TÜRK BİLİM ARAŞTIRMA VAKFI
TÜBAV
1995
TURKISH SCIENCE-RESEARCH FOUNDATION
TUBAV BILIM DERGISI

Yıl: 2017, Cilt:10, Sayı:2, Sayfa: 27-42

BİLGİ SİSTEMLERİNDE GÜNCEL GÜVENLİK PROBLEMLERİ VE ÖNERİLEN ÇÖZÜMLER

Ecem İREN[1], Özgü CAN[2]

[1]Ege Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, ecem.iren@gmail.com
[2]Ege Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, ozgucan@gmail.com

Özet

Günümüzde hizmet veren bilgi tabanlı sistemlerin birçoğunda güvenliği sağlamak önemli ve zor bir problem olmaktadır. Özellikle veritabanı yönetim sistemleri, hareketli araç ağları, bulut bilişim, nesnelerin interneti gibi alanlarda bilgi güvenliğinin temel ilkeleri olan gizlilik, bütünlük ve kullanılabilirlik kavramları oldukça büyük bir önem arz etmektedir. Sistemlerin sağlıklı bir şekilde işleyebilmesi ve kullanıcılarına eksiksiz hizmet verebilmesi açısından bu kavramların korunması gerekmektedir. Bu makalede söz konusu sistemler tanıtılmış ve bu sistemlere karşı oluşabilecek güvenlik saldırılarından bahsedilmektedir. Ayrıca, her sistemin güvenlik problemleri belirtildikten sonra problemlere ilişkin bazı çözüm tekniklerine yer verilmektedir. Ek olarak, internet kullanıcılarının genellikle maruz kaldığı tehditler ve bu tehditlere yönelik çözüm önerileri de anlatılmaktadır. Son bölümde ise insanlara yönelik tehditleri ile sistemlerde meydana gelen tehditler karşılaştırılıp bu konuda bilinçlendirme faaliyetlerinin yapılması gerektiği vurgulanmıştır.

Anahtar Kelimeler: Bilgi güvenliği, araç ad hoc ağları, bulut bilişim, veritabanı yönetim sistemleri, nesnelerin interneti, güvenlik tehditleri, bilgi güvenliği farkındalığı.

CURRENT SECURITY PROBLEMS AND PROPOSED SOLUTIONS IN INFORMATION SYSTEMS

Abstract

Today, maintaining security in information systems that provide several services has become a difficult and significant problem. Confidentiality, integrity and availability that are the basic principals in information security represent a great importance especially in areas such as database management systems, vehicular ad hoc networks (VANETs), cloud computing and internet of things. These concepts must be protected for systems in order to function properly and give complete services to users of the systems. In this article, these systems are introduced and security threats that may occur against these systems are mentioned. Also, after defining security threats associated with each system, security solutions related with these threats are given. In addition to them, the threats which the users of Internet are usually exposed to are explained and some solutions are advised preventing from them. In the last part, the threats to people are compared with the ones for the systems and it is stressed that awareness activities should be done in this context.

Keywords: Information security, vehicular ad hoc networks, cloud computing, database management systems, internet of things, security threats, information security awareness.

1. Giriş

Bilgi sistemleri, bilgi teknolojileri ve kullanıcıların etkileşim içerisinde bulundukları yönetimsel ve karar destek sistemleridir. Günümüzde bilgi teknolojileri alanında ortaya çıkan yenilikler, insanların bilgi sistemleriyle daha çok ilgilenmesini sağlamaktadır. Ancak, bu yeniliklerin yanı sıra sistemlerin getirdiği bazı tehlikeler de mevcuttur. Bilgi teknolojilerinin kökeninde insan olduğundan, bilgi sistemleriyle alakalı tehdit ve risklerin büyük çoğunluğu gerek bilinçli gerekse ihmal sonucu olarak yine insan kaynaklı olarak doğmaktadır. Bu tehditler; sistemleri bozma, sistemi etkisiz kılma, sisteme sızma, bilgiye izinsiz erişme, bilgi çalma veya menfaatleri uğruna bilgiyi kötüye kullanma gibi eylemler olarak sayılmaktadır. Tehdit ve risklerle başa çıkabilmek için bilgi güvenliği kavramının organizasyonlarda sürdürülmesi gerekmektedir. Bilgi güvenliğiyle ilişkili olan gizlilik ve bilgisayar güvenliği kavramları, bilgisayar sistemleri ve uygulamalarıyla ilişkili problemler olarak tanımlanmaktadır. Gizliliği sağlayan bir sistem, kullanıcılarına kendi bilgilerinin nasıl, ne amaçla ve kim tarafından kullanılıyor ve saklanıyor olduğunu kontrol etme

olanağı vermektedir [1, 2]. Bilgisayar güvenliği ise veriye yetkisiz erişim, verinin değiştirilmesi, verinin yayılması gibi eylemlere karşı uygulanacak önlemleri içermektedir. Kullanıcı verilerini işleyen ve pek çok kullanıcıya hizmet sağlayan tüm bilgi tabanlı sistemlerde yetkisiz erişim veya veri bütünlüğü bozulmasına karşı güvenlik önlemleri alınmalıdır. Bilgi güvenliği, kuruluşun sürekliliğinin sağlanmasında büyük rol oynamakta ve kuruluşun bilgi varlıklarının korunmasını sağlamaktadır. Özetle, sistemlerin sağlıklı bir şekilde işleyebilmesi ve kullanıcılarına eksiksiz hizmet verebilmesi açısından gizlilik, bütünlük ve kullanılabilirlik kavramlarının korunması gerekmektedir.

Gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması ya da bilginin yetkisiz kişilerce ifşa edilmesinin engellenmesidir. Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi ve silinmesi gibi eylemlere karşı içeriğinin korunmasıdır. Kullanılabilirlik, bilginin ihtiyaç duyulduğu anda kullanıma hazır durumda olması anlamına gelmektedir. Günümüzde hizmet veren bilgi tabanlı sistemlerin birçoğunda güvenliği sağlamak önemli ve zor bir problem olmaktadır. Bu problem genel anlamıyla tam olarak çözülememiştir [1, 2]. Bilgi ve bilgi teknolojileri güvenliğine ilişkin bu problemlerin üstesinden gelmek için her kurum kendi yapısı çerçevesinde birtakım çözüm metodolojileri benimsemeli ve buna uygun uygulamaları seçmeli ya da kendisi geliştirmelidir.

Bilgi güvenliği alanında söz konusu problemleri çözebilmek için çeşitli çalışmalar yapılmış ve hala da yapılmaya devam edilmektedir. Her bir çalışmada sistemlere ilişkin farklı teknikler ortaya atılmaktadır. Bu çalışmada, güncel sistemler tanıtılmakta ve bu sistemlere karşı oluşabilecek güvenlik tehditlerinden bahsedilmektedir. Ayrıca, saldırıları önlemek ve azaltmak için geliştirilen ve tavsiye edilen uygulamalar tanıtılmaktadır. Bu çalışmanın ikinci bölümünde hareketli araç ağları, üçüncü bölümünde bulut bilişim, dördüncü bölümünde veri tabanı yönetim sistemleri, beşinci bölümünde ise nesnelerin interneti özetlenmektedir. Altıncı bölümde ise önceki bölümlerden farklı olarak günlük hayatta İnternet kullanıcılarının karşılaştığı sorunlar ele alınmaktadır. Her bölüm içerisinde mevcut sistemlere yönelik olası güvenlik tehditleri ve bu tehditleri için alınacak güvenlik önlemleri açıklanmaktadır. Sonuç bölümünde ise yapılan çalışmanın özeti ve önemine yer verilmektedir. Bunun yanında, insanların maruz kaldığı tehditler ile sistemlerde oluşan tehlikeler karşılaştırılıp bu bağlamda yapılacak olan bilinçlendirme faaliyetlerinin önemi vurgulanmaktadır.

2. Araç Ad Hoc Ağları (Vehicular Ad Hoc Networks-VANETs)

Bu bölümde; öncelikle hareketli araç ağları tanıtılmakta, ardından da sisteme ilişkin güvenlik tehditlerine yer verilmektedir. Son olarak da güvenlik tehditlerine karşı alınabilecek güvenlik önlemleri listelenmektedir.

2.1 Araç Ad Hoc Ağları Yapısı

Günümüzde karayolundaki yoğun trafik hacmi, trafik ortamının güvenliğini ve verimliliğini etkilemektedir. Karayolu trafiğinin güvenliği trafik yönetiminde de zorlu bir konu olmuştur. Bilgi akışının sağlanması için gerekli olan trafik bilgisi araçlara iletilmekte ve böylece araçlar bu bilgiyi trafik ortamını analiz etmede kullanmaktadırlar. Bu akış, trafik ortamına ilişkin bilginin araçlar arasında paylaşılması ile elde edilmektedir. Tüm araçlar hareketli olduğundan bu yapının gerçekleştirilmesi, kendi kendini organize eden ve altyapı desteği olmadan çalışabilen mobil bir ağa dayanmaktadır. Mikro-elektroniğin gelişmesiyle birlikte düğüm ve ağ cihazını tek bir birime entegre edip kablosuz ağ iletişimini uygulamak artık mümkündür. Bu ağ hareketli *ad hoc ağı* olarak gelişmiştir. Gezgin Ad Hoc ağlar, sabit bir altyapı gerektirmeyen, ortam koşullarına hızla ve ön hazırlıksız kendi kendini uyarlayarak hizmet ettiği uç birimler arasında iletişimi sağlayan dinamik varlıklardır [3, 4]. VANET, hareketli ad hoc ağın bir uygulamasıdır. Sürüş güvenliğini arttırmak ve trafik yönetimini geliştirmek amacıyla internet erişimi ile araçları birbirine bağlamaktadır. VANET sisteminin iki tipi vardır. Birincisi, hiçbir altyapı olmadan araçlar arasında saf kablosuz bir ad hoc ağ, ikincisi ise sabit bir altyapı gerektiren ve yol birimleri ile araçlar arasında iletişimi kuran bir ad hoc ağdır. Bu ağda düğüm olarak adlandırılan her bir araç, yönetim ve uygulama olarak nitelendirilen iki çeşit birim ile donatılmıştır. Yönetim birimi haberleşme yeteneğine sahipken uygulama birimi yönetim biriminin çalışmasından sorumludur [3]. Trafik güvenliğini sağlamak amacıyla pek çok uygulama VANET tarafından gerçekleştirilmektedir. Bu tür uygulamalarda ağ üzerinden değiştirilen mesajların farklı bir yapısı ve amacı vardır. Bu durum dikkate alınarak VANET'te aşağıdaki haberleşme yöntemleri tanımlanmıştır:

1. ***Araçlar Arası Uyarı Mesajları (Vehicle to Vehicle Warning Propogation):*** Belirli bir araç veya araç grubuna mesaj göndermenin gerekli olduğu durumlar oluşmaktadır. Örneğin; bir kaza tespit edildiğinde trafik güvenliğini arttırmak için yeni gelecek olan araçlara bir uyarı mesajı gönderilmelidir. Öte yandan, acil bir kamu aracı (ambulans gibi) geliyorsa aracın önünde bulunan diğer araçlara da bir uyarı mesajı iletilmelidir. Bu şekilde acil kamu aracının ilerlemesi daha kolay olacaktır. Her iki durumda da mesajın

iletilebilmesi için yönlendirme protokolüne ihtiyaç duyulmaktadır.

2. ***Araçlar Arası Grup Haberleşmeleri (Vehicle to Vehicle Group Communication):*** Bu yöntem kapsamında, sadece belirli özelliklere sahip araçlar haberleşmeye katılmaktadırlar. Bu özellikler statik veya dinamik olarak nitelendirilmektedir. Aynı işletmeye sahip olan araçların bir grupta toplanması statik takıma örnektir. Herhangi bir zaman aralığında aynı bölgede bulunan araçların bir grup oluşturması ise dinamik takıma örnek teşkil eder.
3. ***Araçlar Arası Sinyal Mesajları (Vehicle to Vehicle Beaconing):*** Sinyal mesajları, periyodik olarak yakındaki araçlara gönderilen mesajlardır. Bu mesajlar, mesajı gönderen araca ait mevcut hız, frenleme ve güzergâh gibi bilgileri içermektedir. Sinyal mesajları komşu farkındalığını arttırmak adına faydalı olmaktadır. Mesajlar sadece bir yandaki araca gönderilip daha sonra diğer araçlara iletilmemektedir. Sinyaller, mesajı yönlendirmede araçlara en iyi komşuyu seçmelerine izin verdiklerinden yönlendirme protokollerine de yardımcı olurlar [5].

2.2 Araç Ad Hoc Ağlarına Yönelik Güvenlik Tehditleri

VANET üzerinde yer değiştiren veri, trafik güvenliğinde büyük rol oynamaktadır. Örneğin; 2007 yılında yapılmış olan eCall projesinde bir ambulansın sensörlerine uygulanan acil bir çağrı ile araç bir kaza geldiğini anlamıştır. İnsan yaşamı bu uygulamaya bağlı olduğundan, bilginin kesin ve doğru olması gerekmektedir. Bunun yanı sıra, sürücülerin gizli bilgileri korunmalı ve bu nedenle araç yetkisiz kişiler tarafından kolayca izlenmemelidir [5]. Bu ağda meydana gelebilecek temel tehditler aşağıda listelenmektedir:

- ***Doğrulama ve tanımlamaya yönelik saldırılar***: Saldırgan, ağda bulunan bir sürücünün kimliğini çalarak sürücüymüş gibi davranır. Bunun sonucunda, diğer sürücülere sanki kimliği çalınan sürücüden mesaj geliyor gibi yanlış uyarılar gider.
- ***Gizliliğe yönelik saldırılar***: Araçlar hakkındaki hassas bilginin ele geçirilmesine yönelik tehditler olarak da nitelendirilmektedir. Sürücü ile araç arasında bir ilişki olduğundan, aracın durumu hakkında bilgi edinilmesi sürücünün gizliliğini de etkileyecektir.
    - *Kimliğin açığa çıkarılması:* Belirli bir aracın sürücüsüne ait kişisel bilgilerin açığa çıkarılmasıdır.
    - *Konum bilgisine erişme:* Aracın belirli bir zamanda konumuna veya izlediği güzergâha erişmek yine kişisel bilgilere müdahale etme ile eşdeğerdir.

  VANET üzerindeki dinleme saldırıları da (eavesdropping) gizliliği ihlal eden saldırılardır. Bu saldırıların amacı, gizli veriye ulaşmaktır. Grup haberleşmelerinde gizliliğe ihtiyaç duyulduğundan verinin korunması için gereken mekanizmaların kurulması gerekmektedir.
- ***Veri bütünlüğüne yönelik saldırılar:*** Verinin bütünlüğü birçok şekilde tehlikeye girmektedir. Verinin yanlış hesaplanması ve gönderilmesi mesajın güvenilirliğini azaltmaktadır. Bu olay, araca ait sensör ayarlarının veya gönderilen mesajın değiştirilmesiyle tatbik edilebilmektedir. Örneğin, herhangi bir kaza durumunda kaza yerine ait bilgi değiştirilirse veya kaza olmadığında kaza varmış gibi gösterilip yanlış bir alarm verilirse sistemin güvenilirliği olumsuz yönde etkilenecektir [5, 6].
- ***Kullanılabilirliğe yönelik saldırılar:*** VANET içinde, haberleşme kanallarının ve haberleşen düğümlerin kullanılabilirliği sağlanmalıdır. Kullanılabilirliğe yönelik saldırılar, iletişim kanallarında tıkanıklığa yol açarak kanalları kullanılamaz hale getirmektedir. Araca belirli bir süre içinde çok sayıda sinyal gönderilerek saldırı gerçekleştirilir. Bu problem, kritik bilginin araçlara ulaşmasını engeller. Bu durum uygulamayı kullanılamaz hale getirmekle beraber aynı zamanda sürücü uygulama bilgisini kullandığı için hayati tehlikesini de arttırır. Örneğin; iyi niyetli olmayan bir kişi büyük bir zincirleme kaza oluşturmak isteyebilir. Bir kaza durumunda ağa hizmet reddi saldırısı uygulayarak olay yerine yaklaşan araçlara yavaşlama uyarısı bilgisini içeren sinyalin ulaşmasını engeller.

2.3 Araç Ad Hoc Ağlarına Yönelik Güvenlik Tehditlerine Yönelik Çözümler

Ad hoc ağlar için güvenli bir yönlendirme protokolü olarak tanımlanmış olan ARAN (Authenticated Routing Ad Hoc Network)**,** bilgi sızdırılmasına ilişkin saldırıları önleme amaçlı olarak geliştirilmiştir [7]. Bu protokol, AODV (Ad hoc On-Demand Distance Vector Routing) yönlendirme sistemine bağlıdır. AODV, hareketli bilgisayarlar arasındaki mesajların yönlendirilmesine yardımcı olmakta ve ağdaki bilgisayarlara ya da düğümlere komşuları aracılığıyla, asıl iletişim kurmak istedikleri düğümlere mesajları iletme olanağı vermektedir. AODV, mesajların hangi yollar boyunca gidebileceğini keşfederek bu işlemi yapmaktadır. Aynı zamanda; AODV, döngüler içermeyen ve en kısa yolu barındıran yönlendirmeyi bulmaya çalışmaktadır. AODV, yollarda meydana gelen değişiklikleri yönetmekte ve herhangi bir hata durumunda yönlendirme için yeni yollar yaratmaktadır. ARAN, araçsal takip

sisteminde taklit ve yanlış uyarma gibi saldırıları kontrol etmektedir [7, 8]. Açık anahtar şifrelemeyi kullanan ARAN, ağdaki tüm düğümler tarafından açık anahtarı bilinen bir sunucuya ihtiyaç duymaktadır. Kaynak düğüm, tüm komşu düğümlere rota keşif paketi (RDP) yollar. Her bir komşu düğüm, kaynak düğümden gelen şifreli mesajı kaydedip imzalayarak bir sonraki komşu düğümüne iletmektedir. Hedef düğüm ise mesajı aldığında kaynak düğümü cevaplamak amacıyla kendisine mesajı ileten ilk düğüme cevap göndermektedir [7]. Başka bir deyişle ARAN, mesaj doğrulamayı ve mesaj bütünlüğünü korumayı amaçlamaktadır. Bu ağda, düğümlere sertifika dağıtan bir sunucu bulunmaktadır. İletişim boyunca her bir düğüm, bir önceki düğümden gelen mesajın imzasını doğrulamaktadır. ARAN, güvenlik ve rotaların keşfi açısından AODV'ye oranla daha iyi bir performans sağlamasına rağmen yüksek paket ve işlemci yükü gibi problemleri vardır [9].

Doğrulama ve tanımlamaya yönelik bir çözüm sunan SPAAR (Secure Position Aided Ad Hoc Routing), yönlendirmede pozisyon bilgisini kullanmaktadır. Mesaj gizliliği ve bütünlüğü için asimetrik anahtar şifrelemeyi esas almaktadır. Bu kapsamda ARAN'da olduğu gibi, düğümlere sertifika dağıtan bir otorite bulunmaktadır. Protokolün temel amacı, kötü niyetli düğümleri algılayıp tanımaktır. SLPS gibi yine ortalama paket ve yüksek işlemci yüküne sahiptir. SLOSR [10], OLSR (Optimized Link State Routing Protocol) protokolünün geliştirilmiş halidir [11]. Paketler için doğrulama yapan ve ağı tekrarlı gönderme saldırılarından koruyan bir sistemdir. Düğümleri korumak için HMAC (Hash Message Authentication Code) kodlarını kullanmaktadır. Küçük ağlar için uygundur ve işlem yükünü hafifleten simetrik şifrelemeyi kullanmaktadır. CONFIDANT protokolünün amacı ise kötü niyetleri düğümleri tespit ederek onları rota keşif evresinin dışında tutmaktır [9].

SLPS (Secure Link State Routing), gizliliğe yönelik bir çözüm sunmaktadır. Bağlantı durum bilgisini koruyan, ağ topolojisinin keşfini ve bağlantı bilgisinin dağıtılmasını önleyen bir protokoldür. Protokolün altında yatan güvenlik mekanizmasını sertifika otoritesi oluşturmaktadır. Bu otorite, maskeleme saldırılarını kontrol ederek saldırganlarla başa çıkmaktadır. Yüksek ölçeklenebilirliğe sahip olduğundan büyük ağlar için uygun olan bu protokol, ortalama paket ve yüksek işlemci yüküne sahiptir [9].

Kullanılabilirliğe yönelik bir çözüm olarak önerilen ARIADNE [12], DSR (Dynamic Source Routing)'in uzantısı olarak geliştirilmiştir ve simetrik anahtar şifrelemeyi kullanmaktadır. Bu protokol, yönlendirmede TESLA güvenlik şemasını esas almaktadır. Bu şema, düğümlerin doğrulanmasında HMAC yapısını kullanmaktadır. Servisin reddi (Denial of Service) olarak nitelendirilen saldırıları önlemeye çalışan bu protokol, düşük paket ve işlemci yüküne sahiptir [9, 12].

Saldırganların düğümler üzerinde yanlış yönlendirmeler oluşturmalarını engellemeye çalışan SEAD (Secure and Efficient Ad Hoc Distance Vector) protokolü [13], DSDV (Destination Sequenced Distance Vector) yönlendirmeye bağlı olarak çalışmaktadır. DSDV, bilinen yönlendirme protokolünden uyarlanmıştır. Ek olarak, yönlendirme tablosunun her bir satırına sıra numarası eklenmiştir. Bu yeni eklenen özellik sayesinde, hareketli düğüm eski yönlendirme bilgisini yenisinden ayırt edip yönlendirme döngülerinin oluşmasını engellemektedir [14]. SEAD, doğrulama işlemini gerçekleştirmek için maliyetli şifreleme algoritmaları yerine tek yönlü hash fonksiyonunu kullanmaktadır. Bu durumda, güvenlik mekanizmasının temelini hash zincirleri ve sıra numaraları oluşturmaktadır. SEAD, ağda tıkanıklık yaratan yüksek paket yüküne sahiptir. Ancak, asimetrik anahtar şifrelemesi kullanmadığından daha az kaynak tüketmektedir. SEAD, işlemci yeteneği düşük düğümü desteklemekle birlikte; düğümü, saldırganların bant genişliğini tüketme girişiminde bulundukları servisin reddi saldırılarından da korumaktadır [3, 9, 13].

3. Bulut Bilişim

Bu bölümde öncelikle bulut bilişim hakkında bilgi verilmekte, daha sonra sisteme ilişkin güvenlik tehditlerine yer verilmekte ve bulut bilişime yönelik güvenlik tehditlerine karşı alınabilecek önlemler listelenmektedir.

3.1 Bulut Bilişim Yapısı

Bulut bilişim günümüzde birçok bilgisayar kullanıcısının ilgisini çeken bir teknolojidir. Bu kullanıcıların arasında; bireysel kullanıcılar, büyük ve küçük ölçekli işletmeler bulunmaktadır. Bulut bilişim internet üzerinden herkesin erişebileceği bilgisayar hizmetleri sağlamaktadır. Bu teknolojiyle birlikte, kuruluşların bilgisayar ve internet hizmetlerini destekleyecek fiziksel donanımlara ya da sunuculara ihtiyaçları kalmamaktadır. Böylelikle, teknolojinin kullanımıyla bilgisayar sistemlerinin bakımı için ayrılan şirket giderleri de azalmaktadır. Bulut bilişim, kullanıcıların ihtiyaçlarını karşılamak amacıyla Servis Tabanlı Mimariler (SOA), Web 2.0 ve sanallaştırma gibi birçok teknolojiyi

bir araya getirerek web sunucuları sayesinde iş uygulamaları gerçekleştirmektedir. Bulut bilişim yapısının temel amacı; güvenli, hızlı ve uygun veri depolama birimleri ile kullanıcılarına hizmet etmektir. Bulut, artan talebe göre çevikliği, ölçeklenebilirliği ve kullanılabilirliği arttırmaktadır. Bulut bilişimin önerdiği avantajların yanı sıra, kullanıcılara güvenlik ve verimlilik konusunda endişe veren güvenlik problemleri de bulunmaktadır [15, 16].

Bulut bilişim; altyapı, platform ve yazılım hizmetlerinin verildiği üç katmandan oluşmaktadır. Alt katman; sunucu, ağ cihazları, bellek ve depolama birimlerinin altyapılarını sağlamada ihtiyaç duyulan kaynakları içermektedir. Aynı zamanda *Servis olarak Altyapı (Infrastructure as a Service-IaaS)* olarak bilinmektedir. Sanallaştırma teknolojisiyle, IaaS, müşterilerine karmaşık ağ altyapıları oluşturma olanağı tanımaktadır. Bu yaklaşım sadece fiziksel donanım satın almanın maliyetini hafifletmekle kalmayıp, ağ yönetiminin yükünü de hafifletmektedir. Böylelikle, fiziksel donanım kullanılmadığından, bunları izlemekle zorunlu yetkin kişilere de ihtiyaç kalmamaktadır. Bu katmana bir örnek olan Amazon EC2 [17], web hizmet ara yüzleriyle sanal bir hesaplama ortamı yaratmaktadır. Platform katmanı olan orta katman *Servis olarak Platform (Platform as a Service-PaaS)* olarak bilinmektedir. Kullanıcılara kendi özel uygulamalarını geliştirme olanağı sağlayan PaaS, içerdiği kütüphaneler sayesinde kullanıcıların uygulamaların yapılandırma ayarlarını kontrol etmelerini sağlamaktadır. Bu katman, yazılım geliştirme aracı satın almayı ortadan kaldırdığı için kullanıcı maliyetini de hafifletmektedir [18]. Google App Engine [19] ve Windows Azure [20], bu modele örnek olarak verilebilmektedir. Uygulama katmanı olan üst katman *Servis olarak Yazılım (Software as a Service-SaaS)* olarak adlandırılmaktadır. SaaS, uygulamaları satın almak yerine bulut üzerinde çalışan uygulamaları kiralama olanağı vermektedir. Maliyeti düşürdüğü için; e-posta, üretkenlik uygulamaları, müşteri ilişkileri yönetimi (CRM), kurumsal kaynak planlama (ERP) ve belge yönetimi gibi kurumsal kullanımlar için popüler bir duruma gelmiştir. Atlassian [21], SalesForce [22], Lucidchart [23] ve Gliffy [24] bu katmanda hizmet veren firma örnekleri olarak verilebilir.

3.2 Bulut Bilişime Yönelik Güvenlik Tehditleri

Bulut bilişim teknolojisinde meydana gelebilecek tehditler aşağıda sınıflandırılmaktadır:

- ***Servisin reddi saldırıları:*** Bulut, birçok kullanıcı tarafından paylaşıldığı için servisin reddi saldırılarına karşı daha savunmasızdır. Bu nedenle, bu tip saldırılar çok daha yıkıcı sonuçlar doğurmaktadır. Servisin reddi saldırısında; saldırgan, sunucuya çok sayıda istek göndermekte ve sunucuyu diğer kullanıcılar için hizmet veremez bir duruma getirmektedir. Güvenliğin temel ilkesi olan kullanılabilirliğe zarar vermek amaçlanmıştır. Bulutta gerçekleşen servisin reddi saldırıları aşağıda gruplanmaktadır:
    - ***Hacim (Bant genişliği) tabanlı saldırılar (Volume based attacks):*** Saldırgan, hedef sunucuyu büyük miktarda önemsiz veri ile doldurmaya çalışmaktadır. Böylelikle, ağdaki bant genişliğini ve kaynakları tüketmektedir. UDP ve ICMP tabanlı saldırılar bu tür saldırıya örnektir.
    - ***Protokol saldırıları (Protocol attacks):*** Saldırgan**,** çeşitli ağ protokollerinin eksiklik veya zafiyetlerinden kaynaklanan güvenlik açıklarını kullanmaktadır**.** Ölüm Pingi (Ping of Death), Smurf, SYN ve parçalanmış paket saldırıları bu tür saldırıya örnektir.
- ***Uygulama katman saldırıları:*** Bu saldırı belirli web uygulamalarına odaklanmaktadır ve uygulamalara çok sayıda HTTP isteği göndermektedir. HTTP, XML ve REST tabanlı servisin reddi saldırıları bu grup içinde yer almaktadır.
- ***Doğrulamaya yönelik saldırılar:*** Kimlik doğrulama işlemi genellikle sanal hizmetlerde saldırganlarca zayıf nokta olarak görülmektedir. Doğrulama sürecini koruyan mekanizmalar saldırganların hedefi haline gelmiştir.
- ***Veri gizliliği ve bütünlüğüne yönelik saldırılar:*** Bu başlıktaki saldırılar aşağıda gibi gruplanmıştır:
    - ***Ortadaki adam saldırıları:*** Bu senaryoda saldırgan kendisini iki kullanıcı arasında konumlandırmaktadır. Saldırganın amacı, haberleşme esnasında akan veriyi değiştirmek veya önemli bilgiyi ele geçirmektir.
    - ***İş ortamı saldırıları:*** Sistem işleyişi hakkında bilgi sahibi olan ofis personelleri kendi menfaatleri doğrultusunda buluttaki bilgileri yok etmek için sistemde zararlı kodları çalıştırmaktadırlar.
    - ***Yan kanal saldırıları:*** Saldırgan, hedef bulut sunucusunun yakınına kötü niyetli bir sanal makine yerleştirip yan kanal saldırısı başlatır. Yan kanal saldırısında amaç, makine başarılı bir şekilde konumlandıktan sonra buluttan dosya veya evrak gibi gizli bilgilerin çekilmesidir. Güvenlik duvarı veya şifreleme yöntemleri kullanılarak bu saldırı önlenmektedir. Çünkü, saldırgan şifrelenmiş bilgiyi ele geçirse bile gizli anahtarı bilmediğinden şifreyi çözemeyecektir [16, 18, 25, 26].

3.3 Bulut Bilişim Güvenlik Tehditlerine Yönelik Çözümler

Bölüm 3.2'de bahsedilen saldırıları önlemek veya azaltmak amacıyla çeşitli çözüm yöntemlerine başvurulmuştur. Bu yöntemler aşağıda açıklanmaktadır:

- ***Veri gizliliği ve bütünlüğüne yönelik çözümler***
  - ***Veri bölmeye dayanan çözümler:*** Veriyi koruma amaçlı geliştirilen geleneksel yaklaşımların incelendiği [27] çalışmasında, verinin saklanması ve yedeğinin alınması tek bir sunucuda yapılmaktadır. Verinin değişmesi durumunda ise sunucuya erişim bir şifre aracılığıyla gerçekleşmektedir. Fakat, kullanıcılar arasında şifreyi basit ve hatırlanabilir şekilde oluşturma gibi bir eğilim vardır. Bu eğilim ise kaba kuvvet saldırısı olarak adlandırılan (brute-force attack) saldırısına neden olmaktadır. Bu nedenle, önerilen yaklaşımda, depolanan veri güvenliğini sağlamak amacıyla bir algoritma geliştirmiştir. Bu algoritmada veri, d_1,d_2, $d_{3.....}$,d_k şeklinde K parçaya ayrılır. Her bir veri parçası, S_1, S_2, $S_{3.....}$,S_m olarak parçalara ayrılmış farklı sunucularda saklanır. Böylelikle veriler farklı sunucularda saklandıklarından veri de korunmuş olmaktadır. [28] çalışmasında; verilerin güvenliği, gizlilik ve kullanılabilirliğin korunması yönünden incelenmiştir. Depoda bulunan veri birçok bulut sağlayıcısına bölünerek güvenlik sağlanmaya çalışılmıştır. Bu öneri, verinin gizli paylaşımına dayanan bir algoritma ile desteklenmektedir. Algoritmada veri, farklı sağlayıcılar arasında paylaşılmaktadır. Verinin bu şekilde dağıtılması verinin kötü niyetli kullanıcı tarafından anlaşılıp yetkisiz olarak kullanılmasını önlemektedir.
  - ***Şifreleme çözümleri:*** Şifreleme teknikleri uzun yıllar boyunca hassas verinin korunması için kullanılmıştır. AES (Advanced Encryption Standard) ve RSA (Rivest Shamir Adleman) gibi iyi bilinen şifreleme teknikleri mevcuttur. Ek olarak, SSL (Secure Sockets Layer) teknolojisi de verinin güvenli biçimde iletilmesini desteklemektedir. SSL teknolojisi, bulut depolarına yönelik yan kanal saldırıları durdurmak için kullanılmaktadır. Ancak, kişisel anahtarları açığa çıkaran sözlük saldırılarına da neden olabilmektedir [29]. Ağ üzerinde dolaşan verinin şifrelenmesi, veri bütünlüğünü bozan ortadaki adam saldırılarını önlemede de kullanılmaktadır. Dijital imza da internet üzerindeki veriyi korumak için başvurulan bir yöntemdir. Bu yöntem, RSA şifreleme algoritması ile kullanılmaktadır. [15] çalışmasında geliştirilen yöntem, homomorfik şifreleme algoritmasına dayanmaktadır. Geleneksel homomorfik şifreleme, toplama ya da çarpma gibi homomorfik işlemleri sınırlı derecede desteklemektedir. Çalışmada geliştirilen homomorfik şifreleme ise, şifreli metinleri deşifrelemeden metinler üzerinde isteğe bağlı olarak birtakım hesaplamalar yapmaktadır. Bazı bulut uygulamalarını hayata geçirebilmek için bu hesaplamalar kullanılmaktadır. Ancak, kullanıcıya döndürülen yanıt zamanını ve güç tüketimini etkileyen yüksek oranda işleme gücüne ihtiyaç duyulmaktadır.
  - ***Güvenlik tekniklerine dayanan çözümler:*** Sistemde zararlı kod çalıştırılması önemli bir güvenlik problemi haline gelmiştir. Bu kapsamda, donanım seviyesinde veri bütünlüğü göz önünde bulundurulmaktadır. Çünkü, IaaS düzeyinde saldırganın içeriye sızması çok zordur. Bu amaçla, Dosya Ayırma Tablosu (File Allocation Table) yöntemi geliştirilmiştir. Tablodan, müşterinin çalıştıracağı kod ya da uygulama önceden tahmin edilmektedir. Müşterinin kendi makinesinde daha önce çalıştırdığı uygulama ile o an çalıştırmak istediği uygulama karşılaştırılmakta ve yeni çalıştırılacak olan uygulamanın bütünlüğü ve geçerliliği belirlenmektedir. Tablonun uygulanması için bulut sağlayıcısı tarafında bir hipervizör bulundurulmadır. Hipervizör, tüm uygulama servislerinin zamanlamasından sorumludur ve zamanlama yapmadan önce, müşteri uygulamalarının bütünlüğünü tablodan kontrol etmektedir. Ayrıca, tüm sanal işletim sistemleri tarafından bu mekanizma desteklenmektedir [30, 31]. Kötü amaçlı yazılımı önlemenin başka bir yolu ise özgün hizmet uygulamasının görüntü dosyasında hash değerini saklamaktır. Özgün uygulama görüntüsü ile yeni çalıştırılacak uygulama görüntüsü hash bütünlüğü bakımından karşılaştırıldığında, zararlı programlar tanımlanmaktadır [30].
- ***Doğrulamaya yönelik çözümler***
  - ***Erişim kontrol mekanizmalarına dayanan çözümler:*** Kullanıcılara ait olan veri son derece hassas ve gizlidir. Bu nedenle, erişim kontrol mekanizmaları, kullanıcı verilerine sadece yetkisi olan kişiler tarafından erişim yapılmasına izin vermelidir. Buluttaki tüm hizmet sağlayıcılarının kendilerine istekte bulunan kullanıcılarından kullanıcı kimliği ve yetki bilgisini istemelidir [15, 16]. Aynı zamanda, verinin saklandığı fiziksel bilgi tabanlı sistemlerin sürekli olarak

gözlemlenmesiyle birlikte, veriye yapılan erişim trafiğinin de güvenlik tekniklerince sınırlandırılması gerekmektedir. Güvenlik duvarı uygulamaları ve güvenlik ihlalini tespit eden sistemler, güvensiz kaynaklarca yapılan erişimi sınırlandırıp kötü niyetli faaliyetleri de gözlemlemektedir. Ek olarak, SAML (Security Assertion Markup Language) [32] ve XACML (Extensible Access Control Markup Language) [33] gibi standartlar erişim kontrollerinde kullanılmaktadır. SAML, iş birliği içinde olan taraflar arasında doğrulama ve yetkilendirme kararlarını transfer etmektedir. XACML ise XML tabanlı olup web servisleri için güvenlik politikalarını ve erişim haklarını ifade etmek için tasarlanmıştır [15, 29]. Bulut Güvenlik İttifak'ı (Cloud Security Alliance) [34], bulut ortamlarında güvenliği sağlama adına en iyi uygulamaları kullanmayı teşvik eden ve kâr amacı gütmeyen bir kuruluştur. Bu kuruluş, tecrübe edilmiş en iyi önerileri içeren *Kimlik ve Erişim Yönetimi Kılavuzu* adında bir yayın çıkarmıştır. Kılavuz; merkezi dizin, erişim yönetimi, rol tabanlı erişim kontrolü, kullanıcı erişim onayı, öncelikli kullanıcı, kimlik ve erişim raporlaması gibi konuları içermektedir. Bir başka yöntem ise, dinamik kimlik bilgilerinin kullanımıdır. Hareketli bulut sistemleri için bunu gerçekleştiren algoritma; kullanıcı, konumunu veya veri paketlerini değiştirdiğinde güvenlik için kullanıcı kimlik bilgilerini de değiştirmektedir [15].

- ***Şifrelemeye dayanan çözümler:*** [29] çalışmasında geliştirilen modelde, verilere gerçekleştirilen erişim ve verilerin saklanmasıyla ilgili şifreleme çözümleri üretilmiştir. Bu modelde, veri bulutta şifrelenerek depolanmaktadır. Anahtar dağıtım merkezlerinin bulunması modelin getirdiği bir yenilik olup, *Bulutta Dağıtık Erişim Kontrolü* algoritması ile anahtar dağıtım merkezleri veri sahiplerine ve kullanıcılara anahtar dağıtmaktadır. Bunun yanı sıra, başka bir çalışmada [35], bulutta ABE (Attribute Based Encryption), KP-ABE (Key Policy Attribute Based Encryption), CP-ABE (Ciphertext-PolicyABE), HIBE (Hierarchical Identity BasedEncryption) gibi farklı şifreleme yöntemleri üzerine araştırmalar yapılmıştır. Araştırmada amaç, en etkili erişim kontrolü yapan şifreleme algoritmasını bulmaktır. Sonuç olarak, HASBE şifreleme yönteminin en esnek ve ölçeklenebilir olduğu sonucuna varılmıştır.
- ***Servisin reddine yönelik çözümler:*** Ağ trafiğini sınıflandıran servisin reddi saldırılarını tespit eden araçlar tasarlanmalıdır. Bu araçlar geçerli kullanıcılara ağ üzerinde dolaşma izni verirken, geçersiz kullanıcılara ise trafiği bloklamalıdır. Bir başka yol ise; erişim protokollerini, portları veya IP adreslerini kontrol eden güvenlik duvarları kullanmaktır. Bilinmeyen IP adreslerinden gelebilecek saldırı durumları düşünülerek, tüm yetkisiz erişim trafiğini önlemek amacıyla bazı kurallar uygulanmalıdır. Bunun yanı sıra, otomatik filtreleme ve dengeleme yoluyla servisin reddi saldırılarını tespit eden anahtar ve yönlendiriciler de mevcuttur. Bu araçların çoğu, hız sınırlama ve derin ölçüde paket inceleme yeteneğine sahip olmakla beraber erişim kontrol listesi bulundurmaktadırlar. Saldırılar farklı imzalarla düzenlendiği zaman saldırı önleme sistemleri etkili olmaktadır. Bu sistemler içerik tanıma tabanlı çalışmakta olup davranış tabanlı hizmet reddi saldırılarını bloke edememektedirler. Önerilen diğer bir araç, uygulamaların önünde bulunan ve trafiğin sunucu tarafına geçmesini önleyen akıllı bir donanım cihazıdır. Cihaz, yönlendirici ve anahtarlara bağlanarak çalışmakta ve veri paketlerini analiz ederek onları tanımlamaktadır [31].

4. Veritabanı Yönetim Sistemleri

Bu bölümde; öncelikle, veritabanı sistemine ilişkin güvenlik tehditlerine Bölüm 4.1'de açıklanmaktadır. Bölüm 4.2'de, güvenlik tehditlerine karşı alınabilecek güvenlik önlemleri listelenmektedir.

4.1 Veritabanı Yönetim Sistemlerine Yönelik Güvenlik Tehditleri

Veritabanı yönetim sistemlerine yönelik olarak oluşabilecek güvenlik tehditleri aşağıda listelenmektedir:

- ***Aşırı ayrıcalıkların kötüye kullanılması:*** Kullanıcılara kendi görevleri dışındaki işleri yapmalarına izin veren erişim hakları tanımlandığında büyük sıkıntılar ortaya çıkmaktadır. Bu tür durumlarda kişiler, sahip oldukları hakları kötü amaçlarla kullanmaktadırlar. Bir üniversite bilgi işlem biriminde sistem yöneticisinin tüm veritabanlarına erişimi olduğunu ve aynı zamanda herhangi bir öğrenciye ait kaydı değiştirebildiğini düşünelim. Sistem yöneticisi elindeki ayrıcalıkları kötüye kullanarak herhangi bir öğrencinin notunu değiştirebilmekte veya öğrencinin okula ödemesi gereken ücret miktarında oynamalar yapabilmektedir. Başka bir örnek ise, bankada çalışan ve görevi sadece müşteri irtibat bilgilerini değiştirmek olan bir personel daha fazla ayrıcalık kullanarak müşterilerin hesap numaralarını da kendi menfaatleri için değiştirebilmektedir.

- ***Veritabanı ortamından kaynaklanan riskler:*** İşletim sistemlerindeki güvenlik açıkları veritabanında veri kayıplarına, bozulmalarına veya servisin reddi saldırılarına neden olmaktadır. Örneğin, Windows 2000'de bulunan bir açıktan dolayı blaster solucanı adı verilen zararlı yazılım, servisin reddi saldırısına neden olmuştur [36].
- ***Veri gizliliğine yönelik tehditler:*** Bu başlıktaki saldırılar aşağıda gruplandırılmaktadır:
    - ***SQL enjeksiyon saldırıları:*** SQL enjeksiyonunda, kötü hedefli kullanıcılar doğrulama amacıyla tasarlanmış SQL ifadelerine özel parametreler ekleyerek veritabanına erişmeye çalışmaktadırlar. Bunu yaparken de web sayfaları veya saklı yordamlar (stored procedures) kullanırlar. Çünkü, birçok web uygulaması kullanıcılardan parametre değerleri alıp veritabanına bağlanarak sorgulamalar yapmaktadır. Kullanıcı, web sayfasına giriş yaparken kullanıcı adı ve şifreyi girdiğinde, veritabanında bu bilgilerin doğrulaması yapılmaktadır. Bilgiler geçerli ise kullanıcının girişine izin verimektedir. Bu saldırıda; saldırgan, kimliğin doğrulamasında kullanılan SQL ifadesini kendi gireceği bilgilere göre değiştirerek veritabanına bağlanabilmektedir.
    - ***Anlam çıkarma yöntemleri:*** Bu saldırı tipi, karmaşık veritabanlarından yüksek ölçüde bilgi toplamaya çalışmaktadır. Saldırgan, veriyi analiz ederek veritabanı hakkında bilgi edinmeye çalışmaktadır. Veri madenciliği yöntemlerinden anlam çıkarma işlemi, veritabanı bütünlüğünü tehlikeye sokmaktadır. Bu yöntemin iki türü aşağıda örneklendirilmektedir:
        - ***Verileri ilişkilendirerek anlam çıkarma:*** Örneğin, öğrenci veritabanında öğrencinin not ve isimlerini tutan farklı iki liste bulunduğunda; listeler tek başına kullanıldıklarında bir anlam ifade etmezken, öğrenci isimlerinin notlarla ilişkilendirilerek tek bir listede toplanması sonucunda anlamlı bir veri seti oluşmaktadır.
        - ***Verileri toplayarak anlam çıkarma:*** Örneğin, uluslararası bir organizasyonda her bir şubenin kazanç bilgisi kritik veri olarak görülmezken tüm şubelerin kazanç bilgilerinin toplamı değerli olarak tanımlanmaktadır [37].
    - ***İç tehditler:*** Veritabanı ihlallerini tespit etmeye çalışan düzenekler, normalde güvenlik duvarı gibi davranıp sadece dış saldırılara yönelik olarak çalışmaktadır. Ancak, saldırılar içten yani geçerli kullanıcılar tarafından da gerçekleştirilmektedir. Böyle bir saldırının söz konusu düzeneklerle tespit edilmesi mümkün değildir. Bu nedenle, bu tür kullanıcılar sistemde büyük bir problem yaratmaktadır [38].

4.2 Veritabanı Yönetim Sistemleri Güvenlik Tehditlerine Yönelik Çözümler

Bölüm 4.1'de bahsedilen tehditleri önlemek ya da azaltmak amacıyla geliştirilen çözüm yöntemleri aşağıda açıklanmaktadır:

- ***Ayrıcalıklara yönelik çözümler:*** Bu kapsamdaki tehditlere yönelik olarak erişim kontrol mekanizmaları kullanılmaktadır. Erişim kontrol mekanizmaları verinin gizliliğini sürdürebilmek için başvurulan yöntemlerdir. Bir kullanıcı, veri nesnesine ulaşmaya çalıştığı zaman erişim kontrol mekanizmaları kullanıcının veritabanı üzerindeki haklarını kontrol etmektedir. Bu haklar genellikle güvenlik yöneticisi tarafından tanımlanmaktadır. Güçlü bir erişim kontrol mekanizması sistemin geçerli kullanıcılarını doğrulamalı, yetkisiz kullanıcıları ise tespit edip erişimlerini kısıtlamalıdır. Buna ek olarak, mekanizmalar farklı veriler için farklı erişim izinleri belirlemede rol oynamaktadır. Aşağıda ilişkisel veritabanı sistemleri için önerilmiş erişim kontrol mekanizmaları açıklanmaktadır:
    - ***İsteğe bağlı uygulanan kontrol mekanizmaları:*** Bu yaklaşımda kullanıcılar, diğer kullanıcılara veriye ilişkin birtakım yetkiler tanımlayabilmektedir. Model, bu esnekliğinden dolayı pek çok kurumda yaygın olarak kullanılmaktadır. Sistemdeki yetkiler, yetki yönetimi tarafından tanımlanabilmekte ya da silinebilmektedir. Merkezi yönetim ve sahip yönetim olmak üzere iki çeşit yönetim bulunmaktadır. Merkezi yönetimde, ayrıcalıklı kullanıcılar yetkileri tanımlayabilmekte ya da kaldırabilmektedir. Sahip yönetimde ise, sadece veriyi yaratan kişi tarafından veri üzerindeki haklar tanımlanmakta veya kaldırılmaktadır [39]. İsteğe bağlı kontrol mekanizmaları üçe ayrılmaktadır:
        - ***Sistem R Yetkilendirme Modeli (System R Authorization Model):*** Bu modelde tablo ve *view* olarak adlandırılan yapıların korunması amaçlanmaktadır. Önemli veritabanı işlemlerinden olan `select`, `insert`, `update` ve `delete` fonksiyonları modeli tetikleyen veritabanı işlemleridir. Sadece tabloları oluşturan kişiler tabloyla ilgili erişim haklarına karar verebilmektedirler. Başka bir kullanıcıya tablo üzerinde belirli bir işlem yapma yetkisi verilmediyse, o kullanıcı tabloya erişememektedir. R modelde, bir kullanıcıdan herhangi bir yetki alındığında, o yetki kullanıcı tarafından başkalarına da

önceden verildiyse özyinelemeli olarak diğer kullanıcılardan da geri alınmaktadır. Bu olay sık yaşandığı için *non-cascading geri alma* işleminin kullanılması daha verimli olmaktadır. Bu yaklaşımda, belirli bir kullanıcıdan yetki geri alındıktan sonra diğer kullanıcılardan da yetki geri alınmamamaktadır. `Grant` ve `Revoke` işlemleri *kullanıcı (user), ayrıcalık (privilege)* ve *veri nesnesi (data object)* olmak üzere üç parametre ile kullanılmaktadır. Örneğin;

```
GRANT SELECT ON ogrenci TO ecem
```

Bu komut, `ecem` kullanıcısına `ogrenci` tablosu üzerinde `SELECT` işlemini yapabilmesini sağlamaktadır.

```
REVOKE SELECT ON ogrenci FROM ecem
```

`ecem` kullanıcısından `ogrenci` tablosu üzerinde elde ettiği hak geri alınmaktadır.

```
GRANT SELECT ON ogrenci TO Ecem WITH GRANT OPTION
```

`ecem` kullanıcısı, `GRANT OPTION` ile başka bir kullanıcıya aynı yetkiyi atama ayrıcalığına sahip olamaktadır. Ayrıca, `ecem` kullanıcısından bu yetki geri alındığında, özyinelemeli olarak diğer kullanıcılardan aynı yetki geri alınmayacaktır [37, 39].

- ***İçerik Tabanlı Erişim Kontrolü (Content Based Access Control):*** Bu modelde erişim kontrol kararları veri içeriğine bağlı olmaktadır. Örneğin, bir kurumda tüm müşteri bilgilerinin `müsteri` tablosunda tutulduğunu varsayalım. Böylelikle, bu tabloya sadece müşteri bilgilerini kullanan yetkililer erişebilmelidir. Bu yaklaşım genellikle *view* yapıları kullanılarak uygulanmaktadır. *View* yapılarının içerikleri veritabanı tablolarında bulunan verilerden türetilmektedir. *Selection*, *Projection* veya *Aggregation* gibi fonksiyonlar kullanıldığında bu fonksiyonlardan üretilen sonuçları da tutmaktadır. İlişkisel bir veritabanında, *view*'lar sorgulamalar yazılarak tanımlanır ve tablo gibi davranırlar. Bir bakıma, ilişkisel view'lar sanal tablolar olarak da nitelendirilebilmektedir. *View* yapıları kullanıcı ihtiyaçlarına yönelik bilgileri barındırmaktadır. Bu nedenle, kullanıcılar da ana tablolara bakmak yerine işlerine yarar bilgilere ulaşmak için view'ları kullanmaktadırlar. Böylelikle, ana tablolardaki bilgilerin ya da ilişkisel yapıların kullanıcılar tarafından yanlışlıkla değiştirilmesi gibi olayların yaşanması da önlenmektedir. Ana tablolarda meydana gelen değişiklikler ise veritabanı yöneticisi tarafında kullanıcı *view*'larına yansıtılmaktadır. Erişim kuralları yüksek seviye bir dilde ifade edilmektedir. *View*'ların güvenlik kapsamında getirdiği fayda ise şöyle açıklanabilir: `ogrenci` tablosunda isim, numara, sınıf ve üniversite hakkında bilgiler bulunmaktadır. Bu bilgiler kullanılarak sadece herhangi bir üniversiteye ait olan öğrencilerin bilgilerinin tutulduğu bir *view* yaratılmaktadır. Kullanıcılar ana tablodaki bilgileri görmeden sadece bu *view*'ı kullanarak istedikleri bilgiye erişebilmektedirler. Bunun sonucunda ana tablolar üzerinde güvenlik sağlanmaktadır [37, 39, 40].
- ***Satır tabanlı erişim kontrol (Row based access control):*** Erişimi bireysel kullanıma göre sınırlandırmaktır. Burada satır düzeyinde erişim yapılmasına izin verilmektedir. Örneğin, kurumdaki personel sadece kendisini ilgilendiren satırları görme hakkına sahip olmaktadır. Aşağıda satır düzeyinde güvenliğin nasıl uygulandığı gösterilmektedir:

  ```
  CREATE VIEW View_Name AS SELECT * FROM Table_Name WHERE AttributeName=USER;
  ```

  Bu komut ile belirli bir kullanıcıya ait olan tüm bilgiler ilgili tablodan satır halinde çekilerek bir *view* yapısı oluşturulmaktadır [37].

- ***Rol Tabanlı Erişim Kontrolü (Rol Based Acess Control):*** Bu modelde kişilerin belirli bir faaliyet veya görevi gerçekleştirmeleri için rol bazında yetkilendirilmeleri yapılmaktadır. Kişi rolünü değiştirdiğinde önceki rolüyle ilişkili olan ayrıcalıklar da kendisinden geri alınmaktadır. Bu modelde alt rol grup ilişkilerini tanımlayan rol hiyerarşisi kavramı da bulunmaktadır. Model, görevlerin kullanıcılar açısından kısıtlanmasını da desteklemektedir. Bu özelliğiyle bir kullanıcının çok sayıda erişim hakkına sahip olmasını önlemektedir.
- ***Zorunlu uygulanan kontrol mekanizmaları:*** Zorunlu erişim kontrolü veri nesneleri ve kullanıcıların sınıflandırılmasına bağlı olmaktadır. Sınıflandırma, erişim sınıfları adı verilen kümelere göre yapılmaktadır. Erişim sınıfları güvenlik düzey ve kategorilerini içermektedir. Güvenlik düzeyi bilginin hassaslığını temsil etmektedir. Erişim kontrolünde iki prensip esas alınmaktadır [39]:
  - ***Okuma Yasağı:*** Sadece veri nesnelerini okuma iznine sahip kullanıcılar okuma işlemi yapmaktadır.

- ***Yazma Yasağı:*** Sadece veri nesnelerine yazma iznine sahip kullanıcılar yazma işlemi yapmaktadır.

- ***Saldırıları duyuran mekanizmalar:*** Bu mekanizma, erişim güvenliği kategorisine de girmektedir. Erişimlerin engellenemediği olağan dışı durumlarda sisteme giriş yapan yetkisiz kişilerin haber verilmesi mümkündür. Veritabanı erişimi, gizli olarak tutulan kullanıcı adı ve şifre ile kısıtlanmaktadır. Ancak, bazı durumlarda kazayla veya bilinçli olarak gizli bilgilerin yetkisi olmayan bir kişiye geçmesi olabilmektedir. Saldırgan bilgileri ele geçirince, veritabanındaki bilgilere de kolayca ulaşmış olacaktır. Bunu önlemek için yetkisiz erişimleri yetkili kişilere duyuran sistemler kullanılmaktadır. Bu sistemler, cep telefonuna bilgilendirme mesajı göndererek ilgili duyurma işlemini yaparlar. Mesaj ile yetkisiz erişimden kaynaklanacak kazalarda kısıtlanmış olmaktadır [37].

- ***Veri gizliliğine yönelik çözümler:*** Bu kapsamda şifreleme yöntemleri ile ilgili çözümler yer almaktadır. Veri, şifreleme anahtarı ve algoritması kullanılarak veritabanında saklanmakta ve kullanılmak istendiğinde ise tekrar deşifrelenerek eski haline geri getirilmektedir. Simetrik ve asimetrik olmak üzere temel olarak kullanılan iki çeşit şifreleme yöntemi bulunmaktadır. Simetrik şifrelemede, şifreleme ve deşifreleme süreçleri için kullanılan anahtar aynıdır. Asimetrik şifrelemede ise her süreç için farklı iki anahtar kullanılmaktadır. Şifrelemede anahtarların nasıl yönetileceği önemli bir konudur. Bu konuyla ilişkili olarak, anahtarların saldırganlardan nasıl korunacağı, anahtarlara olan erişimlerin nasıl sınırlandırılacağı, gereksinim duyulan anahtar sayısı, anahtarların hangi sıklıkla değiştirileceği gibi problemleri dikkate almak gerekmektedir. Anahtarların korunması için doğrulama mekanizmaları kullanılmalıdır. Bu mekanizmalar kullanılmazsa, sosyal mühendislik teknikleri ile anahtarlar ele geçirilebilmektedir. Veritabanında bulunan anahtar ve verinin birbirinden ayrılması anahtarların korunmasıyla ilgili önerilen bir yaklaşımdır. Anahtarlar sınırlı erişime sahip dosyalarda saklanabilmektedir. Şifreleme ise veritabanı içinde veya dışında olabilmektedir. Şifreleme veritabanında olursa, operasyon uygulama ortamını da düşük düzeyde etkilemektedir. Ayrı şifreleme sunucularında veriyi şifrelemek tavsiye edilen başka bir tekniktir. Böylelikle, veritabanı yönetim sistemi şifreleme yükünden kurtulmuş olup yükü şifreleme sunucusuna kaydırmış olmaktadır. Veritabanı tarafından desteklenen şifreleme algoritmaları genellikle DES (Data Encryption Standard), Üçlü DES (Triple Data Encryption Standard), RC2 (Ron's Code), RC4, DESX ve AES (Advanced Encryption Standard) algoritmalarıdır [39]. Şifreleme görsel olarak da yapılabilmektedir. Görsel şifreleme; resim, metin, diyagram gibi bilgileri şifrelemede kullanılabilmektedir. Resim içerisinde gizlenen bilgi, uygun bir anahtar resim tarafından tekrar eski haline geri getirilmektedir. Görsel şifreleme, Moni Naor ve Adi Shamir tarafından geliştirilmiştir. Uygulamada iki saydam resim kullanılmaktadır. Resimlerden biri, rastgele piksel değerlerini, diğeri ise gizli bilgiyi içermektedir. Gizli bilgiyi iki resimden birini kullanarak ortaya çıkarmak neredeyse olanaksızdır. Görsel şifrelemenin farklı bir uygulaması resimde katmanların kullanılmasıyla yapılmaktadır. Örneğin, özgün resmin *n* sayıda katmandan oluştuğunu varsayarsak, sadece *n* tane katmanı elinde bulunduran kişi resmi çözebilmektedir. Kişi, *n-1* sayıda katmana sahip olsa da resim hakkında bilgi edinememektedir [37].
- ***SQL enjeksiyonuna yönelik çözümler:*** [41] çalışmasında; SQL enjeksiyon olasılığı, filtreleme yeteneğine sahip bir proxy sunucu ile ortadan kaldırılmaktadır. Sunucu, web uygulaması ile veritabanı arasında konumlandırılmaktadır. Model, öncelikle SQL sorgu komutlarının yapısını analiz etmekte, kabul edilebilir SQL sorgu kalıplarını algılayan bir ayrıştırıcı oluşturmaktadır. Daha sonra, sık kullanılan SQL komutlarının listesi oluşturulmakta ve tehlikeli komutların kullanılması durumunda veritabanı yöneticisini uyaracak bir proxy sunucu yaratılmaktadır. [42] çalışmasında ise, web uygulamaları üzerinde şifreleme ve dizgeciklere ayırma ile SQL enjeksiyonu önlenmeye çalışılmaktadır. Dizgeciklere ayırma işleminde girilen sorgunun boşluk, tek tırnak, eşitlik gibi işaretleri tespit edilmektedir. Sorgu, bu işaretlerden ayrılarak parçalara bölünmekte ve istemci tarafında dinamik bir tabloda saklanmaktadır. İstemci tarafındaki tablo ile sunucu tarafındaki tablo karşılaştırıldığında tablolar farklıysa sorgu reddedilmekte ve veritabanına iletilmemektedir. Aksi durumda ise, sonuç almak için veritabanına bağlanılmaktadır.
- ***İç saldırıları önleme çözümleri:*** Bu problemin üstesinden gelebilmek için veritabanında günlükleri (log) analiz ederek, sorgulamaları kümeleyerek ve kullanıcı kuralları oluşturarak bazı yaklaşımlar önerilmiştir [38]. Güvenlik için veri madenciliği kullanılarak günlük analizi yapılan [43] çalışmasında, veritabanında her bir işlem (transaction), işlem günlüklerine bakılarak analiz edilmektedir. Günlük analizleri sonucunda işlemlerle ilgili birtakım veri sonuçlarına ulaşılmaktadır. Sonuçlar üzerinde eşik değeri kullanılarak ve veri sonuçları arasındaki ilişkiler değerlendirilerek bazı kurallar belirlenmektedir. Belirlenen bu kurallar test işlemleriyle çalıştırılmaktadır. Eğer test verileri kurallara uygun çıkarsa, o işlemler normal olarak kabul edilmektedir. Başka bir teknik ise sorgulamaların kümelenmesi yöntemidir. Bu yöntem ile ilgili sunulan bir çalışmada [44] güvenlik için sorgulamaların anlamsallığı incelenmektedir. Bu kapsam, sorgulamaların

sözdizimlerine göre daha güçlü sonuç vermektedir. Kullanıcı sorgulamalarından geriye belirli sayıda satır dönmektedir. Bu satırlar hakkında istatistiksel bilgiler toplanıp, istatistiksel bilgilere göre sorgulamalar gruplandırılmaktadır. Test aşamasında, test sorguları kullanılarak saldırı durumları tespit edilmeye çalışılmaktadır. Herhangi bir kullanıcı tarafından çalıştırılan sorgulamanın geçerli sorgulamalar kümelerinden birine ait olup olmadığı kontrol edilmektedir. Sorgu, en az bir küme ile eşleşirse kullanıcı normal, eşleşmezse saldırgan olarak belirtilmektedir.

5. Nesnelerin İnterneti (Internet of Things-IoT)

Nesnelerin interneti insanlara ve nesnelere herhangi bir zamanda veya ortamda bir ağ ya da hizmet sağlayarak bağlanma olanağı tanımaktadır. İnternette nesneler birbirlerine bağlı olarak bulunmaktadırlar. Örneğin, RFID teknolojisi ile; lazer tarayıcılar, kızılötesi sensörler ve diğer bilgi algılama cihazları veri alışverişi ve iletişim hizmetleri için ağ üzerinde başka nesnelere bağlanmaktadırlar. Günümüzde; akıllı cihazların izlenebilmesi, konumlandırılabilmesi, ağ fonksiyonlarının yönetilebilmesi ve bilgi teknolojileri alt yapısıyla beraber fiziksel altyapının da güçlendirilmesi için nesnelerin interneti en çok ihtiyaç duyulan kavramlardan birisi haline gelmiştir. Nesnelerin interneti ile akıllı nesnelerin ağda otantik olarak tanımlanması ve bu nesnelerin kendi kendilerini organize ederek yönetebilmesi gibi konular öne çıkmaktadır [45, 46].

5.1 Nesnelerin İnternetine Yönelik Güvenlik Tehditleri

Nesnelerin internetine yönelik olarak gerçekleşebilecek tehditler dört başlıkta listelenmektedir:

- ***Cihazlara yönelik tehditler:*** Hassas bilgiler, cihazların yetkisiz bir şekilde kullanılması veya cihazlarda bulunan yazılıma müdahale edilmesi ile ele geçirilebilmektedir. Örneğin; saldırgan, bir güvenlik kamerasını sadece sunucuya değil aynı zamanda kendisine de veri gönderecek şekilde programlayabilmektedir. Bu noktada, hassas veri toplayan cihazlar için sağlamlık ve kötü kullanıma karşı dayanıklılık önem kazanmaktadır [46].
- ***Haberleşmeye yönelik tehditler:*** Ağ üzerinde veri iletimi sırasında gizliliği sağlamak için kullanılan en yaygın yaklaşım şifrelemedir. Şifreleme yapılırken bazı durumlarda, verinin izlenebilmesi amacıyla paketlere sıra numarası (IPsec Güvenlik Parametre İndeksi vs.) eklenmektedir. Sıra numaraları, saldırgan tarafından trafiği analiz etmede kullanılabilmektedir [47].
- ***Depolama birimlerine yönelik tehditler:*** Depolama birimlerinde bulunan gizli veri yetkisiz olarak kullanılabilmektedir.
- ***Verilerin işlenmesine yönelik tehditler:*** Veri sahibinin bilgisi olmadan kişisel bilgileri üçüncü partilere verilebilmekte veya bazen bu bilgiler amacına uygun olarak kullanılmamaktadır [46].

5.2 Nesnelerin İnterneti Güvenlik Tehditlerine Yönelik Çözümler

Nesnelerin internetine yönelik olarak gerçekleşebilecek saldırıları önlemek veya azaltmak için yukarıda verilen tehditlere yönelik çözüm teknikleri aşağıda listelenmektedir:

- ***Cihazlara Yönelik Çözümler:*** Cihazlarda gizliliği sağlama konusunda çözülmesi gereken çeşitli problemler bulunmaktadır. Bu problemlerden biri, cihaz sahibinin konumunun gizliliğidir. Cihazın çalınması, kaybolması veya yan kanal saldırıları durumlarında kişisel bilgilerin korunması son derece önemlidir. [48] çalışmasında, konum gizliliği kablosuz sensörlerde Rastgele Çoklu Yönlendirme (Multi Routing) algoritması ile gerçekleştirilmiştir. Bu algoritmada yukarıda bahsedilen durumlarda kişisel bilgilerin açığa çıkmasını önlemek amacıyla Hızlı Yanıt Kodu (Quick Response Code) tekniği kullanılmaktadır. Yan kanal saldırılarına karşı, rastgele veya gürültülü veriler eklenmesi ya da hesaplamalarda kör değerler kullanılması çözüm olabilmektedir.
- ***Haberleşmeye Yönelik Çözümler:*** Haberleşme sırasında güvenlik açığını kapatmak için takma isimler şifrelenirken değiştirilebilmektedir. Bilinen örneklerden biri Geçici Mobil Abone Kimliği (Temporary Mobile Subscriber Identity)'dir. Cihazlar sadece bir gereksinim olduğu anda haberleşmelidir. 3GPP (3rd Generation Partnership Project) kapsamında makine tipi iletişimlerde, konum bilgilerinin ele geçirilmesini önlemek için aktif olmayan makineler belirli bir süre sonra ağdan ayrılmaktadır [46].
- ***Depolama Birimlerine Yönelik Çözümler:*** Depolama birimlerinin gizliliğini korumak için aşağıdaki ilkeler dikkate alınmalıdır:
    - Mümkün olduğunca en az miktarda bilgi saklanmalıdır.
    - Kişisel bilgiler zorunluluk durumunda depolanmalıdır.
    - Bilgiler sadece gereksinim duyulduğunda ortaya çıkarılmalıdır.

Verilerle ilişkili olarak depolanan gerçek kimlikleri gizlemek adına veri anonimleştirme yöntemleri kullanılmalıdır. Böylelikle, veritabanı herhangi bir özel kaydı açığa çıkarmadan sadece istatistiksel veriye (toplam, ortalama vb.) müdahaleye izin vermektedir.

- ***Verilerin İşlenmesine Yönelik Çözümler:*** Bu konuda Dijital Haklar Yönetim (Digital Rights Management) sistemi en uygun çözüm olmaktadır. Bu sistem, ticari medya tüketimini kontrol edip bilgileri yasadışı olarak yeniden dağıtıma karşı korumaktadır. Sistemin etkin ve verimli çalışabilmesi için güvenilir cihazlara ihtiyacı vardır [49].

6. İnternet Kullanıcıları

İnternet, dünyadaki tüm bilgisayarları birbirine bağlayarak istenilen bilgiye erişimi ve her türlü veri paylaşımını mümkün kılmaktadır. İnternet, teknolojinin değişmesi ve gelişmesiyle beraber insan hayatının her parçasına girmiştir. Haberleşme, sağlık, eğitim ve ticaret gibi birçok sektörde kullanılan bu teknoloji, hayatın kolaylaşmasını sağlamış ve bireylere kontrolsüz bir özgürlük imkânı sunmuştur. İnternet sürekli değişen bir yapı olduğundan kullanıcıları da bu dinamizmden etkilenmektedirler. Bu etki olumlu olmakla birlikte pek çok olumsuzlukları da beraberinde getirmektedir. Özellikle barındırdığı uygunsuz içeriklerden ötürü artan bir kaygıya neden olmaktadır. Olumsuzlukların başında internette gezinirken cinsel istismar, müstehcenlik, pornografi gibi tehlikelerle karşılaşılması ve kumar, uyuşturucu gibi bağımlılık sorunları gelmektedir Bunların yanında, insan sağlığını tehlikeye atacak problemler de söz konusudur. Örneğin; internet başında saatlerce oturulduğunda psikolojik ve fiziki olarak oluşabilecek sorunlar mevcuttur [50, 51]. İnternette meydana gelebilecek güvenlik açıklarını önleyebilmek için öncelikle insanların bu konuda bilinçlendirilmesi gerekmektedir. Bu bölümde öncelikle kişilerin en fazla karşılaştıkları güvenlik problemlerinden bahsedip daha sonra bu problemlerin üstesinden gelebilmek adına ne tür bilinçlendirme etkinliklerinin yapıldığı incelenecektir.

6.1. İnternet Kullanıcılarına Yönelik Güvenlik Tehditleri ve Önerilen Bilinçlendirme Yöntemleri

Öğrenciler üzerinde yapılan bir çalışmada [50], bireylerin daha çok siber zorbalığıyla karşılaştıkları görülmüştür. Siber zorbalık, zorbalık yapan kişinin bilgisayar ve cep telefonu kullanarak bireylerin internet üzerindeki hesaplarına müstehcen veya utandırıcı mesajlar göndermesidir [52]. Siber zorbalığın bir çeşidi olan elektronik zorbalık ise, şifreleri ve web sitelerini ele geçirme, servis reddi saldırıları kapsamında spam mailleri gönderme gibi zararlı faaliyetleri barındırmaktadır. Çalışmada siber zorbalığa önlem olarak her kullanıcıya hitap eden bilinçli bir web sitesi önerilmektedir. Bu web sitesinin, interneti doğru ve amacına uygun kullanma, kişisel güvenliğin sağlanması, hedeflenen bilgiye ulaşma gibi konulara cevap verecek şekilde tasarlanması gerekmektedir. Aynı zamanda, suç etkenlerinin tanımlanması ve sosyal ağ kullanımı ve suç faktörlerinin tanımlanması gibi faydalı bölümlere yer verilerek bölümlerin interaktif olacak ve sorular sorulup cevap alınacak şekilde geliştirilmesi web sitesinde de aranılan bir özelliktir.

Yine öğrenciler üzerinde yapılan başka bir çalışmada [51], öğrencilerin internete daha çok oyun oynamak için başvurdukları ortaya çıkmıştır. Bireylerin sosyal paylaşım siteleri aracılığıyla kişisel bilgilerini, gönderilerini, fotoğraflarını ve e-posta adreslerini herkesle veya arkadaşlarıyla yüksek oranda paylaştıkları görülmüştür. Bu durum bireyler için bir güvenlik tehdidi oluşturmaktadır. Bir başka dikkat çekilen tehdit ise, ebeveynlerin yeterli oranda filtre kullanmamasıdır. Hatta, ebeveynler antivirüs programlarının filtre görevi gördüğünü zannetmektedirler. Ayrıca, yine ebeveynlerin sadece yarısı internette aile koruması şifresi kullanmaktadır. Çalışmada, öğrencilerin interneti sağlıklı olarak kullanmaları için ebeveynlerin kontrolü ve okullarda gerçekleştirilecek aktivitelerin önemli olduğu vurgulanmaktadır. Bu kapsamda, Milli Eğitim Bakanlığının öğrencileri bilinçlendirmek için ilköğretim ve lise programlarında bilişim teknolojileri dersine daha fazla önem vermesi gerektiğine yer verilmiştir. Yine MEB'in tedbir olarak uyguladığı katı filtreleme, öğrencilerin araştırma yaparken zorlanmalarına sebep olduğundan filtre sisteminin tekrardan incelenip daha uygulanabilir okul prosedürlerinin yaratılmasına dikkat çekilmektedir.

Bilgi güvenliği üzerine yapılan diğer bir çalışmada [53], kişilerin bilgisizlik ve zaaflarını kullanan sosyal mühendislik yöntemleri, kritik ve kişisel bilgilerin kötü niyetli kişilere gönderimi sistem açıklarından faydalanılması ve zararlı yazılımların teknolojik değişimlerce şekillenmesiyle birlikte web teknolojilerinin de bu yazılımların yayılmasına destek vermesi günümüzde var olan tehditler olarak sıralanmaktadır. Konuya gereken önemin verilmesi ve önlemlerin alınıp farkındalık oluşturulması gibi çözüm önerilerden bahsedilmiştir. Ek olarak, e-Dönüşüm Türkiye 2005 Eylem Planında [54] bulunan 5 ve 33 nolu eylemler ve elektronik imza kanunu güvenlik adına olumlu bir gelişme olarak nitelendirilip bir an önce bu eylemlerin tamamlanmasının faydalı olacağından söz edilmiştir.

Diğer bir araştırma bulgusunda [55], çoğu öğrencinin antivirüs kullanımı, güncellenmesi ve yedekleme konusuna dikkat etmediği görülmüştür. Ek olarak; öğrencilerin çok az bir kısmının parola güvenliği konusunda tedbir aldığı saptanmıştır. Bu konularda öğrenci bilgi ve farkındalığının arttırılması gerektiği söylenmiştir.

Kimlik avı (phishing attack) ile ilgili yapılmış bir çalışmada [56] insanların kimlik avı saldırısını engelleme konusunda bilgisayar seviyesini ölçen bir model oluşturulmuştur. Model aracılığıyla, bilgisayar kullanıcılarının bilgisi arttıkça kimlik saldırılarına gerekli önlemleri almada kendilerine daha özgüvenli olduğu tespit edilmiştir. Ayrıca bilgi güvenliğinde prosedürel ve kavramsal bilgilerin birleştirilmesinin önemi açığa çıkmıştır. Bunu gerçekleştirmenin yolu ise iyi tasarlanmış güvenlik eğitimlerinden geçmektedir. Eğitici oyunlar ve web tabanlı eğitim materyalleri, kullanıcıları bilinçlendirmede yapılacak eğitimler arasındadır. Diğer önerilen bir çözüm ise, kimlik avında sık rastlanılan URL yeniden yönlendirme olayına yöneliktir. Bununla mücadele etmek için URL yönlendirmesini güvenli bir şekilde yapan Mozilla, Firefox,Google Chrome, Safari ve IE gibi tarayıcıların tercih edilmesi ve Kaspersky Lab gibi anti-phishing teknolojilerine başvurulması tavsiye edilmektedir. Bu teknolojiler, site alan isminin IP adresine karşılık gelip gelmediğine karar verdikten sonra olası bir tehlike anında saldırganın girişimini bloklamaktadır.

Yapılan başka bir çalışmada [57], bilgi güvenliği kapsamında teknik ve teknik olmayan (insan kaynaklı) sorunların var olduğu belirtilmiştir. Teknik bilgi güvenliği sorunları ağırlıklı olarak teknik bilgi ve araçlara (şifreleme teknikleri gibi) yönelmektedir. Teknik olmayan bilgi güvenliği sorunları ise etik, yasal konular ve bilgi güvenliği kültürü gibi konuları içermektedir. Aynı zamanda, insanların güvenlik üzerindeki etkileri incelenmekte ve bu etkiler kasıtlı ve kazara olarak sınıflandırılmaktadır. Çalışmada, bilgi güvenliğinde karşılaşılan saldırıların farkındalık eksikliğinden kaynaklandığı belirtilmiş olup zafiyetin giderilmesi amacıyla bilgi güvenliği sağlama ve farkındalığına yönelik çok boyutlu ve endüstri ile uyumlu bir model oluşturulmuştur. Önerilen model, bilgi geri getirimi ve farkındalığı, ölçme ve gözlemleme ve boyutlar olmak üzere 3 parçadan oluşmaktadır. Birinci parça, üç boyutlu bir yaklaşım sergileyip sırasıyla teknik olmayan bilgi güvenliği konularını, bilgi güvenliği yetki düzeylerini ve modern bilgi güvenliği dokümanlarını birbiriyle bütünleştirmektedir. İkinci bölüm, modelin boyutlarından ilgili bilgiye ulaşmaya odaklanmıştır. Bu bilgi, bilgi güvenliği ihtiyacına bağlı olarak değişen farklı bilgi teknolojileri yetki seviyeleri tarafından talep edilmiş olabilmektedir. Yine, bu bölümde elde edilen veri, tüm bilgi güvenliği düzeyleri tarafından bilinci arttırmak için kullanılmaktadır. Bilgi güvenliği süreçleri hakkında karar verirken de buradan erişilen bilgiden faydalanılması çok önemli olacaktır. Üçüncü bölümde yürütülen ölçme ve izlemenin amacı kuruluşların bilgi güvenliği farkındalığında kendi mevcut durumlarını görmelerini sağlamaktır. Buna ek olarak, yeni ortaya çıkan bilgi güvenliği sorunlarının dahil edilip ele alınmasını sağlamak için bu alandaki gelişmelerin izlenmesi de amaçlanmaktadır. Bu model ile özellikle organizasyonlarda çalışan personel hedef alınmıştır.

Diğer bir çalışma [58], tehlikeler konusunda yapılan uyarılara rağmen şaşırtıcı sayıda kullanıcının güvenlik standartlarına uymadığından bahsetmektedir. Spam postalar, casus yazılımlar, bilgisayar virüsleri, sahte e-postalar, kimlik avı (phishing) ve kötü amaçlı yazılımlar gibi tehditlerin güvenlik sorunları listesinde en üst sıralarda yer aldığı belirtilmektedir. Bunun yanında, kullanıcıların beklenmeyen e-posta eklerini açarak ve e-postalarda bulunan bağlantılara tıklayarak kendilerini tehlikeye attıkları da söylenmektedir. Çalışma, güvenlik konusunda teşviki arttırmak amacıyla kullanıcı bilgisi, kişisel sorumluluk ve eğitim teknikleri arasındaki etkileşimi incelemektedir. Bu bağlamda, kullanıcının sahip olduğu sorumluluğa göre güvenlik eğitiminin verilmesi hipotezi analiz edilmektedir. Ayrıca çalışma, kullanıcının sahip olduğu deneyimin güvenlik konusu üzerindeki etkinliğini de incelemektedir. Sonuç olarak ise kullanıcıları kendi bilgileri doğrultusunda sınıflandırmanın çok önemli olduğuna ve kullanıcı seviyesine göre bilgi güvenliği eğitiminin verilmesi gerektiğine dikkat çekilmektedir. Bunun yanı sıra, Internet sağlayıcıları ve yazılım şirketlerinin işbirliği ile kullanıcılar için tutarlı ve kullanışlı bir formatta korunma talimatlarının hazırlanması gerektiği söylenmektedir.

7. Sonuçlar

Bilgi güvenliği; bilgi sistemlerinin ve sistemin sahip olduğu bilginin yetkisiz erişime, kullanıma, ifşa edilmesine, değiştirilmesine, incelenmesine, hasar verilmesine veya yok edilmesine karşı korunması ve bu olaylara karşı alınacak tedbirlerin bir bütünü olarak ifade edilmektedir. Bilgi güvenliği, bir bilgi sisteminin işlevlerini yerine getirirken kesintisiz, kaliteli ve güvenli hizmetin sağlanmasını amaçlamaktadır. Günümüzde önemi gittikçe artan bilgi sistemlerine yönelik pek çok çeşitli saldırı bulunmaktadır. Saldırılar, bu teknolojileri oluşturan, kullanan ve açıklarını da en iyi şekilde bilen insanlardan kaynaklanmaktadır. [2]. Bu makalede araç ad-hoc ağları, veritabanı yönetim sistemleri, bulut bilişim ve nesnelerin interneti gibi farklı bilgi sistemlerinin karşılaşabileceği en temel ve yaygın güvenlik tehditleri anlatılmış; tehditleri azaltmak ve önlemek için farklı çözüm yöntemleri açıklanmıştır.

Yöntemler kendi içinde sınıflandırılarak, her birinin önemi vurgulanmıştır. Ayrıca, ilgili sistemlerin yapıları tanıtılarak bu sistemler hakkında fikir edinilmesi amaçlanmıştır. Bilgi sistemlerinin en önemli bir parçası ve zayıf halkası olan İnternet kullanıcılarının da karşılaştığı tehditlerin bu konu kapsamında anlatılması bir elzemdir. Çünkü, aslında yukarıda bahsedilen sistemlerin işleyişine yönelik var olan tehlikeler bu sistemleri kullanan insanların dikkatli bir şekilde davranması yoluyla önlenebilmektedir. Bir önceki bölümde incelenen araştırmalar sonucunda insanların çoğunlukla siber zorbalık, bilgilerin sosyal paylaşım siteleri aracılığıyla herkese açılması, filtre kullanmama, sosyal mühendislik, sistem açıklarından faydalanma, zararlı yazılımlar, az derecede antivirüs kullanımı ve güncellenmesi, yeterli ölçüde yedekleme yapılmaması, korsan yazılım, kimlik avı saldırısı (phishing) gibi saldırılarla karşı karşıya kaldığı saptanmıştır. Bu saldırılar, sistemlerde görülen tehditler ile karşılaştırıldığında neredeyse birebir eşleştikleri anlaşılmıştır. Örnek vermek gerekirse; siber zorbalık, kimlik avı saldırısı, bilgilerin sosyal ağ ile ifşa olması veri gizliliği, doğrulama ve tanımlamaya yönelik tehdit oluştururken sistem açıklarından faydalanma, yeterli olarak filtre ve antivirüs kullanılmaması, yedekleme yapılmaması ve korsan yazılımlar hem servis reddi saldırılarına hem de yine veri gizliliğinin bozulmasına ortam hazırlayacaktır. Sosyal mühendislik, insan zaaflarından faydalanma ile hassas bilgilerin ele geçirilmesidir. Dolayısıyla, bu bilgilerin kullanıcı adı ve şifre olabileceği düşünüldüğünde yetkisiz olarak diğer bilgilerin de ele geçirilmesi olasıdır. Bu nedenle, veri gizliliği, doğrulama ve tanımlamaya karşı bir saldırı söz konusu olacaktır. Yapılan çalışmalara göre, söz edilen saldırılarla mücadele etme konusunda insanları bilinçlendirmek büyük önem teşkil etmektedir. Bu amaçla, insanların bilgi eksikliğini gidermek ve söz konusu saldırıları önlemek için eğitici bilinçlendirme faaliyetlerine ihtiyaç duyulmaktadır. Söz konusu bilgi sistemlerinde güvenliği sağlamak ve düzenli işleyişi devam ettirmek için bahsedilen teknik çözümler uygulanabilir veya çözümler daha da geliştirilerek hayata geçirilebilir. Bu aşamada, kurumların bu çözümleri uygulayabilmesi için bir yapılabilirlik çalışması yapmaları gerekmektedir. Fakat teknik çözümlerin yanında öncelikle insanları bilgi güvenliği alanında yetiştirmek en etkili çözüm önerisi olacaktır. Bilgi güvenliği, hem kamu kurumlarında hem de özel sektörde ana gereksinim olarak görülmeli ve bu alanda farkındalık arttırıcı faaliyetler desteklenmelidir.

Kaynaklar

[1] W. H. Ware, “Security and Privacy in Computer Systems”, Proceedings of the 1967 Spring Joint Computer Conference (AFIPS Conference Proceedings), Vol. 30, 279-282, 1967.
[2] M. Güngör, “Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma”, Yayımlanmış Uzmanlık Tezi, Bilgi Toplumu Dairesi Başkanlığı, 2015.
[3] R. S. Raw, M. Kumar, N. Singh, “Security Challenges, Issues and Their Solutions for VANET”, International Journal of Network Security & Its Applications (IJNSA), 5 (5), 95-105, 2013.
[4] M. Soytürk, A. E. Harmancı, E. Çayırcı, “Gezgin Ad Hoc Ağlar ve Yol Atama”, Bilişim Zirvesi’01, İstanbul, 4-7 Eylül 2001.
[5] J. M. de Fuentes, A. I. González-Tablas, A. Ribagorda, “Overview of Security Issues in Vehicular Ad-hoc Networks”, Handbook of Research on Mobility and Computing, IGI Global, Chapter 56, 894-911, 2011.
[6] B. Parno, A. Perrig, “Challenges in Securing Vehicular Networks”, Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV), 2005.
[7] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks", Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP’02), 78-89, 2002.
[8] L. Klein-Berndt, “A Quick Guide to AODV Routing”, National Institute of Standards and Technology (NIST)-Wireless Communications Technologies Group, http://www.itl.nist.gov/div892/wctg/aodv_kernel/aodv_guide.pdf . (Son Erişim: Ağustos 2016)
[9] S. K. Bhoi, P. M. Khilar, “Vehicular communication: A survey”, IET Networks, 3 (3), 204-217, 2013.
[10] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, Muhlethaler, D. Raffo, “Securing the OLSR protocol”, Proc. IFIP Med-Hoc-Net, 2003.
[11] S. K. Bhoi, “SGIRP: A Secure and Greedy Intersection-Based Routing Protocol for VANET using Guarding Nodes”, Master Thesis, Department of Computer Science and Engineering National Institute of Technology Rourkela, India, 2013.
[12] Y. Hu, A. Perrig, D. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks”, Wireless Networks, Volume 11, Issue 1, 21-38, 2005.
[13] Y. C. Hu, D. B. Johnson, A. Perrig, " SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks ", Ad Hoc Networks, 1(1):175-192, 2003.
[14] G. He, “Destination-Sequenced Distance Vector (DSDV) Protocol”, Networking Laboratory, Helsinki University of Technology, 2002.

[15] K. Hashizume, D. G. Rosado, E. Fernández-Medina, E. B. Fernandez, "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services and Applications, 4(5), 2013.
[16] J. S. Hwan, Y. E. Gelogo, B. Park, "Next Generation Cloud Computing Issues and Solutions," International Journal of Control and Automation, 5(1), 63-70, 2012.
[17] Amazon EC2, Virtual Server Hosting, https://aws.amazon.com/ec2/ . (Son Erişim: Ağustos 2016)
[18] B. Meena, K. A. Challa, "Cloud Computing Security Issues with Possible Solutions", International Journal of Computer Science and Technology, Vol. 3, Issue 1, 2012.
[19] Google Cloud Platform-Google App Engine, https://appengine.google.com . (Son Erişim: Ağustos 2016)
[20] Microsoft Azure, https://azure.microsoft.com . (Son Erişim: Ağustos 2016)
[21] Atlassian: Software Development and Collaboration Tools, https://www.atlassian.com . (Son Erişim: Ağustos 2016)
[22] SalesForce, https://www.salesforce.com . (Son Erişim: Ağustos 2016)
[23] Lucidchart, https://www.lucidchart.com . (Son Erişim: Ağustos 2016)
[24] Gliffy, https://www.gliffy.com . (Son Erişim: Ağustos 2016)
[25] V. Vidhya, "A Review of DOS Attacks in Cloud Computing", IOSR Journal of Computer Engineering (IOSR-JCE), 16 (5), 32-35, 2014.
[26] B. Sevak, "Security against Side Channel Attack in Cloud Computing", International Journal of Engineering and Advanced Technology (IJEAT), 2(2), 2012.
[27] A. Parakh, S. Kak, "Online data storage using implicit security," Information Sciences, Vol.179, 3323-3331, 2009.
[28] Y. Ghebghoub, S. Oukid, O. Boussaid, "A Survey on Security Issues and the Existing Solutions in Cloud Computing", International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, 2013.
[29] SearchCIO, "XACML (Extensible Access Control Markup Language) definition", http://searchcio.techtarget.com (Son Erişim: Ağustos 2016).
[30] T.-S. Chou, "Security Threats On Cloud Computing Vulnerabilities", International Journal of Computer Science & Information Technology (IJCSIT), Vol 5, No 3, 2013.
[31] S. Singh, B. K. Pandey, R. Srivastava, N. Rawat, P. Rawat, A. Awantika, "Cloud Computing Attacks: A Discussion with Solutions", Open Journal of Mobile Computing and Cloud Computing, Volume 1, No. 1, 1-8, 2014.
[32] OASIS Security Services (SAML), https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security . (Son Erişim: Ağustos 2016)
[33] OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html . (Son Erişim: Ağustos 2016)
[34] Cloud Security Alliance, Security Guidance, https://cloudsecurityalliance.org . (Son Erişim: Ağustos 2016)
[35] N. Antony, A. A. R. Melvin, "A Survey on Encryption Schemes in the Clouds for Access Control", International Journal of Computer Science and Management Research, 1(5), 1135-1139, 2012.
[36] I. Basharat, F. Azam, A. W. Muzaffar, "Database Security and Encryption: A Survey Study", International Journal of Computer Applications, 47(12), 28-34, 2012.
[37] M. Rafiq, "Database Security Threats and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 4(2), 2014.
[38] A. Sartape, Vasgi B.P., "Database Security Using Different techniques: A Survey", International Journal of Computer Trends and Technology (IJCTT), 4(4), 2013.
[39] S. Kulkarni, S. Urolagin, "Review of Attacks on Databases and Database Security Techniques", International Journal of Emerging Technology and Advanced Engineering, 2(11), 2012.
[40] A. Rosenthal, E. Sciore, "Content-Based and View-Based Access Control", Encyclopedia of Cryptography and Security, 249-253, 2011.
[41] K. Elshazly, Y. Fouad, M. Saleh, A. Sewisy, "A Survey of SQL Injection Attack Detection and Prevention". Journal of Computer and Communications, 2, 1-9, 2014.
[42] S. Anjugam, A. Murugan, "Efficient Method for Preventing SQL Injection Attacks on Web Applications Using Encryption and Tokenization", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 4(4), 173-177, 2014.
[43] Y. Ru, A. Campan, J. Walden, I. Vorobyeva, J. Shelton, "An Effective Log Mining Approach For Database intrusion Detection", 2010 IEEE International Conference on Systems Man and Cybernetics (SMC), 2010.
[44] S. Mathew, M. Petropoulos, H. Q. Ngo, S. Upadhyaya, "A Data-Centric Approach to Insider Attack Detection in Database Systems", Proceedings of the 13th international conference on Recent advances in intrusion detection (RAID'10), 382-401, 2010.
[45] O. Köroğlu, "Nesnelerin İnterneti, Algılayıcı Ağları ve Medya", Akademik Bilişim'2015, 2015.
[46] S. J. Kumar, D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", International Journal of

Computer Applications, 90(11), 2014.
[47] M. Giannikos, K. Kokoli, N. Fotiou, G. F. Marias, G. C. Polyzos, "Towards secure and context-aware information lookup for the Internet of Things", 2013 International Conference on Computing, Networking and Communications (ICNC), 632-636, 2013.
[48] B. Tepekule, U. Yavuz, A. E. Pusane, "On the Use of Modern Coding Techniques in QR Applications", 2013 21st Signal Processing and Communications Applications Conference (SIU), 1-4, 2013.
[49] E. Liu, Z. Liu, F. Shao, "Digital Rights Management and Access Control in Multimedia Social Networks", Proceedings of the Seventh International Conference on Genetic and Evolutionary Computing (ICGEC 2013), 257-266, 2014.
[50] Küçükali, M., & Bülbül, H. İ. (2015). Fatih projesi kapsamında internetin bilinçli ve güvenli kullanımının artırılması. TÜBAV Bilim Dergisi, 8(2), 1-17.
[51] Mert, M., Bülbül, H. İ., & Sağıroğlu, Ş. (2012). Milli eğitim bakanlığına bağlı okullarda güvenli internet kullanımı. Türk Bilim Araştırma Vakfı Bilim Dergisi, 5(4), 1-12.
[52] Aksaray, S. (2011). Siber Zorbalık**.** Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi, 20 (2), 405-432
[53] Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. Gazi Üniversitesi Politeknik Dergisi, 9(3).
[54] Kesmez, N., "Kişisel Verilerin Korunması Kanunu (Taslak)", Türkiye Bilişim Şurası, 2002, http://bilisimsurasi.org.tr/dosyalar/42.doc (2005). [Son Erişim: Ekim 2016]
[55] Karaoğlan Yılmaz, F. G., Yılmaz, R., & Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. Bartın Üniversitesi Eğitim Fakültesi Dergisi, 3(1), 176-199.
[56] Arachchilage, N.A.G., Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312.
[57] Kritzinger, E., & Smith, E. (2008). Information security management: an information security retrieval and awareness model for industry. Computers & Security, 27(5 -6), 224 -231.
[58] Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior, 48, 199-207.