Mühendislik Bilimleri ve Tasarım Dergisi
12(2), 403–415, 2024
e-ISSN: 1308-6693

Journal of Engineering Sciences and Design
DOI: 10.21923/jesd.1231326

Araştırma Makalesi Research Article

IOT CİHAZLARINDA İNSAN HATASINDAN KAYNAKLANAN GÜVENLİK AÇIKLARININ ANALİZİ

Mevlüt SEVİNÇ[1*], İsa AVCI[2]

[1] Karabük Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Bölümü, Karabük, Türkiye
[2] Karabük Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Karabük, Türkiye

Anahtar Kelimeler
Iot Cihazları,
Iot Güvenlik,
Iot Güvenlik Saldırıları,
İnsan Kaynaklı Hatalar.

Öz

1970'li yıllarda başlayan kişisel bilgisayarların kullanımı günümüzde artık yüzlerde çeşit kişisel ürünün kullanımı olarak devam etmektedir. Cep telefonları, akıllı bileklikler ve saatler, tabletler, hatta okullarda kullanılan tahtalar bile artık internete bağlı ve etkileşim halindedirler. Günümüzde IoT (Internet of Things) olarak adlandırılan bu etkileşim, bilim insanlarının da dikkatini çekmektedir. IoT cihazları sadece günlük yaşamda değil, kurumsal, endüstriyel, sağlık, tarım vb. birçok alanda da kullanılmaktadır. Özellikle akıllı cihazların günlük yaşamda kullanımının artmasıyla beraber bir cihaz ekosistemi de kendiliğinden ortaya çıkmıştır. Kalp ritminin ölçümü, derin uyku uyuma süreleri, günlük adım sayısı gibi bilgiler bu cihazlar sayesinde insanların 7/24 takibini sağlamaktadır. Bu durum da beraberinde birçok güvenlik sorununu açığa çıkarmaktadır. Kişisel verilerin çalınması, değiştirilmesi ve ikinci şahıslara satılması gibi muhtemel sebepler bilgisayar korsanları açısından ilgi çekici olarak görülmektedir. Özellikle kredi kartı bilgileri, bankacılık bilgilerinin korunması büyük önem arz etmektedir. Bahsedilen bu güvenlik açıklarının sebeplerinden birisi bu cihazları birincil olarak kullanan insandan kaynaklı hatalardır. Bu çalışmada; insan hayatında bu derece yer eden IoT cihazlarının güvenliğini tehdit eden unsurlar, güvenlik önlemlerini sağlamak için insanların yapması gerekenler incelenecektir. Ayrıca, bu cihazlarda güvenlik açığı oluşturan ve insanlardan kaynaklı güvenlik hataları ile kullanıcıların alabileceği çözüm önerileri analiz edilecektir.

ANALYSIS OF SECURITY VULNERABILITIES CAUSED BY HUMAN ERROR IN IOT DEVICES

Keywords
IoT Devices,
IoT Security,
IoT Security Attacks,
Human-Caused Faults.

Abstract

The use of personal computers, which started in the 1970s, is now a use of hundreds of different personal products. Cell phones, smart wristbands and watches, tablets, and even the blackboards used in schools are now connected to the internet and interact with each other. This interaction, now called IoT (Internet of Things), is also attracting the attention of scientists. IoT devices are used not only in daily life but also in many areas such as corporate, industrial, health, agriculture, etc. Especially with the increasing use of smart devices in daily life, a device ecosystem has emerged spontaneously. Information such as heart rhythm measurement, deep sleep sleep times, daily step count, etc. are tracked 24/7 by these devices. This raises many security issues. Possible reasons such as theft, alteration, and sale of personal data to second parties are seen as interesting for hackers. Especially the protection of credit card information and banking information is of great importance. One of the reasons for these security vulnerabilities is the human error that is the primary user of these devices. This study will examine the factors that threaten the security of IoT devices, which have such a place in human life, and what people should do to ensure security measures. In addition, security flaws that create security vulnerabilities in these devices and security errors caused by humans and the solutions that users can take will be analyzed.

Alıntı / Cite

Sevinç, M., Avcı, İ., (2024). IoT Cihazlarında İnsan Hatasından Kaynaklanan Güvenlik Açıklarının Analizi, Mühendislik Bilimleri ve Tasarım Dergisi, 12(2), 403-415.

Yazar Kimliği / Author ID (ORCID Number)
M. Sevinç, 0000-0001-6609-1927
İ. Avcı, 0000-0001-7032-8018

Makale Süreci / Article Process	
Başvuru Tarihi / Submission Date	09.01.2023
Revizyon Tarihi / Revision Date	07.04.2024
Kabul Tarihi / Accepted Date	13.04.2024
Yayım Tarihi / Published Date	30.06.2024

[*] İlgili yazar / Corresponding author: mvlt.sevinc@gmail.com, +90-545-908-75-77

ANALYSIS OF SECURITY VULNERABILITIES CAUSED BY HUMAN ERROR IN IOT DEVICES

Mevlüt SEVİNÇ[1†], İsa AVCI[2]
[1] Karabük University, Graduate Education Institute, Department of Computer Engineering, Karabük, Turkiye
[2] Karabük University, Faculty of Engineering, Department of Computer Engineering, Karabük, Turkiye

Highlights

- IoT, refers to a world where various physical devices are uniquely connected to each other.
- IoT devices face challenges arising from the use of standard internet protocols for communication.
- Especially the use of IoT devices and user errors caused by humans are increasing day by day.

Purpose and Scope
In this article, information about attacks on IoT devices will be given and security vulnerabilities created by users will be emphasized.

Design/methodology/approach
In this article, studies on the security of the Internet of Things (IoT) are analyzed. Attacks and measures found as a result of the studies are mentioned.

Findings
As technology advances, the use of electronic devices, particularly IoT devices, has increased, along with associated user errors. Due to users' security vulnerabilities, attacks on these devices are increasing, and such attacks do not require physical proximity. Consequently, every device connected to the internet is at risk if adequate security measures are not implemented. It is crucial to enhance users' security awareness, inform them, and provide regular awareness training.

Social Implications
Information sharing among devices via the IoT system is feasible, and connecting to any internet-enabled device has simplified operations. However, ensuring the security of users and devices is crucial. As a result of this study, awareness-raising visuals regarding the secure use of IoT devices should be prepared for end users, and topics on attack methods and security measures should be included in IT courses in schools. Additionally, public service announcements should emphasize the importance of cybersecurity, and cybersecurity topics should be prominently included in product manuals. Institutions should prioritize in-service training to enhance cybersecurity awareness. Both users and IoT manufacturers must be prepared for commonly encountered security vulnerabilities identified in the reviewed studies, such as weak encryption, default usernames and passwords, lack of updates and patches, poor design, weak network security, and physical security vulnerabilities. Users should employ strong encryption, change default credentials, and use up-to-date software. Companies should regularly release updates and patches, and security software firms should conduct frequent penetration testing. Furthermore, users must ensure the physical security of their IoT devices to prevent theft, hardware damage, and the installation of malicious sensors.

Originality
This article highlights human-induced security vulnerabilities. It aims to describe the security measures that users can take to counteract these errors.

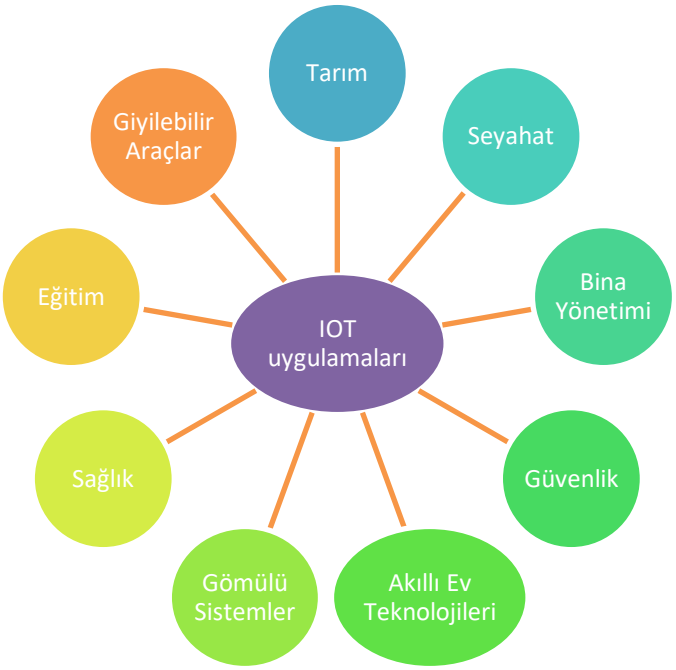
† Corresponding author: mvlt.sevinc@gmail.com, +90-545-908-75-77

1. Giriş (Introduction)

2011 yılında Almanya'da düzenlenen Hannover Fuarı'nda dördüncü sanayi devriminden bahsedilmeye başlanmıştır. Bununla beraber sensörlerin kullanımı, bulut bilişim, büyük veri bilimi, simülasyon ve sanallaştırma sistemleri, siber güvenlik gibi teknolojik gelişmelerin önemi artmıştır (Uyanık, Gökdemir, Karayiğit, & Yücel, 2020). Bunula beraber akıllı gömülü sistemlerin kullanımın giderek artması cihazların birbiri ile bağlantılı kurmasını zorunlu hale getirmiştir.

İnternet of Things (IoT), çeşitli fiziksel cihazların birbirine bağlı olduğu ve benzersiz bir şekilde tanımlanabilir olduğu bir dünyayı öngören bir kavramdır (Li vd., 2014). Bu bağlantılı ağ, RFID etiketleri, sensörler, aktüatörler ve akıllı cihazlar gibi geniş bir yelpazedeki cihazları içerir; hepsi sorunsuz bir şekilde entegre edilmiştir ve çok sayıda dijital hizmet sunmak üzere bir araya getirilmiştir(Zanella vd., 2014).

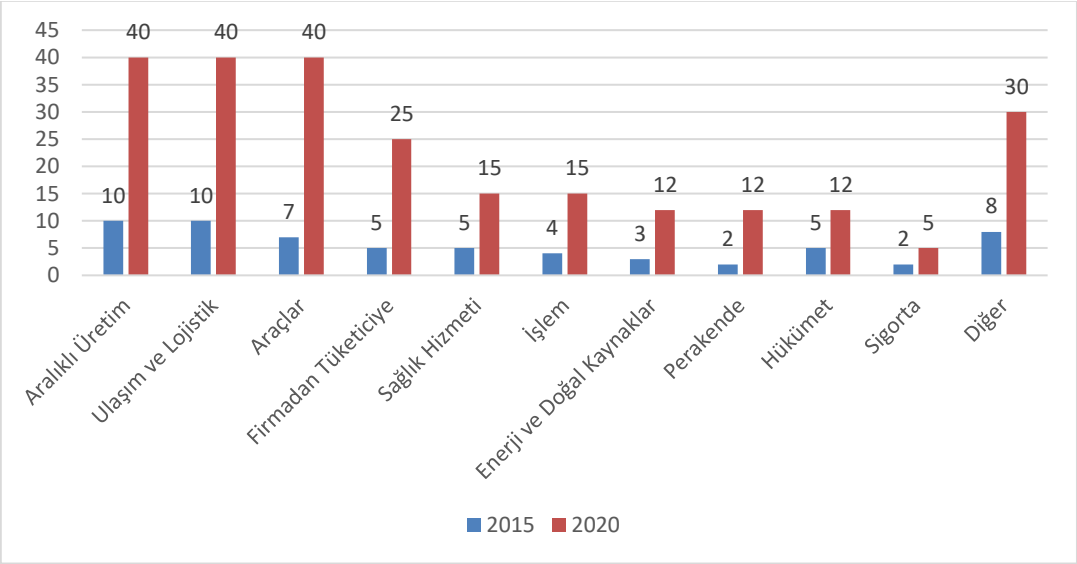
IoT altyapısı, heterojen son sistemlerin geniş bir yelpazesinin bağlantısına izin verirken, dijital hizmetlerin geliştirilmesi için seçici veri erişimini sağlar (Zanella vd., 2014). Bu bağlı cihazlar ağı, kaynak kısıtlı cihazlar ve sensörler arasında kablolu ve kablosuz ağlar aracılığıyla iletişimi kolaylaştırır (Said & Zolkipli, 2022). IoT, sadece günlük yaşamı geliştirmekle kalmaz, aynı zamanda toplum üzerinde derin bir etkiye sahiptir (Guo & Li, 2021).
Diğer yaygın bir tanımıyla IoT; bilgi toplumu için küresel bir alt yapı oluşturan, gün geçti gelişen, birbirleri ile haberleşerek bilgi paylaşımı gerçekleştiren cihazlar topluluğudur (ITU, 2012). Şekil 1'de IoT cihazlar topluluğuna ait kullanım alanları gösterilmeye çalışılmıştır.



Şekil 1. IoT Cihazları Uygulama Alanları (IoT Devices Application Areas)

Güvenlik, IoT'un kritik bir yönüdür ve gömülü ağlar içinde iletişim için standart internet protokollerinin kullanımından kaynaklanan zorluklarla karşılaşmaktadır (Heer vd., 2021). Ayrıca, IoT, akıllı üretim, akıllı şehirler, ulusal savunma ve diğer endüstrilerde önemli bir rol oynamaktadır ve uygulamalarında güvenlik ve etkileşim yeteneği gereksinimini vurgulamaktadır (Xu, 2021).

Nesnelerin İnterneti'nin (IoT) maliyetleri düşürme, yeni iş modellerini etkinleştirme ve uygulama geliştirme potansiyeline sahip olduğu görülmektedir. IoT, Bulut Hizmetleri ve API (Application Programming Interface - Uygulama Programlama Arabirimi) uygulamalarının ve bunları sunan pazaryerlerinin daha hızlı çoğalmasını sağlamıştır. API'ler, sistemler arasında en az hata ile gerçek zamanlı entegrasyon işlemi sağlayarak IoT projelerinin daha hızlı ve daha doğru bir şekilde başarıya ulaşmasında öncülük etmektedir. Yüksek hızlı kablosuz ağlar, IoT için önemli bir büyüme faktörüdür. Bu nedenle Samsung, Qualcomm, LG, Huawei ve Intel gibi birçok teknoloji firması patentlerle ürün liderliği oluşturmak için yoğun bir şekilde rekabet etmektedirler. Bu ilk beş patent sahibi firma, bugün 13.300'den fazla IoT patentini kontrol etmektedirler (Columbus, 2018). 2015 ve 2020'de dikey olarak dünya çapında Nesnelerin İnterneti harcamaları (Şekil 2) incelendiğinde beş yılda büyük bir farkın olduğu açık ara bir şekilde oldukça belirgindir.



Şekil 2. 2015 ve 2020'de dikey olarak dünya çapında Nesnelerin İnterneti harcamaları (Statista, 2021)
(Worldwide IoT spending vertically in 2015 and 2020)

Yapılan incelemeler neticesinde güvenlik açıklarından bahsedilmiş, çözüm yolları üzerinde çalışmalar yapılmıştır. Fakat kullanıcı tarafından meydana gelen güvenlik açıklarına değinilmemiştir. IoT sisteminin giderek yaygınlaşması, kullanıcı sayısının her gün artması, güvenlik konusunda büyük açıklıklar oluşmasına neden olmuştur. Sistemlerin sürekli güncellenmesi güvenliği artırsa da insanlar maalesef güvenli kullanım konusunda yetersiz kalmaktadır. Bu çalışmada, en zayıf halka olan kullanıcıların yaptıkları hatalar ve çözümleri analiz edilerek açıklanmıştır. Bu çalışmanın ikinci bölümünde IoT konusunda daha önce yapılmış çalışmalar incelenmiş, insan hatasından kaynaklı güvenlik açıkları açıklanmaya çalışılmış, tartışma ve değerlendirme yapılmış ve son olarak da bu çalışma sonuçları analiz edilmiştir.

2. Literatür Araştırması (Literature Reviwer)

Uludağ ve Uçar (2018), "Nesnelerin İnterneti (IoT) ile Akıllı Sınıf ve Öğrenci Takip Sistemi Tasarımı" isimli makalelerinde yazılım ve donanım aşamalarından oluşan Akıllı sınıf ve Öğrenci takip sistemi geliştirmişlerdir. Donanım aşamasında Radyo Frekansı ile Tanımlama (Radio Frequency Identification, RFID) etiketi içeren öğrenci kimlik kartları yoklama alınabilen, sınıfın kapısını açan ve ışıkları kontrol eden elektronik bir sistem, yazılım aşamasında ise bu sistemin otomasyonunu geliştirmişlerdir (Uludağ & Uçar, 2018).

Kumar ve Deora (2021); yaptıkları bildiride IoT'nin mimari yapısından, güvenlik sorunlarından ve gereksinimlerinden bahsetmişlerdir, gelecekte IoT'de çıkabilecek güvenlik sorunlarını ayrıntılı olarak tartışmış ve bu güvenlik açıklarının giderilmesi için ortaya konan farklı teknikleri karşılaştırmışlardır. Literatürdeki farklı makaleleri incelemişler, artı ve eksi yönlerini ortaya koymuşladır. Bu çalışma sonucunda verilerin gizliliğinin yüksek verimle elde edildiği güvenli bir kriptografi tabanlı mekanizma önermişlerdir (Kumar & Deora, 2021).

Toutsop, Das ve Kornegay (2021); yaptıkları çalışmalarında akıllı evlerde kullanılan dört farklı IoT cihazına DoS (Denial-of-service attack – Servis dışı bırakma) saldırıları düzenleyerek sensörlerin güvenlik açıklarından yararlanmışlar, kullanıcı verilerini ele geçirebildiklerini ortaya koymuşladır. Saldırıları düzenlemek için sanal sunuculara kurdukları Kali Linux'tan faydalanmışlardır. Yaptıkları deneyde bilgisayar korsanlarının yetkisiz ağ erişimi elde etmek, çeşitli IoT cihazları ile kullanıcı verilerini kullanmak için sensörlerden yararlanabileceklerini göstermişlerdir. Ayrıca makine öğrenmesi ve derin öğrenme kombinasyonları ile saldırıların tespitini ve saldırıları azaltmaya yönelik saldırı tespiti tekniğini önermişlerdir (Toutsop, Das, & Kornegay, 2021).

Monia, Sharma ve Dhir (2021); yaptıkları bildiride sis bilişim ve IoT cihazlarının gerçek dünyadaki uygulamalarını incelemişlerdir. Sis bilişimin, bulut bilişime kıyasla bazı güvenlik sorunlarını ele almışlardır. Bu güvenlik sorunları ve olası çözümleri üzerinde durmuşlar, zorluklarını ortaya koymuşlar, etkisini azaltmak için çözüm sunmuşlardır. Aşağıdaki Tablo 1'de olası güvenlik sorunlarını ve çözümlerini göstermeye çalışmışlardır (Monia, Sharma, & Dhir, 2021).

Tablo 1. Olası Güvenlik Sorunlarını ve Çözümleri (Possible Security Issues and Solutions)

Roller	Güvenlik Zorlukları	Olası Çözümler
Veri İşleme	• Veri Yayma • Veri Dağıtımı • Veri İhlali • Veri Şifreleme • Veri Paylaşımı • Büyük Veri Analizi • Adli Bilişim	• Güvenilir Platform • Yetki İptali • Simetrik Şifreleme ve Asimetrik Şifreleme • Veri Maskeleme • Veri Ve Konum Kayıt Veritabanının İzlenmesi • Doğrulanabilir Hesaplama Şeması • Verilerin Gizlenmesi
Ağ Hizmetleri ve İletişim	• Kimlik Doğrulama • Hafifletilmiş Protokoller • Ağ İzleme • Paket Filtreleme • Tespit Sistemi • Güven Yönetimi • Sanallaştırma • Erişim Kontrolü • Arızaya Dayanıklılık	• Açık Anahtarlı Şifreleme, Biyometrik Tabanlı Kimlik Doğrula • Yerel ve küresel algılama sistemima • Dijital İmza ve Dijital Sertifika Tahsisi • Rol Tabanlı ve Öznitelik Tabanlı Kontrol Politikası • Sis Tabanlı Gizlilik • Anahtar Yönetimi • Gizliliği Koruyan Paket İletimi
Cihaz Gizliliği	• Hassas Veri Koruması • Veri Bütünlüğü • Güvenli Veri Paylaşımı • Veri Kaybı • Konum Gizliliği • Kullanım Gizliliği • Yedekleme ve Kurtarma	• Hafif şifreleme algoritması ve maskeleme teknikleri • Homomorfik Şifreleme • Ev Alanı Ağı Şifreleme Yöntemleri • Takma Ad Yöntemleri • Simetrik ve Asimetrik Şifreleme • Kimlik gizleme

Atham ve Wills (2020); "Dijital İkiz Teknolojiler ve Akıllı Şehirler" kitabının bir bölümünde IoT cihazlarının güvenliği, gizliliğine dair genel bir çalışma ortaya koymuşlardır. IoT mimarisi ve temel özelliklerinden bahsetmişlerdir. IoT güvenlik gereksinimlerini, güvenlik saldırı çeşitlerini ve IoT cihazlarının güvenliğine dair zorluklar hakkında tartışmışlardır. Gizlilik tehditlerini araştırmışlar, bu konuda çözüm önerilerini vurgulamışladır. Sonucunda IoT güvenlik tehditleri, güvenlik önlemleri, güvenli bir akıllı şehir tasarımı üzerinde çalışmışlardır (Atlam & Wills, 2020).

Chong, Xiong ve Proctor (2019); yaptıkları çalışmada IoT cihazları tasarlanırken gizlilik ve güvenlik konularında insan faktörünün benimsenmesini ele almışladır. Çalışmalarında teknoloji kullanıcılarını, cihaz tasarımlarının ilk aşamasından itibaren hesaba katılması gerektiğini vurgulamışladır. Araştırmacıların ve tasarımcıların, IoT cihazlarında güvenliği ve gizliliği ihlal eden saldırganlara karşı başarılı olmak istiyorlarsa, IoT kullanıcılarını da içeren çok yönlü bir yaklaşım geliştirmeleri gerektiğini benimsemişlerdir (Chong, Xiong, & Proctor, 2019).

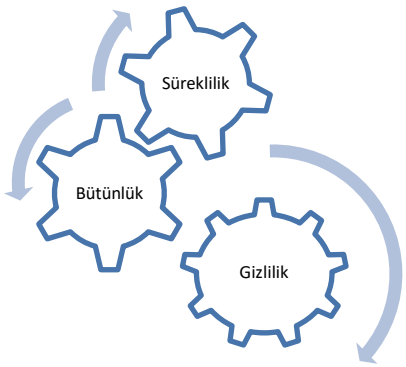
Ahmed, Tahir ve Habaebi (2021); yaptıkları çalışmalarında IoT'de doğrulama ve kimlik yetkilendirme için makine öğrenimi yöntemini incelemişlerdir. Birbirine bağlı cihazlar arasındaki iletişimi engellemeye yönelik saldırılara karşı makine öğrenmesi yöntemiyle kimlik doğrulama ve yetkilendirme savunma hattını güçlendirme çalışmalarını incelemişlerdir (Ahmed vd., 2021).

İncelemeleri yapılan çalışmalarda insan hatasından kaynaklı açıklara değinilmemiştir. Oldukça fazla sayıda kullanıcıdan meydana gelen iletişim ağında en zayıf güvenlik halkasını insanlar oluşturmaktadır. Çalışmanın devamında kullanıcılardan kaynaklı oluşabilecek güvenlik açıklarına değinilecektir.

3. İnsan Hatasından Kaynaklı Güvenlik Açıkları (Security Vulnerabilities Caused by Human Fault)

3.1. Bilgi ve Bilgi Güvenliği (Information and Information Security)

TDK'ye göre bilgi, kurallardan yararlanarak kişinin veriye yönelttiği anlam olarak tanımlanmaktadır (TDK, 2021). Bilişim teknolojilerinde ise teknolojik araçlar ile işlenmekte olan verilerin tümünü ifade etmektedir (Uyanık, Gökdemir, Karayiğit, & Yücel, 2020). Bilgi güvenliği; bilgi sahibinin rızası olmadan bilginin yetkisiz kişilerce elde edilmesine, değiştirilmesine, bilgiye zarar verilmesine karşı alınan önlemler olarak tanımlanır. Şekil 3'te yer alan gizlilik, bütünlük, süreklilik (erişebilirdik) unsurlarından herhangi biri zarar görürse güvenlik açığı meydana gelir (Şen & Yerlikaya, 2013). Örneğin fotoğraflar, ses kayıtları, özel kutlamalarda çekilen her video, internet tarayıcısı geçmişi, kredi kartı bilgileri gibi veriler kullanıcılar için oldukça önemli olan bilgilerdir. Bunların herhangi bir şekilde farklı mecralarda yayınlanması hiçbir kullanıcı tarafından istenmeyecektir. Bu sebeple bilgi ve bilgi güvenliği IoT kullanıcıları için önemlidir.



Şekil 3. Temel Güvenlik İlkeleri (Basic Security Principles)

3.2. Temel Güvenlik Prensipleri (Basic Security Principles)

3.2.1. Açılış Güvenliği (Boot Security)

Açılış güvenliği; IoT cihazları içinde yer alan kişisel verilerin güvenliğinin alınmasında ilk adımı ifade etmektedir. Bu cihazların Şekil 4'te de gösterildiği gibi hem fiziksel olarak hem de yazılımsal olarak güvenliği sağlanmalıdır. Çalınan bir IoT cihazının açılış şifresinin olması, içindeki verilere erişimi zorlaştıracaktır.

Şekil 1 IoT Güvenliği (IoT Security)

3.2.2. Parola Güvenliği Prensipleri (Password Security Principles)

Basit parolalar kullanmak bilgilere erişimi kolay hale getirmektedir. Zayıf parolaların aşılması saldırganlar için oldukça kısa zaman almaktadır. Bu sebeple kullanıcıların güçlü şifreler kullanmaları sağlanmalıdır. Birbirini tekrar eden sayılar ya da harfler, içinde doğum günü gibi bilgileri içeren parolalar yerine daha karmaşık şifreler kullanılmalıdır (Uyanık, Gökdemir, Karayiğit, & Yücel, 2020).

3.2.3. İnternet Erişim Güvenliği (Internet Access Security)

İnternet, insanların yaşamını her yönüyle kolaylaştırmıştır. Alışveriş, bilgiye erişim, haberleşme gibi oldukça hayati konularda kolaylıklar sağlamaktadır. Fakat dikkatsiz kullanımında önemli birçok verinin el değiştirmesine sebep olmaktadır. Çevrimiçi ortamda hangi web sitelerinin güvenli olduğu iyi bilinmelidir. Web sitelerinin https bağlantısına sahip olduğuna bakılmalı, geçerli bir güvenlik sertifikasının olduğu kontrol edilmelidir. (BTK, 2019)

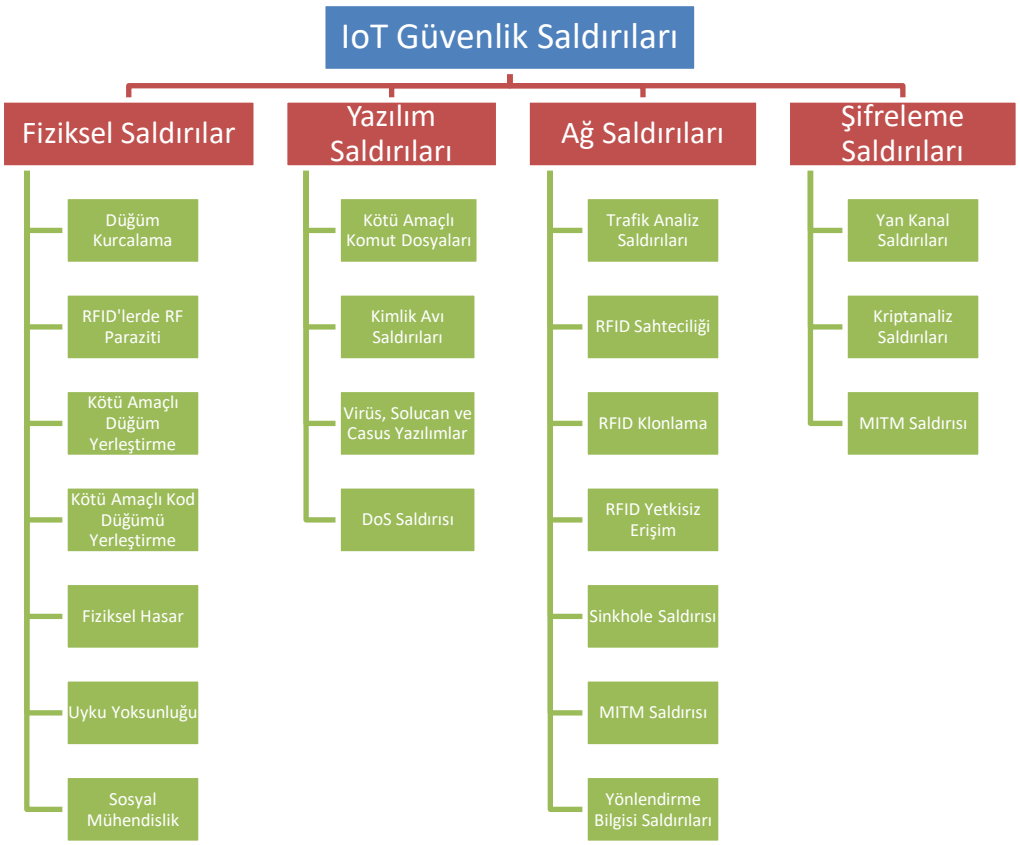
3.2.4. Zararlı Yazılımlardan Korunma Prensipleri (Malware Protection Principles)

Akıllı cihaz sayısının giderek arttığı bu günlerde bilgilerin korunması oldukça önemlidir. Kullanıcıların zararlı yazılımlara ve saldırılara karşı alabileceği önlemler aşağıda sıralanmıştır (Aytekin, Ayaz, Tüminçin, & Bektaş, 2019):

- Yeterince güvenlik bilgisine sahip olunmalı,
- Yeterli ve güncel bir anti virüs yazılımı kullanılmalı,
- Güvenirliği düşük kaynaklardan dosya paylaşımı yapılmamalı, cihazlara veri indirilmemeli,
- Çalınma riskine karşı çeşitli kaynaklar aracılığı ile yedek alınmalı,
- Güçlü şifreler kullanılmalı,

3.3. IoT Güvenlik Saldırıları (IoT Security Attacks)

IoT cihazlarının güvenlik kontrollerini sağlamak için öncelikle ne gibi saldırılara maruz kaldığına bakmak gerekmektedir. IoT sisteminde; Şekil 5'te gösterildiği gibi fiziksel, yazılım, ağ ve şifreleme saldırıları olmak üzere dört ana saldırı türü vardır (Atlam & Wills, 2020).



Şekil 2. IoT Sisteminde Çeşitli Güvenlik Saldırıları (Various Security Attacks in IoT System)

3.3.1. Fiziksel Saldırılar (Physical Attacks)

Bu tür saldırılarda saldırganın IoT sistemine yakın olması gerekmektedir. Saldırgan, IoT cihazlarına fiziksel olarak yakın olmalı ve sistemin donanım öğelerine zarar vermesi gerekmektedir. (Babar, Stango, Prasad, Sen, & Prasad, 2011).

- **Düğüm Kurcalama (Node Tampering):** Bir sensör düğümü yada donanımın bir parçasını değiştirerek, önemli bilgilere erişim sağlama, bilgilere zarar verme hedeflenmektedir (Sopori, Pawar, Patil, & Ravindran, 2017).

- **RFID'lerde RF Paraziti (RF Interference on RFIDs):** Saldırgan burada, radyo frekansı sinyalleri ile sensörlere DoS saldırısı düzenleyerek sensörlerin çalışmasını engeller (Deogirikar & Vidhate, 2017).
- **Kötü Amaçlı Düğüm Yerleştirme Malicious Node Injection)**: Hassas bilgilere erişim için iletişim düğümleri arasına fiziksel olarak düğüm ekleyerek bilgi elde eder. Düğümler arasındaki bilgi akışı kontrol edilmeye çalışılır (Atlam & Wills, 2020).
- **Kötü Amaçlı Kod Düğümü Yerleştirme (Malicious Code Injection):** Cihaza erişim sağlamaya yarayan kod içeren düğüm eklenerek bilgi akışı sağlanmaya çalışılır (Atlam & Wills, 2020).
- **Fiziksel Hasar Physical Damage):** Saldırgan IoT cihazlarına fiziksel olarak zarar verir. Saldırı için IoT cihazlarının bulunduğu binaya veya alana giriş yapılması gerekmektedir. Buradaki durumda binanın güvenliği de önem arz etmektedir (Sopori, Pawar, Patil, & Ravindran, 2017).
- **Uyku Yoksunluğu Saldırısı (Sleep Deprivation):** Çoğu sensör, bataryalar, değiştirebilir piller ile çalıştırılır. Kullanılmayan sensörler, donanımlar uyku moduna geçmesi için programlanmıştır. Bu saldırıda sensörler sürekli aktif tutularak enerjinin çabuk bitmesi ve cihazın kapanması hedef alınır (Sopori, Pawar, Patil, & Ravindran, 2017).
- **Sosyal Mühendislik (Social Engineering):** Saldırgan, kullanıcıların özel bilgilerini çıkarmak için onlarla fiziksel olarak etkileşimde olmak zorundadır. Onları manipüle ederek önemli bilgileri elde eder (Atlam & Wills, 2020).

3.3.2. Yazılım Saldırıları (Software Attacks)

Herhangi bir bilgisayarlı sistemde güvenlik açığının ana kaynağı yazılım saldırılarıdır. Bu saldırılar bilgi çalabilen, verileri bozabilen, IoT sisteminin cihazlarına zarar verebilen Truva atı, solucan, virüs veya kötü amaçlı komut dosyası içerebilir (Sopori, Pawar, Patil, & Ravindran, 2017).

- **Kötü Amaçlı Komut Dosyaları (Malicious Scripts):** IoT sistemi internete bağlı bir topluluktur. Saldırgan bu özellikten faydalanarak kullanıcının bilgilerini çalmak için kötü niyetli komut dosyaları kullanır. Saldırgan burada kullanıcının güvenlik zafiyetinden faydalanarak zararlı içerikleri çalıştırmasını sağlar (Heer, ve diğerleri, 2021).
- **Kimlik Avı Saldırıları (Phishing Attacks):** Saldırgan virüslü e-postalar yada web siteleri aracılığı ile kullanıcı giriş bilgilerini ve diğer önemli bilgileri elde etmeyi amaçlamaktadır. Günümüzde özellikle internet bankacılığı, mobil bankacılık işlemlerini gerçekleştirmek için kullanıcıları kandırmak amacıyla oldukça orijinal yapıda web sayfaları ve mobil uygulamalar yapılabilmektedir.
- **Virüs, Solucan ve Casus Yazılımlar (Virus, Worms and Spyware):** Saldırgan sisteme yerleştirdiği yazılım sayesinde erişim sağlayarak bilgileri çalmayı veya sistemin kullanılabilirliğini bozmayı hedefler (Heer, ve diğerleri, 2021).
- **DoS Saldırısı (DoS Attack):** Saldırgan, uygulama katmanı aracılığı ile IoT ağında DoS saldırıları düzenleyerek ağdaki tüm kullanıcıları etkiler. Erişim yetkisi olan kullanıcıları engelleyebilir. Veri tabanında yer alan hassas bilgilere erişim sağlayabilir (Babar, Stango, Prasad, Sen, & Prasad, 2011).

3.3.3. Ağ Saldırıları (Network Attacks)

IoT sistemi, çeşitli cihazların arasında veri aktarmak için birbirine bağlı ağların bir kombinasyonudur. Ağ saldırılarında saldırganın ağa fiziki olarak yakın olmasına gerek yoktur.

- **Trafik Analiz Saldırıları (Traffic Analysis Attacks):** Kablosuz bağlantıların izlenmesiyle önemli bilgilerin toplanmasını ifade eder. Saldırgan ağ verilerini toplar (Khoo, 2011).
- **RFID Sahteciliği (RFID Spoofing):** RFID etiketinde saklanan verilerin elde edilerek, orijinal verilerin yerine saldırganın bilgilerinin gönderildiği saldırı türüdür. Saldırgan burada kendi verilerini göndermek için orijinal etiket kimliğini kullanır ve yasal bir kullanıcı gibi tüm sisteme erişim sağlar (Mitrokotsa, Rieback, & Tanenbaum, 2008).
- **RFID Klonlama (RFID Cloning):** Saldırgan, kullanıcının RFID etiketinden gelen bilgileri başka bir RFID etiketine kopyalar. İki farklı RFID etiketi aynı bilgilere sahip olur (Sopori, Pawar, Patil, & Ravindran, 2017).
- **RFID Yetkisiz Erişim (RFID Unauthorized Access):** Kimlik doğrulama tekniklerinin olmaması nedeniyle izinsiz girişlerin kolayca yapılmasını ifade eder. Bu şekilde saldırgan, RFID etiketlerdeki bilgileri okuyabilir, değiştirebilir ve silebilir (Uttarkar & Kulkarni, 2014).
- **Sinkhole Saldırısı (Sinkhole Attack):** Verilerin gizliliğini hedefler ve ağ içinde tüm paketleri iletmek yerine atarak, ağın işleyişini bozar (Raju & Parwekar, 2016).
- **MITM Saldırısı (MITM Attack):** İletişim kuran düğümler arasına kötü niyetli bir düğüm koyarak, aralarındaki trafiği izlemek ve engellemek için kullanılır. IoT sisteminin ağ iletişim protokollerine bağlı olarak gerçekleştirilir, saldırganın cihazlara fiziksel olarak yakın olmasına gerek yoktur (Padhy, Patra, & Satapathy, 2011).

- **Yönlendirme Bilgisi Saldırıları (Routing Information Attacks):** Yönlendirme tablosu bilgileri ağ tarafından kullanılmaktadır. Bu saldırıların hedefi ağ hedefini bozma, taklit etme, içeriği değiştirme amacını taşımaktadır (Mitrokotsa, Rieback, & Tanenbaum, 2008).

3.3.4. Şifreleme Saldırıları (Encryption Attacks)

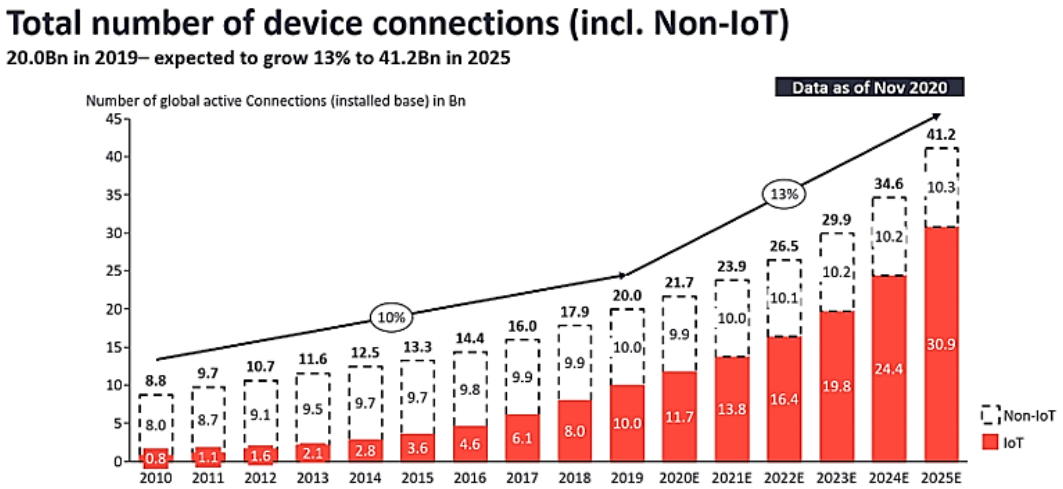
IoT sisteminin bir ağ ile birbirine bağlı olduğunu bilinmektedir. Bu ağdaki cihazlar birbirleri ile iletişim kurarken şifreleme algoritmaları kullanırlar. Şifreleme saldırılarında bu algoritmaları ihlal etmek hedeflenmektedir.

- **Yan Kanal Saldırıları (Side Channel Attacks):** IoT sistemindeki veri şifreleme ve şifre çözme anahtarlarına ulaşmayı hedefler (Atlam & Wills, 2020).
- **Kriptanaliz Saldırıları (Cryptanalysis Attacks):** Saldırganın şifreli metinden yola çıkarak orijinal metini elde etmesini ve gizli anahtarları çözmesini ifade etmektedir (Sopori, Pawar, Patil, & Ravindran, 2017).
- **MITM Saldırısı (MITM Attack):** İki düğüm arasında gönderilen sinyalleri yakalayarak bu bilgilere erişim elde etmeye çalışır ve bir anahtar değişimi gerçekleştirmeye hedefler. İki düğüm birbirleri iletişim yaptığını düşünür, fakat saldırgan iki düğüm arasındaki bilgi alışverişini kontrol eder (Padhy, Patra, & Satapathy, 2011).

3.4. İnsan Kaynaklı Güvenlik Sorunları (Human Originated Security Issues)

3.4.1. Şifre Korumasız Cihaz Kullanma (Using a Password Unprotected Device)

Kişisel ve önemli birçok veriyi depolayan cihazlarınızı üçüncü kişilerden korumak için en temel yöntemlerden biri açılış şifresi koymaktır. Şekil 6'da gösterilen 2019 yılındaki verilerine göre 20 milyar cihaz birbiri ile iletişim halindedir. Bu sistemin içinden saldırganların elde edebileceği hassas veriler kişiler için tehlikeli sonuçlar ortaya çıkaracaktır.



Şekil 3. Toplam Bağlantı Kuran Aygıtlar (Total Number of Device Connections) (IoT Analytics, 2022)

3.4.2. Yetersiz, Düşük Güvenlikli Şifreler Ayarlama (Setting Inadequate, Low-Security Passwords)

IoT cihazlarının güvenliğini artırmak için zayıf parolalar sorununu ele almak çok önemlidir. Varsayılan veya kolayca tahmin edilebilen parolalar, IoT cihazlarını Mirai ve Hajime (kötü amaçlı yazılmış botnetler) gibi kötü amaçlı yazılım saldırıları da dahil olmak üzere çeşitli siber tehditlere karşı savunmasız hale getirmektedir (McDermott vd., 2018). Hatırlanması kolay veya varsayılan parolaların kullanılması, cihazları güvenlik ihlallerine ve DDoS (Dağıtılmış Hizmet Reddi Saldırıları) gibi sofistike saldırılara maruz bırakır (Nam vd., 2020). IoT cihazlarına yetkisiz erişimi önlemek için güçlü parola yönetimi uygulamalarının hayata geçirilmesi şarttır.

Kullanıcılar gerek akılda tutulmasının kolay olması, gerek yazımının basit olması gibi nedenlerle şifrelerini kolay kırılabilir şekilde belirlemektedirler. Tablo 2'de SplashData adlı güvenlik firması ve NordPass şirketinin yaptıkları araştırmaya göre dünyada ve Türkiye'de en çok kullanılan şifreleri yer almaktadır. Görüldüğü gibi son derece zayıf şifreler birçok kişi tarafından 2022 yılında dahi kullanılmaktadır.

Tablo 2. Dünyada ve Türkiye'de En Yaygın Şifreler (Most Common Passwords in the World and Turkey) **(NordPass, 2022)**

Kullanılma Sıklığı	Tüm Dünya	Türkiye
1	123456	123456
2	admin	123456789
3	12345678	admin
4	123456789	12345
5	1234	12345678
6	12345	123123
7	Password	123321
8	123	turktelekom
9	Aa123456	Asd123
10	1234567890	superonlie

3.4.3. Kullanıcının Bilgi Eksikliği (User's Lack of Knowledge)

IoT cihazlarının çok yaygın olması doğru kullanıldığı anlamını taşımamaktadır. Birçok kullanıcı cihazlarını kullanırken hala zorluk yaşamaktadır. Bu da maalesef güvenlik açıklarını meydana getirmektedir. Kullanıcılar hala açılış ekranlarına şifre koymamakta, güvenlik yamalarının ne işe yaradığını bilmemekte, cihazları kullanırken fiziksel olarak onlara zarar vermekte ve kamuya açık alanlarda gerekli güvenlik tedbirlerini almadan dosya ve bilgi paylaşımı yapmaktadırlar. Özellikle Türkiye'deki çocukların bilişim okuryazarlığına baktığımızda %46'sının nasıl güvenli bir şekilde bilgi paylaşımı yapacaklarını bilmedikleri ortaya koyulmuştur (Çağıltay, ve diğerleri, 2011)

3.4.4. Fiziksel Tehditlere Karşı Önlem Almama Çalınma, Elektrik Arızası vb. (Not Taking Precautions Against Physical Threats Theft, Electrical Failure Etc.)

Thegardian'da yayınlanan verilere göre en çok çalınan eşyalar arasında cüzdan ve paradan sonra elektronik eşyalar gelmektedir (Thegardian, 2010). Günümüzde özellikle çip krizinin de yaşanmasıyla birlikte elektronik cihazların fiyatları oldukça artmıştır. Erişimlerinin kolay olması ve güvenlik önlemlerinin yetersiz olması durumunda cep telefonları, dizüstü bilgisayarlar, tabletler, dijital kameralar, modemler de kolayca çalınabilmektedir. Bunun yanı sıra güç beslemelerinin yetersiz kalması durumunda, şebeke elektriğindeki dalgalanmalar nedeniyle elektronik aksamın arıza vermesi de olası bir durumdur.

3.4.5. Korsan Yazılım Kullanma (Using Pirated Software)

Korsan yazılım kullanımı bireyler ve kuruluşlar için önemli tehlikeler ve riskler oluşturmaktadır. Korsan yazılımlar genellikle kritik güvenlik yamaları ve güncellemelerinden yoksundur, bu da onları siber saldırılara ve kötü amaçlı yazılım bulaşmalarına karşı daha savunmasız hale getirir (Kim vd., 2014).
BSA'nın (Business Software Alliance) raporlarına göre kullanılan yazılımların %49'unun gerçek olduğu, %51'inin sahte olduğunu tahmin edilmektedir (1995 yılından itibaren rapor tutulmaya başlanmıştır). Lisansı illegal yollar ile kaldırılan yazılımların içinde Truva atları, solucanlar, botnetler yer alabilmektedir.

Sonuç olarak, korsan yazılım kullanımı sadece güvenlik açıkları ve destek eksikliği nedeniyle teknik riskler oluşturmakla kalmamakta, aynı zamanda fikri mülkiyet hakları ve yazılım geliştiricileri için ekonomik sonuçlara ilişkin etik endişeleri de beraberinde getirmektedir. Kurumlar ve bireyler bu riskleri azaltmak ve dijital ortamda yasal ve etik standartları korumak için yasal yazılım kullanımına öncelik vermelidir.

3.4.6. Güncellemeleri Zamanında Yapmama (Not Making Updates On Time)

IoT cihazlarını zamanında güncellemek, güvenliği korumak ve olası riskleri azaltmak için çok önemlidir. IoT cihazlarının zamanında güncellenmemesi, bu cihazları güvenlik ihlallerine ve saldırılara karşı savunmasız bırakabilmektedir. Araştırmacılar, IoT cihazlarının genellikle saldırganlar tarafından istismar edilebilecek güvenlik açıklarına maruz bırakıldığını vurgulamışlardır (Zhang vd. 2014). Bu güvenlik açıkları, cihazlar en son güvenlik yamaları ve yazılım güncellemelerini zamanında yapılmadığında daha da kötüleşebilmektedir. (Zandberg vd., 2019).

Kullanıcıların yapabileceği en büyük IoT güvenlik hatalarından biri, cihazlarını en yeni yazılım ve güvenlik yamaları ile düzenli olarak güncellememeleridir. Birçok IoT cihazı sahibi için, güncelleme süreci veya güncellemenin önemi göz ardı edilebilir. Ancak, bu basit hatanın ciddi sonuçları olabilir. Güncellemelerin ihmal edilmesi, bilgisayar korsanlarının, cihazlardaki zayıf noktaları tespit edip istismar etmelerini kolaylaştırabilir. Sonuç olarak, kullanıcılar güncelleme yapmamakla sadece cihazlarının güvenliğini riske atmakla kalmaz, aynı zamanda maddi ve itibari zararlara da yol açabilirler. Bu nedenle, düzenli güncellemelerin sağlanması ve güvenlik yamalarının uygulanması, IoT cihazlarının güvenliğini korumak için kritik bir adımdır.

3.4.7. Güvenilir Olmayan Kaynaklardan Uygulama/Yazılım Yükleme (Installing Applications/Software from Untrusted Sources)

Güvenilir olmayan kaynaklardan uygulama veya yazılım yüklemek kullanıcılar ve cihazları için önemli tehlikeler oluşturmaktadır. Kullanıcılar güvenilir olmayan kaynaklardan yazılım indirdiklerinde, kendilerini kötü amaçlı yazılım enfeksiyonları, veri ihlalleri ve gizlilik ihlalleri dahil olmak üzere çeşitli risklere maruz bırakırlar. Kötü niyetli üçüncü taraf uygulamaları, cihazın güvenliğini ve kullanıcının hassas bilgilerini tehlikeye atabilecek casus yazılım içerebilmektedir. Bu uygulamalar aynı zamanda kullanıcı gizliliğinin ortadan kaldırılması için bir kaynak görevi görerek potansiyel kimlik hırsızlığına veya kişisel verilere yetkisiz erişime yol açabilmektedir (Gómez-Hernández vd., 2021).

Mobil işletim sistemlerinin uygulama indirme merkezlerinin dışında herhangi bir kaynaktan indirilen uygulamalar cihazınız için tehdit oluşturmaktadır. Virüsler kolaylıkla bulaşmakta, bozuk dosyalar bozulmakta, bu bozuk dosyalar cihazın doğru çalışmasını engellemektedir, son adımda da kişisel bilgileriniz çalınabilmektedir. Aynı zamanda uygulama yüklerken verilen izinler kontrol edilmediği durumlarda kullanıcının isteği dışında verileriniz üçüncü kişilerin eline geçebilmektedir.

3.4.8. Varsayılan Kullanıcı Adı ve Şifreleri Değiştirmeme (Not Changing Default Usernames and Passwords)

IoT cihazları genellikle varsayılan veya zayıf şifreler nedeniyle zayıf korumadan muzdariptir ve bu da onları siber saldırılara karşı savunmasız hale getirir (Huszti vd., 2022). Üreticilerin güvenli parola yönetimi yönergeleri sağlamaları ve parolalar gibi hassas bilgileri kamuya açık belgelerde paylaşmaktan kaçınmaları gerekir (Karam, 2022). Dağıtılmış saldırı tespit sistemlerinin uygulanması, varsayılan parolalar gibi temel sorunlardan kaynaklanan güvenlik açıklarının tespit edilmesine ve azaltılmasına yardımcı olabilir (Kfouri vd., 2019).
Yeni alınan cihazların ayarlarını değiştirmek için şirketler tarafından oluşturulmuş varsayılan kullanıcı adı ve şifreleri vardır. Giriş seviyesinde güvenlik sunan bu ayarların mutlaka güncellenip, güçlü parolalar ile korunması gerekmektedir. Aksi halde saldırılar karşısında hızlı bir şekilde cihaz devre dışı bırakılıp, korsanların bilgileri ele geçirmesi kolaylaşacaktır.

3.4.9. Kamuya Açık Alanlarda Cihazların Wi-Fi ve Bluetooth Araçlarını Açık Tutma (Keeping Devices Wi-Fi and Bluetooth Tools On in Public Spaces)

Kalabalık mekanlar olan kafelerde, sinemalarda, okullarda ya da herkesin bulunduğu açık alanlarda cep telefonlarının, tabletlerin, diz üstü bilgisayarların aktif durumda olan Wi-Fi ve bluetooth iletişim araçları kullanıcı için tehlike barındırmaktadır. İzinsiz bağlantılar nedeniyle istenmeyen yazılımlar IoT cihazlarına yüklenmekte ve güvenlik zafiyeti oluşturmaktadır.

5. Sonuç ve Tartışma (Result and Discussion)

Teknoloji geliştikçe insanların kullanması için birçok elektronik cihaz üretilmiştir. Bununla beraber bu cihazların insanlar tarafından kullanılması aynı hızda gerçekleşmemiştir. Özellikle IoT cihazlarının kullanımı ve insanlardan kaynaklanan kullanım hataları her geçen gün artmaktadır. Bu sistemleri kullanan kullanıcıların, bu konulardaki zafiyetlerinden dolayı bu cihazlara karşı hırsızların, saldırganların ya da kötü niyetli diğer kullanıcıların saldırıları giderek artması kaçınılmazdır. Her geçen gün kullanıcılar tarafından bilerek ya da bilmeyerek açığa çıkan güvenlik zafiyetlerinden dolayı kişisel veriler saldırganlar tarafından çalınmakta, işlenmekte ve değiştirilmektedir. Bu nedenlere bağlı olarak oluşan güvenlik sorunlarının oluşabilmesi için artık fiziksel olarak kullanıcılara veya cihazlara yakın olmaya dahi gerek duyulmamaktadır. Sonuç olarak internete bağlı olan her cihaz güvenlik önlemleri alınmadığı takdirde tehlike altındadır. Bu konularda kullanıcılarda güvenlik farkındalığının artırılması, kullanıcıların bilgilendirilmesi ve farkındalık eğitimlerinin düzenli olarak verilmesi gerekmektedir.

Kullanıcılar tarafından bireysel olarak alınabilecek önlemler kapsamında; bilgisayarların, IoT cihazlarının, modemlerin, cep telefonlarının vb. cihazların varsayılan ayarlarının değiştirilmesi önemlidir. Varsayılan olarak gelen ağ adları kişisel olarak adlandırılmalı, güçlü parolalar oluşturulmalı ve sık sık parolalar değiştirilmelidir. Bu şekilde alınan önlemler ile saldırganların elektronik cihazlara, IoT sistemlerine erişimleri zorlaşacaktır. Ayrıca eve gelen misafirler ve farklı kullanıcılar için farklı bir kısıtlı ağ tanımlaması yapılabilir. Böylece hassas veriler tehlikeye atılmadan ağ paylaşımı yapılarak koruma sağlamak mümkün hale gelebilir. Açılış parolaları, BİOS şifresi gibi başlangıç seviye güvenlik önlemlerinin alınması gerekmektedir. IoT sistemlerinde kullanılan firewall güncellemeleri zamanında yapılmalı ve güvenlik yamaları takip edilmelidir. Lisanslı yazılımlar tercih edilmeli, korsan yazılımlar ve bilinmeyen uygulamaları kullanmaktan kaçınılmalıdır. Lisansız yazılımların içinde bilinmeyen zararlı kodların olması mümkündür ve bunların kullanılmaması gerekmektedir. Kaynağı bilinmeyen

sitelerden herhangi bir dosya indirilmemeli ve kullanılması engellenmelidir. Tüm cihazlarda açık olan Wi-Fi, Zigbee ve bluetooth özelliği kullanıcılar tarafından kullanılmadığı durumlarda kapatılmalıdır. Bu tür önlemlerin alınması durumunda hem kullanılan cihazların ve sistemlerin enerji tüketmesi önlenecek, hem de bulunulan ağa izinsiz erişim sağlamak isteyen saldırganlar engellenecektir.

IoT sistemi ile bilgi paylaşımının tüm cihazlar arasında yapmak mümkündür. İnternete bağlı her cihaza bağlanarak iş ve işlemleri yürütmek kolaylaşmıştır. Önemli nokta kullanıcıların ve elektronik araçların güvenliğini sağlayabilmektir. Bu çalışmanın sonucuna bağlı olarak IoT cihazlarının genel kullanımı ile ilgili, son kullanıcılara yönelik görseller hazırlanmalı, güvenliğini sağlamaya yönelik farkındalıklar oluşturulmalıdır. Okullarda bilişim teknolojileri ders içeriğine saldırı yöntemleri ve güvenlik önlemleri ile ilgili daha geniş bir konu eklenmeli, kamu spotları ile siber güvenliğin önemi vurgulanmalıdır. IoT cihazları ürün kullanım kılavuzlarına siber güvenlik konuları daha belirgin şekilde eklenmelidir. Özellikle siber güvenlik farkındalığının artırılması için kurum ve kuruluşlarda hizmet içi eğitimlere önem verilmelidir. Böylelikle son kullanıcılardan kaynaklanacak hatalar minimum seviyeye indirilebilir.

İncelenen çalışmalarda belirtilen ve sıkça karşılaşılan güvenlik açıklarından olan zayıf şifreleme, standart kullanıcı adı ve şifreler, güncelleme ve yama eksikliği, kötü tasarım ve uygulama hataları, zayıf ağ güvenliği, fiziksel güvenlik zafiyetleri gibi tehditlere karşı kullanıcılar ve IoT üretimi yapan şirketler mutlaka hazırlıklı olmalıdır. Kullanıcılar güçlü şifreleme ve annahtar yönetimi kullanmalı, varsayılan kimlik bilgilerini mutlaka değiştirmelidirler. Şirketler düzenli olarak açıklara karşı güncelleme ve yamaları yayınlamalı, kullanıcılar güncel yazılımları kullanmalıdırlar. Güvenlik yazılımı firmaları sızma testleri ve denetimlerini sık sık yapmalıdırlar, gerekli önlemleri testlere göre yayınlamalıdırlar. Kullanıcılar IoT cihazlarının çalınmaya, donanımsal hasara uğramaya, farklı kötü amaçlı sensörler yerleştirilmesini önlemeye yönelik fiziksel güvenliklerini sağlamalıdır.

Teşekkür (Acknowledgement)

Bu çalışma Karabük Üniversitesi Lisansüstü Enstitüsü Bilgisayar Mühendisliği tez çalışması kapsamında hazırlanmıştır.

Çıkar Çatışması (Conflict of Interest)

Yazarlar arasında herhangi bir çıkar çatışması yoktur. There is no conflict of interest between the authors.

Kaynaklar (References)

Ahmed, K., Tahir, M., Habaebi, M., Lau, S., & Ahad, A. (2021). Machine learning for authentication and authorization in iot: taxonomy, challenges and future research direction. Sensors, 21(15), 5122. https://doi.org/10.3390/s21155122

Atlam, H. F., & Wills, G. (2020). IoT Security, Privacy, Safety and Ethics. In Digital Twin Technologies and Smart Cities (pp. 123-149). Switzerland: Springer. doi:10.1007/978-3-030-18732-3_8

Aytekin, A., Ayaz, A., Tüminçin, F., & Bektaş, E. (2019). Mobil Cihazları Etkileyen Zararlı Yazılımlar ve Korunma Yöntemleri. SADAB 5th International Social Research and Behavioral Sciences Symposium, (p. 244252). Tiflis, Gürcistan.

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for Internet of Things (IoT). 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE) (pp. 1-5). Chennai, Hindistan: IEEE. doi:10.1109/WIRELESSVITAE.2011.5940923

BTK. (2019, Haziran 12). https://internet.btk.gov.tr/kisisel-veriler-ve-kisisel-bilgi-guvenligi. Retrieved 01 05, 2022, from https://internet.btk.gov.tr/.

Chong, I., Xiong, A., & Proctor, R. W. (2019). Human Factors in the Privacy and Security of the Internet of Things. Ergonomics in Design, 510. doi:10.1177/1064804617750321

Columbus, L. (2018, Haziran 6). 10 Charts That Will Challenge Your Perspective Of IoT's Growth. Retrieved from Forbes: https://www.forbes.com/sites/louiscolumbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/?sh=307fc3943ecc

Çağıltay, K., Bayzan, Ş., Karakuş, Y. T., Kaşıkçı, D. N., Kurşun, E., & Cankar, İ. (2011). The Use Of Social Networks Among Children in Turkey. EU Kids Online 2 Final Conference. Londra.

Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017 (pp. 32-37). Institute of Electrical and Electronics Engineers Inc. doi:10.1109/I-SMAC.2017.8058363

Guo, C. and Li, D. (2021). Iot security privacy protection mechanism and mechanical structure design simulation optimization. Eurasip Journal on Advances in Signal Processing, 2021(1). https://doi.org/10.1186/s13634-021-00737-3

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2021). Security Challenges in the IP-based Internet of Things. Wireless Personal Communications, 527-542. doi:https://doi.org/10.1007/s11277-011-0385-5

Huszti, A., Kovács, S. & Oláh, N. Scalable, password-based and threshold authentication for smart homes. Int. J. Inf. Secur. 21, 707–723 (2022). https://doi.org/10.1007/s10207-022-00578-7

IoT Analytics. (2022, Ocak 10). Retrieved from https://iot-analytics.com/: https://iot-analytics.com/wp/wp-content/uploads/2020/11/IoT-connections-total-number-of-device-connections-min.png

ITU. (2012, 06 15). Overview of the Internet of things. Serıes Y: Global Informatıon Infrastructure, Internet Protocol Aspects And Next-Generatıon Networks. ITU-T.

J. A. Gómez-Hernández, J. Camacho, J. A. Holgado-Terriza, P. García-Teodoro and G. Maciá-Fernández, "ARANAC: A Bring-Your-Own-Permissions Network Access Control Methodology for Android Devices," in IEEE Access, vol. 9, pp. 101321-101334, 2021, doi: 10.1109/ACCESS.2021.3097152.

K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig and E. Baccelli, "Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check," in IEEE Access, vol. 7, pp. 71907-71920, 2019, doi: 10.1109/ACCESS.2019.2919760.

Karam, A. (2022). Investigating the importance of ethics and security on internet of medical things (iomt). International Journal of Computations Information and Manufacturing (Ijcim), 2(2). https://doi.org/10.54489/ijcim.v2i2.114

Kfouri, G. d. O., Gonçalves, D. R., Dutra, B. V., Alencastro, J. F. d., Filho, F. L. d. C., Martins, L. M. C. e., … & Sousa, R. T. d. (2019). Design of a distributed hids for iot backbone components. Communication Papers of the 2019 Federated Conference on Computer Science and Information Systems. https://doi.org/10.15439/2019f329

Khoo, B. (2011). RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing (pp. 709-712). Dalian, Çin: IEEE. doi:10.1109/iThings/CPSCom.2011.83

Kim, D., Moon, J., Cho, S., Choi, J., Park, M., & Chung, L. (2014). A birthmark-based method for intellectual software asset management.. https://doi.org/10.1145/2557977.2558062

Kumar, S., & Deora, S. S. (2021). Security Challenges and Issues in IoT. 6. IEEE International Conference on Signal Processing, Computing and Control (ISPCC 2k21) (pp. 171-175). Solan: IEEE. doi:10.1109/ISPCC53510.2021.9609486

Li, S., Xu, L., & Zhao, S. (2014). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259. https://doi.org/10.1007/s10796-014-9492-7

McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018). Botnet Detection in the Internet of Things using Deep Learning

Approaches. 2018 International Joint Conference on Neural Networks (IJCNN) (s. 1-8). Rio de Janeiro: IEEE.

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2008). Classification of RFID Attacks. 10th International Conference on Enterprise Information Systems (pp. 73-86). Barcelona, İspanya: INSTICC Press.

Monia, Sharma, N., & Dhir, R. (2021). Fog computing: An overview of IoT applications with security issues and challenges. 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1-8). Noida: IEEE. doi:10.1109/ICRITO51393.2021.9596158

Nam, S., Jeon, S., Kim, H., & Moon, J. (2020). Recurrent gans password cracker for iot password security enhancement. Sensors, 20(11), 3106. https://doi.org/10.3390/s20113106

NordPass. (2021). Retrieved 12 25, 2021, from https://nordpass.com/: https://nordpass.com/most-common-passwords-list/

Padhy, R. P., Patra, R. P., & Satapathy, S. (2011). Cloud Computing: Security Issues and Research Challenges. IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), 136-146.

Raju, I., & Parwekar, P. (2016). Detection of Sinkhole Attack in Wireless Sensor Network. Proceedings of the Second International Conference on Computer and Communication Technologies (pp. 629-636). Delhi: Springer, New Delhi. doi:https://doi.org/10.1007/978-81-322-2526-3_65

Said, Z. and Zolkipli, M. (2022). Internet of things (iot): a study of security issues and challenges. International Journal of Recent Contributions From Engineering Science & It (Ijes), 10(02), 16-31. https://doi.org/10.3991/ijes.v10i02.29301

Sopori, D., Pawar, T., Patil, M., & Ravindran, R. (2017, Mart). Internet of Things: Security Threats. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 6(3), 263-267.

Statista. (2021, Haziran 22). IoT spending by vertical worldwide. Retrieved from Statist: https://www.statista.com/statistics/666864/iot-spending-by-vertical-worldwide/

Şen, Ş., & Yerlikaya, T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. Akademik Bilişim 2013 (pp. 677-681). Antalya: Akdeniz Üniversitesi.

TDK. (2021, 12 25). Türk Dil Kurumu Sözlükleri. Retrieved from https://sozluk.gov.tr/

Thegardian. (2010). Retrieved 01 10, 2022, from https://www.theguardian.com/: https://www.theguardian.com/news/datablog/2010/oct/22/burglary-statistics-police-crime-data

Toutsop, O., Das, S., & Kornegay, K. (2021). Exploring The Security Issues in Home-Based IoT Devices Through Denial of Service Attacks. 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI) (pp. 407-415). Atlanta: IEEE. doi:10.1109/SWC50871.2021.00062

Uludağ, M. H., & Uçar, A. (2018). Nesnelerin İnterneti (IoT) ile Akıllı Sınıf ve Öğrenci Takip Sistemi Tasarımı. DÜMF Mühendislik Dergisi, 591-600. Retrieved from https://dergipark.org.tr/en/download/article-file/532378

Uttarkar, R., & Kulkarni, R. (2014). Internet of Things: Architecture and Security. International Journal of Computer Application, 3(4), 12-17.

Uyanık, A. S., Gökdemir, A., Karayiğit, H., & Yücel, R. T. (2020). BİLİŞİM TEKNOLOJİLERİNİN TEMELLERİ 9. Ankara: Milli Eğitim Bakanlığı.

Xu, H. (2021). Key technologies of Secure Multi-Party Computing for Perceived Data Transmission in Internet of Things. International Journal of Frontiers in Engineering Technology, 3(5).

Z. -K. Zhang, M. C. Y. Cho, C. -W. Wang, C. -W. Hsu, C. -K. Chen and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, 2014, pp. 230-234, doi: 10.1109/SOCA.2014.58.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. Ieee Internet of Things Journal, 1(1), 22-32. https://doi.org/10.1109/jiot.2014.2306328