik eğri E ve $\phi: E \to E/\langle S \rangle$izojenini tanımlayan $\ell_A^{e_A}$-burulma noktası S, protokolün gizli parametreleridir. E ve $E/\langle S \rangle$ eğrileri, $E[\ell_B^{e_B}]$'nin üreteçleri *P, Q* ve bunların görüntü noktaları olan $\phi(P)$ ve $\phi(Q)$ ise açık parametrelerdir.

Kimlik belirleme protokolünün gerçekleşmesi için aşağıdaki adımlar sırasıyla m defa tekrar edilir.

Pelin rastgele olarak $\ell_B^{e_B}$-burulma noktası *R*'yi seçer ve Şekil 12.5'ü uygular.

1. Pelin $E_1 = E/\langle R \rangle$ ve $E_2 = E/\langle S, R \rangle$ eğrilerini Veli'ye gönderir.
2. Veli rastgele bir bit olan *b*'yi (0 ya da 1) seçer ve Pelin'e gönderir.
3. Eğer *b*=0 ise, Pelin $\phi(R')$ noktalarını açıklar. Veli bu noktaların mertebesi $\ell_B^{e_B}$ ise ve R ve $\phi(R')$ noktaları, sırasıyla $E \to E_1$ ve $E/\langle S \rangle \to E_2$ izojenlerinin çekirdekleri ise Pelin'in yanıtını kabul eder.
4. Eğer $b = 1$ ise, Pelin $\psi(S)$ noktasını açıklar. Veli bu noktanın mertebesi $\ell_A^{e_A}$ ise ve bu nokta $E_1 \to E_2$ izojeninin çekirdeği ise Pelin'in yanıtını kabul eder.

Bu işlemlerin m defa yapılmasının sebebi hile yapılma olasılığını ortadan kaldırmaktır. Her bir adımda Pelin'in dürüst olmaması durumunda rastgele olarak doğru yanıt gönderme olasılığı %50'dir. Bu nedenle bu işlemler defalarca tekrarlanarak kimlik doğrulama işlemi gerçekleştirilir. Bu protokole Fiat-Shamir dönüşümü [40] uygulandığında ise süpersingüler izojen tabanlı sayısal imza protokolü oluşturulur. Böylece protokol etkileşimsiz hale gelir.

Süpersingüler izojeni tabanlı imza protokolleri diğer kuantum sonrası imza protokollerine kıyasla daha büyük boyutlu imzalar üretmektedir, buna karşın

kullandıkları anahtar boyutları diğerlerinden daha küçüktür. Bu nedenle performans ve imza boyutu açısından gerekli iyileştirmeler yapılması durumunda rakiplerine göre daha çok tercih edilmesi mümkündür.

Süpersingüler izojeni tabanlı imza protokolleri diğer kuantum sonrası imza protokollerine kıyasla daha büyük boyutlu imzalar üretmektedir, buna karşın kullandıkları anahtar boyutları diğerlerinden daha küçüktür. Bu nedenle performans ve imza boyutu açısından gerekli iyileştirmeler yapılması durumunda rakiplerine göre daha çok tercih edilmesi mümkündür.

12.4. ELİPTİK EĞRİLERİN UYGULAMALARI

İnternete bağlı her cihaz gerekli önlemler alınmadığı takdirde birçok güvenlik tehdidi ile karşı karşıyadır. Yaşamlarımızın vazgeçilmez birer parçası haline gelen bilgisayarlar, akıllı telefonlar, tabletler, akıllı cihazlar, çevrimiçi uygulamalar, hayatlarımızı kolaylaştıran nesnelerin interneti ve daha birçoğu bu tip siber tehditlerden korunmak üzere çeşitli yöntemler kullanmaktadır. Bu yöntemlerin belki de en önemlisi güvenli kriptografik protokollerin tercih edilmesidir. Eliptik eğri kriptosistemler sağladığı güvenlik seviyesi ve diğer açık anahtarlı kriptosistemlere göre daha verimli olması nedenleriyle bu tip çevrimiçi altyapıların güvenliğinin sağlanmasında sıklıkla kullanılır. Bu bölümde eliptik eğri kriptosistemlerden yararlanan taşıma katmanı güvenliği protokolü ve uçtan uca şifreleme alt başlıklarıyla haberleşme güvenliği (Bölüm 12.4.1) ve nesnelerin interneti güvenliği (Bölüm 12.4.2) konuları açıklanmıştır.

12.4.1. Haberleşme Güvenliği

Günümüzde iletişim büyük çoğunlukla internet ortamında gerçekleştirilir. İnsanlar kişisel bilgilerini, kurumlar hassas verilerini internet üzerinden çalışan protokoller aracılığıyla birbirlerine göndermektedir. Fakat kullandığımız internet, milyarlarca insanın kullanımına açık, herkesin gözlemleyebildiği bir protokol kullanarak veri iletimi hizmeti sunmaktadır. Bu durum da iletilen verinin kötü niyetli kullanıcılar tarafından elde edilmesi ve kullanılması gibi

tehditler oluşturur. Bu tip saldırılardan korunmak amacıyla kullanılan protokollerin en gözde araçlarından biri de eliptik eğri kriptografidir. Sağladığı güvenlik seviyesi ve küçük anahtar boyutları sayesinde güncel olarak kullanılan birçok haberleşme uygulamasında anahtar değişimi, imza protokolleri, kimlik belirleme, kimlik doğrulama amaçlarıyla diğer açık anahtarlı rakiplerine göre daha çok tercih edilir duruma gelmiştir. Bu bölümde, günlük olarak en çok tercih edilen internet haberleşmelerinde kullanılan TLS ve anlık mesajlaşma uygulamalarında uygulanan Signal protokolleri incelenmiştir. Her iki protokol de güvenliğin sağlanması için eliptik eğri kriptografi protokollerinden yararlanmaktadır.

12.4.1.1. Taşıma Katmanı Güvenliği

Taşıma katmanı güvenliği (*Transport Layer Security – TLS*), bankacılık, çevrimiçi ödemeler gibi finansal işlemler, e-ticaret, sağlık verilerinin güvenli bir şekilde saklanması ve iletilmesi, e-posta ve sosyal medya gibi birçok alanda çevrimiçi güvenliği sağlamak için kullanılan protokollerden oluşur.

Hassas ve değerli veri iletimi ya da saklama işlemleri sunan her ağ servisinin bu verinin güvenliğini düzgün bir biçimde sağlaması gerekir. TLS, sunucu ve istemci (*client*) arasında veri transferinin yapılması için korumalı bir kanal oluşturur. TLS, güvenilir bir taşıma protokolünün (genellikle İletim Kontrol Protokolü (*Transmission Control Protocol – TCP*) üzerinde çalışan, katmanlı bir protokoldür. HTTP (*Hypertext Transfer Protocol*) ve IMAP (*Internet Message Access Protocol*) gibi uygulama protokolleri TLS altında çalışabilir. Yani, TLS, ağ üzerinden veri aktarımı yapan uygulamalarda güvenliği sağlayan ve uygulama bağımsız çalışan bir protokoldür [41].

Bir internet uygulaması TLS olmadan da çalışabilir. Bu nedenle istemcinin sunucuya TLS bağlantısı için kurulum belirtmesi gerekir. Bunun için genellikle, bağlantı noktası (*port*) numaraları kullanılır. Örneğin 80 bağlantı noktası numarası şifresiz HTTP trafiği için, 443 bağlantı noktası numarası ise şifreli HTTPS trafiği için kullanılır. İstemci ve sunucu TLS kullanacakları zaman uzlaşma prosedürü (*handshaking procedure*) uygulayarak durum bilgisi olan bir bağlantı üzerinde uzlaşırlar. Bu uzlaşma protokolü, şifreleme

ayarlarını belirlemenin yanı sıra oturum-özel (*session-specific*) ortak anahtar belirlemek amacıyla asimetrik şifreleme kullanır. Ardından, iletilecek verinin şifrelemesi belirlenen anahtarlarla simetrik kriptosistemler kullanılarak yapılır.

Güvenli Soket Katmanı (*Secure Socket Layer – SSL*) protokolü Netscape tarafından istemci ve sunucu arasında yapılan işlemlerin güvenliğini sağlamak amacıyla geliştirilmiştir. Protokolün ilk versiyonu olan SSL 1.0 hiç kullanılmamış, SSL 2.0 yayınlanmış ancak SSL 3.0 yayınlandığında SSL 2.0'da güvenlik açıkları olduğu anlaşılmıştır. TLS 1.0, İnternet Mühendisliği Görev Kuvveti *(Internet Engineering Task Force – IETF)* tarafından geliştirilmiştir. TLS protokolünün ilk versiyonu, SSL 3.0'a dayanan bir protokoldür [42], bu nedenle aralarında çok önemli bir fark bulunmaz. TLS 1.0'da bulunan başlangıç vektörü seçimi ve dolgulama (*padding*) hataları TLS 1.1'de düzeltilmiştir. Doğrulanabilir şifreleme, özet fonksiyonları gibi kriptografik genişletmeler TLS 1.2'de yayınlanmıştır. Son olarak 2018 yılında, uzlaşma protokolü ve anahtar üretim işlemi güncellenmiş olan TLS 1.3'e geçilmiştir.

TLS protokolü oturum bağlantılarını kontrol etmek adına uzlaşma, şifre özelliklerini değiştirme ve uyarı olmak üzere üç alt protokolden oluşur. Uzlaşma protokolü daha önce de söz edildiği gibi oturum parametrelerinin belirlenmesi ve bu parametreler üzerinde uzlaşılması işlemini sağlar. Şifre özelliklerini değiştirme protokolü kriptografik parametrelerin güncellenmesi için kullanılır. Bu alt protokol TLS 1.0, 1.1 ve 1.2'de kullanılır. Uyarı protokolü ise bir hata oluşması durumunda tarafları hatadan haberdar etme işlemini gerçekleştirir.

TLS sunucusu, bir veya daha fazla ortak anahtar sertifikası ve bağlantılı özel anahtarlarla yapılandırılır. TLS sunucu uygulamaları, algoritma ve anahtar boyutu çevikliğini desteklemek için bağlantılı özel anahtarlarla birden çok sunucu sertifikasının kullanımını desteklemelidir. NIST tarafından onaylanan sertifikalar şu şekildedir [43]:

- RSA imza sertifikası,
- Eliptik Eğri Dijital İmza Algoritması (ECDSA) imza sertifikası,
- Dijital İmza Algoritması (DSA) imza sertifikası,

- Diffie-Hellman (DH) sertifikası,
- Eliptik Eğri Diffie-Hellman (ECDH) sertifikası.

Sunucu bir ECDSA imza sertifikası ile yapılandırılmışsa, sertifikadaki ortak anahtar için eğri *P-256* ya da eğri *P-384* kullanılmalıdır [43]. RSA, ECDSA veya DSA ortak anahtarlarını içeren sertifikalar sırasıyla aynı imza algoritmalarıyla imzalanmalıdır. Diffie-Hellman ortak anahtarlarını içeren sertifikalar DSA ile imzalanmalıdır ve ECDH ortak anahtarlarını içeren sertifikalar ECDSA ile imzalanmalıdır.

12.4.1.2. Uçtan Uca Şifreleme

Son yıllarda anlık mesajlaşma uygulamaları, mobil cihazların kullanımının artmasıyla beraber yaşantılarımızda vazgeçilemeyecek bir konuma ulaşmıştır. Yediden yetmişe her yaş aralığındaki insanlar günlük konuşmalarını, toplantılarını bu platformlar üzerinden yapmaktadır. Bu platformlar üzerinden belge, resim, video paylaşılmakta ve kişisel ya da hassas öneme sahip veriler bu uygulamalar aracılığıyla insanlar arasında iletilmektedir. Fakat bu gibi uygulamaları kullanan herkesin bu tip verilerinin güvenliğinden yana endişesi olduğu aşikardır. Büyük tartışmalara sebep olsa da Whatsapp gibi uygulamalar, iletilen verilerin uçtan uca şifrelendiğini ve kullanıcıların verilerinin güvende olduğunu iddia etmektedir. Fakat burada asıl tartışılan konu iletilen mesajların üçüncü kişiler tarafından değil bu hizmetleri sağlayan şirketler tarafından kullanılıyor olması ihtimalidir.

Endişe duyulan tüm bu kişisel verilerin korunması ile ilgili konular gündemden hiç düşmeyecek olsa da, bu tip uygulamaları hayatlarımızdan çıkarmamız da pek olası görünmüyor. O nedenle bu tip sistemlerin arka planında çalışan güvenlik mekanizmalarını biraz daha detaylı bilmek fayda sağlayabilir. Bu kapsamda, en çok tercih edilen anlık mesajlaşma uygulamalarından biri olan biri olan Whatsapp örneğini ele alalım.

Whatsapp uçtan uca şifreleme yaparak çalışan, Signal protokolünü kullanan bir anlık mesajlaşma uygulamasıdır [44]. Açık anahtarlar ve oturum anahtarları olmak üzere iki çeşit anahtar sistemi kullanır.

Açık anahtar türleri:

- Kimlik anahtar çifti: Yükleme sırasında, *Curve25519* ile üretilen uzun kullanım zamanlı anahtar çiftidir.
- İmzalı ön anahtar: Bir önceki adımda oluşturulan kimlik anahtarı ile imzalanan orta zaman kullanımlı *Curve25519* anahtar çiftidir.
- Bir defalık ön anahtarlar: Yükleme anında oluşturulan ve gereksinim duyulduğunda yeniden oluşturulabilen *Curve25519* anahtarlar listesidir.

Oturum anahtarı türleri:

- Kök anahtar: Zincir anahtarları üretmek için kullanılan 32-baytlık bir değerdir.
- Zincir anahtar: Mesaj anahtarını oluşturmak için kullanılan 32-baytlık bir değerdir.
- Mesaj anahtarı: Mesajları şifrelemek için kullanılan 80-baytlık bir değerdir. Bu değerin 32-baytı AES-256 anahtarı olarak, 32-baytı HMAC-SHA256 anahtarı olarak ve 16-baytı başlatma vektörü olarak kullanılır.

Kullanıcılar sisteme kaydolurken, Whatsapp istemcisi açık kimlik anahtarını, imzalı ön anahtarı ve bir miktar bir defalık ön anahtarları Whatsapp sunucusuna gönderir ve sunucu bu anahtarları kullanıcının kimliği ile ilişkili bir şekilde depolar. Kayıt işlemi tamamlandıktan sonra bir kullanıcı başka bir kullanıcı ile mesajlaşmak için şifreli bir oturum başlatır.

Başka bir kullanıcı ile mesajlaşmak isteyen bir kullanıcı, Tablo 12.3'de verilen şifreli oturum başlatma işlemini uygular. Oturum sağlandıktan sonra, kullanıcıların uygulamayı yeniden yüklemesi veya cihaz değişikliği gibi durumlar gerçekleşmediği sürece istemcilerin birbirleri arasında yeni bir oturum oluşturmaları gerekmez. Uzun süreli bir şifreleme oturumu oluşturduktan sonra, alıcı çevrimdışı olsa bile oturumu başlatan istemci, alıcıya hemen mesaj göndermeye başlayabilir. Alıcı yanıt verene kadar başlatıcı, alıcının karşılık gelen bir oturum oluşturmak için ihtiyaç duyduğu bilgileri (gönderilen tüm iletilerin başlığında) içerir. Bu, başlatan istemcinin $E_{initiator}$ ve $I_{initiator}$ bilgilerini içerir.

Tablo 12.3. Signal Protokolü

Şifreli oturum başlatma: - Oturumu başlatan istemci, alıcı için açık kimlik anahtarı, açık imzalı ön anahtar ve bir adet ortak ön anahtar ister. Bu ön anahtar bir açık anahtardır ve bir defalığına kullanılabilir. - Sunucu, istenen ortak anahtar değerlerini döndürür. Bir defalık ön anahtar yalnızca bir kez kullanılır, bu nedenle istendikten sonra sunucu deposundan kaldırılır. - Başlatan istemci, alıcının kimlik anahtarını $I_{recipient}$ olarak, imzalı ön $S_{recipient}$ olarak ve bir defalık ön anahtarı $O_{recipient}$ olarak kaydeder. - Başlatan istemci, geçici (*ephemeral*) bir *Curve25519* anahtar çifti oluşturur, bu anahtar çifti olarak adlandırlır. - Başlatan istemci, başlatıcı olarak kendi kimlik anahtarını yükler. - Başlatan istemci, ana sırrı (*master secret*) hesaplar: $master\_secret = ECDH(I_{initiator}, S_{recipient}) \|\|ECDH(E_{initiator}, I_{recipient})\|\| ECDH(E_{initiator}, E_{recipient})\|\|ECDH(O_{initiator}, S_{recipient})$ - Başlatan istemci, ana sırdan bir kök anahtar ve zincir anahtarları oluşturmak için özet anahtar üretim fonksiyonunu (*hash-based key derivation function – HKDF*) kullanır.
Oturum kurulumunun alınması: - Alıcı, kendi gizli anahtarlarını ve gelen mesajın başlığında tanıtılan açık anahtarları kullanarak karşılık gelen ana sırrı hesaplar. - Alıcı, başlatan istemci tarafından kullanılan bir defalık ön anahtarı siler. - Başlatıcı, ana sırra karşılık gelen bir kök anahtar ve zincir anahtarları türetmek için HKDF'yi kullanır.

Bir oturum kurulduktan sonra istemciler, şifreleme için CBC modunda AES-256 ve kimlik doğrulama için HMAC-SHA-256 özet fonksiyonunu kullanarak bir ileti anahtarı ile korunan iletileri birbirlerine gönderir. İletilen her

mesajda yeni bir mesaj anahtarı kullanılır ve bir mesajı şifrelemek için kullanılan mesaj anahtarı, bir mesaj iletildikten veya alındıktan sonra oturumdan çıkarım yapılarak yeniden üretilemez.

Mesaj anahtarı, göndericinin gönderilen her mesajla birlikte "mandallanan" (*rachet*) zincir anahtarından türetilir. Ayrıca her mesaj gidiş-dönüşü için yeni bir ECDH anlaşması sağlanır. Bu yöntemlerin kullanılması ileriye dönük güvenlik (*forward secrecy*) sağlar [44].

12.4.2. Nesnelerin İnterneti Güvenliği

Nesnelerin interneti (*Internet of Things – IoT*), sensörler, yazılımlar, internet bağlantısı gibi yapıların gömülü olduğu cihazların ve sistemlerin interneti kullanarak birbirleriyle sürekli iletişim kurabildikleri bir teknolojidir. Günümüzde akıllı şehirler, akıllı evler, hastaneler, endüstri (*Industrial Internet of Things – IIoT*), çevre izleme, yangın önleme vb. birçok alanda kullanılmaktadır. Hayatı oldukça kolaylaştıran ve kullanım alanı bu kadar geniş olan bu teknolojide siber tehditler ortaya çıktığı için güvenliğini sağlamak önem kazanmıştır. Şekil 12.6'da nesnelerin internetinin kullanıldığı bazı alan gösterilmiştir.

Şekil 12.6. Nesnelerin internetinin kullanıldığı bazı alanlar

Hali hazırda kullanılan IoT cihazlarının genellikle zayıf bir şekilde korunduğu kabul edilmekle birlikte, 5G haberleşmenin de ortaya çıkmasıyla IoT kullanımının daha da artması beklenmektedir. Bu durumda, zayıf korumanın güçlendirilmesi için bu küçük IoT cihazlarına güncel ve güvenilir kriptografik korumaların yerleştirilmesi gerekmektedir. Ancak uygulama geliştiriciler bunu zor bulmaktadırlar. Eliptik eğri kriptografi, daha az hafıza, enerji ve hesaplama kullandığı için bu noktada büyük önem taşımaktadır [45]. Eliptik eğri kriptografi, nesnelerin internetinde kimlik doğrulama, anahtar değişimi gibi protokollerde kullanılır.

ECC, RSA'da kullanılan üst alma işlemini, iki kat al-ve-topla işlemine uyarlayarak daha verimli hale getirir. Tablo 12.2.1'den de görülebileceği gibi RSA açık anahtarlı kriptosistemin 1024-bit anahtar boyutuyla sağladığı güvenlik seviyesini ECC 160 bitlik anahtar ile sağlamaktadır. Bu nedenle, ECC akıllı kartlar (*smart cards*), mobil cihazlar gibi kaynak kısıtlı cihazlar (*resource constraint devices*) için çok kullanışlıdır [46].

Nesnelerin internetinde genellikle NIST standartlarındaki eğriler [23], *Secp256r1* [23], Montgomery *Ed25519* [27] ve Edwards *Curve25519* [27] eğrileri kullanılır. [47]'de, ECDSA ve RSA'yı kullanan TLS kimlik doğrulama algoritmalarının enerji tüketimi ve veri kullanımları ölçülmüştür. ECDSA kaynak kısıtlı IoT cihazların güvenliğini sağlama konusunda RSA'dan daha iyi sonuç vermiştir. [45]'te, IoT cihazlarda kullanılan 32-bit işlemcilerde eliptik eğri protokollerini çalıştırırken yüksek-seviye diller olan C ya da C++ yerine assembly dilini kullanmıştır. Bu sayede eliptik eğri protokollerin performansları assembly dili kullanılarak hızlandırılmıştır.

12.5. BLOKZİNCİRDE ELİPTİK EĞRİLERİN KULLANILMASI

Blokzincir, Satoshi Nakamoto (kimliği bilinmeyen bir kişi ya da topluluk) tarafından, 2008 yılında, Bitcoin adı verilen elektronik nakit sistemine ait, herkese açık bir işlem kayıt defteri (*public transaction ledger*) olarak kullanılması amacıyla önerildi [48]. En önemli özelliği merkezi bir otoriteye gereksinim duymadan çift harcama problemini ortadan kaldırmayı hedeflemek olan Bitcoin her ne kadar bir elektronik nakit olarak sunulsa da kullanılan blokzincir yapısı birçok farklı alanda merkezi otorite ihtiyacını

ortadan kaldırarak güvenli bir sistem sağlar. Finanstan sağlık hizmetlerine, resmi işlemlerden hukuki verilerin işlenmesine kadar neredeyse her alanda kullanılabilen, tüm sektörlerin işleyiş biçimini kökten değiştirebilecek bir teknolojidir.

Bu bölümde blokzincir ve eliptik eğrilerin blokzincirde kullanımı anlatılmıştır. Bölüm 12.5.1'de blokzincire dair temel kavramlar, Bölüm 12.5.2'de kimlik doğrulama, Bölüm 12.5.3'te blokzincirde güvenlik ve Bölüm 12.5.4'te mahremiyet konuları açıklanmıştır.

12.5.1. Blokzincir

Elektronik nakit ya da sayısal para kavramları Bitcoin ile yaşantılarımıza girmiş gibi görünse de aslında bu kavramların tarihi daha öncelere dayanmaktadır. David Chaum'un 1983'te önerdiği [49] blokzincir benzeri model aslında elektronik nakit kavramının temelidir. Bitcoin, diğer kripto para birimleri ve blokzincir teknolojisini anlamak için e-nakit (*elektronik nakit*) kavramını anlamak büyük önem taşır. E-nakit sistemlerinde bulunan iki temel sorun blokzincirde de karşımıza çıkmaktadır. Bu sorunlardan biri kullanıcıların kimliğinin gizliliğini korumayı hedefleyen anonimliktir. Fiziksel nakitte de olduğu gibi harcamaları parayı gerçekten ödeyen kişiye kadar takip etmek neredeyse imkansızdır. Nakdin yalnızca bir kez harcanabilmesini (*çift harcama sorunu*) ve yalnızca gerçek sahibi tarafından harcanabilmesini sağlamak için ise hesap verebilirlik gerekir. Aynı para iki kez harcanabildiğinde çift harcama sorunu ortaya çıkar. Dijital verilerin kopyalarını çıkarmak oldukça kolay olduğu için, aynı dijital paradan birçok kopya oluşturmak mümkündür, bu da dijital para birimlerinde büyük bir sorun yaratmaktadır. David Chaum, 1980'lerdeki çalışmaları sırasında, kör imzalar (*blind signatures*) ve gizli paylaşım (*secret sharing*) olmak üzere iki şifreleme işlemi kullanarak bu sorunların her ikisine de çözüm önermiştir.

Bitcoin aslında bir e-nakit sistemi olarak ortaya çıkmıştır. Kripto para terimi ise sonradan yaşamımıza girmiştir [50]. Bitcoin ile birlikte ilk kez güvenilir olmayan bir ağda dağıtık fikir birliği (*distributed consensus*) sorunu çözüldü. İş kanıtı (*proof of work – PoW*) mekanizmasıyla ortak anahtar şifrelemesi kullanılarak güvenli, merkezi olmayan fakat kontrollü bir sayısal para basma yöntemi önerildi.

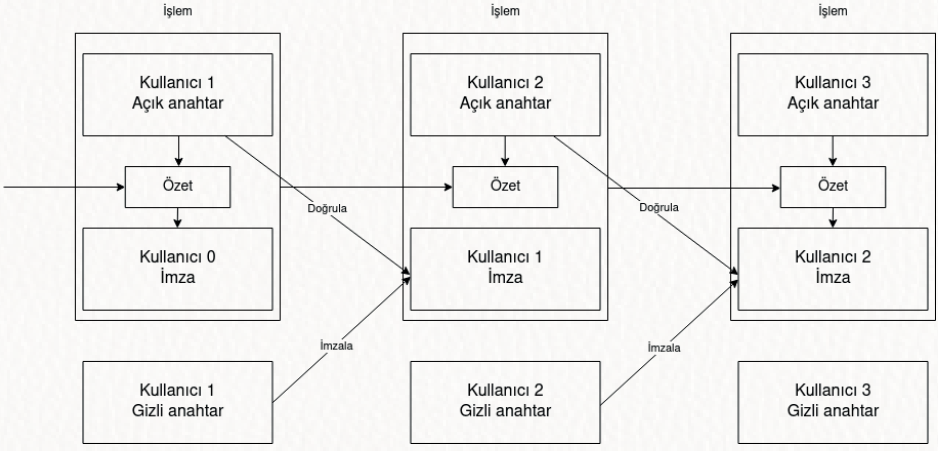
Blokzincir mekanizmasını biraz daha yakından inceleyebilmek için bazı terimlere göz atalım.

- Bir sistemin kötüye kullanıma karşı kriptografi yöntemleriyle güvenli hale getirilmiş olması bu sistemin **kriptografik olarak güvenli** olduğu anlamına gelir. Eğer bir sistem kriptografik yöntemler sayesinde reddedilememe (*non-repudiation*), veri bütünlüğü (*integrity*) ve veri merkezi doğrulanması (*data origin authentication*) özelliklerini karşılıyorsa bu sistem kriptografik olarak güvenlidir.
- Bir sistemde yeni veri yalnızca sondan eklenebiliyorsa bu sisteme **sondan eklemeli sistem** denir. Yani bir blokzincirde veri yalnızca verinin geldiği zamanın önceliğine göre zincire eklenir. Daha sonra gelen bir veri zincirde daha önce gelen bir verinin öncesine eklenemez. Bu durum zincirdeki verinin pratikte değiştirilemez olmasını sağlar.
- Merkezi bir denetleyici olmadan tüm katılımcıların doğrudan birbirleriyle iletişim kurabildiği ağlar **eşler arası ağlar** (*peer-to-peer networks*) olarak tanımlanır. Örneğin, eşler arası ağda katılımcılar arasındaki para aktarımı sırasında banka gibi üçüncü bir katılımcının yani denetleyicinin olmasına gereksinim yoktur.
- Blokzincire ait tüm işlemleri tutan bir kayıt defterine ağdaki tüm katılımcılar sahiptir. Bu kayıt defterine **dağıtık kayıt defteri** (*distributed ledger*) adı verilir.
- Bir **blok**, yalnızca bir araya getirilmiş ve mantıksal olarak organize edilmiş işlemlerden oluşur. Burada söz edilen işlem, ağdaki iki kullanıcı arasında yapılan para transferi olarak görülebilir. Bu işlemlerin bir araya getirilmesiyle oluşan blokların büyüklüğü blokzincirin tasarımına göre değişiklik gösterebilir. Her blok kendisinden önceki blokun referansını içerir. Yalnızca **genesis blok** adı verilen, blokzincir oluşturulurken sabit olarak kodlanmış, blokzincirin ilk blokunda bu referans bulunmaz.
- **Nonce** birçok kriptografik protokolde kullanılan, oluşturulduktan sonra yalnızca bir defa kullanılan bir sayıdır. Blokzincirde yapılan bir iş-

lemin bir kez daha yapılmasını engellemek ve fikir birliği oluşturma amaçlarıyla kullanılır.

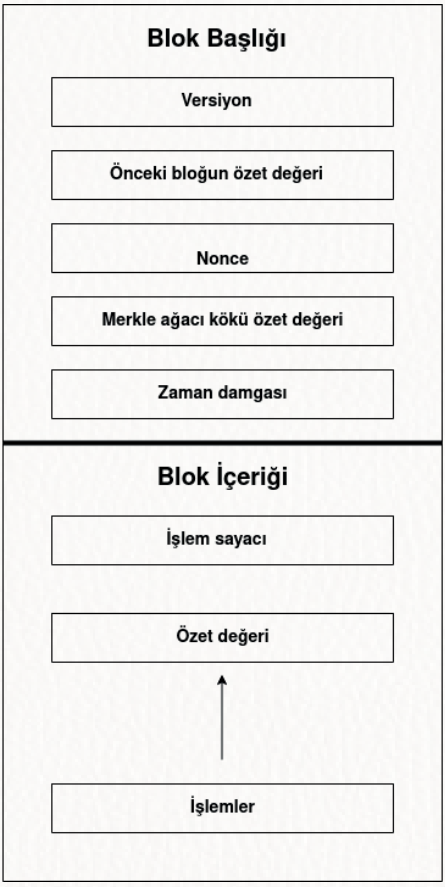
- **Merkle ağaçları** büyük veri yapılarını güvenli ve verimli bir şekilde doğrulamak için yaygın olarak kullanılmaktadır. Merkle ağacı düğümler, yapraklar ve Merkle ağacı kökünden oluşur. Her bir yaprak ilgili verinin özet değerini (*hash value*) tutar. Yaprakların üzerindeki elemanlar yani düğümler kendilerine bağlı olan yaprak elemanlarının birbirine eklenmiş hallerinin özet değerini tutar. En tepede bulunan kök ise tüm ağacın özet bilgisini tutar. Blokzincir dünyasında, Merkle ağaçları, işlemlerin verimli bir şekilde doğrulanmasına izin vermek için yaygın olarak kullanılır. Bir blokzincirdeki Merkle kökü, bir bloktaki tüm işlemlerin özet değeri olan bir blokun blok başlığı bölümünde bulunur. Bu, tüm işlemleri tek tek doğrulamak yerine, Merkle ağacında bulunan tüm işlemleri doğrulamak için yalnızca Merkle kökünün doğrulanması gerektiği anlamına gelir.

Blokzincirde işlemlerin nasıl oluşturulduğu Şekil 12.7'de gösterilmiştir.



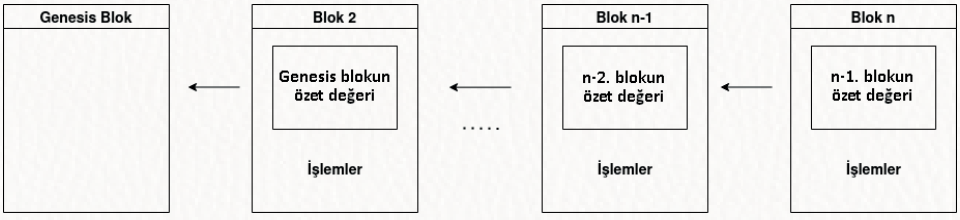
Şekil 12.7. Blokzincirde işlemlerin oluşturulması [48]

Şekil 12.8'de blokzincirde yer alan bir blokun yapısı gösterilmiştir.



Şekil 12.8. Blok yapısı [51]

Şekil 12.9'da ise Şekil 12.8'deki blokların bir araya gelmesiyle oluşan bir blokzincir gösterilmiştir.



Şekil 12.9. Blokzincir [51]

Blokzincirin temel elemanı olan bir blok, blok başlığı ve blok içeriği olmak üzere iki bölümden oluşur. Şekil 12.8'de gösterildiği gibi blok başlığı blok versiyonunu, bir önceki blokun özet değerini, nonce sayısını, Merkle ağaç kökü özet değerini ve zaman damgasını içerir [51]. Blok içeriğinde ise işlemler ve işlem sayacı bulunur. Bloka her bir işlem eklenmesinde bloka ait özet değerinin güncellenmesi gerekir.

[48] makalesinde üzerinde durulan konu, güven yerine kriptografik kanıtlara dayalı bir elektronik ödeme sistemi oluşturmaktır. Bu sistem herhangi iki tarafın güvenilir bir üçüncü tarafa ihtiyaç duymadan doğrudan birbirleriyle işlem yapmasına izin verir. Hesaplama açısından tersine çevrilmesi güç olan işlemler kullanarak ağdaki kullanıcıları dolandırıcılık durumlarından korumayı hedefler. Eşler arası dağıtık bir zaman damgası sunucusu sayesinde, yapılan işlemlerin kronolojik sırasının hesaplamalı kanıtını oluşturarak çift harcama problemi ortadan kalkar. Sistemin güvenliği, kötü niyetli grupların bir araya gelerek dürüst düğümlerin oluşturduğu zincirden daha uzun bir zincir üretememesine dayanır. Yani saldırgan grupların kullandıkları işlemci gücünün daha az olması gereklidir. Saldırganların oluşturduğu zincirin daha uzun olma olasılığı durumu güvensiz kılar mı sorusunun yanıtı bu makalede sunulan sistem biraz daha yakından incelenerek bulunabilir.

12.5.2. Kimlik Doğrulama

Veride yapılan yetkisiz değişiklikleri tespit etmek ve imzacının kimliğini doğrulamak için sayısal imzalar kullanılır. Sayısal imzalar özet fonksiyonları ve ortak anahtar şifrelemelerinden oluşan bir kombinasyon kullanır. Gönderilecek mesaj ilk olarak özet fonksiyonuna sokulur ve mesaja dair özet değeri elde edilir. Mesajın özet değeri imzacının gizli anahtarıyla şifrelenir ve imza oluşturulur. İmzanın doğruluğunu kontrol etmek isteyen kullanıcılar imzacının açık anahtarı ile doğrulamayı yapar.

Secp256k1 [52] olarak bilinen, Standards for Efficient Cryptography (*SEC*)'de tanımlanmış olan eliptik eğri parametre sistemi, Bitcoin gibi birçok blokzincir sisteminde eliptik eğri sayısal imza algoritmasında kullanılmaktadır. *Secp256k1* parametresi Bitcoin öncesinde yaygın olarak kullanılan bir standart değildi. Eliptik eğri kriptosistemlerde rastgele olarak oluşturulan eğriler güvenlik açısından daha çok tercih edilir. Ancak *Secp256k1* parametresinin sağladığı bazı özellikler sayesinde blokzincir uygulamaları çok daha verimli hale gelmektedir [53].

Bitcoin ve diğer birçok kripto para biriminde kripto para değerlerinin aktarımı açık anahtar, gizli anahtar ve adresler aracılığıyla sağlanır. Açık ve gizli anahtarların üretimi ECDSA kullanılarak yapılır. Gizli anahtar, işlemlerin kime ait olduğunu kanıtlamak amacıyla işlemlerin sayısal olarak imzalanmasını sağlar. Açık anahtar ise sayısal olarak imzalanmış bir işlemin ilgili kullanıcının gizli anahtarıyla imzalandığını doğrulama işinde kullanılır.

Bu tip sistemlerde kullanılan gizli anahtarlar genelde *Secp256k1 ECDSA* eğri önerilerindeki aralıkta belirlenen, 256-bit uzunluğundaki rastgele sayılardır. 16'lık tabanda gösterilen, 0x1 ile 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF BAAE DCE6 AF48 A03B BFD2 5E8C D036 4140 arasındaki tüm sayılar geçerli birer gizli anahtar olarak sayılır [50].

Ancak bu anahtarlar işlemlerin ve iletişimin daha verimli olması amacıyla sıkıştırılarak daha küçük boyutlu anahtarlar elde edilir.

Açık anahtar, matematiksel olarak gizli anahtar ile ilişkilidir. Anahtar çifti üretildikten sonra, açık anahtar ağ üzerinden herkesin ulaşabileceği biçimde yayınlanır. İlgili gizli anahtar ile imzalanmış bir işlemi, diğer kullanıcılar daha önce ellerine ulaşan açık anahtar ile doğrularlar. Açık anahtar boyutu gizli anahtarda olduğu gibi 256 bitlik bir uzunluğa sahiptir. Açık anahtar imza sisteminde kullanılan eğri üzerinde bir noktanın *x* ve *y* koordinatlarından oluşur. Her iki koordinat da 32-bayt uzunluğundadır. Açık anahtarın sıkıştırma işlemi için karşı tarafa yalnızca *x* koordinatı gönderilir. Çünkü, *x* koordinatı ile eğri denklemi üzerinden *y* koordinatı kolaylıkla elde edilebilir. Toplamda elde edilen açık anahtar boyutu sıkıştırılmış sistemde 32-bayttır [50].

Bitcoin'de adres oluşturulurken, açık ve gizli anahtarların birleşiminin önce SHA-256 ardından da RIPEMD-160 özet fonksiyonlarına sokulmasıyla elde edilen 160 bitlik özet değerine versiyon numarası ön eki eklenir, elde edilen çıktıya *Base58Check* kodlaması yapılır. Sonunda çıkan Bitcoin adresi 26-35 aralığında karakterden oluşur ve ilk karakterleri 1 ya da 3 olur [50]. Başka kripto paralar ve blokzincirlerde farkı kodlama ve özet fonksiyonları kullanılarak farklı türde adresler elde edilebilir.

Bölüm 12.5.4'te daha detaylı incelenecek olan, mahremiyet konusuna Bitcoin ve benzeri yapıdaki blokzincirlerden daha çok odaklanan Monero, anahtar üretimi ve kimlik doğrulama için *Secp256k1* yerine [27]'de önerilen *Ed25519* eğrisini kullanır [54]. Bu eğri sonlu cismi üzerine tanımlanır. NIST'in öner-

diği eliptik eğri tabanlı rastgele sayı üretecinde ortaya çıkan arka kapı (*backdoor*) zafiyetinden dolayı bu kurumun önerdiği diğer eliptik eğri kriptografik sistemlere karşı da bir güvensizlik oluşmuştur [55]. Bu nedenle, güvenliği daha ön planda tutan bu kripto para birimi şu an için güvenli olduğu düşünülen *Ed25519* eğrisini kullanmaktadır.

$\mathbb{F}_{2^{255}-19}$'un elemanları 256-bit tam sayılardan oluşur. Yani bu sayılar, 32-bayt kullanılarak temsil edilir. Bu asal üzerine tanımlanan bir eğride herhangi bir nokta 64-bayt kullanılarak temsil edilir. Ancak nokta sıkıştırma tekniklerinin uygulanmasıyla uzunlukları 32-bayta indirmek mümkündür.

12.5.3. Blokzincirde Güvenlik

Elektronik nakit aslında dijital imzalar zinciri olarak tanımlanabilir. Ağdaki her bir kullanıcı bir önceki işleme ait özet değerini ve bir sonraki kullanıcının açık anahtarını sayısal olarak imzalar ve bu bilgiyi elektronik nakdin sonuna ekler. Nakit transferi bu şekilde gerçekleşir. Elektronik nakdi alacak kişi ise zincirin doğruluğunu, sayısal imzaları kontrol ederek test edebilir. Fakat alacaklı kişi aldığı transferin ikinci kez kullanılıp kullanılmadığını tespit edemez. Bu sorunun çözümü olarak genelde merkezi sunucular tercih edilir. Çünkü merkezi sunucular ağda gerçekleşen tüm işlemlerin kaydını tutar ve kontrol eder. Ancak blokzincir tüm bu işlemlerin kontrolünün banka gibi merkezi bir otoriteye bağlanmasını sorunlu görerek buna bir çözüm olarak tek bir merkezi denetçi yerine ağdaki tüm kullanıcıların işlem geçmişine sahip olmasını önerir. Bunun için bir zaman damgası sunucusu kullanılır. Bir zaman damgası sunucusu, zaman damgası uygulanacak bir blokun özet değerini hesaplar ve herkese açık olarak duyurur. Zaman damgası verinin o sırada var olması durumunu özet değerinde var olabilmek adına kanıtlar. Zaman damgaları, kendilerinden önceki zaman damgasını kendi özet değerinde barındırır ve bunlardan bir zincir oluşturur. Her bir zaman damgası kendinden önceki zaman damgalarını güçlendirmektedir.

Zaman damgasını dağıtık olarak çalıştırmak için ise iş kanıtı sistemi kullanılır. SHA-256 gibi bir özet fonksiyonu kullanılarak elde edilen bir özet değerinin ilk basamaklarında belirli sayıda 0 bulunur. İş kanıtında bu 0'ların sayısını tarama işlemi yapılır. Gereken ortalama iş, gereken sıfır bit sayısına oranla üsteldir ve tek bir özet değeri denenerek doğrulanabilir.

Zaman damgası ağında, blokun özet değerinin sıfır bitlerini veren bir değer bulunana kadar iş kanıtı, blokta tanımlanan nonce değeri arttırılarak uygulanır. İş kanıtı için gerekli işlemci gücü harcandıktan sonra oluşan blokun değiştirilmesi için işin yeniden yapılması gerekir. Ancak blokun ardına yeni bloklar eklendikçe, ilgili bloku değiştirmek için eklenen yeni blokların da yeniden hesaplanması gerekir, bu da zincirde değişiklik yapmanın neredeyse imkansız olduğu anlamına gelir.

Genel olarak, bir blokzincir işleyişinde ilk önce yeni işlemler tüm düğümlere yayınlanır. Her düğüm yeni işlemleri bir blokta toplar. Her düğüm, bloku için zor bir iş kanıtı bulmaya çalışır. Bir düğüm bir iş kanıtı bulduğunda, bloku tüm düğümlere yayınlar. Düğümler, yalnızca içindeki tüm işlemler geçerliyse ve henüz harcanmamışsa bloku kabul eder. Düğümler, kabul edilen blokun özet değerini önceki özet değeri olarak kullanarak zincirde bir sonraki bloku oluşturmaya çalışır ve bloku kabul ettiklerini ifade eder.

Eğer aynı anda iki blok yayınlanırsa bu blokları alan düğümler ellerine ilk geçen blok üzerinde doğrulama yaparlar. Ancak diğer blok da kaydedilir. Sonrasında ise eğer en uzun zincir ikinci bloku içeriyorsa ilk blok üzerinde doğrulama yapmaya çalışan düğümler uzun zincire geçiş yaparlar.

Ödeme kontrolleri yapılırken tüm ağın kontrol edilmesine gerek kalmadan, en uzun iş kanıtının blok başlıklarının kontrol edilmesi yeterlidir. Sistemin güvenliğini tehlikeye sokan şey daha önce de söz ettiğimiz gibi, dürüst olmayan kullanıcıların daha çok işlemci gücüne sahip olmaları durumudur. Bunun üstesinden gelmek için önerilen şey, ağda bulunan düğümlerden gelen hata mesajlarının dikkate alınmasıyla sağlanmasıdır. Hatalı bir blokun alınması halinde ilgili düğümün bu bloku indirmesinin önlenmesi gerekir. Bu durumda geçersiz blok en uzun zincire dahil edilmemiş olur. Ne var ki Bitcoin gibi blokzincirlerde günümüzde gelinen noktada şu ana kadarki onaylanmış blokların dürüst olmayan kullanıcılar tarafından manipüle edilmesi için gerekli olan işlem gücünü üretmek neredeyse imkansızdır.

Bu kadar büyük bir dağıtık sistemde veri büyüklüğünün zaman içinde kontrol edilemez bir noktaya gelmemesi için yukarıda da söz ettiğimiz Merkle ağaçları kullanılır. Düğümler yalnızca blokların Merkle ağacı köklerini blok özet değerlerinin içine dahil ederler. Böylelikle depolama alanında büyük ölçekli sorunlardan kaçınılmış olunur.

Bitcoin sisteminde tespit edilen bazı sorunlara çözüm getirmeyi hedefleyen, kripto paralarda kullanılması için tasarlanan bir uygulama katmanı protokolü olan CryptoNote [56] ise güvenlik konusunda daha kapsamlı bir bakış açısı tercih etmektedir. Monero, Bytecoin gibi kripto para birimlerinin kullandığı CryptoNote protokolü Bitcoin'de sağlanmayan takip edilemezlik ve bağlanamazlık özelliklerini sunmaktadır.

Bu sistemde Bitcoin'de tercih edilen, *Secp256k1* eğrisi üzerinde uygulanan ECDSA imza şeması yerine EdDSA yani Edwards eğirisi üzerinde ECDSA kullanılıyor. CryptoNote protokolünde kullanılan parametreler aşağıda verilmiştir:

- q: Asal sayı $q = 2^{255} - 19$,
- d: $\mathbb{F}_q$ cisminin bir elemanı $d = -21665/121666$,
- E: Eliptik eğri denklemi $-x^2 + y^2 = 1 + dx^2y^2$,
- G: Baz nokta $G = (x, -4/5)$,
- l: G noktasının asal mertebesi

  $l = 2^{252} +$
  $27742317777372353535851937790883648493$,
- $\mathcal{H}_s$: Kriptografik özet fonksiyonu $\{0,1\}^* \rightarrow \mathbb{F}_q$,
- $\mathcal{H}_p$: Deterministik özet fonksiyonu $E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_q)$.

Protokolde kullanılan terimler ise şu şekildedir:

- **Gizli eliptik eğri-anahtarı:** Standart bir eliptik eğri anahtarıdır. $a \in [1, l-1]$ olarak tanımlanmış bir sayıdır.
- **Açık eliptik eğri-anahtarı:** Standart bir eliptik eğri noktasıdır. $A = aG$ olarak hesaplanır.
- **Tek kullanımlık anahtar çifti**: Açık ve gizli eliptik eğri anahtar çiftidir.
- **Gizli kullanıcı anahtarı:** Iki farklı gizli eliptik eğri anahtarından oluşan bir anahtar çiftidir: (a, b).

- **Takip anahtarı:** Eliptik eğri noktası olan ve $a \neq b$ olacak şekilde $B = bG$ işlemi ile oluşturulan açık anahtar ve a gizli anahtarından oluşan anahtar çifti: (a, B).
- **Açık kullanıcı anahtarı:** (a, b)'den türetilmiş olan (A, B) açık eliptik eğri anahtar çiftidir.
- **Standart adres:** Hata düzeltme işlemi uygulanmış ve daha kullanıcı dostu hale getirilmiş, kullanıcının açık anahtarıdır.
- **Kısaltılmış adres:** Standart adresin ikinci yarısı olan B noktasıdır.

Bu protokolde işlemler Bitcoin işlemlerinin yapısına benzemektedir. Kullanıcılar birkaç bağımsız ödeme işlemi çıktısı seçer ve bunlara karşılık gelen özel anahtarlarla imzalayarak farklı hedeflere gönderir. CryptoNote algoritmasında standart bir işlem aşağıdaki gibi oluşmaktadır:

1. Daha önceden adresini yayınlamış olan Barış'a ödeme göndermek isteyen Ayşe, Barış'ın adresini çözümler ve Barış'ın açık anahtarı (A, B)'yi elde eder.
2. Ayşe $[1, l-1]$ aralığında rastgele bir r sayısı seçer ve tek kullanımlık anahtar $P = \mathcal{H}_s(rA)G + B$ hesaplamasını yapar.
3. Ayşe P'yi, çıktı değerinin varış noktası anahtarı olarak kullanır. Ayrıca Diffie-Hellman anahtar değişiminin bir parçası olarak $R = rG$ değerini oluşturarak işlem içine yerleştirir.
4. Ayşe işlemi gönderir.
5. Barış, geçen her işlemi kendi gizli anahtar çifti (a, b) ile kontrol eder ve $P' = \mathcal{H}_s(aR)G + B$ hesaplamasını yapar. Eğer işlem doğruysa, $aR = arG = rA$ ve $P = P'$ sonucuna ulaşır.
6. Barış ilgili tek kullanımlık gizli anahtarı hesaplar: $x = \mathcal{H}_s(aR)$, $P = xG$. Barış bu çıktıyı, işlemi x ile imzalayarak istediği zaman harcayabilir.

Tek seferlik halka imzalarına dayalı bir protokol, kullanıcıların koşulsuz bağlanamazlık elde etmelerini sağlar. Ancak genelde diğer kriptografik imza türleri, ilgili göndericiler ve alıcılar arasında yapılan işlemlerin izlenmesine izin

verir. Bu sorunun üstesinden gelmek için diğer elektronik nakit sistemlerinde kullanılan imza türlerinden farklı bir imza türü olan tek seferlik halka imza yöntemi kullanılmıştır. Tek seferlik halka imzalar (GEN, SIG, VER, LNK) olmak üzere dört algoritma içerir.

- GEN: Açık parametreleri girdi olarak kullanarak bir eliptik eğri çifti (P, x) ve açık anahtar I değerini döndürür.
- SIG: Girdi olarak mesaj m, açık anahtarlardan oluşan $\mathcal{S}' = \{P_i\}_{i \neq s}$ kümesi ve (P_s, x_s) çiftini alır. Çıktı olarak imza σ'yı ve $\mathcal{S} = \mathcal{S}' \cup \{P_S\}$ kümesini döndürür.
- VER: Girdi olarak mesaj m, $\mathcal{S}$ kümesi ve imza σ'yı alarak $doğru$ ya da $yanlış$ değerlerini döndürür.
- LNK: Girdi olarak $\mathcal{I} = \{I_i\}$ kümesini ve imza σ'yı alır. Çıktı olarak $bağlı$ ya da $bağımsız$ değerlerini döndürür.

Bir kullanıcı, benzersiz bir ortak anahtar yerine bir dizi ortak anahtar tarafından kontrol edilebilen bir imza üretir. İmzalayanın kimliği, kişi aynı anahtar çiftini kullanarak ikinci bir imza üretene kadar ortak anahtarlar kümesinde olan diğer kullanıcılar tarafından ayırt edilemez. Tek seferlik halka imzasının kullanılması bu protokole aşağıdaki özellikleri sağlamaktadır:

- **Bağlanabilirlik (*linkability*):** Tüm gizli anahtarların $x_i, i = \{1, 2, \dots, n\}$ verilmesi durumunda, $\mathcal{S}$ kümesi için $n + 1$ adet geçerli imza üretilmesi olanaksızdır. Çünkü tümü LNK adımından geçmektedir. Bu özellik çift harcama sorununun önüne geçilmesini sağlar.
- **Suçlanabilirlik (exculpability):** $\mathcal{S}$ kümesi, en fazla $n - 1$ adet ilgili gizli anahtar x_i $(i = j$ dışında) ve x_j'ye bağlı görüntü $\mathcal{I}_j$ değerlerinin bilinmesi durumunda $\mathcal{I}_j$ ile geçerli bir imza üretilmes olanaksızdır. Bu özellik protokole hırsızlık koruması özelliği kazandırmaktadır.
- **Taklit edilemezlik (unforgeability):** Yalnızca açık anahtar kümesi $\mathcal{S}$'nin verilmesi durumunda geçerli bir imza üretilmesi mümkün değildir.

12.5.4. Mahremiyet

Blokzincir için en önemli konulardan biri de mahremiyettir. Yani kullanıcıların blokzincir ağında yaptıkları işlemlerle ilişkilendirilememesi beklenir. Merkezi sistemlerde kullanıcı bilgilerini elinde tutan merkez tarafından halka açık hale getirilmez ve mahremiyet bu şekilde sağlanır. Ancak merkez tüm kullanıcı bilgilerine sahiptir, bu nedenle aslında mahremiyet tam anlamıyla sağlanmaz. Bitcoin ağı gibi dağıtık sistemlerde ise her kullanıcının gizli ve açık anahtarları vardır. Açık anahtarlar halka açık olarak paylaşılır fakat kullanıcılar ile bağlantı bilgisi açık değildir. Kullanıcıların ağ üzerinde yaptıkları işlemler üzerinden kimliklerinin ilişkilendirilmemesi için ise her işlem için ayrı anahtar çiftleri kullanılması gerekir.

Gizlilik eksikliğini gidermek için, Bitcoin gibi kripto para birimi kullanıcıları, geçici adresler kullanarak işlemlerinin anahtarlarıyla ilişkilendirilmesini engelleyebilir. Fakat uygun araçlar kullanılarak yapılan analizler sayesinde bu ilişkilendirmeyi yapmak mümkündür. Bir önceki bölümde de söz ettiğimiz gibi mahremiyet ve güvenlik konusunu daha ön planda tutan kripto para birimleri ya da blokzincirler halka imza yapılarını kullanarak mahremiyet sorununu çözmeyi hedefler [54]. Halka imzalar ve geçici adreslerin depolanması yöntemleriyle, gönderilerin kullanıcılarla ilişkilendirilmesinin önüne geçilir.

12.5.4.1. Halka İmzalar

Gizlilik bakımından halka imzaların blokzincirleri nasıl daha güçlü hale getirdiğini anlamak için halka imzaları kabaca incelemek gerekir.

Halka imzalar, tek bir gizli anahtar ve bu anahtardan bağımsız açık anahtarlar kullanılarak oluşturulur. Tüm bu anahtarların oluşturduğu kümeye halka adı verilir. İmzayı doğrulayan taraf imzanın halkadaki hangi gizli anahtar ile üretildiğini belirleyemez. Halka imzalar anonimlik, bağlanabilirlik gibi özellikler sunar. Örnek olarak Monero'nun kullandığı sistem verilebilir [54].

- **Anonimlik:** İmzalanmış bir mesajın hangi kullanıcı tarafından imzalandığı başka kişiler tarafından belirlenemez. Yalnızca halka içinde herhangi bir açık anahtara ait bir gizli anahtar ile imzalandığı bilinebilir, fakat halka içindeki hangi açık anahtar ile ilişkili olduğu belirlenemez.

- **Bağlanabilirlik:** Eğer bir gizli anahtar birden fazla mesajı imzalamak için kullanıldıysa bu gizli anahtar ile imzalanan mesajlar birbirleriyle ilişkilendirilir. Bu özellik bazı kripto paralarda çift harcama durumunu engellemekte kullanılır.

Monero'nun altyapısını oluşturan CryptoNote protokolünde bağlanabilirlik özelliğinin nasıl sağlandığı Bölüm 12.5.3'te verilmiştir. Halka imza yapısının Diffie-Hellman Karar (Decisional Diffie-Hellman – DDH) Karar Problemi altında anonimlik özelliğini taşıdığı şu şekilde gösterilebilir:

Bir saldırganın, imzacının gizli indisi j'yi, $p = \frac{1}{n} + \epsilon$ olasılığı ile tespit edebildiğini varsayıldığında, oluşturulacak $\mathcal{A}$ algoritması DDH Problemini, $E(\mathbb{F}_q)$ için $\frac{1}{2} + \frac{\epsilon}{2}$ olasılığında çözebilir.

$orn = (G_1, G_2, Q_1, Q_2) \in E(\mathbb{F}_q)$, DDH için bir örnek olsun. Hedef, $\log_{G_1} Q_1 = \log_{G_2} Q_2$ eşitliğinin sağlanma durumunu tespit etmektir. $\mathcal{A}$, $P_j = x_j G_1 = Q_1$ ve $I = Q_2$ olacak şekilde, saldırgana geçerli bir imza olan $\sigma_0 = (I, \dots)$ bilgisini verir ve $H_p(P_j)$ için G_2 döndüren H_p'yi simüle eder.

Saldırgan, indis değeri için tahmin ettiği k değerini döndürür. Eğer $k = j$ eşitliği sağlanıyorsa $\mathcal{A}$, 1 (doğru) yanıtını döndürür. Aksi durumda rastgele bir $r \in \{1,0\}$ değeri döndürür. $\mathcal{A}$'nın doğru değeri döndürme olasılığı $\frac{1}{2}$ olarak hesaplanır.

Bu sistem, ECC tabanlı her sistemde olduğu gibi kuantum dayanıklı değildir. Gelecekte kuantum bilgisayarların geliştirilmesiyle birlikte blokzincir teknolojisinde de kuantum dayanıklı algoritmalara gereksinim doğacaktır. [57]'de sunulan süpersingüler izojen tabanlı halka imza protokolü, kuantum dayanıklı algoritmalara örnek olarak verilebilir.

12.5.4.2. Taahhütler ve Aralık Kanıtı

Blokzinciri mahremiyet konusunda bir üst düzeye çıkaran bir diğer özellik ise kullanılan kriptografik protokollerdir. Örneğin, Pedersen taahhütleri, bir kanıtlayıcının bir sayıyı bildiğini, bu sayının ne olduğunu belli etmeden, doğrulayıcıya kanıtlamasını sağlayan bir sistem önerir [58]. Bu altyapıyı kullanan sistemlerde, kullanıcılar transfer işlemi yaptıklarında gönderilen miktar alıcı

ve gönderici dışında kimse tarafından görüntülenemez. İşlemler yapılırken girdi ve çıktı değerleri şifrelenir ve ağdaki diğer kullanıcılar tarafından bu şifreler çözülemez. Pedersen taahhütleri, işlemlerin gizliliğini sağlamanın yanı sıra, zincirdeki işlemlerin geçerliliğini ve üretilen değerlerin gerçek kullanıcılar tarafından üretildiğini kanıtlamayı da sağlamaktadır. Aynı zamanda, gizlilik sağlamayı hedefleyen sistemlerde kullanıcıların cüzdanlarındaki bakiye miktarı da açık olarak tutulmaz, taahhüt sistemleri sayesinde şifreli olarak tutulur. Göndericinin cüzdan bakiyesi taahhüt formlarında tutulurken göndericinin işlemlerinin girdi ve çıktılarının aynı tutarı gösterdiğini kanıtlaması beklenir. Ayrıca cüzdan bakiyesinin izin verilen aralıkta olduğunun kanıtlanması gerekir. Burada da aralık kanıtı (*range proof*) [54] devreye girmektedir. Aralık kanıtı basitçe taahhüt değerinin belirli bir aralıkta olduğunu kanıtlamak adına kullanılır. Örneğin, Monero'nun kriptografik altyapısında mertebesi q olan döngüsel bir grup bulunur. Bu durumda -1'in taahhütü q-1'in taahhütü ile aynı olmaktadır. Cüzdanında 1 TL'si olan bir kullanıcı aralık kanıtları kullanılmazsa, 2 TL ya da q-1 TL'lik işlem yapabilir. Göndericinin tüm taahhütlerini küçük bir aralık arasında sınırlı tutması zorunlu kılınırsa bu tip saldırılar önlenebilir [59]. Aralık kanıtı aynı zamanda anonimlik ve mahremiyeti sağlamak için e-oylama gibi sistemlerde de tercih edilir.

12.6. SONUÇ VE DEĞERLENDİRMELER

Bilgi güvenliği günümüzün en büyük gereksinimlerinden biri durumuna gelmiştir. Bilgi güvenliğinin en önemli bileşenlerinden biri de kriptografidir. Açık anahtarlı bir kriptosistem olan eliptik eğri kriptografi özellikle internet kullanımının son zamanlarda oldukça yaygınlaşmasıyla birlikte pratikte birçok uygulama alanı bulmuştur. Kitabın bu bölümünde eliptik eğrilerin matematiksel altyapısı, eliptik eğri kriptosistemler ve uygulama alanları açıklanmıştır. Haberleşme güvenliği, nesnelerin interneti ve blokzincir alanlarında eliptik eğrilerin nasıl kullanıldığı ve ne gibi avantajlar sağladığı incelenmiştir. Ayrıca, süpersingüler eliptik eğrilerde izojen bulma zorluğuna dayanan kuantum sonrası protokollere dair temel bilgi verilmiştir.

Teknolojinin hızlı gelişimi, akıllı cihaz kullanımının yaygınlaşması ve geçmişte klasik yöntemlerle gerçekleştirilen birçok işin sanal ortamlara aktarılması, bilgi güvenliği ve kriptografiye olan gereksinimin artacağının habercisidir. Kaynak kısıtlı cihazlarda, gündelik olarak kullanılan uygulamalarda,

kurum ve devletlere ait gizli verilerin saklanması ve iletilmesinde, hızlı çalışabilen ve güvenlikten ödün vermeyen protokoller tasarlanması büyük önem taşımaktadır. Aynı zamanda mevcut açıkların kapatılması ve gelecekte geliştirilmesi mümkün olan saldırılara karşı önlemler alınması gerekmektedir. Eliptik eğri kriptografi, açık anahtarlı kriptografide performans ve güvenlik bakımından en verimli sonuçları veren kriptosistemlerden birisidir. Ne var ki, açık anahtarlı kriptosistemlerden hiçbiri simetrik sistemler kadar verimli çalışmamaktadır. Öte yandan açık anahtarlı kriptografi sayesinde simetrik kriptografinin en önemli sorunu olan anahtar paylaşım problemi çözülmektedir. Bu bağlamda mevcutta, her iki kriptosistemin de dahil olduğu hibrit protokoller kullanılmaktadır.

Günümüzde ECC tabanlı protokoller birçok kurum tarafından standart olarak belirlendiği için yaygın bir kullanım alanına sahiptir. Her ne kadar eliptik eğri kriptografinin kullanımı yaygın olsa da var olan sistemlerin geliştirilmesi gereksinimi mevcuttur. Verimliliği arttırmak amacıyla Bölüm 12.2.5'te söz edilen eliptik eğri aritmetiği ve sonlu cisim aritmetiğinde var olan hızlandırma işlemlerinin geliştirilmesi ya da yeni hızlandırma işlemlerinin tasarlanması gereksinimi vardır. Öte yandan eliptik eğriler üzerinde bulunan noktaların ifade edilmesinde kullanılan sıkıştırma yöntemleri, protokollerin gereksinim duyduğu depolama alanlarını küçültülmesi için üzerinde geliştirilme yapılması gereken bir başka alandır. Yine Bölüm 12.2.5'te söz edildiği üzere, eliptik eğri tabanlı protokollerde kullanılacak eğrilerin tanımlı olduğu cisimlerin inşasında kullanılan asalların özellikleri de uygulamada hem güvenlik hem de verimlilik açısından büyük önem taşımaktadır. Bu kapsamda, hızlı aritmetik olanakları sağlarken güvenlikten ödün vermeyen yeni asal sayıların belirlenmesi ve bu sayılara yönelik ilgili analizlerin yapılması gereksinimi bulunmaktadır. Ek olarak, kuantum bilgisayarların kullanımının yaygınlaşmasıyla birlikte bu bilgisayarların gücü kullanılarak uygulanabilecek saldırılara yönelik yeni güvenlik önlemleri alınmasının gerekliliği de göz ardı edilemeyecek bir gerçektir. Bu nedenle mevcut olarak kullanılan ve bilgi güvenliği gerektiren uygulamaların güncele ayak durması gerekmektedir. Bölüm 12.3.3'te ifade edildiği üzere, eliptik eğriler kuantum sonrasında da gelecek vaat eden bir altyapı sunmaktadır. Klasik ECC'nin aksine, güvenliği süpersingüler eğriler arasında izojen bulmaya dayanan süpersingüler izojen tabanlı kriptografi kuantum sonrası protokoller arasında en küçük anahtar boyutunu sağlayan sistemdir. Özellikle SIDH ve SIKE algoritmalarının gelecekte yaygın olarak

kullanılması beklenmektedir. Bu nedenle bu alanlarda hızlandırma ve verimlileştirme çalışmaları yapılması, süpersingüler izojen problemini temel alan yeni protokoller geliştirilmesi ve bunların analizlerinin yapılması gereksinimi bulunmaktadır.

Bu kapsamda, bilgi güvenliğinin sağlanmasında hem kuantum öncesinde hem de kuantum sonrasında önemli bir rol oynayan eliptik eğriler üzerine yapılan çalışmaların artarak devam etmesinin büyük bir öneme sahip olduğu görüşündeyiz.

Teşekkür

2. yazar, TÜBİTAK 2244 - Sanayi Doktora Programı 118C077 numaralı proje kapsamında desteklenmektedir. 3. yazar, 100/2000 YÖK Doktora Bursu kapsamında desteklenmektedir. Desteklerinden dolayı YÖK ve TÜBİTAK'a teşekkür ederiz.

KAYNAKLAR

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory,* vol. 22, no. 6, pp. 644-654, 1976.

[2] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the Theory and Application of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 1985, pp. 417-426.

[3] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation,* vol. 48, no. 177, pp. 203-209, 1987.

[4] D. Hankerson, A. J. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer Science & Business Media, 2006.

[5] H. Hisil, "Elliptic curves, group law, and efficient computation," Ph.D dissertation, Information Security Institute, Queensland University of Technology, Brisbane, Queensland, Australia, 2010.

[6] J. Hoffstein, J. Pipher and J. H. Silverman, An Introduction to Mathematical Cryptography, vol. 1, New York: Springer, 2008.

[7] R. Schoof, "Counting points on elliptic curves over finite fields," *Journal de Théorie des Nombres de Bordeaux,* vol. 7, no. 1, pp. 219-254, 1995.

[8] L. Dewaghe, "Remarks on the Schoof-Elkies-Atkin algorithm," *Mathematics of Computation,* vol. 67, no. 223, pp. 1247-1252, 1998.

[9] E. Barker, E. Barker, W. Burr, W. Polk, M. Smid and others, Recommendation for Key Management: Part 1: General, National Institute of Standards and Technology, Technology Administration, 2006.

[10] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, United Kingdom: Chapman and Hall/CRC, 2005.

[11] H. Hisil, K. K.-H. Wong, G. Carter and E. Dawson, "Jacobi quartic curves revisited," in *Australasian Conference on Information Security and Privacy*, Springer, 2009, pp. 452-468.

[12] N. G. Orhon and H. Hisil, "Speeding up Huff form of elliptic curves," *Designs, Codes and Cryptography,* vol. 86, no. 12, pp. 2807-2823.

[13] H. Hisil, K. K.-H. Wong, G. Carter and E. Dawson, "Twisted Edwards curves revisited," in *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, vol. 5350, Springer, 2008, pp. 326-343.

[14] D. J. Bernstein, C. Chuengsatiansup, D. Kohel and T. Lange, "Twisted Hessian Curves," in *International Conference on Cryptology and Information Security in Latin America*, vol. 9230, Springer, 2015, pp. 269-294.

[15] D. J. Bernstein and T. Lange, "Explicit-formulas database," 2017. [Online]. Available: http://www.hyperelliptic.org/EFD. [Accessed 09 August 2021].

[16] A. A. Karatsuba and Y. Ofman, "Multiplication of multidigit numbers on automata," *Soviet physics doklady,* vol. 7, pp. 595-596, 1963.

[17] M. Cenk, "Karatsuba-like formulae and their associated techniques," *Journal of Cryptographic Engineering,* vol. 8, no. 3, pp. 259-269, 2018.

[18] S. Ali and M. Cenk, "Faster residue multiplication modulo 521-bit Mersenne prime and an application to ECC," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 65, no. 8, pp. 2477-2490, 2018.

[19] H. K. Taşkın and M. Cenk, "Speeding up curve25519 using toeplitz matrix-vector multiplication," in *Proceedings of the Fifth Workshop on Cryptography and Security in Computing Systems*, 2018, pp. 1-6.

[20] H. K. Taşkın and M. Cenk, "TMVP-Friendly Primes for Efficient Elliptic Curve Cryptography," in *2020 International Conference on Information Security and Cryptology (ISCTURKEY)*, IEEE, 2020, pp. 80-87.

[21] P. L. Montgomery, "Modular multiplication without trial division," *Mathematics of computation,* vol. 44, no. 170, pp. 519-521, 1985.

[22] P. Barrett, "Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor," in *Advances in Cryptology - CRYPTO' 86*, A. M. Odlyzko, Ed., Springer Berlin Heidelberg, 1987, pp. 311-323.

[23] National Institute of Standards and Technology, "Digital Signature Standard (DSS)," *Federal Information Processing Standards Publication (FIPS) 186-4,* 2013.

[24] Association American Bankers and others, "Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ecdsa)," *ANSI X9,* pp. 62-1998.

[25] M. Lochter and J. Merkle, "Elliptic curve cryptography (ECC) brainpool standard curves and curve generation," *RFC 5639, March,* 2010.

[26] D. Jablon, "IEEE P1363 standard specifications for public-key cryptography," in *CTO Phoenix Technologies Treasurer, IEEE P1363 NIST Key Management Workshop*, 2001.

[27] D. J. Bernstein, "Curve25519: new Diffie-Hellman speed records," in *International Workshop on Public Key Cryptography*, Springer, 2006, pp. 207-228.

[28] D. J. Bernstein and T. Lange, "SafeCurves: choosing safe curves for elliptic-curve cryptography," [Online]. Available: https://safecurves.cr.yp.to. [Accessed 16 June 2021].

[29] A. K. Yadav, "Significance of Elliptic Curve Cryptography in Blockchain IoT with Comparative Analysis of RSA Algorithm," in *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, IEEE, 2021, pp. 256-262.

[30] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134.

[31] J. Vélu, «Isogenies entre courbes elliptiques,» *Communications de l'Académie royale des Sciences de Paris,* vol. 273, pp. 238-241, 1971.

[32] A. Childs, D. Jao and V. Soukharev, "Constructing elliptic curve isogenies in quantum subexponential time," *Journal of Mathematical Cryptology,* vol. 8, no. 1, pp. 1-29, 2014.

[33] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *International Workshop on Post-Quantum Cryptography*, Springer, 2011, pp. 19-34.

[34] A. Rostovtsev and A. Stolbunov, "Public-Key Cryptosystem Based on Isogenies," *IACR Cryptology ePrint Archive,* vol. 2006, p. 145, 2006.

[35] C. Costello, P. Longa and M. Naehrig, "Efficient algorithms for supersingular isogeny Diffie-Hellman," in *Annual International Cryptology Conference*, Springer, 2016, pp. 572-601.

[36] B. Koziel, A. Jalali, R. Azarderakhsh, D. Jao and M. Mozaffari-Kermani, "NEON-SIDH: Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange Protocol on ARM," in *Cryptology and Network Security*, S. Foresti and G. Persiano, Eds., Cham, Springer International Publishing, 2016, pp. 88-103.

[37] A. Karmakar, S. S. Roy, F. Vercauteren and I. Verbauwhede, "Efficient Finite Field Multiplication for Isogeny Based Post Quantum Cryptography," in *Arithmetic of Finite Fields*, S. Duquesne and S. Petkova-Nikova, Eds., Cham, Springer International Publishing, 2016, pp. 193-207.

[38] S. D. Galbraith, C. Petit, B. Shani and Y. B. Ti, "On the security of supersingular isogeny cryptosystems," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2016, pp. 63-91.

[39] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao and V. Soukharev, "A post-quantum digital signature scheme based on supersingular isogenies," in *International Conference on Financial Cryptography and Data Security*, Springer, 2017, pp. 163-181.

[40] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Conference on the theory and application of cryptographic techniques*, Springer, 1986, pp. 186-194.

[41] W. Stallings, Cryptography and Network Security, 4/E, Pearson Education India, 2006.

[42] M. Cenk, "Siber Güvenlikte Kriptografi," in *Siber Güvenlik ve Savunma: Problemler ve Çözümler*, Ankara, Grafiker Yayınları, 2019, pp. 61-83.

[43] T. Polk, K. McKay, S. Chokhani and others, "Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations," *NIST special publication,* vol. 800, no. 52, p. 32, 2014.

[44] Whatsapp, "WhatsApp Encryption Overview Technical white paper," [Online]. Available: https://scontent.whatsapp.net/v/t39.8562-34/122 249142_4698577206 42275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-3&_nc_sid=2fbf2a&_nc_ohc=xr-C2fji7PEAX_FnyR1&_nc_ht=scontent.whatsapp.net&oh=5b150605b97f74baceb3a07896d73b5d&oe=60EEA559. [Accessed 5 April 2021].

[45] M. Scott, "On the Deployment of curve based cryptography for the Internet of Things," *IACR Cryptol. ePrint Arch.,* vol. 2020, p. 514, 2020.

[46] P. Shruti and R. Chandraleka, "Elliptic curve cryptography security in the context of internet of things," *International Journal of Scientific & Engineering Research,* vol. 8, no. 5, pp. 90-3, 2017.

[47] M. Suárez-Albela, P. Fraga-Lamas and T. M. Fernández-Caramés, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors,* vol. 18, no. 11, p. 3868, 2018.

[48] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review,* p. 21260, 2008.

[49] D. Chaum, "Blind signatures for untraceable payments," Boston, Springer, 1983, pp. 199-203.

[50] I. Bashir, Mastering Blockchain, Packt Publishing Ltd, 2017.

[51] S. Chandel, W. Cao, Z. Sun, J. Yang, B. Zhang and T.-Y. Ni, "A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption," in *Future of Information and Communication Conference*, Springer, 2019, pp. 988-1003.

[52] D. Brown, "SEC 2: Recommended elliptic curve domain parameters," *Standars for Efficient Cryptography,* 2010.

[53] W. Bi, X. Jia and M. Zheng, "A secure multiple elliptic curves digital signature algorithm for blockchain," *arXiv preprint arXiv:1808.02988,* 2018.

[54] K. M. Alonso, "Monero-privacy in the blockchain," 2018.

[55] D. J. Bernstein, T. Chou, C. Chuengsatiansup, A. Hülsing, E. Lambooij, T. Lange, R. Niederhagen and C. Van Vredendaal, "How to Manipulate Curve Standards: A White Paper for the Black Hat http://bada55.cr.yp.to," in *International Conference on Research in Security Standardisation*, Springer, 2015, pp. 109-139.

[56] N. Van Saberhagen, „CryptoNote v 2.0," 2013.

[57] M. S. Garjan, N. G. Orhon Kılıç and M. Cenk, "A Supersingular Isogeny-Based Ring Signature," *Cryptology ePrint Archive,* Report 2021/1318, 2021.

[58] "Moneropedia: Pedersen Commitment," getmonero.org, The Monero Project, [Online]. Available: https://www.getmonero.org/resources/moneropedia/pedersen-commitment.html. [Accessed 5 April 2021].

[59] K. Li, R. Yang, M. H. Au and Q. Xu, "Practical range proof for cryptocurrency monero with provable security," in *International Conference on Information and Communications Security*, Springer, 2017, pp. 255-262.

DİZİN

O

S

U

Y

YAZARLAR

EDİTÖRLER

Prof. Dr. Şeref Sağıroğlu

Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü
Bilgi Güvenliği Derneği Ulusal Bilim Kurulu Başkanı
Future Tech Genel Müdürü
IPv6 Forum Turkey Başkanı
IEEE Biometric Task Force Member
ss@gazi.edu.tr

Prof. Sağıroğlu, ülkemizde bilgi güvenliği, siber güvenlik ve büyük veri analitiği, güvenliği ve mahremiyeti konularında çalışmalar yapmaktadır. 20'nin üzerinde yayınlanmış kitabı bulunmaktadır. Biri amerikan patenti olmak üzere alınmış ve müracaat aşamasında olan 10'un üzerinde patenti, 100'ün üzerinde ulusal ve uluslararası indeksli dergilerde yayınlanmış makalesi ile 300'e yakın ulusal ve uluslararası yayımlanmış bildirisi ve 6000'in üzerinde atıfı bulunmaktadır. Bilgi güvenliği alanında iki akademik derginin de editörlüğünü yapmaktadır.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (www.iscturkey.org), IEEE Uluslararası Bilgisayar Bilimleri ve Mühendisliği Konferansı (www. ubmk.org), IEEE Uluslararası Makine Öğrenmesi ve Uygulamaları Konferansı (www.icmla-conferences.org), Büyük Veri Analitiği, Güvenliği ve Mahremiyeti Ulusal Kamu Çalıştayı (bigdatacenter.gazi.edu.tr), Ulusal Siber Terör Konferansı (www.siberteror.org), Açık Veri Türkiye Konferansı (www.acikveriturkiye.org), Siber Güvenlik ve Savunma Çalıştayı (www.iscturkey.org) gibi konferansların başkanlığını veya eşbaşkanlığını yürütmüş/yürütmektedir.

Bilgi Güvenliği Derneği (BGD), Türk Bilim Araştırma Vakfı (TÜBAV), Geleceği Önemseyenler Derneği (GÖNDER) Kurucu Üyesidir. İlki dönem, BGD Yönetim Kurulu Başkanlığı ve TÜBAV Genel Başkanlığı Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürlüğü gibi görevleri yürütmüştür.

Gönüllü olarak pek çok sosyal projeyi de yürütmüş olan Sağıroğlu, TÜBİTAK, Avrupa Birliği, BAP gibi Bilimsel Araştırma Projelerinde de görev almış ve projeler yürütmüştür. Ulusal ve uluslararası konferanslarda, Bilgi Güvenliği, Büyük Veri, Siber Güvenlik ve Savunma, Yapay Zekâ, Biyometrik Uygulamalar, İnovasyon Kültürü Oluşturma gibi konularda davetli konuşmacı olarak seminer ve konferanslar vermiştir.

Gazi Üniversitesi ve Erciyes Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanlığı, ISACA Ankara Chapter Akademi Koordinatörlüğü gibi görevleri yürütmüştür. Yükseköğretim Kurulu Siber Güvenlik Çalışma Grubu Üyeliği, Bilim Sanayi ve Teknoloji Bakanlığı Yazılım Sektörü Çalışma Grubu Üyeliği, BGD Yönetim Kurulu Üyeliği, IPV6Forum Turkey Başkanlığı, IEEE üyeliği, ACM Üyeliği, Avrupa ETSI Standartları Gözlemci Komisyon Üyeliği gibi görevleri yürütmektedir. Havelsan, Kişisel Verileri Koruma Kurumu, Bilgi Teknolojileri ve İletişim Kurumu gibi kurumlarda danışmanlık yapmıştır. Şu anda ise Gazi Üniversitesi Mühendislik Fakültesi Dekanlığı görevini yürütmektedir.

Sedat Akleylek

2011 yılından beri OMÜ Bilgisayar Mühendisliği Bölümü'nde Öğretim Üyesi olarak görev yapmaktadır. 2004 yılında Ege Üniversitesi Matematik Bölümü'nde lisans eğitimini tamamlamıştır. Öğretim Üyesi Yetiştirme Programı kapsamında sırasıyla 2008 ve 2010 yıllarında yüksek lisans ve doktora çalışmalarını ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Programı'nda tamamlamıştır. 2012 yılında Almanya Bochum Ruhr Üniversitesi Donanım Güvenliği Grubu'nda, Almanya'da ve 2014-2015 yıllarında Almanya Darmstadt Teknik Üniversitesi Kriptografi ve Bilgisayar Cebri Grubu'nda misafir öğretim üyesi olarak görev almıştır. 2016 yılında Bilgisayar/Bilişim Bilimleri ve Mühendisliği, Bilgi Güvenliği ve Kriptoloji alt alanında doçent unvanını almıştır. Doç. Dr. Sedat Akleylek, kuantum sonrası kriptografi, verimli kriptografik hesaplamalar, Boolean fonksiyonlar ve siber güvenlik için uygulamalı kriptografi alanlarında çalışmalarını sürdürmektedir. Ulusal ve uluslararası kapsamda bilgi güvenliği ve kriptoloji alanında TÜBİTAK, KOSGEB, Üniversite-Sanayi İş birliği Projeleri ve Üniversiteler tarafından desteklenen Bilimsel Araştırma Projelerinde yürütücü, araştırmacı ve danışman olarak görevler almıştır. Doç. Dr. Sedat Akleylek, uluslararası saygın iki dergide bilgi güvenliği ve kriptoloji alan editörlüğü görevlerini sürdürmektedir.

İletişim: sedat.akleylek@bil.omu.edu.tr

YAZARLAR

Doç. Dr. Özgü Can
Ege Üniversitesi
Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü
ozgu.can@ege.edu.tr

Özgü Can, lisans derecesini "Selçuk Üniversitesi Bilgisayar Mühendisliği"nden, yüksek lisans derecesini "Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü"nden "Asal Sayı Örüntüleri ve Goldbach Sanısı Üzerine Bir Çalışma" başlıklı tezi ile ve doktora derecesini "Ege Üniversitesi Bilgisayar Mühendisliği"nden "Anlamsal Web için Kişiselleştirilebilir Ontoloji Tabanlı Erişim Denetimi ve Politika Yönetimi" başlıklı tezi ile almıştır. Dr. Can, ayrıca, "Anadolu Üniversitesi, İşletme Fakültesi, İşletme Bölümü"nden lisans derecesine de sahiptir. Doktora çalışmaları sırasında Fransa'da "University of Poitiers, LISI/ENSMA"da, doktora sonrasında da Ziyaretçi Öğretim Üyesi olarak ABD'nin Texas eyaletindeki "University of Texas at Dallas (UTD), Erik Jonsson School Of Engineering And Computer Science"da bulunmuştur. 1999-2002 yılları arasında Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü'nde Araştırma Görevlisi; 2000-2005 yılları arasında "Ege Üniversitesi, Bilgi ve İletişim Teknolojileri Araştırma ve Uygulama Merkezi (BİTAM) Network Yönetim Grubu"nda Unix Sistem Yöneticisi, Cisco Unix Akademi Programı Eğitmeni ve Cisco Network Akademi Programı Eğitmeni; 2003-2011 yılları arasında Ege Üniversitesi Bilgisayar Mühendisliği Bölümü'nde Araştırma Görevlisi; 2011-2021 yılları arasında Ege Üniversitesi Bilgisayar Mühendisliği Bölümü'nde Dr. Öğr. Üyesi olarak görev yapmış olan Dr. Can, 2020 yılında Doçentlik unvanını almış ve 2021 yılından itibaren Ege Üniversitesi Bilgisayar Mühendisliği Bölümü'nde Doç. Dr. olarak görevine devam etmektedir. Ayrıca, 2013 yılından itibaren Ege Üniversitesi Bilgisayar Mühendisliği Bölümü Bitirme Tezi Koordinatörlüğü görevini sürdürmektedir.

Akademik uzmanlık olarak Bilgi Güvenliği, Gizlilik, Bilgi Mühendisliği, Anlamsal Web ve Ontoloji Mühendisliği alanları başta olmak üzere çalışmalar yapmakta olan Dr. Can'ın ulusal ve uluslararası dergilerde ve konferanslarda yayınlanmış makaleleri ve bildirileri, yürüttüğü yüksek lisans ve doktora tez çalışmaları, yürütücü ve araştırmacı olarak görev aldığı bilimsel projeleri, teknik komite ve kurul üyelikleri bulunmaktadır.

Ali Melih Kanca

İstanbul Üniversitesi Elektrik-Elektronik Mühendisliği Bölümü'nden mezun olmuştur. Yüksek lisansını Gazi Üniversitesi Bilgi Güvenliği Mühendisliği bölümünde tamamlamıştır. Karabük Üniversitesi Bilgisayar Mühendisliği Bölümünde doktora çalışmasını sürdürmektedir. Bilgi güvenliği ve siber güvenlik üzerine çalışmalarına devam etmektedir.

Yunus Geçer

Erciyes Üniversitesi Matematik Bölümü ve Anadolu Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde öğrenim gördü. Yüksek lisansını Ahi Evran Üniversitesi'nde Eğitim Teknolojileri üzerine yaptı. Gazi Üniversitesi, Bilişim Enstitüsünde Yönetim Bilişim Sistemleri Anabilim Dalı'nda doktora tez çalışmasını sürdürmektedir. Eğitim teknolojileri ile bilgi güvenliği ve siber güvenlik üzerine akademik çalışmaları vardır. Araştırma alanları arasında matematiksel modelleme de bulunmaktadır.

Mehmet Yavuz Yağcı
İstanbul Üniversitesi-Cerrahpaşa

Lise eğitimini İstanbul'da Maçka Teknik Lisesi Bilişim Teknolojisi Alanında tamamladı. Lise yıllarında PHP ile yazılım geliştirme ve web güvenliği konularına ilgi duydu. Bilgisayara duyduğu ilginin peşinden giderek K.T.Ü. Bilgisayar Mühendisliği Lisans eğitiminden 2017 yılında derece ile mezun oldu. Lisans eğitimini tamamlayıncaya kadar çeşitli pozisyonlarda yarı zamanlı çalıştı. 2018 yılından itibaren İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Bölümünde Siber Güvenlik Anabilim Dalında araştırma görevlisi olarak çalışmaktadır. İstanbul Kalkınma Ajansı 2018 yılı mali destek programı kapsamında desteklenen Nesnelerin İnterneti Ekosistemi Test ve Değerlendirme Merkezinde donanım ve haberleşme testlerini gerçekleştirmek üzere çalışmalar yürütmektedir. 2020 yılının başında İstanbul Üniversitesi-Cerrahpaşa Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Bölümünde SCADA sistemlerinin siber güvenliği üzerine yüksek lisansını tamamlamıştır. Doktora eğitimine aynı üniversitede kritik altyapıların siber güvenliği üzerine devam etmektedir.

Ebu Yusuf Güven

İstanbul Üniversitesi-Cerrahpaşa

Ebu Yusuf GÜVEN İstanbul Üniversitesi Bilgisayar Mühendisliği Bölümü Siber Güvenlik Anabilim Dalında 2018 yılından beri Araştırma Görevlisi olarak çalışmaktadır. Yüksek Lisans Eğitimini Fatih Sultan Mehmet Vakıf Üniversitesinde Bilgisayar Mühendisliği dalında Kenar Bilişim güvenliği üzerine çalışmalar yapmıştır. Doktora Eğitiminde İstanbul Üniversitesi-Cerrahpaşa'da Siber Güvenlik Alanında Siber Tehdit İstihbaratı üzerine çalışmaktadır. 2018 Nisan Ayından beri İstanbul Üniversitesi-Cerrahpaşa bünyesinde İstanbul Kalkınma Ajansı desteği ile kurulan Nesnelerin İnterneti Ekosistemi Güvenlik Test ve Değerlendirme Merkezinde Araştırmacı olarak görev almaktadır.

Sevda Altan

İstanbul Üniversitesi-Cerrahpaşa

Sevda Altan, Karadeniz Teknik Üniversitesi Elektrik-Elektronik Bölümünden 2018 yılında derece ile mezun olmuştur. Kritik altyapılarda ve endüstriyel sistemlerde iş güvenliği ve sağlığını denetlemek amacıyla 2019 yılında C sınıfı iş güvenliği ve sağlığı uzmanlığını almıştır. 2021 yılında Akdeniz Üniversitesinde yüksek lisansını tamamlamış olup, İstanbul Üniversitesi-Cerrahpaşa'da doktora eğitimine devam etmektedir.

Muhammed Ali Aydın
İstanbul Üniversitesi-Cerrahpaşa

Doç. Dr. Muhammed Ali AYDIN, 2001 yılında İstanbul Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nü tamamladı. 2001 yılında aynı bölümde Araştırma Görevlisi olarak göreve başladı. 2005 yılında İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında yüksek lisansını, 2009 yılında ise İstanbul Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında doktora eğitimini tamamladı. Doktora eğitimi süresince ve sonrasında farklı zamanlarda Fransa'da Telecom SudParis adlı enstitüde (Institut National des Télécommunications) araştırmacı olarak çalışmıştır. 2009 yılında Yardımcı Doçent, 2019 yılında Doçent ünvanını almıştır.

2010-2016 yılları arasında Bilgisayar Mühendisliği Bölüm Başkan Yardımcısı, 2013-2016 yılları arasında Mühendislik Fakültesi Yönetim Kurulu Üyesi, 2018-2021 yılları arasında Bilgi İşlem Daire Başkanı, 2018-2020 yılları arasında İstanbul Üniversitesi-Cerrahpaşa Proje ve Teknoloji Ofisi'nde (PROTEK) Müdür Yardımcısı ve Yönetim Kurulu Üyesi olarak görev yapmıştır. 2015 yılından beri Mühendislik Fakültesi Dekan Yardımcılığı, 2016 yılından beri Bilgisayar Mühendisliği Siber Güvenlik Anabilim Dalı Başkanlığı görevlerini sürdürmektedir.

Çalışmalarını Bilgi Güvenliği ve Analizi, Siber Güvenlik, Bilgisayar Yazılımı, Nesnelerin İnterneti, Bilgisayar Ağları ve Haberleşmesi alanlarında sürdürmektedir.

Süreyya Atasever
Milli Eğitim Bakanlığı

2010 yılında Marmara Üniversitesi Elektronik-Bilgisayar Eğitimi Yüksek Lisans mezunudur. 2013 yılında Gazi Üniversitesi Bilgisayar Bilimleri doktora eğitimine başlamıştır. Bilgi ve bilgisayar güvenliği, makine öğrenmesi, DDoS savunma ile ilgili çalışmalarını sürdürmektedir.

Dr. Öğretim Üyesi İlker Özçelik

1981 yılında doğdu, Syracuse Üniversitesi, Mühendislik Fakültesi, Elektrik Mühendisliği Bölümü'nde "Voice Activity Detection using Stochastic Resonance" adlı Yüksek Lisans tezini 2010 yılında tamamladı.

2015 yılında Clemson Üniversitesi, Mühendislik Fakültesi, Elektrik Mühendisliği Bölümü, Akıllı ve Etkileşimli Sistemler Anabilim Dalı'nda "DoS Detection and Mitigation" adlı Doktora tezini verdi. Aynı yıl Türkiye`ye döndü ve Recep Tayyip Erdoğan Üniversitesi Mühendislik Fakültesi bünyesinde akademik kariyerine başladı. 2017 – 2019 yılları arasında Bilişim Sistemleri Mühendisliği Bölümü başkanlığını yürüttü.

2019 yılında TÜBİTAK 2219 Yurtdışı Doktora Sonrası Araştırma programı kapsamında University of Tennessee at Chattanooga, SimCenter Araştırma merkezinde güvenlik çalışmalarını sürdürdü. Aynı sene "Distributed Denial of Service Attacks: Real-world Detection and Mitigation" adlı kitabını tamamlayıp yayınladı.

Temmuz 2020 tarihinde Eskişehir Osmangazi Üniversitesi, Yazılım Mühendisliği Bölümüne Dr. Öğretim Üyesi olarak atandı. Burada Akıllı Sistemler Güvenliği Araştırma Grubunu kurdu.

İlgi alanları; Ağ güvenliği, Dağıtık Sistemler, Yazılım Tanımlı Ağlar, Blok Zincir ve Akıllı Sistemlerde Güvenlik ve Mahremiyettir.

Dr. Özgür Yürekten

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
Proje Müdürü
ozgur.yurekten@cbddo.gov.tr

Dr. Özgür Yürekten Başkent Üniversitesi bilgisayar mühendisliği bölümünden 2001 yılında mezun oldu. Yüksek lisans ve doktora çalışmalarını Gazi Üniversitesi Bilgisayar Mühendisliği ana bilim dalında tamamladı.

2001-2015 tarihleri arasında TÜBİTAK'ta araştırmacı olarak çeşitli askeri ve kamu projelerinde yazılım geliştirme uzmanı, teknik lider ve proje yöneticisi olarak görev yaptı.

2015-2016 yılları arasında TÜBİTAK-BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü'nde e-Devlet Planlama Birim Yöneticiliği görevini yürüttü. Bu süreçte kamu kurumları için gerçekleştirilen dijital dönüşüm projelerinde proje yöneticiliği ve danışmanlık yaptı.

2016-2020 yılları arasında kamu kurumlarının siber güvenlik kapasitesinin iyileştirilmesini ve siber güvenlik teknolojilerinin kazanımını amaçlayan ve TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü tarafından yürütülen projelerde yer aldı.

2021 yılından itibaren Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi bünyesinde Proje Müdürü görevini yürütmektedir.

Nurşah Çevik

2022 yılından bu yana HAVELSAN'da Platform Güvenlik Mühendisi olarak görev yapmaktadır. 2015 yılında Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun olmuştur. 2018 yılında, Ondokuz Mayıs Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında, "Kafes Tabanlı Yeni Anahtar Değişim Protokolleri ve Verimli Polinom Çarpımı" başlıklı tez çalışmasını tamamlamıştır. Ardından YÖK 100/2000 bursu kapsamında, Ondokuz Mayıs Üniversitesi Hesaplamalı Bilimler Anabilim Dalı'nda "Bilgi Güvenliği" alanında doktora eğitimine başlamıştır. Kuantum sonrası kriptografik protokol tasarımı ve bilgi güvenliği alanlarında çalışmalar yapmıştır. TÜBİTAK tarafından desteklenen ulusal ve uluslararası projelerde araştırmacı ve yürütücü olarak görev almıştır. Mesleki yaşamında 2019-2021 yılları arasında IBSS Danışmanlık firmasında AR-GE mühendisi olarak görev almış, kimlik doğrulama alanında makine öğrenmesi ve derin öğrenme yöntemlerinin kullanımına odaklanmıştır. Ardından TÜBİTAK Blokzincir Laboratuvarında "Dijital Para Teknolojileri ve Kripto Mimarileri" konusunda Araştırmacı olarak çalışmıştır.

İletişim: nursah.kaya@bil.omu.edu.tr

Halil İbrahim Çelenli

2021 yılında beri Moneye firmasında Veri Bilimi alanında çalışmalar yapmaktadır. 2012 yılında Cumhuriyet Üniversitesi Bilgisayar Mühendisliği bölümünden mezun olmuştur. 2020 yılında, Kocaeli Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında "Gizli Dirichlet Ayrımı ve Word2vec Yöntemlerinin Birleşimi ile Özgün Bir Metin Temsil Modeli Geliştirilmesi" başlıklı tez çalışması ile yüksek lisansını tamamlamıştır. 2019-2021 yılları arasında IBSS Danışmanlık firmasında Doğal Dil İşleme ve Makine Öğrenmesi alanlarında çalışmalar yapmıştır.

İletişim: halilibrahimcelenli@gmail.com

İhsan Çiçek

Dr. Çiçek İstanbul Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği Bölümü'nden 2002 yılında Siemens Mühendislikte Mükemmellik ödülünü alarak yüksek onur derecesiyle mezun oldu. Yüksek lisansını 2004 yılında Sabancı Üniversitesi Elektronik Mühendisliği Bölümü'nde tamamladı. Akademik kariyerine Boğaziçi Üniversitesi'nde devam edip 2014 yılında Elektrik-Elektronik Mühendisliği Bölümü'nden doktora derecesini aldı. 2009-2015 yılları arasında TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırmaları Enstitüsünde uzman donanım tasarımcısı ve iletişim güvenliği analisti olarak çalışan Dr. Çiçek, 2015-2017 yılları arasında Kaliforniya Üniversitesi, Santa Barbara kampüsünde doktora sonrası araştırmacı olarak bulundu. 2017-2020 yılları arasında İstanbul Şehir Üniversitesi Tümleşik Devreler Laboratuvarının direktörlüğü görevini yürüttü. 2020 yılında İstinye Üniversitesi'nde Elektrik-Elektronik Mühendisliği Bölüm başkanlığı görevini üstlenen Dr. Çiçek, kurduğu Dijital Sistemler Laboratuvarı çatısı altında araştırmalarına devam etmektedir. Araştırma ilgi alanları, güvenli gömülü sistem tasarımı, rastsal sayı üreteçleri, yeniden yapılandırılabilir analog ve sayısal tümleşik devreler olarak özetlenebilir. Dr. Çiçek, Journal of Cryptographic Engineering, IEEE Transactions on Circuits and Systems I/II, IEEE Transactions on VLSI, Integration-The VLSI Journal, IET Electronic Letters, International Journal of Bifurcation and Chaos, Turkish Journal of Electrical Engineering and Computer Science gibi ulusal ve uluslararası bilimsel dergilerde ve IEEE ISCAS, IEEE NEWCAS, IEEE ECCTD, IEEE SMACD, IEEE SİU gibi bilimsel konferanslarda uzmanlık alanlarında hakemlik ve yazarlık yapmaktadır.

Murat Cenk

Doç. Dr. Murat Cenk ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi programı öğretim üyesidir. Doktorasini ODTÜ'de 2009 yılında yaptıktan sonra 2010 - 2014 yılları arasında Waterloo Universitesi Elektrik ve Bilgisayar Mühendisligi bölümünde kriptografik algoritmaların verimli gerçekleştirilmesi üzerine doktora sonrası araştırmalar yapmıştır. Araştırma konuları yüksek hızlı kriptografi, kriptografik protokoller, kuantum sonrası kriptografi ve uygulamalı kriptografidir.

N. Gamze Orhon Kılıç

N. Gamze Orhon Kılıç 2014 yılında Yaşar Üniversitesi Yazılım Mühendisliği bölümünden mezun olmuştur. 2017 yılında Yaşar Üniversitesi Bilgisayar Mühendisliği bölümünden yüksek lisans derecesi almış ve yüksek lisans eğitimi süresince iki farklı özel şirkette yazılım mühendisi olarak görev yapmıştır. 2019 yılında TOBB Ekonomi ve Teknoloji Üniversitesi Mühendislik Fakültesi bünyesinde öğretim görevlisi olarak görev almış ve mühendislik öğrencileri için programlamaya giriş dersinin koordinatörlüğünü yürütmüştür. Lisans ve yüksek lisans eğitiminde eliptik eğri kriptografinin verimli uygulamaları üzerine çalışan Orhon Kılıç, 2019 yılında Orta Doğu Teknik Üniversitesi Kriptografi programında doktora eğitimine başlamıştır. ODTÜ Kuantum Sonrası Kriptografi Araştırma Grubu çatısı altında kuantum sonrası kriptografi, eliptik eğri kriptografi ve kriptografik protokoller üzerine akademik çalışmalar sürdürmektedir.

Linkedin: https://www.linkedin.com/in/ngorhon/

Google Scholar: https://scholar.google.com/citations?user=WRzFiugAAAAJ&hl=en

E-posta: gamze.kilic@metu.edu.tr

Arş. Gör. Burcu Ecem Karakaş

Orta Doğu Teknik Üniversitesi,
Uygulamalı Matematik Enstitüsü, Kriptografi Bölümü

TOBB Ekonomi ve Teknoloji Üniversitesi, Matematik Bölümü'nden 2016 yılında lisans, 2019 yılında yüksek lisans derecelerini almasını müteakiben Orta Doğu Teknik Üniversitesi Kriptografi programında doktora öğrenimine başlamıştır. Kriptografi bölümünde araştırma görevlisi olarak çalışmalarına devam etmektedir. Yüksek Lisans süresince kod tabanlı kuantum sonrası algoritmalar üzerine çalışmış olup doktorada ise kaynak kısıtlı cihazlar için verimli kriptografik protokollerin geliştirilmesi üzerine çalışmaktadır.

E-posta: burcu.yilmaz@metu.edu.tr

Dr. Ceren GÜZEL Turhan

Gazi Üniversitesi Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü Araştırma Görevlisi Dr, Ankara.

Ankara doğumlu olan Turhan, 2011 yılında Çankaya Üniversitesi Bilgisayar Mühendisliği Bölümünde lisans, 2014 yılında Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalında yüksek lisansını tamamlamıştır. 2020 yılında ise Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalından Doktora derecesini kazanmıştır. Yüksek lisans çalışmalarında Örüntü Tanıma ve Biyometrik Sistemler üzerine araştırmalar yapan Turhan, doktora süresince Derin Öğrenme Bilgisayarlı Görü uygulamaları konularında çalışmalar gerçekleştirmiştir. Üretici Derin Ağlar ile nesne oluşturma, görüntü oluşturma, nesne tespiti ve görüntü başlıklandırma konularında çalışmalarına devam etmektedir. Doktora sonrasında, bölümünde Bilgisayarlı Görü, Veri Madenciliği gibi lisans derslerini vermiştir.

Dr. Öğr. Üyesi Eyüp Burak Ceyhan

Bartın Üniversitesi Mühendislik Mimarlık ve Tasarım Fakültesi
Bilgisayar Mühendisliği Bölümü, ebceyhan@bartin.edu.tr

Dr. Eyüp Burak CEYHAN, Yapay Zeka, Biyometrik Sistemler, Siber Güvenlik ve Büyük Veri alanlarında çalışmalar yapmaktadır.

Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü'nde danışmanı Prof. Dr. Şeref Sağıroğlu ile tamamladığı yüksek lisans ve doktora tezlerinden ürettiği zeki sistemler ile Türkiye, Amerika ve Avrupa'ya yaptığı patent başvuruları sonucunda bu sistemlerin patentini alarak güvenlik alanında önemli olan sistemleri Türkiye'ye kazandırmıştır.

Dr. Ceyhan, lisans, yüksek lisans ve doktora derecelerini Bilgisayar Mühendisliği alanlarında almıştır. 2011-2016 yılları arasında Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü'nde araştırma görevlisi olarak görev yapmış, 2016 yılından itibaren halen çalışmakta olduğu Bartın Üniversitesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır. 2016-2020 arasında Bölüm Başkanlığı görevini yürütmüş, 2021 yılından itibaren ise Dekan Yardımcılığı görevini yürütmektedir. Bartın Üniversitesi'nde Akıllı Lojistik Sistemler Laboratuvarı ve Siber Güvenlik ve Biyometri Laboratuvarlarında yönetici olarak çalışmaktadır. Yine Bartın Üniversitesi Proje Teknoloji Ofisi'nde Patent Koordinatörü olarak görev yapmaktadır. Bartın Kamu-Üniversite-Sanayi İşbirliği (KÜSİ) Temsilcisi olarak Sanayi ve Teknoloji Bakanlığı'nda görev almıştır.

Doktora eğitiminden sonra 12 ay boyunca Amerika'da, TÜBİTAK 2219 Yurt Dışı Doktora Sonrası Araştırma Burs Programı desteği ile University of Miami'de biyometrik güvenlik sistemleri alanında çalışmalarına devam etmiştir.

Çoğu biyometrik sistemler, bilgi güvenliği, yapay zeka, veri madenciliği konularında olmak üzere 30'un üzerinde ulusal ve uluslararası indeksli dergilerde yayınlanan makaleleri ve uluslararası konferanslarda sunduğu bildirileri bulunmaktadır. Ayrıca TÜBİTAK, Ankara Kalkınma Ajansı, Gazi Üniversitesi ve Bartın Üniversitesi destekli ulusal projelerde de proje yürütücüsü ve araştırmacı olarak çok sayıda projede yer almıştır. Uluslararası düzenlenen 18 konferansta düzenleme kurulu üyesi olarak görev almıştır. 30'un üzerinde uluslararası konferansta bilim kurulu üyeliği ve çeşitli SCI dergilerde hakemlik de yapmıştır. DERGİPARK'a kayıtlı 1 dergide editörlük ve çok sayıda dergide de hakemlik yapmaktadır.

Yıldız Teknik Üniversitesi'nde IEEE destekli düzenlenen İş Fikri Yarışması'na sunduğu proje 1.lik ödülü almış ve 7.000TL para ödülü kazanmıştır. Ayrıca Gazi Üniversitesi Bilim Şenliği Proje Yarışması'nda 1.lik, 2. İş Fikri Yarışması'nda mansiyon, 3. Endüstri ve Teknoloji Tezleri Yarışması'nda Teşvik Ödülleri elde etmiş ve sırasıyla 10.000TL, 5.000TL ve 1.000TL para ödülleri kazanmıştır.

Çeşitli kamu ve özel sektör kurum ve kuruluşlarına biyometrik sistemler, siber güvenlik, mobil güvenlik, bilgi güvenliği eğitimleri ve danışmanlık hizmeti de vermektedir.

Siber Güvenlik ve Savunma

SİBER GÜVENLİK ONTOLOJİSİ, TEHDİTLER VE ÇÖZÜMLER

Editörler
Prof. Dr. Şeref Sağıroğlu
Doç. Dr. Sedat Akleylek

Siber güvenlik ve savunma konularında çalışmalarına uzun yıllardır devam eden ve akademik katkı sağlayan bu kitap serisinin editörleri, hazırladıkları seriyle; sahip olunan ulusal bilgi birikiminin bir çatı altında toplanması, Türkçe içerik üretilmesi, yeni çözümler geliştirmesinde ihtiyaç duyulan nitelikli bilgi konusunda kaynak oluşturulması, bilginin kolaylıkla yaygınlaştırılması ve topluma açık kaynak olarak aktarılması, başta kamuoyu farkındalığının artırılması olmak üzere siber ortamlarda bilgi güvenliğinin kişisel, kurumsal ve ulusal boyutta sağlanması hususlarına katkı sunmayı amaçlamışlardır.

Tehditlerin ve çeşitlerinin artması, boyut ve yön değiştirmesi, siber tehdit skalasının büyümesi, kritik altyapıların hedef hâline gelmesi, bilgi hırsızlığının çoğalması, yeraltında çalışan korsanların etkinleşmesi, siber tehditlerin artık savaşa dönüşmesi, siber suçların ve suçluların çoğalması, siber terörün artması nedenleriyle siber saldırılarla, suçlarla, terörizmle, zafiyetlerle mücadeleye her zamankinden daha fazla ihtiyaç duyulmaktadır. Kapsamlı bir mücadele için ulusal stratejilerin ve eylem planlarının hayata geçirilmesi, etkili araştırma merkezlerinin ve üniversitelerde yeni programların açılması, yeni altyapılar kurulması, mükemmeliyet merkezi kurulumu, ulusal siber olaylara müdahale çalışmaları büyük önem arz etmektedir.

Tehditlerin boyutlarını, risklerini ve gelecekte verebilecekleri zararlarını daha iyi anlamak ancak ve ancak bu alanın kapsamını iyi anlamak, gelecekte karşılaşılacak olan tehditleri öngörmek ve önlem almak, buna hazır olmak için konunun etkileşim içerisinde olduğu tüm alanları iyi bilmek, etkileşim içerisinde olan alanları iyi tanımak, yeni alanlarda çalışmalar yapmak ve riskleri ortadan kaldıracak çözümler geliştirmekle mümkündür.

Siber güvenlik ve savunma konularını kapsamlı bir bakış açısıyla sunan Siber Güvenlik ve Savunma Kitap Serisi'nin "Siber Güvenlik Ontolojisi, Tehditler ve Çözümler" isimli bu 6. kitabının; ele aldığı on iki farklı konuyla yerli ve millî teknolojiler üretilmesine katkı sağlaması beklenmektedir.

nobel AKADEMİK YAYINCILIK

ISBN 978-625-417-877-1