Nesnelerin İnternetine (Iot) İlişkin Zafiyetler ve Güvenlik Önlemlerine İlişkin Çalışmaların Analizi

***

Analysis of Studies on Internet of Things (Iot) Related Vulnerabilities and Security Measures

Müzeyyen BARLAS[1]
Burcu ERTEKIN[2]
Türkay HENKOĞLU[3]

DOI:10.33461/uybisbbd.1756160

Makale Bilgileri

Makale Türü:
Araştırma Makalesi

Geliş Tarihi:
01.08.2025

Kabul Tarihi:
12.09.2025

Öz

Nesnelerin interneti (IoT), bireyin günlük hayatından endüstri sektörüne, sağlık sektöründen akıllı ev teknolojilerine kadar geniş bir uygulama alanında kullanılmaktadır. Ancak IoT uygulamalarının hayatımıza girişi, günlük yaşamı kolaylaştırdığı gibi yeni zorlukları, güvenlik açıklarını ve endişeleri de beraberinde getirmiştir. Bu çalışmanın amacı, IoT cihazlarının risk ve zafiyetlerinin kapsamlı bir literatür araştırmasıyla ortaya konulması, IoT güvenliğinin sağlanmasına yönelik çalışmalarda odaklanılan hususların belirlenmesi, olası risk ve tehditlerin sınıflandırılması ve IoT cihazlarının güvenli kullanımı için alınması gereken bilgi güvenliği önlemlerine dikkat çekilerek farkındalığın oluşturulmasıdır. Bu amaçla etki faktörü yüksek ve prestijli çalışmaları içeren ScienceDirect veritabanı üzerinden IoT risklerini, zafiyetlerini ve güvenliğini ele alan çalışmalar içerik analizi yapılarak incelenmiştir. Bu çalışmanın, IoT sistemlerine yönelik risk ve tehditlerin neler olduğu, bu sistemlere yönelik saldırıların nasıl sınıflandırılabileceği ve zafiyetlerin giderilmesi amacıyla ne tür önlemlerin alınması gerektiğine ilişkin sorulara kapsamlı bir literatür araştırmasına dayanarak yanıt vereceği ve bu sayede gündelik yaşamın parçası haline gelen IoT cihazlarının barındırdığı risklere yönelik farkındalığın oluşturulmasına katkı sağlayacağı düşünülmektedir. Çalışmada IoT sistemleri üzerindeki güvenlik zafiyetlerinin neler olduğu, IoT saldırılarının kapsamlı ve güncel sınıflandırmasının nasıl yapıldığı, IoT sistemlerinin gizlilik ve güvenliğine yönelik potansiyel tehditlerin neler olduğu ve üretici ve/veya tüketicilerin IoT sistemlerine yönelik tehditlere karşı ne tür önlemler alabileceğine yönelik sorulara yanıt verilmektedir.

Anahtar Kelimeler: *Nesnelerin interneti (IoT), IoT zafiyetleri, IoT riskleri, IoT tehditleri, IoT güvenliği.*

Article Info

Paper Type:
Research Paper

Received:
01.08.2025

Accepted:
12.09.2025

Abstract

The Internet of Things (IoT) is used in a wide range of applications, from individuals' daily lives to industrial sectors, from healthcare to smart home technologies. However, the introduction of IoT applications into our lives has not only made daily life easier but also brought new challenges, security vulnerabilities, and concerns. The aim of this study is to identify the risks and vulnerabilities of IoT devices through a comprehensive literature review, identify the areas of focus in studies on ensuring IoT security, classify potential risks and threats, and raise awareness by highlighting the information security measures that should be taken for the safe use of IoT devices. For this purpose, a content analysis was conducted to examine studies addressing IoT risks, vulnerabilities, and security from the ScienceDirect database, which contains high-impact and prestigious studies. This study is expected to answer questions such as what the risks and threats to IoT systems are, how attacks against these systems can be classified, and what measures should be taken to address these vulnerabilities, based on a comprehensive literature review. Thus, it is believed that this study will contribute to raising awareness of the risks posed by IoT devices that have become a part of everyday life. The study answers questions such as what the security vulnerabilities are in IoT systems, how a comprehensive and up-to-date classification of IoT attacks is made, what the potential threats are to the privacy and security of IoT systems, and what precautions manufacturers and/or consumers can take against threats to IoT systems.

Keywords: *Internet of things (IoT), IoT vulnerabilities, IoT risks, IoT threats, IoT security.*

Atıf/ to Cite (APA): Barlas M., Ertekin B. & Henkoğlu T. (2025). Nesnelerin İnternetine (Iot) İlişkin Zafiyetler ve Güvenlik Önlemlerine İlişkin Çalışmaların Analizi. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 9(2), 121-141. DOI: 10.33461/uybisbbd.1756160

[1] Aydın Adnan Menderes Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, muzeyyenbarlas21@gmail.com, Aydın, Türkiye.
[2] Aydın Adnan Menderes Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, burcuertekin18@gmail.com, Aydın, Türkiye.
[3] Aydın Adnan Menderes Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, turkay.henkoglu@adu.edu.tr, Aydın, Türkiye.

1. GİRİŞ

Nesnelerin İnterneti (IoT) kavramı ilk kez 1999 yılında Kevin Ashton tarafından kullanılmış, ilk somut uygulaması ise 1991 yılında Cambridge Üniversitesi'nin kahve makinesi projesiyle gerçekleştirilmiştir. IoT, sensörler aracılığıyla internete bağlanan, veri toplayan ve işleyen akıllı cihazlardan oluşmaktadır (Ogonji, Okeyo ve Wafula, 2020). Başka bir ifadeyle IoT, sensör, cihaz ve makinelerin internete bağlanıp veri topladığı, ilettiği ve görevleri otonom biçimde yerine getirdiği bir teknolojidir. Sağlık, tarım, akıllı şehir ve ev sistemlerinde yaygın olarak kullanılan bu cihazlar, insansız iletişim sağlayarak günlük yaşamda kolaylık ve tasarruf sunmaktadır (Thabit, Can, Aljahdali, Al-Gaphari ve Alkhzaimi, 2023). IoT sistemleri, çevresel verileri toplayarak analiz etmekte, diğer sistemlerle paylaşmakta ve süreçleri otomatikleştirerek verimliliği arttırmaktgadır. Bu durum sanayi, sağlık, tarım ve ulaşım gibi sektörlerde üretkenlik ve hizmet kalitesini artırırken, akıllı şehirler, ev otomasyonu ve giyilebilir teknolojilerle yaşam konforunu da yükseltmektedir. Gerçek zamanlı veri paylaşımı sayesinde karar süreçleri hızlanmakta, sistemler daha etkin çalışmaktadır. Ancak bu sistemlerin sınırlı donanım kapasitesine sahip olması nedeniyle klasik güvenlik önlemleri doğrudan uygulanamamaktadır ve IoT siber saldırılara daha fazla maruz kalabilmektedir (Turak, 2015; Sengupta, Ruj ve Das Bit, 2020; Cirne, Sousa, Resende ve Antunes, 2022). Üreticilerin güvenlik önlemlerini ihmal etmesi ve kullanıcı farkındalığının düşük olması, gizlilik, bütünlük ve kullanılabilirlik gibi temel güvenlik ilkeleri açısından önemli riskler doğurmaktadır (Axelrod, 2015; Schiller, Aidoo, Fuhrer, Stahl, Ziörjen ve Stiller, 2022). Ayrıca veri güvenliği, kullanıcı mahremiyeti ve altyapı eşitsizliği gibi sorunlar da IoT sistemlerinin kullanımıyla ilişkili olarak dikkat çekmektedir. Son kullanıcılar ise yeterince araştırma yapmadan, güvenlik ve gizlilik kavramlarıyla ilgili yeterli bilgi ve farkındalığa sahip olmadan yeni nesil cihazları satın alma eğilimi göstermektedirler. Üretici firmalar da kullanıcıların oluşturduğu zafiyetlerin sorumluluğunu almaktan kaçınmaktadırlar. Tüm bu zorluklara rağmen IoT'nin sunduğu ekonomik ve toplumsal faydalar onu dijital çağın vazgeçilmez teknolojilerinden biri hâline getirmiştir (Abdul-Qawy, Pramod, Magesh ve Srinivasulu, 2015, s. 71–74).

IoT, sahip olduğu yüksek etki potansiyeli sayesinde pek çok sektörde yaygın biçimde kullanılmaktadır. Bu teknoloji, endüstri, çevre ve toplum olmak üzere üç ana kategoride sınıflandırılmaktadır. Endüstriyel uygulamalarda Endüstriyel IoT, üretim sektöründe dijital dönüşümün temel bileşeni olarak konumlanmakta ve Endüstri 4.0'ın merkezinde yer almaktadır. Akıllı sensörler ve makineler aracılığıyla elde edilen gerçek zamanlı veriler, akıllı fabrikalar, lojistik ve tedarik zinciri yönetimi gibi alanlarda verimlilik ve güvenliği artırmaktadır. Çevresel uygulamalarda hava kalitesi izleme, su kaynaklarının takibi ve enerji yönetimi gibi konular ön plana çıkmakta ve sürdürülebilirlik hedeflenmektedir. Toplumsal alanlarda ise akıllı şehirler, e-sağlık sistemleri ve yaşlı bireylerin uzaktan izlenmesi gibi uygulamalarla yaşam kalitesi yükseltilmektedir. Sağlıkta "Internet of Medical Things" (IoMT) kullanımı erken teşhis ve uzaktan müdahale imkânı sunarken, tarımda sensör destekli izleme ile üretkenlik artırılmaktadır. Ayrıca akıllı ev sistemleri, ulaşım çözümleri ve giyilebilir teknolojiler bireysel konforu ve güvenliği artırmakta, kullanıcı deneyimini kişiselleştirmektedir (Shahin, Maghanaki, Hsseinzadeh ve Chen, 2024, s. 6; Abdul-Qaw vd., 2015, s. 78-80).

IoT uygulamalarının birbirinden farklı sektörlerde farklı ihtiyaçlara hitap etmesi nedeniyle, IoT teknolojilerine yönelik saldırıları ve var olan zafiyetleri tek bir kaynakta toplayan, açıklayan ve sınıflandıran çalışmalar bulunmamaktadır. Var olan çalışmalar belirli bir kullanım amacına yönelik IoT sisteminin zafiyetlerini ele almaktadır veya bu sisteme yönelik olarak gerçekleştirilen bir saldırı üzerinden çözüm önerileri sunmaktadır. Bu konuya ilişkin kapsamlı bir çalışmanın ve eğitim rehberinin olmaması, bireylerin, kurumların ve bilgi güvenliğinin sağlanması konusunda sorumluluk sahibi olan olay müdahale ekiplerinin bu konuda bilinçlenmelerini ve yeterli düzeyde önlem almalarını zorlaştırmaktadır. Bu çalışma, IoT sistemlerindeki güvenlik zafiyetlerini ele alan çalışmaları analiz ederek olası tehditleri sınıflandırmayı, IoT bilgi güvenliği önlemlerine ilişkin

önerileri sunmayı ve ilgili paydaşların rollerini ortaya koyarak IoT sistemlerinin güvenli kullanımına yönelik farkındalık oluşturmayı amaçlamaktadır.

2. IOT GÜVENLİK AÇIKLARININ ÇOK BOYUTLU SINIFLANDIRILMASI

IoT farklı alanlardaki dijitalleşme süreçlerini hızlandırmasına rağmen, beraberinde çok katmanlı ve çeşitli güvenlik zafiyetlerini de getirmiştir. Literatürde IoT güvenliği üzerine çok sayıda çalışma bulunsa da bu zafiyetleri bütüncül ve sistematik bir çerçevede ele alan sınırlı sayıda kaynak bulunmaktadır. Bu bağlamda, Neshenko ve arkadaşları (2019) tarafından geliştirilen ve Şekil 1'de gösterilen IoT Güvenlik Açıkları Taksonomisi, IoT güvenlik açıklarını beş temel boyut altında sınıflandırarak literatürdeki önemli bir boşluğu doldurmaktadır. Buna göre IOT güvenlik açıklıklarına yönelik temel sınıflandırma; (i) mimari katmanlar, (ii) güvenlik hedeflerine etkileri, (iii) bu zafiyetlerden faydalanan saldırı türleri, (iv) önerilen karşı önlemler ve (v) durumsal farkındalık mekanizmaları başlıkları altında yapılmıştır.

IoT sistemleri genellikle üç temel mimari katman çerçevesinde yapılandırılmaktadır. Bunlar cihaz (donanım), ağ (iletişim) ve yazılım (uygulama) katmanlarıdır. Her katman kendine özgü teknolojik bileşenler ve işlevlerle birlikte farklı türde güvenlik zafiyetlerine açık hale gelmektedir (Neshenko vd., 2019, s. 7). Cihaz katmanı, işlemci gücü, enerji ve bellek kısıtları nedeniyle klasik güvenlik önlemlerinin uygulanmasını zorlaştırmaktadır (Neshenko vd., 2019). IoT sistemlerinde cihazlar arası iletişim ZigBee, 6LoWPAN, CoAP, MQTT gibi protokollerle sağlanmaktadır ancak düşük enerji önceliği, güvenliği ikincil kılmaktadır. Yazılım tabanlı IoT açıkları ise güncelleme eksikliği, zayıf kimlik bilgileri, güvensiz API'ler ve web arayüzleriyle ilişkilidir.

IoT sistemlerinin yaygınlaşması, sadece verimlilik ve otomasyon avantajları değil, aynı zamanda çok katmanlı ve karmaşık bir siber tehdit yelpazesiyle karşı karşıya kalmamıza neden olmuştur. Bu bağlamda, literatürde IoT sistemlerinin güvenliği çerçevesinde "gizlilik", "bütünlük", "kullanılabilirlik" ve "hesap verebilirliği" esas alan dört temel güvenlik etkisi öne çıkmaktadır. Gizlilik, bilgi güvenliği üçlüsü (CIA- Confidentiality, Integrity, Availability) olarak da adlandırılan, bilginin korunmaya değer karakteristik özelliklerinden biridir ve ISO/IEC 27001 gibi uluslararası bilgi güvenliği standartlarında da temel güvenlik ilkelerinden biri olarak tanımlanmaktadır (ISO, 2022). IoT sistemlerinin doğası gereği yüksek hacimli veri üretmesi, bu verilerin kullanıcı kimliğiyle kolayca ilişkilendirilebilmesi riskini artırmaktadır. Bu nedenle sistem güvenliğinin sürdürülebilirliğinin sağlanmasının yanı sıra gizlilik bireysel mahremiyetin korunması açısından da kritik öneme sahiptir. Bütünlük ilkesi, verinin iletimi veya saklanması sırasında yetkisiz olarak değiştirilmemesini ve doğruluğunun korunmasını ifade etmektedir. Bu ilke, NIST SP 800-53 ve ISO/IEC 27001 gibi güvenlik standartlarında da sistemlerin güvenilirliğinin odak noktasındadır. IoT sistemlerinde veri bütünlüğünün bozulması yalnızca yanlış karar alma riskini doğurmakla kalmayıp, aynı zamanda tüm bağlı sistemleri etkileyebilecek zincirleme güvenlik açıklarına neden olabilmektedir. Kullanılabilirlik ilkesi sistem kaynaklarının ve hizmetlerinin, ihtiyaç duyulduğu anda erişilebilir ve işlevsel olmasını ifade eder. Kullanılabilirlik, ISO/IEC 27001 ve NIST SP 800-53 gibi standartlarda hizmet kesintilerinin önlenmesi, kaynakların verimli yönetimi ve saldırılara karşı dirençli yapıların kurulmasıyla ilişkilendirilmektedir. IoT gibi yoğun bağlantılı ortamlarda kullanılabilirlik, özellikle gerçek zamanlı uygulamalar açısından kritik öneme sahiptir. IoT sistemlerinde kullanılabilirlik, hizmetlerin kesintisiz ve gecikmesiz şekilde sunulmasıyla ilgilidir (ISO/IEC 27001; NIST SP 800-53). Hesap verilebilirlik, bir sistemde gerçekleşen olayların kim tarafından ve hangi koşullar altında gerçekleştirildiğinin izlenebilmesini sağlayan güvenlik ilkesidir. ISO/IEC 27001 standardında bu ilke, özellikle işlem ve etkileşime yönelik olay kayıtlarının tutulması, erişimlerin denetlenebilirliği ve faaliyetlerin izlenebilirliği ile ilişkili olarak tanımlanmaktadır. IoT sistemlerinde ise bu gereklilik, cihaz etkileşimlerinin ve veri işleme süreçlerinin şeffaf bir şekilde izlenmesiyle sağlanmaktadır. Bu boyut genellikle kimlik doğrulama, yetkilendirme, loglama sistemleri ve davranış izleme teknikleri ile desteklenmektedir.

IoT sistemlerinde güvenliğin bütüncül olarak ele alınabilmesi için teknik önlemlerle sınırlı kalmadan, saldırı türlerinin sistem üzerindeki etkilerini de analiz eden yaklaşımlar geliştirilmelidir. Saldırılar teknik önlemlerin yanı sıra, güvenlik etkileri ve hizmet sürekliliği gibi açılardan da değerlendirilmelidir. Gizlilik ve kimlik doğrulamaya karşı saldırılar, cihazlara izinsiz erişim sağlanmasına ve/veya kullanıcıya ait özel bilgilerin açığa çıkarılmasına neden olmaktadır. Veri bütünlüğüne yönelik saldırılar, iletilen verilerin değiştirilmesi, tahrif edilmesi veya gerçekliğinin bozulmasıyla gerçekleşmektedir. IoT sistemlerinde kullanılabilirliğe yönelik saldırılar ise sistem kaynaklarını aşırı yükleyerek hizmetlerin yavaşlamasına veya tamamen durmasına neden olmaktadır. Bu tür saldırılar sistemin erişilebilirliğini hedef almakta ve genellikle ağ trafiğinin arttırılmasına, parazit oluşturulmasına ve fiziksel kaynakların tüketilmesine neden olabilecek yöntemler kullanılarak gerçekleştirilmektedir.

Karşı önlemler, IoT sistemlerinde tespit edilen güvenlik açıklarının olumsuz etkilerini azaltmak veya tamamen ortadan kaldırmak amacıyla geliştirilen savunma stratejilerini kapsamaktadır. Erişim doğrulama kontrolleri, yazılım güvencesi ve güvenlik protokolleri karşı önlemler içinde tanımlanırken, erişim doğrulama kontrolleri de algoritmalar ve kimlik doğrulama şemaları, biyometrik tabanlı modeller ve içeriğe duyarlı izin modellerinden oluşan üç grup altında sınıflandırılmaktadır. IoT ortamlarında güvenli iletişim için geliştirilen algoritma ve kimlik doğrulama şemaları özellikle ECC, hash fonksiyonları, LFSR (linear feedback shift register) gibi hafif kriptografik yöntemleri kullanmaktadır. Bu şemalar cihazlar arasında oturum anahtarı paylaşımı, karşılıklı kimlik doğrulama ve veri bütünlüğü sağlama işlevi görmektedir. Ancak bu konuya ilişkin birçok öneri sınırlı işlem gücü olan cihazlarda yüksek gecikme veya zayıf saldırı direnci gibi sorunlar barındırmaktadır (Kadri, Abdelli ve Ben Othman, 2024, s. 18–19). Biyometrik tabanlı kimlik doğrulama sistemleri, IoT ortamlarında güvenliğin artırılması amacıyla giderek daha fazla tercih edilen yenilikçi çözümler arasında yer almaktadır. Geleneksel parola, PIN veya donanımsal anahtar gibi yöntemler, yetkisiz erişimlere karşı yetersiz kalmakta ve cihazların fiziksel olarak ele geçirilmesi durumunda önemli ölçüde güvenlik zafiyeti oluşmaktadır. Bu bağlamda, parmak izi, yüz tanıma, retina taraması, ses analizi ve davranışsal imzalar gibi biyometrik verilerden yararlanan sistemler, kişiye özgü ve taklit edilmesi güç özellikler üzerinden kimlik doğrulaması sağlayarak daha yüksek güvenlik seviyesi sunmaktadır. İçeriğe duyarlı erişim modelleri (context-aware access control), kullanıcının konumu, zamanı, kullanmakta olduğu cihazı vb. çevresel faktörlere göre dinamik olarak erişim haklarını tanımlar. Özellikle sağlık sistemleri gibi hassas alanlarda bu tür erişim kontrolü veri sızıntılarını azaltmak için kritik öneme sahiptir. Ancak bu sistemlerin karmaşıklığı ve yüksek işlem yükü gibi pratik sınırlılıkları da mevcuttur (Kadri, Abdelli ve Ben Othman, 2024, s. 21). Yazılım güvencesi, IoT sistemlerinde yazılım kaynaklı açıkların tespiti ve önlenmesiyle sistemin güvenilirliğini arttırmayı amaçlamaktadır. Güvenlik protokollerine ilişkin temel beklenti, IoT cihazları arasında gizlilik, bütünlük ve kimlik doğrulamayı sağlarken, bunun düşük işlem yükü ve enerji verimliliği ile gerçekleştirilmesidir.

Durumsal farkındalık, bir sistemin içinde bulunduğu çevresel koşulları algılama, bu koşulları anlamlandırma ve gelecekteki olası durumları öngörebilme yeteneğini ifade etmektedir. Bu yetenek, özellikle dinamik ve tehditlere açık ortamlarda faaliyet gösteren IoT sistemleri için kritik öneme sahiptir. Zira durumsal farkındalık, mevcut tehditlerinin değerlendirilmesinin yanı sıra potansiyel saldırı senaryolarının da proaktif biçimde değerlendirilmesine imkân sağlamaktadır. Böylece sistemin tepkisel kapasitesi artarken, saldırı öncesinde önlem alma imkânı da oluşmaktadır. Bu da genel sistem direncini ve güvenliğini önemli ölçüde arttırmaktadır (Neshenko vd., 2019, s. 19). Zafiyet değerlendirmesi, bal küpleri, ağ keşfi ve davranış temelli veya bilgiye dayalı saldırı tespiti, durumsal farkındalığa ilişkin alt konu başlıklarını oluşturmaktadır. Zafiyet değerlendirmesi, sistem davranışları ve tehditler dikkate alınarak güvenlik açıklarının dinamik biçimde analiz edilmesidir. Bal küpleri, saldırganları yanıltmak ve davranışlarını analiz etmek amacıyla oluşturulan tuzak sistemlerdir (Hassan vd., 2024). Ağ keşfi saldırganların ağdaki cihazları, açık portları ve servisleri tespit ederek sistem hakkında bilgi topladığı ilk saldırı aşamasıdır (Nazir, He, Zhu, Qureshi, Qureshi, Ullah,

Wajahat ve Pathan, 2024). Saldırı tespiti ise IoT ağlarında güvenliği tehdit eden anormal ya da zararlı davranışların belirlenmesi sürecidir ve bu süreçte makine öğrenimi gibi tekniklerle sistemlerin tehditlere karşı proaktif olarak korunması amaçlanmaktadır (Farooq, Tariq ve Asim, 2022, s. 141-160). Literatürde saldırı tespit sistemleri genel olarak davranış temelli ve bilgiye dayalı olmak üzere iki başlık altında değerlendirilmektedir. Davranış temelli saldırı tespiti, sistemin normal işleyişinden sapmaları analiz ederek sıfırıncı gün saldırılarını belirlemede etkilidir (Coulter ve Pan, 2018). Bilgiye dayalı (imza tabanlı) saldırı tespiti ise bilinen tehdit kalıplarını tanıyarak saldırıları belirlemektedir. Ancak sıfırıncı gün tehditlerine karşı zayıftır (Coulter ve Pan, 2018).

3. YÖNTEM

Bu araştırmada, nesnelerin interneti (IoT) teknolojilerinin barındırdığı güvenlik risklerinin ve tehditlerin tespiti, sınıflandırılması ve bu tehditlere karşı alınabilecek önlemlerin ortaya konulması amaçlanmaktadır. Bu doğrultuda araştırma, betimsel araştırma (tarama) modeline dayalı olarak tasarlanmıştır. Betimsel araştırmalar, bir durumu olduğu gibi sistematik biçimde tanımlamayı ve var olan olgular arasında ilişkileri açıklamayı hedeflemektedir (Karasar, 2019).

Araştırmada herhangi bir değişken üzerinde doğrudan müdahale gerçekleştirilmeden, mevcut literatürden elde edilen veriler analiz edilerek kapsamlı çıkarımlar yapılmıştır. Bu yaklaşım, IoT teknolojilerine yönelik mevcut güvenlik zafiyetlerini, tehditleri ve alınabilecek güvenlik önlemlerini derinlemesine anlamada etkili bir yöntem sunmaktadır.

Bu araştırmada aşağıdaki sorulara yanıt bulunması amaçlanmıştır;

- IoT sistemlerine yönelik başlıca risk ve tehditler nelerdir?
- IoT sistemlerine yönelik güvenlik açıklıkları nasıl sınıflandırılır?
- IoT güvenliğine ilişkin çalışmaların içeriklerinin IoT açıkları sınıflandırmasına göre dağılımı nasıldır?
- IoT güvenliğine yönelik olarak yapılan çalışmalarda öne çıkan zafiyetler ve alınacak güvenlik önlemleri nelerdir?
- IoT güvenlik zafiyetlerinin giderilmesi amacıyla tüm kurumlarda alınması gereken temel önlemler nelerdir?

3.1. Araştırma Evreni ve Kapsam

Bu çalışma kapsamında incelenen makalelere ScienceDirect veri tabanı üzerinden çevrimiçi olarak erişilmiştir. Makale arama stratejisine ilişkin bilgiler Tablo 1 üzerinde görülmektedir. Araştırma kapsamında incelenecek olan makalelerin belirlenmesi sürecinde "IoT vulnerabilities" ve "IoT security" anahtar kelimeleri kullanılmıştır. "IoT vulnerabilities" anahtar kelimesiyle ulaşılan 167 çalışma ile "IoT security" anahtar kelimesiyle ulaşılan 3165 çalışma içeriği üzerinde ön inceleme yapılarak, Şekil 1 üzerinde belirtilen uygunluk kriterlerine göre incelenecek çalışmalar araştırmaya dahil edilmiştir. Bu kapsamda uygun niteliğe sahip olan toplam 301 çalışma belirlenmiş ve bu çalışmalar üzerinde detaylı analiz gerçekleştirilmiştir.

Tablo 1. Arama Stratejisinin Özeti

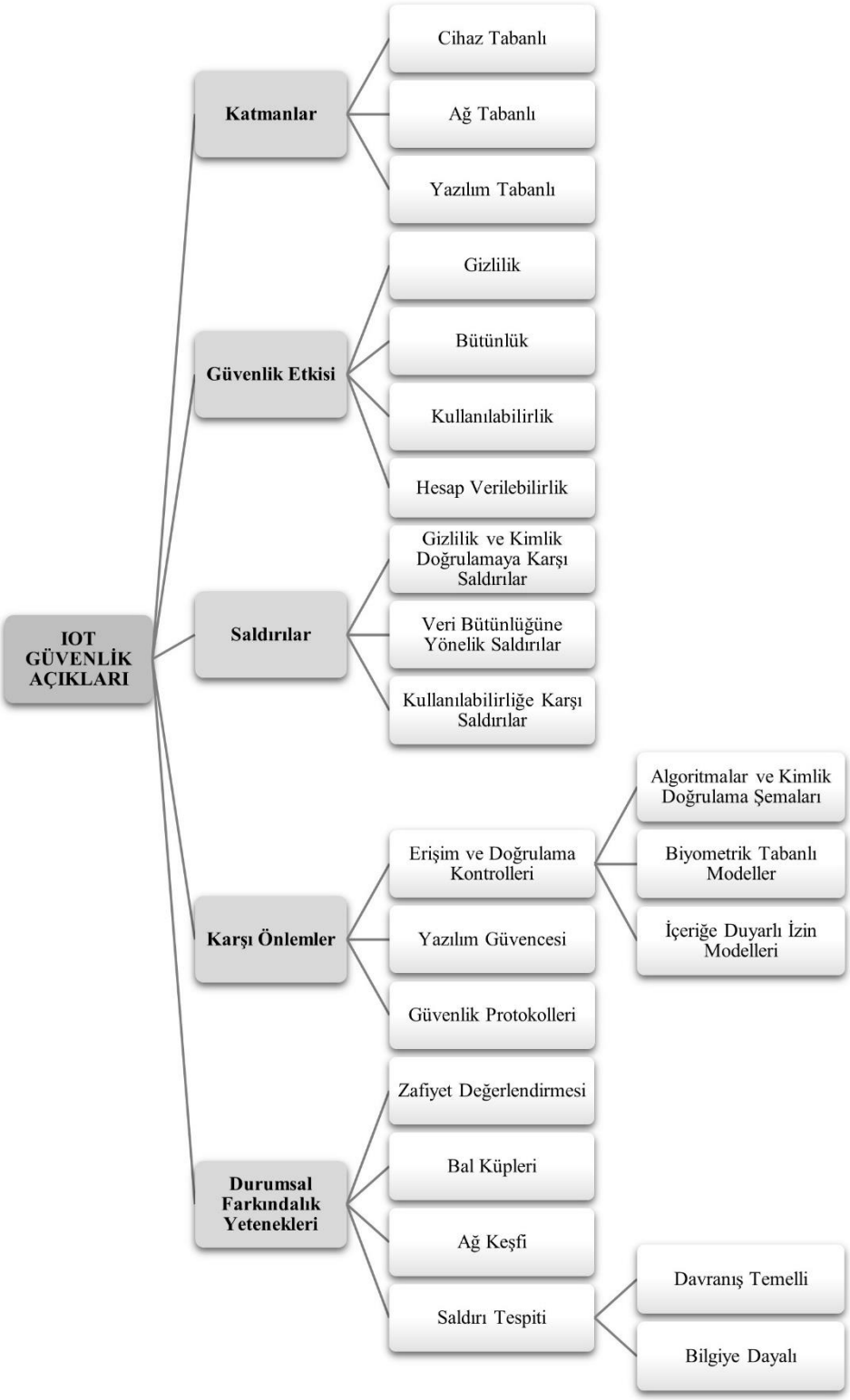
Kriterler	Detaylar
Arama Terimleri	"IoT vulnerabilities", "IoT security"
Dahil Etme	Etki faktörü yüksek ve üniversite internet sunucuları üzerinden erişim sağlanabilen çalışmalar.
Dışlama Kriterleri	Belirtilenen kavramsal çerçeve ile doğrudan ilgili olmayan çalışmalar.

Araştırma Veritabanı	ScienceDirect
Son Arama Tarihi	14.04.2025 tarihi itibariyle inceleme kriterlerini sağlayan çalışmalar belirlenmiş ve araştırmada analiz sürecine geçilmiştir.

Araştırma kapsamında incelenecek makaleler etki faktörünün yüksek olmasına dikkat edilerek belirlenmiştir. Bu çerçevede IoT güvenliğine ilişkin olarak belirlenen 301 akademik çalışma üzerinde sistematik olarak yapılan çok katmanlı içerik incelemesi yalnızca teknik boyutla sınırlı kalmayan, aynı zamanda sosyal ve kurumsal farkındalık düzeyini de yansıtan kapsamlı bir analiz çerçevesi sunmaktadır.

3.2. Veri Toplama Süreci

Araştırma verileri içerik analizine dayalı nitel araştırma yöntemiyle elde edilmiştir. ScienceDirect platformu üzerinden “IoT vulnerabilities” ve “IoT security” gibi anahtar kelimelerle tarama yapılmış, elde edilen sonuçlar özgünlük, atıf sayısı ve konu uygunluğu gibi kriterlere göre filtrelenmiştir. “IoT vulnerabilities” ve “IoT security” anahtar kelimeleriyle yürütülen literatür taraması ve araştırma kapsamına dahil edilecek çalışmaların ön inceleme yapılarak belirlenme işlemleri 4 Ocak 2025 - 14 Nisan 2025 tarihleri arasında yapılmıştır. İlgili çalışmalar, OWASP IoT Top 10 (2018) gibi küresel ölçekte kabul gören referans çerçeveler temel alınarak belirlenen tehdit kategorilerine göre genel olarak sınıflandırılmış ve elde edilen tüm veriler Şekil 1 üzerinde görülen önceden tanımlanmış sınıflandırma temaları (Neshenko, Bou-Harb, Crichigno, Kaddoum ve Ghani, 2019, s. 6) doğrultusunda nihai ve detaylı olarak kategorilere ayrılmıştır.



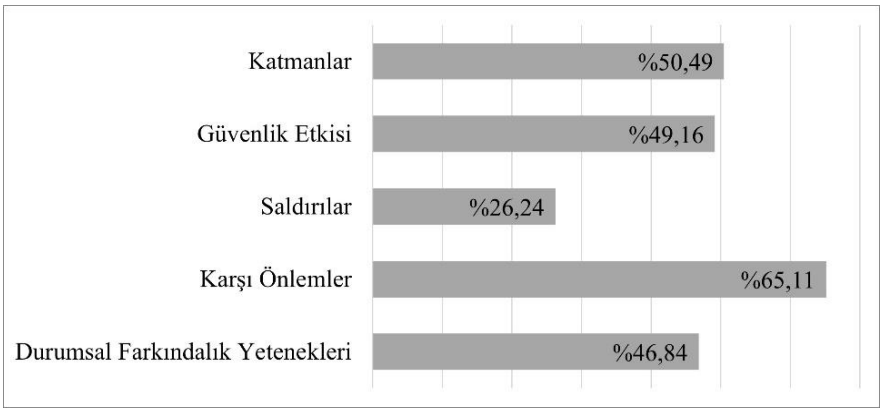
Şekil 1. IoT Güvenlik Açıkları (Neshenko, Bou-Harb, Crichigno, Kaddoum ve Ghani, 2019, s. 6)'den uyarlanmıştır.

4. BULGULAR VE DEĞERLENDİRME

Bu çalışmadaki sınıflandırma işleminin dayanağını oluşturan Şekil 1 üzerinde görülen sınıflandırma çerçevesinde belirlenen çalışmalar detaylı bir şekilde incelenerek, araştırmadan elde edilen veriler doğrultusunda her boyut için literatürde ne tür çözüm önerilerinin sunulduğu, hangi

konuların eksik bırakıldığı ve zafiyetlerin nasıl tartışıldığı sistematik biçimde ortaya konulmaktadır. Böylece literatürdeki eğilimler, boşluklar ve geliştirilmesi gereken noktaların bütüncül bir bakış açısıyla değerlendirilmesi sağlanmıştır. Oluşturulan kavramsal çerçeveye bağlı olarak incelenen çalışmaların güvenlik sınıflandırması bazında dağılımına ilişkin veriler Şekil 2 üzerinde sunulmuştur. Araştırma kapsamında incelenen tüm çalışmalar ilgililik durumuna göre incelenerek ait olduğu başlıklar altında sınıflandırılmıştır.

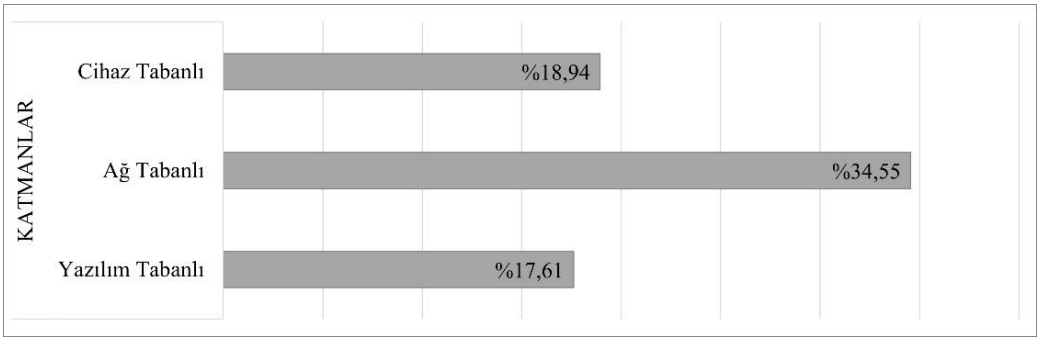
Araştırma kapsamında Şekil 2 üzerinde görülen beş ana sınıflandırma başlığı ve alt konu başlıklarıyla ilişkilendirilen yayınlar, birden fazla ana veya alt konu başlığına ilişkin içeriğe sahip olabilmektedir. Bu durum ana sınıflandırma başlığı veya alt konu başlıklarıyla ilişkili olduğu değerlendirilerek verilen frekansların (f) toplamının, araştırma kapsamında incelenen yayın sayısından (n) farklı olmasına sebebiyet vermektedir.



Şekil 2. İncelenen Çalışma İçeriklerinin IoT Açıkları Sınıflandırmasına Göre Dağılımı

4.1. Katmanlar

Araştırma kapsamında incelenen 301 çalışmanın %50,49'u (f=152) katmanlar başlığı ile ilgilidir. Alt başlıklarda ise Şekil 3 üzerinde görüldüğü gibi en sık kullanılan güvenlik düzeyi ağ tabanlı katman olmuştur. %34,55'lik (f=104) oranla literatürde gizlilik etkisinden sonra en çok ele alınan ağ tabanlı katmana ilişkin konular, genellikle saldırı tespit ve savunma sistemlerinin test edildiği alan olarak öne çıkmaktadır. Bu kapsamda yapılan çalışmaların ağ saldırılarına yönelik olarak geliştirilen savunma araçları üzerinde yoğunlaştığı görülmektedir. Örneğin bu tür çalışmalardan biri olan Zhengwei Zhu ve arkadaşlarının (2024) çalışmasında, derin pekiştirmeli öğrenme yöntemleriyle ağ saldırılarına karşı otomatik savunma ajanları geliştirilmiş ve DQN tabanlı algoritmalarla yüksek başarı oranlarına ulaşılmıştır. Cihaz tabanlı katmana yönelik çalışmaların oranı %18,94 (f=57) ile ikinci sırada yer almaktadır. Bu katmana ilişkin çalışmalarda daha çok fiziksel saldırılar, donanım güvenliği ve gömülü sistem açıklıklarına yönelik sorunlar ve çözüm önerileri öne çıkmaktadır. Yazılım tabanlı katmana ilişkin çalışmaların ise %17,61 oranında (f=53) olduğu ve bu çalışmalarda çoğunlukla uygulama seviyesindeki yazılım açıkları, API zafiyetleri ve güncelleme eksiklikleri üzerinde durulduğu görülmektedir.



Şekil 3. IoT Güvenlik Açıklarına İlişkin Katmanlar ve İncelenen Çalışmaların Dağılımı

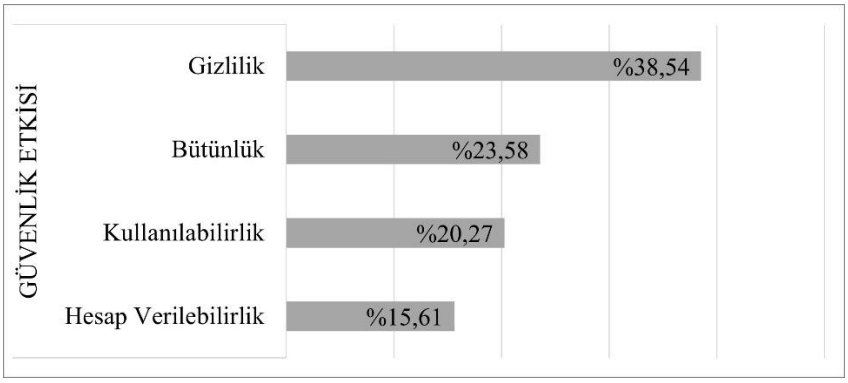
Neshenko ve arkadaşları (2019) tarafından önerilen taksonomi doğrultusunda, cihaz (donanım), ağ (iletişim) ve yazılım (uygulama) katmanı özelinde literatürde tespit edilen başlıca zafiyet türleri sistematik bir biçimde ele alınmış ve açıklanmıştır. Cihaz tabanlı katmanlara ilişkin olarak, Rondon vd. (2022) bu katmanda protokol açıkları ve fiziksel riskleri vurgulanmaktadır. Alomari ve Kumar (2024) kuantum saldırılarına karşı zayıf yönleri belirtmektedir. Allen vd. (2024), akıllı ev cihazlarının fiziksel saldırılara karşı başarısız olduğunu göstermektedir. Sayed vd. (2022), ev altyapısında cihaz düzeyli saldırıların enerji şebekesini de etkileyebileceğini belirtmektedir. Schiller vd. (2022) fiziksel tehditlerin tespit edilemediğini ve cihaz katmanının IoT güvenliğinde en zayıf halka olduğunu savunmaktadır.

Ağ tabanlı Katmanlara ilişkin olarak, Gönen (2024), DoS saldırılarının ağ trafiği ve güç tüketimine etkisini göstermektedir. Bhardwaj vd. (2023) IoT kameralarındaki açık port ve sabit şifrelerin Mirai benzeri saldırıları kolaylaştırdığını belirtmektedir. Zohourian vd. (2023), ZigBee'deki varsayılan anahtarların çok adımlı saldırıları tetiklediğini ortaya koymaktadır. Mahbub (2020) ise CoAP ve MQTT gibi protokollerdeki yerleşik güvenliğin yetersizliğine dikkat çekmektedir.

Yazılım tabanlı Katmanlara ilişkin olarak, HaddadPajouh vd. (2021) uygulama katmanında aşırı yetkilendirme ve yazılım açıklıklarına dikkat çekmiş ve bu açıklığın giderilmesine yönelik olarak DTLS ve güvenli API tasarımını önermektedir. Mahbub (2020), SQL enjeksiyonu ve zayıf oturum yönetimi gibi tehditlere karşı kriptografik ve ML tabanlı çözümler sunmaktadır. Nath ve Nath (2022) XSS, kimlik taklidi ve firmware saldırılarını ele alarak Mirai ve IoTReaper gibi zararlıları analiz etmiş ve bu saldırılara karşı blok zinciri ve hafif kriptografi yöntemlerini önermiştir.

4.2. Güvenlik Etkisi

Araştırma kapsamında incelenen 301 çalışmanın %49,16'sı (f=148) güvenlik etkisi başlığı ile ilgilidir. Bu konu başlığı altında gizliliğe yönelik etkiler Şekil 4 üzerinde görüldüğü gibi %38,54 (f=116) ile en çok ele alınan konudur. İlgili çalışmalar IoT mimarisinin çeşitli katmanlarında gizlilik açıklarını ve bu zafiyetlere karşı alınabilecek önlemleri incelemektedir. İncelenen çalışmalarda, bütünlük ile ilgili olarak veri bütünlüğünü tehdit eden unsurlar ve çözüm yolları, kullanılabilirlikle ilgili olarak sistemin erişilebilirliğini tehdit eden zafiyetler ve hesap verilebilirlik ile ilgili olarak adli ise bilişim süreçlerinin IoT ortamına entegrasyonu ve sertifikasyon eksikliğinin tartışıldığı görülmektedir.



Şekil 4. IoT Güvenlik Açıklarına İlişkin Güvenlik Etkisi ve İncelenen Çalışmaların Dağılımı

Gizliliğin sağlanmasıyla kullanıcıya ait verilerin yetkisiz erişime karşı korunması da dikkate alındığı için güvenlik etkisi açısından IoT sistemlerinde ön plana çıkmaktadır (ISO, 2022). Yüksek veri üretimi bireysel mahremiyet riskini de arttırdığı için literatürdeki birçok çalışmanın gizliliğin korunması için şifreleme, kimlik gizleme ve anonimleştirme tekniklerine yoğunlaştığı görülmektedir. Tewari ve Gupta (2018), veri sızıntısının önemine dikkat çekerek çok katmanlı gizlilik önlemlerinin uygulanmasını önermektedir. Ogonji vd. (2020) ise gizliliği kullanıcı merkezli bir sorun olarak tanımlamakta ve profil çıkarımı ve konum takibi gibi tehditlere karşı kimlik doğrulama, güvenli protokoller ve "privacy by design" yaklaşımını önermektedir. Kokila ve Reddy (2025), PUF ve blockchain gibi çözümleri değerlendirerek bağlama duyarlı gizlilik yaklaşımlarını savunmaktadır. Noor ve Hassan (2019), hafif şifreleme ve çok faktörlü kimlik doğrulama gibi yöntemlerin avantajlarına rağmen anahtar yönetimi sorunlarına dikkat çekmektedir. Tewari ve Gupta (2018), özellikle algılama katmanında şifreleme eksikliği nedeniyle veri sızıntısı riskine vurgu yapmaktadır. Bu çalışmalarda merkezi sistemlerin yerine dağıtık mimarilerin gizlilik açısından daha dirençli olduğu belirtilmektedir.

Bütünlük, IoT ortamında verilerin değiştirilmeden, doğruluğunun korunarak iletilmesini sağlayan kritik bir güvenlik etkisidir (ISO/IEC 27001; NIST SP 800-53). Bu bağlamda blok zincir teknolojileri ve hash temelli doğrulama sistemleri öne çıkmaktadır. Terlapu vd. (2022), PNN modeliyle sağlık verisinde hatalı sınıflandırmayı azaltarak bütünlüğün korunmasını sağlamışlardır. Gharehchopogh ve Abdollahzadeh (2023), MODHHO algoritmasıyla botnet saldırılarını erken tespit ederek veri bütünlüğünü sağlamışlardır. Beyrouti vd. (2024), IoT cihazlarının saldırı taşıyıcısı olabileceğini vurgulayarak etkileşim temelli tehditlerin sistem bütünlüğünü bozduğunu ortaya koymaktadır. Bu çalışmalar, hash doğrulama, risk analizi ve optimizasyonla IoT sistemlerinde veri güvenilirliğini artırmayı amaçlamaktadır.

IoT sistemlerindeki sınırlı kaynaklar, DDoS gibi hizmet aksatmaya yönelik saldırılara karşı savunmasızlık yaratmakta ve kullanılabilirliği doğrudan etkliemektedir. Kumari ve Jain (2023), volumetrik saldırıların hizmetleri aksattığını ve yapay zekâ destekli uyarlanabilir savunma sistemlerine ihtiyaç olduğunu belirtmektedir. Kadri vd. (2024), algı katmanına yönelik saldırıların düşük kaynaklı cihazlarda hizmet kesintisine yol açtığını ve denetimli öğrenme algoritmalarının (RF, SVM, XGBoost) başarı sağladığını vurgulamaktadır. Bu çalışmalarda gerçek zamanlı test ortamlarının eksikliği önemli bir engel olarak sunulmaktadır.

Hesap verebilirlik, IoT sistemlerinde olayların kimin tarafından gerçekleştirildiğinin izlenebilirliğidir (ISO/IEC 27001). Kebande (2022), IoT ortamlarında adli izlenebilirliğin zayıf kaldığını belirterek, Forensics-by-Design yaklaşımını önermektedir. Cirne vd. (2022), güvenlik sertifikalarının izlenebilirliği desteklese de tam uyum sağlamadığını belirtmektedir. Yaqoob vd. (2019), geleneksel adli uygulama modellerinin yetersizliğini vurgulayarak PRoFIT ve Trust-IoV gibi öneriler sunmaktadır. Karale (2021), hukuksal düzenlemelerdeki boşluklara dikkat çekmekte ve GDPR gibi düzenlemelerin sınırlı etkisi nedeniyle, uluslararası normları ve etik ilkeleri esas alan standartlara ihtiyaç olduğunu savunmaktadır.

4.3. Saldırılar

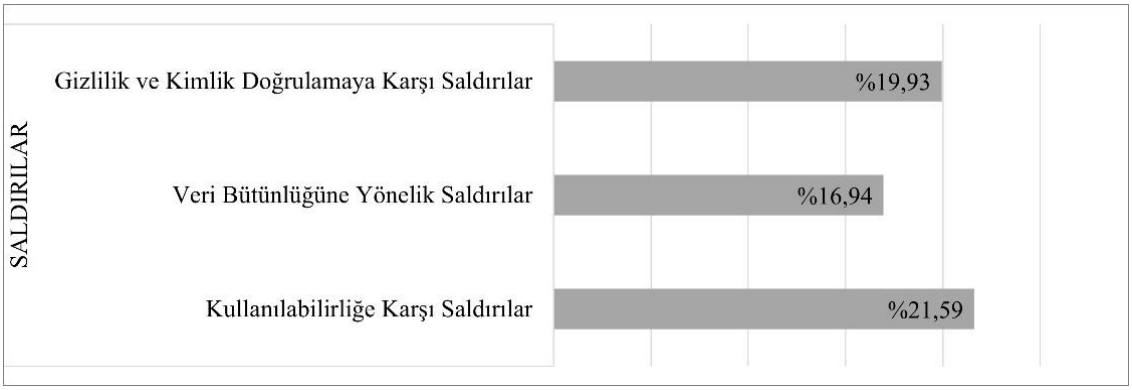
Saldırılara ilişkin olarak literatürde "gizlilik ve kimlik doğrulamaya karşı saldırılar", "veri bütünlüğüne karşı saldırılar" ve "erişilebilirliğe yönelik saldırıların" öne çıktığı görülmektedir. Araştırma kapsamında incelenen çalışmalarda öne çıkan başlıca IoT saldırı türleri ve hedefleri Tablo 2 üzerinde sınıflandırılarak gösterilmiştir.

Tablo 2. IoT Saldırı Türlerinin Sınıflandırılması

IoT Saldırısının Hedefi	Saldırı Türü	Saldırının Tanımı
Gizlilik ve Kimlik Doğrulamaya Karşı Saldırılar	Brute Force Attack	Zayıf/kaba kuvvet şifre denemeleriyle kimlik doğrulamanın aşılmasıdır.
	Replay Attack	Geçmişte kaydedilmiş geçerli verilerin yeniden iletilmesidir.
	Sybil Attack	Birden fazla sahte kimlikle ağın manipülasyonudur.
	Eavesdropping	Ağ üzerindeki veri trafiği dinlenerek verilerin ele geçirilmesidir.
	Side-Channel Attack	Donanım tüketimi/enerji ölçümü ile anahtar çıkarımıdır.
	RFID Spoofing	RFID sistemlerinde sahte bir RFID etiketi ile orijinal etiketi taklit ederek erişim elde etme yöntemidir.
	RFID Skimming	Yetkisiz bir şekilde RFID etiketinden veri okuma işlemi ile kişisel bilgilerin ele geçirilmesidir.
Veri Bütünlüğüne Yönelik Saldırılar	Man-in-the-Middle (MITM)	İki taraf arasındaki iletişimin gizlice yönlendirilmesidir.
	False Data Injection (FDI)	Sisteme sahte veri enjekte edilerek güvenilirliğin bozulmasıdır.
	Firmware Modification	Firmware yazılımına kötü amaçlı kod yüklenmesidir.
Kullanılabilirliğe Yönelik Saldırılar	PDoS (BrickerBot)	Cihazları geri döndürülemez biçimde bozma işlemidir.
	Battery Drain (Vampire Attack)	Enerji tüketimini artırarak cihazları devre dışı bırakmak için kullanılan bir yöntemidir.
	DoS/DDoS	Ağ üzerindeki veri trafiğini arttırarak hizmeti engellemeye yönelik yapılan saldırılardır.
	Flood Attack	Ağa yoğun olarak gereksiz veri göndererek hizmeti aksatmayı amaçlayan saldırı türüdür.
	Sinkhole Attack	Ağa sahte veri yönlendirerek trafiğin manipüle edilmesidir.
	Jamming	Kablosuz sinyalleri bozarak iletişimi engelleme yöntemidir.
	PDoS (BrickerBot)	Cihazları geri dönüşü olmayacak şekilde bozmak için kullanılan yöntemlerden biridir.

Araştırma kapsamında incelenen 301 çalışmanın %32,22'si (f=97) IoT sistemlerini hedef alan saldırılarla ilgilidir. Saldırılar başlığı altında sınıflandırılan çalışmalara ilişkin inceleme verilerine göre en yüksek oranda ele alınan saldırılar Şekil 5 üzerinde görüldüğü gibi %21,59 (f=65) oranıyla kullanılabilirliğe karşı saldırılardır. Bu tür saldırılar, sistemin erişilebilirliğini engelleyen ve servislerin devre dışı kalmasına neden olan tehditleri kapsamaktadır. Literatürde bu başlık altında en sık incelenen saldırı türleri ise hizmet reddi (DoS) ve dağıtık hizmet reddi (DDoS) saldırılarıdır.

İncelenen çalışmalarda %19,93 (f=60) oranında yer verilen gizlilik ve kimlik doğrulamaya karşı saldırılar, genellikle kullanıcı verilerinin sızdırılması ve kimlik sahteciliği gibi tehditleri içerirken, %16,94 (f=51) oranında yer verilen veri bütünlüğüne yönelik saldırılar ise mesajların değiştirilmesi, sahte veri enjeksiyonu ve sistem çıktılarının manipülasyonu gibi durumlarla ilişkilendirilmektedir.



Şekil 5. IoT Sistemlerine Yönelik Saldırılar ve İncelenen Çalışmaların Dağılımı

Gizlilik ve kimlik doğrulamaya karşı saldırıların başlıca hedefleri arasında IoT sistemlerine yetkisiz erişim sağlanması ve/veya kişisel verilerin elde edilmesi bulunmaktadır. Alshammari, Usama ve Azam (2024), IoT tabanlı sağlık sistemlerinde dinleme, ortadaki adam (MitM), flood ve zayıf kimlik doğrulama saldırılarının gizliliği önemli ölçüde tehdit ettiğini belirtmektedir. Zohourian ve arkadaşları (2023), çalışmalarında Zigbee protokolündeki varsayılan anahtar ve şifrelenmemiş başlıkların gizlilik ihlallerine yol açtığını ortaya koymuştur. Nath ve Nath (2022), bilgi kimliği tehditleri ve davranışsal profilleme gibi mahremiyet risklerine dikkat çekerken, Vignau, Khoury, Halle ve Hamou-Lhadj (2021), botnetlerin zaman içinde gizliliği hedef alan tekniklerini geliştirdiğini ortaya koymaktadır. İlgili tüm çalışmalar farkındalığın oluşturulmasına yönelik çözümleri önermektedir.

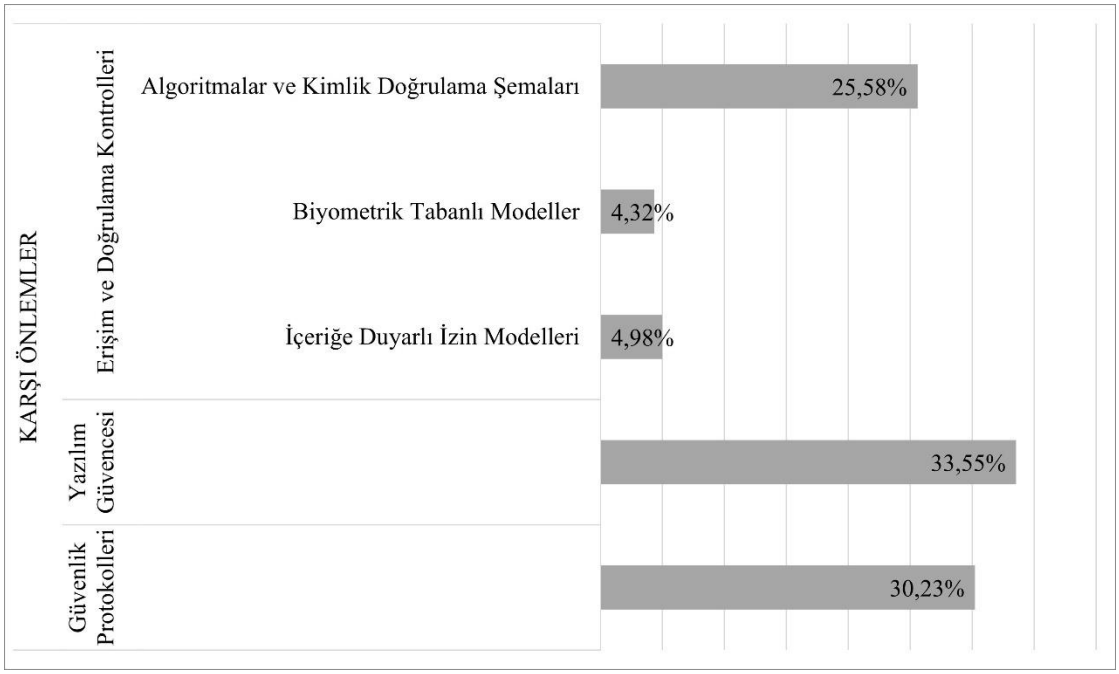
Veri bütünlüğüne yönelik saldırılar, IoT sistemleri üzerinden iletilen verilerin değiştirilmesini ve gerçekliğinin bozulmasını hedef alan saldırılardır. Newaz, Sikder, Rahman ve Uluğaç (2021), sağlık sistemlerinde hasta verilerinin uygulama seviyesinde manipülasyonu sonucu yanlış teşhislerin oluşabileceğini, firmware müdahaleleriyle sistem iç tutarlılığının bozulabileceğini ve MitM saldırılarıyla veri paketlerinin iletim sırasında değiştirilebileceğini ortaya koymaktadır. Sasi, Lashkari, Lu, Xiong ve Iqbal (2024), sahte düğüm ekleme yoluyla sistemin yanlış veriyle yönlendirilebildiğini, yönlendirme manipülasyonu ile verilerin kötü niyetli düğümlere aktarılabildiğini ve SQL enjeksiyonlarının veri tabanı kayıtlarını bozduğunu ortaya koymaktadır. Her iki örnek çalışma da kriptolama, güvenli yazılım kullanımı ve saldırı tespitine yönelik çözümleri önermektedir.

Kullanılabilirliğe yönelik saldırılar sistemin erişilebilirliğini hedef alan ve bunun için ağ trafiğinin arttırılması veya kaynakların tüketilmesine neden olabilecek yöntemlerin kullanıldığı saldırılardır. Gönen (2024), RPL tabanlı IoT ağlarında flood saldırılarının işlemci gücü ve enerji tüketimini artırarak hizmet kesintisine yol açtığını ve yapay zekâ tabanlı NN-ReLU modeliyle bunun %99,9 başarıyla tespit edildiğini belirtmektedir. Quwaider ve Shatnaw (2020), yoğun trafik kaynaklı sıkışmaların dolaylı hizmet reddine sebep olduğunu ve bağışıklık + tepe tırmanma yöntemleriyle tampon taşmalarını önlediklerini ifade etmektedir. Kadri ve arkadaşları (2024), SYN, UDP ve HTTP flood saldırılarının DoS/DDoS bağlamında kullanılabilirliği hedef aldığını ancak Random Forest ve SVM gibi algoritmalarla bu tehditlere karşı savunma geliştirilebildiğini vurgulamaktadır. Ashraf Darwish ve arkadaşlarının (2023) çalışmasında ise ToN-IoT veri seti kullanılarak çok katmanlı yapay sinir ağı (MLP) ile DoS saldırıları tespit edilmiştir. Bu çalışmada yazarlar ağ katmanında

gerçekleştirilen bu tür saldırıların kullanılabilirliği nasıl etkilediğini ortaya koymuş ve geliştirdikleri modelin yüksek doğruluk oranıyla gerçek zamanlı savunma sistemlerinde uygulanabilir olduğunu göstermişlerdir.

4.4. Karşı Önlemler

Araştırma kapsamında incelenen 301 çalışmanın %65,11'i (f=196) IoT sistemlerini hedef alan saldırılara karşı alınabilecek önlemlerle ilgilidir. Karşı önlemlerin altındaki konu başlıklarında ise Şekil 6 üzerinde görüldüğü gibi en çok incelenen konu %33,55'lik (f=101) oranla yazılım güvencedir. Yazılım güvencesi IoT paradigmasını sağlamlaştırmak için hem kaynak hem de ikili kodun güvenlik açıklarını azaltmayı hedeflemekte ve IoT güvenliğinde yazılım temelli güvenlik önlemlerini kapsamaktadır. IoT iletişiminde mimariye uygun ve güvenilir protokol kullanımına ilişkin güvenlik protokolleri ile ilgili içeriğe sahip çalışmaların oranının %30,23 (f=91) olduğu görülmektedir. Erişim ve doğrulama kontrolleri içinde yer alan ve ağırlıklı olarak kriptografik yöntemlerin uygulanışı ve sınırlılıklarına ilişkin çözümler sunan algoritmalar ve kimlik doğrulama şemaları çalışma içeriklerinde %25,58 (f=77) oranında yer bulurken, biyometrik tabanlı modeller ve içeriğe duyarlı izin modellerinin incelenen çalışmalarda %4,32 (f=13) ve %4,98 (f=15) oranlarında yenilikçi çözümler olarak sunulduğu görülmektedir.



Şekil 6. IoT Sistemlerinde Tercih Edilen Karşı Önlemler ve İncelenen Çalışmaların Dağılımı

Erişim ve doğrulama kontrolleri içinde yer alan algoritmalar ve kimlik doğrulama şemalarına ilişkin olarak Kadri, Abdelli ve Ben Othman (2024), ECC ve LFSR gibi hafif algoritmaların IoT cihazlarında yüksek gecikme ve zayıf saldırı direnci sorunları doğurduğunu belirtmektedir. Rana, Mamun ve Islam (2022), PRESENT ve Trivium gibi algoritmaların özellikle anahtar yönetimi ve veri gizliliği açısından zayıf yönlerine dikkat çekmektedir. Thabit ve arkadaşları (2023), GIFT ve RECTANGLE gibi blok şifreleme tekniklerinin düşük enerji tüketimiyle etkili doğrulama sağladığını ortaya koymuştur. Kullanıcı etkileşiminin sınırlı olduğu IoT cihazlarında, biyometrik modeller hem güvenlik hem de kullanılabilirlik açısından etkin bir çözüm olarak değerlendirilmektedir. Omolara ve arkadaşları (2022), RFID tabanlı sistemlerde zayıf kimlik doğrulamanın yaygın olduğunu, buna karşılık parmak izi ve yüz tanıma sistemleri gibi biyometrik temelli modellerin daha güçlü koruma sunduğunu belirtmektedir. Özellikle sağlık ve seçim sistemlerinde yüksek güvenlik ihtiyacı nedeniyle biyometrik doğrulama yönteminin önemi arttığına vurgu yapılmaktır. Kadri, Abdelli ve Ben Othman (2024), içeriğe duyarlı erişim kontrolünün güvenlik açısından önemli olduğunu ancak sistemsel

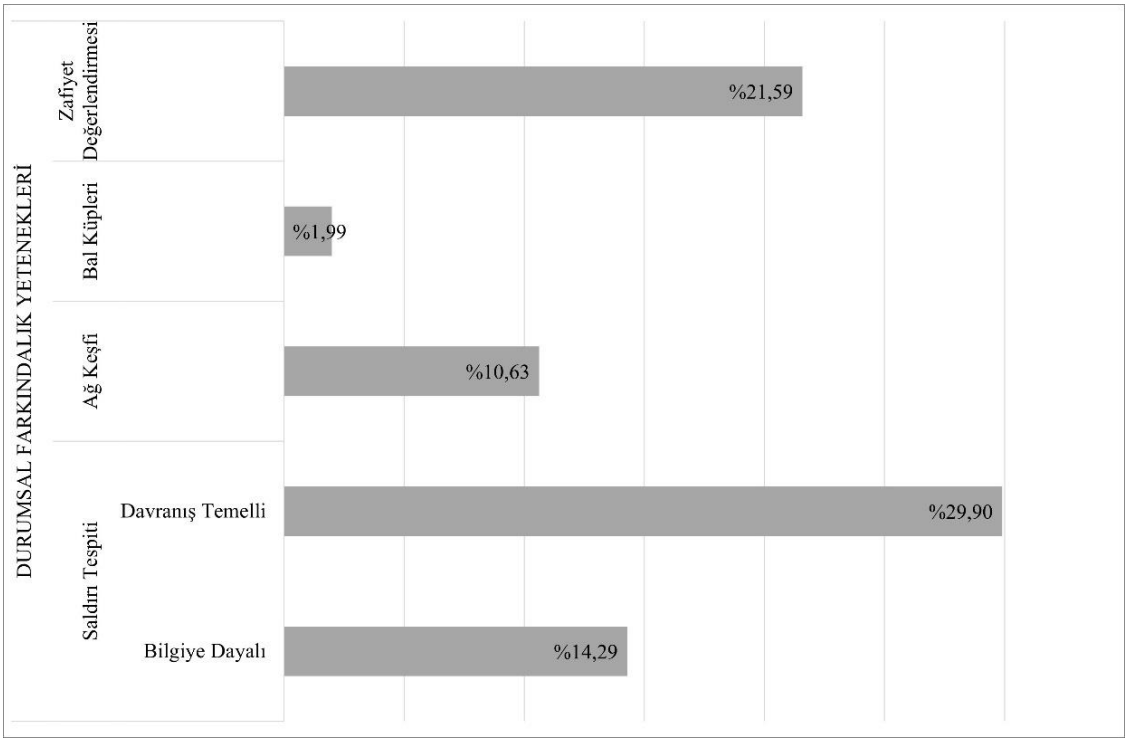
karmaşıklık ve işlem yükü nedeniyle sınırlamalar barındırdığını ifade etmektedir. Harbi ve arkadaşları (2019)ise BAN temelli ve AVISPA ile doğrulanan yeni protokolün kimlik sahteciliği ve DoS saldırılarına karşı etkili olduğunu ortaya koymuştur.

IoT sistemlerinde kullanılan yazılımlardaki açıkların tespiti ve önlenmesi için sistemin güvenilirliğinin arttırılması için yazılım güvencesi büyük öneme sahiptir. Ni ve Li (2024), IoT sistemlerinde yazılım kaynaklı açıklıkları (kimlik doğrulama, zayıf parola, firmware sorunları vb.) makine ve derin öğrenme algoritmalarıyla tespit ederek yazılım güvenliğine katkı sunmuştur. IIoT ortamlarındaki bu açıklıkların SVM, CNN ve Autoencoder gibi algoritmalarla tespit edilebildiğini göstermişlerdir. Ahmad ve Alsmadi (2021), LSTM ve Random Forest gibi tekniklerle botnet saldırılarının yazılım düzeyinde başarıyla tespit edilebildiğini göstermişlerdir. Ayrıca, IoT'ye özgü veri setleri kullanıldığında yazılım güvenliği değerlendirmelerinin daha etkili olduğu belirtilmiştir. İncelenen çalışmalarda genel olarak yazılım güvencesinin otomatik sistemlerle desteklenmesi önerilmektedir.

IoT cihazları arasında gizlilik, bütünlük ve kimlik doğrulama güvenlik protokolleriyle sağlanırken, bu protokollerin düşük işlem gücüyle çalışması ve enerji verimliliğinin arttırılması önem taşımaktadır. Dargaoui ve arkadaşları (2024), 31 kimlik doğrulama protokolünü güvenlik hizmetleri, saldırı direnci ve işlem yüküne göre inceleyerek, ECC ve hash temelli protokollerin düşük güçlü cihazlar için uygun olduğu sonucuna ulaşmıştır. Yugha ve Chithra (2020) ise CoAP, MQTT, DTLS gibi protokollerin katmanlar arası güvenlik sağlamadaki performansını analiz ederek, işlem maliyeti ve enerji verimliliği bakımından farklılıklarını ortaya koymuştur. Her iki çalışmada da güvenli ve ölçeklenebilir IoT için protokol seçiminin önemi vurgulanmaktadır.

4.5. Durumsal Farkındalık Yetenekleri

Araştırma kapsamında incelenen 301 çalışmanın %46,84'ü (f=141) IoT sistemlerinde güvenliğin sağlanmasına yönelik durumsal farkındalığı ele alan içeriği barındırmaktadır. Durumsal farkındalık yetenekleri, sistemin mevcut durumunu doğru okuyabilme, olası tehditleri önceden algılama ve güvenlik açıklarını tespit etme sürecinde kritik bir rol oynamaktadır. Durumsal farkındalık yeteneklerine ilişkin yöntemlerden biri olan davranış temelli saldırı tespitinin %29,90 (f=90) oranıyla incelenen çalışmaların içinde en sık irdelenen yaklaşım olduğu görülmektedir. Bu yöntemde, sistemin normal işleyişine dair davranış kalıpları modellenmekte ve bu modelle uyuşmayan sapmalar potansiyel tehdit veya anomali olarak algılanmaktadır. Farkındalık yeteneklerine yönelik olarak çalışmalarda en çok yer bulan konulardan bir diğeri de %21,59 (f=65) oranıyla zafiyet değerlendirmesidir. Bu yöntemde sistemlerin güvenlik zafiyetleri sistematik biçimde analiz edilerek, olası tehditlerin hangi açıklar üzerinden gerçekleşebileceği tahmin edilmektedir. Bu tür çalışmalar, saldırı öncesinde savunma planlarının geliştirilmesine katkı sunmakta ve sistemin güçlü ve/veya zayıf yönlerini önceden belirlemeye imkân tanımaktadır. Durumsal farkındalık yetenekleri arasında yer alan, saldırganların davranışlarını gözlemlemeye ve sisteme zarar vermeden onları analiz etmeye imkân tanıyan bal küpü (honeypot) sistemlerine yönelik içeriğe %1,99 (f=6) oranla az sayıda çalışmada yer verildiği görülmektedir. Bal küpü sistemleri pasif savunma araçları olarak kullanılmaktadır. Özellikle saldırganların yöntemlerini çözümlemeye ve yeni tehdit türlerini tanımlamaya yönelik fayda sağlamaktadır. Çoğunlukla destekleyici ve ön hazırlık aşamasında kullanılan bir yöntem olan ağ keşfi (network scanning) ile ilgili çalışmaların oranının ise %10,63 (f=32) olduğu görülmektedir. Bu yaklaşım sistemdeki varlıkları, bağlantıları ve açık portları tespit ederek daha sonra uygulanacak savunma ya da saldırı tespit mekanizmalarına veri sağlamaktadır.



Şekil 7. Durumsal Farkındalık Yetenekleri ve İncelenen Çalışmaların Dağılımı

Güvenlik açıklarının dinamik olarak takibi ve analizini sağlayan zafiyet değerlendirmesinde sistem davranışı ve tehditler dikkate alınmaktadır. Bu çerçevede Alomari ve Kumar (2024), kuantum bilişime ilişkin gelişmelerinin mevcut IoT sistemlerindeki şifreleme mekanizmalarını tehdit ettiğini belirterek, zayıf güncelleme süreçleri ve oturum yönetimi hatalarına ilişkin eksiklikleri vurgulamıştır. Çalışmada DREAD modeli ile zafiyetler etkilerine göre önceliklendirilmiş, fiziksel, ağ, algı ve uygulama katmanları ayrı ayrı incelenmiştir. Bu yaklaşım, yalnızca genel risk analizi değil, katman bazlı mimari zafiyetlerin değerlendirilmesini de kapsamaktadır.

IoT sistemlerine yetkisiz erişim sağlamaya çalışan saldırganları yanıltmak ve davranışlarını analiz etmek amacıyla bal küpü tuzakları kullanılmaktadır Alani (2024), 6G destekli akıllı şehirler için geliştirdiği HoneyTwin modelinde SDN, makine öğrenmesi ve honeypot teknolojilerini birleştirerek %99,8 doğrulukla saldırıları tespit etmiş ve proaktif savunma tasarımı geliştirmiştir. Amal ve Venkadesh (2023), çalışmalarında Docker tabanlı H-DOCTOR sisteminde düşük ve yüksek etkileşimli honeypot'ları birleştirerek fidye yazılımlarının %86 doğrulukla erken tespitini yapmış ve güvenlik duvarı kurallarının otomatik güncellenmesini sağlamıştır. Her iki çalışma da bal küplerinin dinamik savunmadaki etkinliğini ortaya koymaktadır.

Saldırganlar ilk aşamada ağ aygıtları üzerindeki port ve servis açıklarını tespit edebilmek için ağ keşfi yöntemlerini kullanmaktadırlar. Nazir ve arkadaşları (2024), IoT ağlarında port tarama, host tarama ve DNS reconnaissance saldırılarını %95'in üzerinde doğrulukla tespit edebilen hibrit bir CNN-LSTM modeli önermektedir. CNN mekânsal bağlantı örüntülerini, LSTM ise zamansal anomalileri analiz etmektedir. Quantization ve pruning teknikleriyle model kaynak kısıtlı cihazlara uyarlanmış ve gerçek zamanlı kullanıma elverişli hâle getirilmiştir. Bu tür çalışmalar ağ tarama saldırılarını başlamadan önce tanımlamayı hedeflemektedir.

IoT sistemlerinin sıra dışı çalışma verilerinin değerlendirildiği ve sıfırıncı gün saldırılarını belirlemede etkili davranış temelli saldırı tespitine ilişkin olarak Zhu, Chen, Zhu ve Zhu (2024), DDQN-DNER modeliyle saldırgan davranışlarını öğrenerek duruma özel savunma üreten bir ajan geliştirmiştir. Nazir ve arkadaşları (2024), CNN-LSTM mimarisiyle zamansal ve mekânsal davranış örüntülerini analiz ederek dinamik saldırı tespiti sağlamıştır. Ahmad ve Alsmadi (2021), davranışsal tespitin özellikle IoT-23 ve N-BaIoT gibi veri setlerinde yüksek doğruluk sağladığını ve sıfırıncı gün

saldırılarına karşı avantaj sunduğunu ortaya koymuştur. Chen ve arkadaşları (2022), IoT ortamlarında XGBoost algoritmasını kullanarak ağ trafiğindeki olağandışı davranışları tespit etmiş ve düşük "yanlış pozitif" oranıyla başarılı sonuçlar elde etmişlerdir. Bu yaklaşım, özellikle gerçek zamanlı saldırı tespiti ve sistem içi öğrenme süreçlerindeki etkinliğiyle dikkat çekmektedir.

Bilinen tehdit kalıpları tanımlanmak suretiyle saldırıların belirlenmesi için bilgiye dayalı (imza tabanlı) saldırı tespiti yöntemleri kullanılmaktadır. Martins ve arkadaşları (2022), bu yöntemin IoT'nin dinamik yapısına uyumda yetersiz kaldığını belirtmiştir. Sıfırıncı gün tehditlerine karşı etkinliğinin zayıf olduğu bilinen bu yönteme ilişkin olarak Ding, Abdel Basset ve Mohamed (2023), TON_IoT gibi veri kümelerinde eğittikleri DeepAK-IoT modeliyle %90'ın üzerinde doğrulukla bilinen saldırıları tanımlamıştır. Lefoane ve arkadaşları (2025) ise IoT cihazlarının kaynak kısıtları nedeniyle bu sistemlerin uç birimlerde değil, 5G/6G destekli merkezî altyapılarda uygulanmasını önermektedir.

5. SONUÇ VE ÖNERİLER

IoT güvenliğine ilişkin 301 akademik yayının sistematik olarak incelendiği ve güvenlik yaklaşımlarının tematik dağılımının değerlendirildiği bu çalışmanın bulguları, IoT güvenliğine yönelik olarak yapılan inceleme ve araştırmaların belirli konu başlıklarında yoğunlaştığını ve literatürde bazı eğilimlerin daha fazla öne çıktığını göstermektedir. Katmanlara dayalı güvenlik analizinin, yapılan çalışmalarda sıkça tercih edilen bir yöntem olduğu görülmektedir. Özellikle ağ tabanlı katman, %34,55 (f=104) oranla bu kategoride en fazla kullanılan güvenlik düzeyi olarak öne çıkmaktadır. Ağ tabanlı katmana ilişkin çalışmalarda saldırı tespit sistemlerinin ve oluşturulan savunma mekanizmalarının test edildiği uygulamaların ağırlıkta olduğu görülmektedir. Cihaz ve yazılım tabanlı katmanlara ilişkin çalışmalarda ise ağırlıklı olarak fiziksel saldırılar, gömülü sistem açıklıkları ve güncelleme eksiklikleri gibi risklerin ele alındığı görülmektedir.

IoT güvenlik açıkları içinde güvenlik etkisine yönelik olarak yapılan 148 (%49,16) çalışmanın büyük bölümünün (f=116) gizlilik konusuna odaklandığı veya içeriğinde gizlilik konusuna yer verdiği görülmektedir. Bu çalışmalardan elde edilen verilere bağlı olarak, veri sızıntısı, kullanıcı profili çıkarımı ve konum takibi gibi tehditlerin önlenmesi için çok katmanlı koruma mekanizmaları ve "gizlilik odaklı tasarım" anlayışı önerilmektedir. Bütünlük ve kullanılabilirlik konularının da incelenen çalışmalarda teknik yönleriyle ele alındığı görülmektedir.

IoT güvenliğini tehdit eden saldırı türleri açısından incelenen çalışmalarda en çok karşılaşılan tehdit türü %21,59 (f=65) oranıyla kullanılabilirliğe karşı saldırılardır. Kullanılabilirliğe yönelik saldırılar arasında en fazla örneği görülen DoS/DDoS saldırıları, bu sınıflandırma içinde hizmetin aksatılmasına ve sistemlerin çevrimdışı kalmasına neden olan önemli tehditler olarak tanımlanmaktadır. Bunun yanı sıra çalışmalarda gizlilik ve veri bütünlüğüne yönelik saldırıların önemine de dikkat çekildiği ve çözüm önerilerinin sunulduğu görülmektedir.

IoT güvenliği kapsamında alınabilecek karşı önlemlere ilişkin literatürün %33,55'inin (f=101) yazılım güvencesi ve buna bağlı savunma yaklaşımlarına odaklandığı görülmektedir. Özellikle makine öğrenmesi ve derin öğrenme algoritmalarıyla yazılım kaynaklı açıklıkların tespiti ve proaktif önlemler geliştirme çalışmalarının son yıllarda yapılan çalışmalarda önemli ölçüde arttığı gözlenmektedir. Güvenlik protokollerinin, kimlik doğrulama algoritmalarının ve biyometrik sistemlerin kullanımı da değerlendirilen ve dikkate alınan diğer güvenlik önlemleri arasında yer almaktadır.

Bu çalışmanın genel çerçevesini oluşturan ana sınıflandırma başlıklarından biri olan durumsal farkındalık yetenekleri ise sistemin güvenliğine yönelik anlık değerlendirmeleri mümkün kılan yapılar olarak öne çıkmaktadır. Bu sınıflandırma başlığına odaklanan çalışmaların %29,90 (f=90) oranıyla en fazla davranış temelli saldırı tespiti yöntemleri üzerinde durduğu görülmektedir. Makine öğrenmesi temelli modellerle olağandışı ağ davranışlarının saptanması, saldırıların erken teşhis

edilmesi için büyük öneme sahiptir. Zafiyet değerlendirmesi, bal küpü sistemleri ve ağ keşfi gibi diğer yöntemlerin ise daha çok destekleyici yaklaşımlar olarak ele alındığı görülmektedir.

IoT güvenlik açıklarının giderilmesine yönelik hâlen kapsamlı bir düzenleme ve uygulama rehberinin bulunmaması nedeniyle, bireylerin, kurumların ve özellikle olay müdahale ekiplerinin konuya dair farkındalık kazanması ve yeterli düzeyde güvenlik önlemlerini doğru zamanda almaları mümkün olamamaktadır. Bu çalışma, dünya genelinde IoT güvenliği ve zafiyetlerine yönelik olarak yapılmış üst düzey çalışmaların konuya yaklaşımlarına, güvenlik stratejilerinin oluşturulmasında odaklanılan teknik yöntemlere ilişkin tercihlere ve zafiyetlerin giderilmesine yönelik çözüm önerilerine dikkat çekmektedir. Literatürde yer alan güncel ve nitelikli çalışmaların sistematik olarak ele alındığı ve analiz edildiği bu çalışmanın bilgi güvenliği stratejilerini belirleyen, yöneten veya uygulayan uzmanların IoT güvenlik açıklarının giderilmesi konusunda farkındalığına katkı sağlayacağı düşünülmektedir. Çalışmada aynı zamanda bireysel IoT kullanıcılarına yönelik olarak da dikkate alınması gereken hususlar vurgulanmıştır. Çalışmadan elde edilen bulgular ve yapılan değerlendirmeler IoT güvenliğinin sağlanmasına yönelik genel stratejik yaklaşım önerilerinin tüm kesimler tarafından dikkate alınması gerektiğini ortaya koymaktadır. Konuya ilişkin temel öneriler aşağıda sıralanmıştır;

- IoT güvenliği politikaları için öncelikle çok katmanlı güvenlik stratejileri geliştirilmelidir. Ağ, yazılım ve cihaz katmanlarına yönelik bütünleşik çözümler sistem güvenliğinin arttırılmasına önemli katkılar sağlamaktadır.

- Gizlilik konusuna özel önem verilmeli ve kullanıcı merkezli tehditlere yönelik gelişmiş doğrulama protokolleri ve veri işleme politikaları geliştirilmelidir.

- IoT sistemlerine yönelik saldırılara karşı proaktif savunma sağlanabilmesi için makine öğrenmesi destekli saldırı tespit sistemleri yaygınlaştırılmalıdır.

- Yazılım güvencesinin ve güncelleme sistemlerinin kullanımının IoT ortamlarında ihmal edilmemesi gerektiği aşikârdır. Bu nedenle açık kaynak kodlu yazılım kullanan sistemlerde güvenli kod geliştirme politikaları titizlikle uygulanmalıdır.

- Durumsal farkındalık sistemlerinin etkinliğini artırmak için hibrit tespit mekanizmalarının (davranışsal ve imzaya dayalı) birlikte kullanılmasına yönelik proje ve çalışmalara öncelik verilmelidir.

KAYNAKÇA

Abdul-Qawy, A. S., Pramod, P. J., Magesh, E., ve Srinivasulu, T. (2015). *The Internet of Things (IoT): An overview*. International Journal of Engineering Research and Applications, 5(12, Part-2), 71–82. Erişim adresi: https://www.researchgate.net/publication/323834996

Abiodun, O. I., Alabdulatif, A., Omolara, A. E., Alawida, M., Alabdulatif, A., Alshoura, W. H. ve Arshad, H. (2021). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, 102494. doi: 10.1016/j.cose.2021.102494

Ahmad, R. ve Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. *Internet of Things, 14*, 100365. doi: 10.1016/j.iot.2021.100365

Alani, M. M. (2024). HoneyTwin: Securing smart cities with machine learning- enabled SDN edge and cloud-based honeypots. Journal of Parallel and Distributed Computing, 187, 104866. doi: 10.1016/j.jpdc.2024.104866

Allen, A., Mylonas, A., Vidalis, S. ve Gritzalis, D. (2024). Smart homes under siege: Assessing the robustness of physical security against wireless network attacks. *Computers & Security*, *131*, 103687. doi: 10.1016/j.cose.2023.103687

Alomari, A. ve Kumar, S., A., P., (2024) Securing IoT systems in a post- quantum environment: Vulnerabilities, attacks, and poossible solutions. doi: 10.1016/j.iot.2024.101132

Alshammari, T., Usama, M. ve Azam, M. A. (2024). A survey on cybersecurity and privacy issues in smart healthcare systems: Attacks, countermeasures and open research directions. Heliyon, 10(1), e100526. doi: 10.1016/j.eij.2024.100526

Amal, M. R. ve Venkadesh, P. (2023). Honey-based ransomware detection in IoT using a hybrid honeynet approach. Measurement: Sensors, 27, 100664. doi: 10.1016/j.measen.2022.100664

Axelrod, C. W. (2015, May). Enforcing security, safety and privacy for the Internet of Things. In *2015 Long Island Systems, Applications and Technology*. IEEE. 10.1109/LISAT.2015.7160214

Beyrouti, M., Lounis, A. ve Lussier, B. (2024). A vulnerability-focused risk assessment framework for IoT security: Design and validation through a healthcare use-case. Internet of Things, 23, 101333. doi: 10.1016/j.iot.2024.101333

Bhardwaj, A., Kaushik, K., Bharany, S. ve Kim, S. (2023). Forensic analysis and security assessment of IoT camera firmware for smart homes. *Egyptian Informatics Journal*, 24. doi: 10.1016/j.eij.2023.100409

Cirne, A., Sousa, P., R., Resende, J., S., ve Antunes, L., (2022). IoT security certifications: Challenges and potential approaches. *Computers & Security,* 116, 102669. doi: 10.1016/j.cose.2022.102669

Coulter, R. ve Pan, L. (2018). Intelligent agents defending for an IoT world: A review. Computers & Security, 77. doi: 10.1016/j.cose.2017.11.014

Dargaoui, S., Azrour, M., El Allaoui, A., Guezzaz, A., Alabdulatif, A. ve Alnajim, A. (2024). Internet of Things Authentication Protocols: Comparative Study. *Computers, Materials & Continua, 79*(1), 65–87. doi: 10.32604/cmc.2024.047625

Ding, W., Abdel Basset, M. ve Mohamed, R. (2023). DeepAK-IoT: An effective deep learning model for cyberattack detection in IoT networks. Information Sciences, 636, 119595. doi: 10.1016/j.ins.2023.03.052

Farooq, U., Tariq, N. ve Asim, M. (2022). A survey on the role of machine learning in enabling IoT-based intrusion detection systems. Journal of Parallel and Distributed Computing, 162. doi: 10.1016/j.jpdc.2022.01.015

Febro, A., Xiao, H., Spring, J. ve Christianson, B. (2022). Edge security for SIP-enabled IoT devices with P4. *Computer Networks*. doi: 10.1016/j.comnet.2021.108698

Gharehchopogh, F. S. ve Abdollahzadeh, B. (2023). A multi-objective dynamic Harris hawks optimization for botnet detection in the Internet of Things. Internet of Things, 23, 100952. doi: 10.1016/j.iot.2023.100952

Gönen, S. (2024). A methodical examination of single and multi-attacker flood attacks using RPL-based approaches. *Computers & Industrial Engineering*. doi: doi.org/10.1016/j.cie.2024.110356

HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M. ve Karimipour, H. (2021). A survey on Internet of Things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, 100129. doi: 10.1016/j.iot.2019.100129

Harbi, Y., Aliouat, Z., Refoufi, A. ve Harous, S. (2019). An enhanced authentication and key management scheme for WSN integrated to IoT. Ad Hoc Networks, 93, 101948. doi: 10.1016/j.adhoc.2019.101948

Hassan, A., Nizam-Uddin, N., Quddus, A. ve Hassan, S. R. (2024). AI-based lightweight security for IoT architecture: A multi-layered analysis. Computers, Materials & Continua, 78(1). doi: 10.32604/cmc.2024.057877

Journal of Imaging Systems and Technology, 33, 100117. doi: 10.1016/j.hcc.2023.100117

Kadri, M. R., Abdelli, A. ve Ben Othman, J. (2024). DoS and DDoS attacks in IoT environments: A systematic review of detection methods, attack types, and validation strategies. Internet of Things, 25, 101021. doi: 10.1016/j.iot.2023.101021

Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. Internet of Things, 15, 100420. doi: 10.1016/j.iot.2021.100420

Karasar, N. (2019). Bilimsel araştırma yöntemi: Kavramlar ilkeler teknikler (34. bs.). Nobel Akademik Yayıncılık.

Kebande, V. R. (2022). Industrial internet of things (IIoT) forensics: The forgotten concept in the race toward industry 4.0. Forensic Science International: Reports, 6, 100257. doi: 10.1016/j.fsir.2022.100257

Khan, S. H., Alahmadi, T. J., Ullah, W., Iqbal, J., Rahim, A., Alkahtani, H. K., Alghamdi, W. ve Almagrabi, A. O. (2023). SB-BR-STM: An ensemble deep learning framework for malware detection in Internet of Things. Computers & Security, 136, 100543. doi: 10.1016/j.prime.2024.100543

Kokila, M. ve Reddy, S. (2025). Authentication, access control and scalability models in Internet of Things Security – A review. Cyber Security and Applications, 100057. doi: 10.1016/j.csa.2024.100057

Kumari, P., ve Jain, A. K. (2023). IoT ortamlarında DDoS saldırılarına yönelik savunma stratejilerinin sistematik analizi. Computers & Security, 130, 103096. doi: 10.1016/j.cose.2023.103096

Landspace of IoT security. *Computer Science Review,* 44, 100467 doi: 10.1016/j.cosrev.2022.100467

Lefoane, M., Ghafir, I., Kabir, S. ve Awan, I. U. (2025). A review of botnet detection mechanisms in the IoT ecosystem: Trends, challenges and future directions. Journal of Network and Computer Applications, 222, 104110. doi: 10.1016/j.jnca.2025.104110

Mahbub, M. (2020). Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *Journal of Network and Computer Applications*, 168, 102761. doi: 10.1016/j.jnca.2020.102761

Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L. ve Gama, J. (2022). Host-based IDS: A review and open issues of an anomaly detection system in IoT. Future Generation Computer Systems, 130. doi: 10.1016/j.future.2022.03.001

Nath, R. N. ve Nath, H. V. (2022). Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges. *Computers and Electrical Engineering, 102*, 107997. doi: 10.1016/j.compeleceng.2022.107997

Nazir, A., He, J., Zhu, N., Qureshi, S. S., Qureshi, S. U., Ullah, F., Wajahat, A. ve Pathan, M. S. (2024). A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem. Ain Shams Engineering Journal, 15(1), 102777. doi: 10.1016/j.asej.2024.102777

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. ve Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, *21*(3), 2702–2733. doi: 10.1109/COMST.2019.2910750

Newaz, A. I., Sikder, A. K. M., Rahman, M. A. ve Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare. doi: 10.1016/j.ins.2019.08.006

Ni, C. ve Li, S. C. (2024). Machine learning enabled Industrial IoT Security: Challenges, Trends and Solutions. *Journal of Industrial Information Integration, 35*, 100549. doi: 10.1016/j.jii.2023.100549

Noor, M. B. M. ve Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer Networks, 148, 283–294. doi: 10.1016/j.comnet.2018.11.025

Ogonji, M. M., Okeyo, G., ve Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review,* 38, 100312. doi: 10.1016/j.cosrev.2020.100312

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H. ve Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 114, 102494. doi: 10.1016/j.cose.2021.102494

Quwaider, M. ve Shatnaw, Y. (2020). An intelligent hybrid congestion control system to secure IoT data reliability using bio-inspired computing. Computers & Security, 95, 102160. doi: 10.1016/j.adhoc.2020.102160

Rana, M., Mamun, Q. ve Islam, R. (2022). A survey on lightweight cryptographic algorithms for resource-constrained IoT devices. Future Generation Computer Systems, 128, 307–324. doi: 10.1016/j.future.2021.11.011

Rondon, L. P., Babun, L., Aris, A., Akkaya, K. ve Uluagac, A. S. (2022). Survey on Enterprise Internet-of-Things systems (E-IoT): A security perspective. *Ad Hoc Networks*, *131*, 102728. doi: 10.1016/j.adhoc.2021.102728

Sasi, T., Lashkari, A., B., Lu, R. ve Xiong, P., (2024). A comprehensive survey on IoT attacks: Taxonomy, detection, mechanisms and challenges. *Journal of Information and Intelligence,* 2, 455-513. doi: 10.1016/j.jiixd.2023.12.001

Sayed, M., A., Atallah, R., Assi, G. ve Debbabi, M., (2022). Electric vehicle attack impact on power grid operation. *International Journal of Electrical Power and Energy Systems, 134*, 107784. doi: 10.1016/j.ijepes.2021.107784

Schiller, E., Aidoo, E., Fuhrer, J., Stahl, J., Ziörjen, M., Stiller, B. (2022).

Sengupta, J., Ruj, S., ve Das Bit, S. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications*, 149, 102481. doi: 10.1016/j.jnca.2019.102481

Shahin, M., Maghanaki, M., Hosseinzadeh, M. ve Chen, F., F. (2024). Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion Detection Systems. *Advanced Engineering Informatics*, 62, 102605. doi: 10.1016/j.aei.2024.102685

Terlapu, P. V., Babu, S., Gangu, V. K. ve Pemula, R. (2022). Olasılıksal sinir ağı temelli bir HCV teşhis modeli: Makine öğrenimi perspektifi.

Tewari, A. ve Gupta, B. B. (2018). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems, 108, 909–920. doi: 10.1016/j.future.2018.04.027

Thabit, F., Can, Ö., Aljahdali, A. O., Al-Gaphari, G. H., ve Alkhzaimi, H. A. (2023). Cryptographic algorithms to enhance IoT security. *Discover Internet of Things, 3*(1), 1–12. doi: 10.1016/j.iot.2023.100759

Turak, Y. (2015). *Nesnelerin İnterneti ve Güvenliği*. İstanbul.

Uluslararası Standardizasyon Örgütü. (2022). *ISO/IEC 27001:2022 – Bilgi güvenliği, siber güvenlik ve gizlilik koruması: Bilgi güvenliği yönetim sistemleri – Gereklilikler*. ISO. Erişim adresi: https://www.iso.org/standard/27001

Vignau, B., Khoury, R., Halle, S. ve Hamou-Lhadj, A. (2021). A taxonomy and analysis of IoT botnet behavior. Journal of Systems Architecture, 119, 102143. doi: 10.1016/j.sysarc.2021.102143

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. M. A., ve Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems, 92, 265–275. doi: 10.1016/j.future.2018.09.058

Yugha, R. ve Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications, 169*, 102763. doi: 10.1016/j.jnca.2020.102763

Zhu, Z., Chen, M., Zhu, C. ve Zhu, Y. (2024). A deep reinforcement learning- based defense model against cyberattacks in dynamic environments. Computers & Security, 135, 103578. doi: 10.1016/j.cose.2023.103578

Zohourian, A., Dadkhah, S., Pinto Neto, E. C., Mahdikhani, H., Danso, P. K., Molyneaux, H. ve Ghorbani, A. A. (2023). IoT Zigbee device security: A comprehensive review. *Internet of Things*, 23, 100791. doi: 10.1016/j.iot.2023.100791