T.C.
İSTANBUL BEYKENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

IoT TABANLI AKILLI EV SİSTEMLERİNDE KULLANICI GİZLİLİĞİ VE SİBER GÜVENLİK ZAFİYETLERİ

Yüksek Lisans Tezi

Tezi Hazırlayan
Habibulla IMRANOV

İstanbul, 2025

T.C.
İSTANBUL BEYKENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

IoT TABANLI AKILLI EV SİSTEMLERİNDE KULLANICI GİZLİLİĞİ VE SİBER GÜVENLİK ZAFİYETLERİ

Yüksek Lisans Tezi

Tezi Hazırlayan
Habibulla IMRANOV

Öğrenci No
2320003040

ORCID ID
0009-0007-5578-7137

Danışman
Dr. Öğr. Üyesi Aykut GÜVEN

İstanbul, 2025

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum **"IoT Tabanlı Akıllı Ev Sistemlerinde Kullanıcı Gizliliği ve Siber Güvenlik Zafiyetleri"** başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını, patent ve telif haklarını ihlal edici bir davranışımın olmadığını belirtir ve bunu onurumla doğrularım. 29/08/2025

Habibulla IMRANOV

T.C.
İSTANBUL BEYKENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜ
TEZLİ YÜKSEK LİSANS SINAV TUTANAĞI

29/08/2025

Enstitümüz ***Bilgisayar Mühendisliği*** Anabilim Dalı ***Bilgisayar Mühendisliği*** Programı yüksek lisans öğrencilerinden ***2320003040*** numaralı ***Habibulla İMRANOV***'un *"İstanbul Beykent Üniversitesi Lisansüstü Eğitim – Öğretim Yönetmeliği"*nin ilgili maddesine göre hazırlayarak, Enstitümüze teslim ettiği ***"IoT Tabanlı Akıllı Ev Sistemlerinde Kullanıcı Gizliliği ve Siber Güvenlik Zafiyetleri"*** konulu tezini, Yönetim Kurulumuzun 20/05/2025 tarih ve 2025/22 sayılı toplantısında seçilen ve On-Line toplanan biz jüri üyeleri huzurunda, İstanbul Beykent Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 29. maddesinin 3. fıkrası gereğince Zoom programı aracılığıyla on-line olarak aday tarafından savunulmuş ve sonuçta adayın tezi hakkında ***"OYBİRLİĞİ"*** ile ***"KABUL"*** kararı verilmiştir.

İşbu tutanak, 2 nüsha olarak hazırlanmış ve Enstitü Müdürlüğü'ne sunulmak üzere tarafımızdan düzenlenmiştir.

DANIŞMAN
Dr. Öğr. Üyesi Ay*** GÜ***
(İstanbul Beykent Üniversitesi)

ÜYE
Dr. Öğr. Üyesi Se*** KI***
(İstanbul Beykent Üniversitesi)

ÜYE
Dr. Öğr. Üyesi Ya*** KA***
(Doğuş Üniversitesi)

Adı ve Soyadı : Habibulla IMRANOV

Danışmanı : Dr. Öğr. Üyesi Aykut GÜVEN

Derecesi ve Tarihi : Yüksek Lisans (Tezli), 2025

Alanı : Bilgisayar Mühendisliği

Anahtar Kelimeler : IoT, Akıllı ev sistemleri, Siber güvenlik, Kullanıcı gizliliği

ÖZ

IoT TABANLI AKILLI EV SİSTEMLERİNDE KULLANICI GİZLİLİĞİ VE SİBER GÜVENLİK ZAFİYETLERİ

Bu çalışma, akıllı ev uygulamalarında kişisel verilerin korunması ve güvenliğini ele almaktadır. Bu teknolojiler günlük hayatı daha pratik hale getirse de bazı tehlikeleri de beraberinde getirmektedir. İnternete bağlı cihazlar özellikle dış müdahalelere karşı savunmasızdır. Böyle bir güvenlik açığı kullanıcı bilgilerinin çalınmasına veya sistemlerin işleyişinde aksaklıklara yol açabilir. Araştırma, akıllı ev çözümlerinin temel işleyişini ve yıllar içindeki dönüşümünü açıklayarak başlamaktadır. Ardından, bu sistemlere karşı gerçekleştirilen saldırı türleri ve bunlara karşı alınabilecek koruma yöntemleri vurgulanmaktadır. Kişisel bilgilerin güvenliği ve kullanıcı haklarına ilişkin güncel düzenlemeler de incelenmektedir. Çalışmanın ilerleyen bölümünde, yeni teknolojilerin ve yöntemlerin bilgileri daha güvenli bir şekilde depolamak için sunduğu fırsatlar araştırılmaktadır. Çalışmanın amacı, kullanıcılar arasında farkındalık yaratmak ve geliştiricilere yol göstermektir. Genel olarak, akıllı ev çözümlerinin hem işlevsel hem de güvenilir olabilmesi için ciddi önlemlerin alınması gerektiği sonucuna varılmıştır.

Name and Surname : Habibulla IMRANOV

Supervisor : Assist. Prof. Dr. Aykut GÜVEN

Degree and Date : Master's (Thesis), 2025

Major : Computer Engineering

Keywords : IoT, Smart home systems, Cybersecurity, User privacy

ABSTRACT

USER PRIVACY AND CYBERSECURITY VULNERABILITIES IN IoT-BASED SMART HOME SYSTEMS

This study focuses on the protection and security of personal data in smart home applications. Although these technologies make daily life more practical, they also bring certain risks. Devices connected to the internet are especially vulnerable to external interference. Such security gaps may lead to the theft of user information or disruptions in the functioning of systems. The research begins by explaining the basic operation of smart home solutions and their transformation over the years. Then, it highlights the types of attacks carried out against these systems and the protection methods that can be applied. Current regulations on personal data security and user rights are also examined. In the later part of the study, the opportunities offered by new technologies and methods for storing data more securely are explored. The main aim of the study is to raise awareness among users and provide guidance for developers. Overall, it concludes that serious precautions are necessary for smart home solutions to be both functional and reliable.

İÇİNDEKİLER

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

BİT : Bilgi ve İletişim Teknolojileri

CCTV : Closed-Circuit Television (Kapalı Devre Kamera Sistemi)

CoAP : Constrained Application Protocol (Kısıtlı Uygulama Protokolü)

CWMP : CPE WAN Management Protocol (Uzak Cihaz Yönetim Protokolü)

DoS : Denial of Service (Hizmet Engelleme Saldırısı)

EDSA : Embedded Device Security Assurance (Gömülü Cihaz Güvenlik Güvencesi)

FPGA : Field-Programmable Gate Array (Alan Programlanabilir Kapı Dizisi)

GDPR : General Data Protection Regulation (Genel Veri Koruma Tüzüğü)

GPIO : General Purpose Input/Output (Genel Amaçlı Giriş/Çıkış)

GPS : Global Positioning System (Küresel Konumlama Sistemi)

GSM : Global System for Mobile Communications (Küresel Mobil İletişim Sistemi)

HTTP : Hyper Text Transfer Protocol (İnternet Veri Aktarım Protokolü)

IEEE : Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)

IoT : Internet of Things (Nesnelerin İnterneti)

KNN : K-Nearest Neighbors (K-En Yakın Komşu Algoritması)

LPWAN : Low Power Wide Area Network (Düşük Güçlü Geniş Alan Ağı)

MCU : Microcontroller Unit (Mikrodenetleyici Birimi)

MiTM : Man-in-the-Middle (Araya Giren Saldırı)

MQTT : Message Queuing Telemetry Transport (Hafif Mesajlaşma Protokolü)

NFC : Near Field Communication (Yakın Alan İletişimi)

NGFW : Next-Generation Firewall (Yeni Nesil Güvenlik Duvarı)

NLP : Natural Language Processing (Doğal Dil İşleme)

PET **:** Privacy-Enhancing Technologies (Gizliliği Artıran Teknolojiler)

RFID **:** Radio Frequency Identification (Radyo Frekansı ile Tanımlama)

SDN **:** Software Defined Networking (Yazılım Tabanlı Ağ Yönetimi)

VPN **:** Virtual Private Network (Sanal Özel Ağ)

WSN **:** Wireless Sensor Network (Kablosuz Sensör Ağı)

XOR **:** Exclusive OR (Özel Veya Mantık Kapısı)

SÖZLÜK

Akıllı Ev Sistemleri: Akıllı ev sistemleri, evdeki cihazların otomatik ve uzaktan yönetilmesini sağlayan teknolojik altyapılardır. Bu sistemler sayesinde kullanıcılar ışıkları, güvenlik kameralarını ve ısıtma sistemlerini kontrol edebilir. Konfor, enerji verimliliği ve güvenlik sağlar.

IoT (Nesnelerin İnterneti): Nesnelerin İnterneti, cihazların internet aracılığıyla birbirine bağlanarak veri alışverişi yapmasını sağlayan bir teknolojidir. Bu sistemde ev aletleri gibi fiziksel nesneler, sensörler ve yazılımlar aracılığıyla uzaktan kontrol edilebilir. IoT, akıllı ev sistemlerinin temelini oluşturur.

Kullanıcı Gizliliği: Kullanıcı gizliliği, bireylerin kişisel verilerinin toplanması, kullanılması ve paylaşılması sürecinde mahremiyetlerinin korunmasıdır. Akıllı ev cihazları kullanıcıların alışkanlıklarına dair veriler topladığı için bu verilerin kimlerle ve nasıl paylaşıldığı önemlidir. Etkili gizlilik politikaları ve kullanıcı izni bu sürecin temelidir.

Siber Güvenlik: Siber güvenlik, dijital sistemlerin yetkisiz erişim, veri hırsızlığı ve saldırılara karşı korunmasını amaçlayan önlemlerin bütünüdür. Akıllı ev sistemlerinde, cihazların ve kullanıcı bilgilerinin korunması için kritik öneme sahiptir. Güçlü şifreleme, güncellemeler ve güvenlik protokolleri siber güvenliğin parçalarıdır.

GİRİŞ

Akıllı ev teknolojileri, Nesnelerin İnterneti (IoT) alanındaki hızlı ilerlemeler sayesinde çağdaş yaşamın önemli bir unsuru haline gelmiştir. Bu çözümler, aydınlatma, iklimlendirme, güvenlik ve enerji kontrolü gibi süreçleri otomatikleştirerek kullanıcılara konfor, kolaylık ve tasarruf imkanı sunmaktadır. Bununla birlikte, bu teknolojilerin günlük yaşama dahil edilmesi, veri gizliliği ve siber güvenlik açısından ciddi kaygıları da gündeme getirmektedir.

Ağ bağlantısı olan cihazların sürekli veri paylaşımı, dış saldırılara ve yetkisiz erişim girişimlerine karşı hassasiyeti artırmaktadır. Dolayısıyla IoT destekli akıllı ev çözümlerinin yapısını kavramak, zayıf noktaları tespit etmek ve uygun güvenlik önlemleri geliştirmek büyük önem taşımaktadır.

Bu araştırma, akıllı ev otomasyonuna temel oluşturan kuramsal çerçeveyi, tarihsel evreleri ve başlıca teknolojileri incelemektedir. Bunun yanı sıra, bu sistemlerde kullanılan simülasyon temelli yöntemleri ve siber savunma stratejilerini ele almaktadır. Ayrıca, çalışmada mahremiyet standartları, kullanıcı hakları, karşılaşılan tehditler ve hem veri güvenliğini hem de sistem sürekliliğini korumaya yönelik en iyi uygulamalar değerlendirilmektedir. Araştırmanın hedefi, IoT tabanlı akıllı ev ortamlarında güvenlik ve gizlilik sorunlarıyla ilgili kapsamlı bir bakış açısı sunmaktır.

1. IoT AKILLI EV SİSTEMLERİNİN TEORİTİK İNCELENMESİ

Bu bölüm, IoT'nin gelişim sürecinden mimarisine ve akıllı ev pazarındaki büyümeye kadar birçok konuyu ele almakta; cihazların sağladığı verimlilik ve konforun ancak güvenlik, gizlilik, kullanıcı dostu arayüzler ve düzenli güncellemelerle sürdürülebileceğini, artan cihaz sayısıyla birlikte risklerin de dikkatle yönetilmesi gerektiğini vurgulamaktadır.

1.1. IoT Tabanlı Ev Sistemlerinin Yıllar İçinde Gelişimi

Nesnelerin İnterneti (IoT), elektronik devreler, yazılımlar ve sensörlerle donatılmış cihazların, araçların, ev eşyalarının veya binaların internet aracılığıyla veri toplamasını ve paylaşmasını sağlayan bir ağ yapısıdır. Bu teknoloji, nesnelerin mevcut ağ altyapısı üzerinden uzaktan izlenmesine ve kontrol edilmesine imkan tanıyarak fiziksel dünyanın bilgisayar sistemleriyle daha yakın bir şekilde bütünleşmesine olanak verir. Böylece daha yüksek doğruluk ve verimlilik elde edilmektedir (Atzori vd., 2010, s. 2787–2788).

Akıllı cihazların birbirine bağlandığı ağ fikri ilk kez 1982 yılında gündeme gelmiş ve Carnegie Mellon Üniversitesi'nde modifiye edilmiş bir Coca-Cola makinesi, içeceklerin sayısını ve soğuk olup olmadığını rapor eden ilk internet bağlantılı cihaz olmuştur. "Nesnelerin İnterneti" terimini ise 1968 doğumlu İngiliz araştırmacı Kevin Ashton ortaya atmıştır. IoT, insan müdahalesi olmadan cihazların etkileşim kurmasına imkan verir. İlk uygulamaları sağlık, ulaşım ve otomotiv sektörlerinde görülmüş, günümüzde ise sensörlerin internete entegrasyonu sayesinde birçok yeni gelişme yaşanmıştır. IoT'nin gelişimi; altyapı, iletişim yöntemleri, protokoller, arayüzler ve standartlar gibi çok sayıda alanı kapsamaktadır (Ashton vd., 2009, s. 1-10).

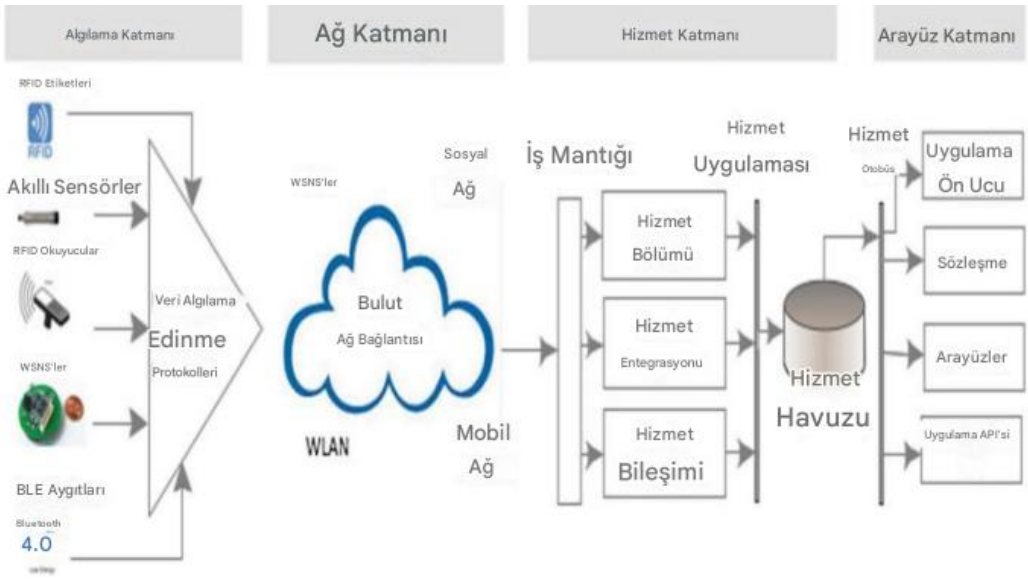
İnternetin tarihsel evrimini beş döneme ayırmak mümkündür:

- Belgelerin İnterneti: e-kütüphaneler ve doküman tabanlı web sayfaları,
- Ticaretin İnterneti: e-ticaret, internet bankacılığı ve borsa işlemleri,
- Uygulamaların İnterneti: Web 2.0,
- İnsanların İnterneti: sosyal medya ağları,
- Nesnelerin İnterneti: bağlı cihazlar ve makineler.

IoT ekosisteminde yer alan fiziksel ya da sanal nesneler, kendilerine özgü kimliklere sahiptir ve akıllı arayüzler aracılığıyla gerçek zamanlı veri paylaşabilmektedir. Kısaca IoT; sensörlere, iletişim teknolojilerine ve veri işleme altyapısına dayalı, küresel ölçekte birbirine bağlı ve benzersiz şekilde tanımlanabilen cihazlardan oluşan bir sistemdir. Bu nedenle IoT, bilgi ve iletişim teknolojilerinin yeni bir evresi olarak değerlendirilmektedir.

Günümüzde IoT sistemleri; RFID, NFC, kablosuz sensör ağları, bulut bilişim ve akıllı algılayıcılar gibi çok sayıda teknolojiyi bünyesinde barındırmaktadır. Fiziksel nesnelerin internet üzerinden erişilebilir ve tanımlanabilir olması, bu anlayışın temelini oluşturur. Ayrıca nesnelerin sanal ortamda da benzersiz kimliklerle temsil edilebilmesi, IoT'nin önemli yapı taşlarından biridir.

IoT sistem mimarisi, fiziksel ve dijital dünyaları uyumlu biçimde birbirine bağlamalıdır. Bu mimari; ağ altyapısı, iletişim protokolleri, güvenlik, süreç yönetimi, iş modelleri ve performans gibi birçok unsuru kapsar. Tasarım sürecinde özellikle farklı cihazların birlikte çalışabilmesi, ölçeklenebilirlik ve esneklik gibi özelliklere dikkat edilmelidir. Çünkü IoT, değişken koşullara uyum sağlayabilen, güvenilir ve sürdürülebilir teknolojik sistemlerin temelini oluşturmaktadır.



Şekil 1. IoT'nin Mimari Katmanları

Kaynak: Bassi, A., Bauer, M., Fiedler, M., Kramp, T., Kranenburg, R. v., Lange, S. ve Meissner, S. (2011). *Enabling things to talk: Designing IoT solutions*. Springer Berlin, Heidelberg.

SoA yaklaşımı, karmaşık sistemleri daha küçük ve açık şekilde tanımlanmış alt birimlere ayırarak inceler. Bu alt sistemler ayrı ayrı korunabildiği ve yeniden kullanılabildiği için, IoT ortamındaki donanım ve yazılım bileşenleri de kolaylıkla güncellenebilir ve verimli biçimde geliştirilebilir. Bu avantajlardan ötürü SoA, yaygın kullanılan bir mimari yapı haline gelmiştir (Balkan ve Yılmaz, 2021, s. 245–246). SoA modeli dört temel katmandan oluşur ve cihazların farklı yollarla birlikte çalışabilmesine imkan tanır:

- Algılama katmanı: Çevredeki nesnelerden bilgi toplayarak sistemle bütünleşir.
- Ağ katmanı: Nesneler arasında kablolu veya kablosuz bağlantıyı sağlar.
- Hizmet katmanı: Uygulama ve kullanıcıların ihtiyaç duyduğu servisleri oluşturur ve yönetir.
- Arayüz katmanı: Kullanıcılarla ya da uygulamalarla etkileşimi mümkün kılar.

Algılama katmanı, mimarinin en temel seviyesidir. Bu katmanda sensörler, RFID etiketleri ve çeşitli algılayıcılar çevreden veri toplar. İnsan duyularına benzetilebilecek bu yapı, ortamı gözlemler, bilgiyi işler ve üst katmanlara aktarır. Böylelikle cihazlar arası veri paylaşımı ve çevresel izleme yapılabilir. Nesneler, benzersiz dijital kimliklerle tanımlanarak takip edilebilir. Çoğu durumda bu kimlikler, UUID adı verilen 128 bitlik özel sayılardan oluşur.

Bu katman konum, hava kalitesi, hareket ya da titreşim gibi pek çok bilgiyi toplayabilir. Kullanılan sensörler ihtiyaca göre değişir; örneğin MEMS sensörleri çevresel değişimleri algılarken, jiroskoplar dönüş hareketlerini, konum sensörleri ise mekansal varlığı ölçer. Böylece örneğin pencerenin açılması ya da bir kişinin odaya girmesi gibi olaylar algılanarak güvenlik veya konfor amaçlı işlemler tetiklenebilir. Sensörler tek seferlik, aşamalı veya rastgele dağıtılabilir ve genellikle çok atlamalı ya da örgü ağ yapılarında düzenlenir.

Algılama katmanı tasarlanırken şu noktalar dikkate alınmalıdır:

- Maliyet, boyut, enerji tüketimi gibi faktörler,
- Sensörlerin dağıtım yöntemi,
- Cihazların iletişim kabiliyeti,
- Ağ yapısının uygun düzenlenmesi.

Ağ katmanı, tüm nesneleri birbirine bağlayarak iletişim kurmalarını sağlar. Bu katmanda cihazların veri paylaşabilmesi, akıllı olay yönetimi ve işleme açısından kritik öneme sahiptir. Ayrıca ağın, cihazları otomatik keşfedip roller atayabilmesi ve gerektiğinde bunları değiştirebilmesi gerekir. Böylelikle işbirlikçi görevler mümkün olur. Ağ katmanında ele alınması gereken başlıca konular: ağ yönetimi teknikleri, QoS gereksinimleri, veri arama ve işleme yöntemleri ile güvenlik ve gizlilik hususlarıdır. Özellikle kullanıcıların kişisel verilerinin korunması IoT'de en hassas noktalardan biridir. Günümüzde mevcut ağ güvenliği çözümleri kısmi koruma sağlasa da IoT için daha kapsamlı çalışmalara ihtiyaç duyulmaktadır (Lu ve Xu, 2019, s. 2103–2105).

1.2. IoT Hizmet Katmanı ve Küresel Yaklaşımlar

Hizmet katmanı, uygulamaları ve servisleri çalıştıran ara yapıdır. Donanım ve yazılımın tekrar kullanılabilmesine olanak tanır ve düşük maliyetli bir platform sunar. Burada hizmet keşfi, hizmetlerin bileştirilmesi ve API'ler aracılığıyla kullanıcılarla etkileşim sağlama gibi görevler yürütülür. Evrensel ölçekte kabul görmüş bir hizmet katmanının bulunması, IoT uygulamalarının standartlaşması için gereklidir (Chernyshev vd., 2018, s. 1637–1639).

"IoT" kavramı ilk kez 1999'da Kevin Ashton tarafından dile getirilmiş ve RFID ile yeni sensör teknolojileri üzerine çalışan Auto-ID Centre aracılığıyla yaygınlaşmıştır. O dönemde net bir tanım yapılmamış olsa da IoT'nin nesneler ve bağlantılardan oluştuğu kabul edilmiştir. Bu kavram üzerinden yıllar geçse de teknoloji hala gelişim aşamasındadır ve günlük yaşamın ayrılmaz bir parçası haline gelmiştir. Bugün dahi pek çok kişi farkında olmadan RFID taşıyıcıları kullanmaktadır (Atzori vd., 2010, s. 2787–2789).

IoT konusunda iki ana yaklaşım söz konusudur:

- Tepkisel yaklaşım: Mevcut altyapı üzerine dijital bir bağlantı katmanı eklenmesi gerektiğini savunur. IoT'yi mevcut iş modelleri içinde yönetilebilir bir gelişim süreci olarak görür.
- Proaktif yaklaşım: IoT'yi mevcut yöntemlerle yönetilemeyecek, yıkıcı bir dönüşüm olarak ele alır. Veri ve süreç anlayışının kökten değişeceğini öngörür.

Her iki yaklaşım da farklı zorluklar barındırmaktadır. Kullanıcıların ve vatandaşların bakış açısından proaktif çözümler kabul edilebilirken, şirketler ve hükümetler genellikle daha ihtiyatlı tepkisel yaklaşımı tercih etmektedir.

Çin'de IoT'ye yönelik entegre stratejiler geliştirilmiş, 2006'da yayınlanan RFID beyaz kitabıyla devlet kurumlarının sürece dahil olması sağlanmıştır. Wuxi şehri, IoT'nin merkezi haline getirilmiş ve "Algılayan Gezegen" vizyonunun parçası olarak tanımlanmıştır. Avrupa Birliği ise IoT'yi kamu-özel iş birlikleri ve dikey yatırımlarla desteklemekte, sağlık, enerji ve otomotiv gibi alanlarda uygulamaları yaygınlaştırmayı hedeflemektedir. Sonuç olarak, IoT'nin küresel ölçekte benimsenmesi farklı ülkelerde farklı yaklaşımlarla ilerlemektedir. Ancak ortak nokta, gizlilik, güvenlik ve sürdürülebilir iş modelleri konularında halen kapsamlı çözümlere ihtiyaç duyulmasıdır (Eur-Lex Europe, 2009).

Avrupa Birliği, IoT konusunda şimdiye kadar kapsamlı risk değerlendirme süreçlerini uygulayan tek büyük siyasi oluşumdur. Ancak IoT'nin araştırma, geliştirme ve yatırım politikalarının doğrudan odak noktası haline gelmemesi durumunda, bu alandaki esas faydayı başka aktörler elde edecektir.

Amerika Birleşik Devletleri'nde ise daha çok kısa ve orta vadeli kazançlara dayalı fırsat odaklı bir yatırım yaklaşımı görülmektedir. Bu yaklaşım, akıllı enerji ve akıllı şehir projeleri ile Savunma Bakanlığı ve Wal-Mart gibi büyük kurumların desteklediği RFID teknolojisiyle güçlendirilmektedir. Büyük veri, bulut çözümleri ve B2B ile B2C yapılarının sosyal medya ağları üzerinden gelişen sinerjisi; konum tabanlı hizmetler, artırılmış gerçeklik uygulamaları, akıllı enerji çözümleri ve taşınabilir cihaz entegrasyonları gibi alanlarda yeni hizmetlerin ortaya çıkmasına yol açmaktadır.

İngiltere Teknoloji Strateji Kurulu'ndan Nick Appleyard, IoT'nin yeni süreçler ve iş modelleri getireceğini belirtmiştir. Alessandro Bassi'ye göre ise nesnelerin satın alınmak yerine ödünç alınması esasına dayalı iş modelleri ortaya çıkabilir. Örneğin pahalı bir matkabın ömrü boyunca yalnızca birkaç dakika kullanılacağı düşünüldüğünde, bu cihazı satın almak yerine, üzerinde yer alan bir çip sayesinde kolayca takip edilip toplum hizmeti aracılığıyla ödünç verilmesi daha uygun olabilir. Bassi ayrıca, nesnelere bağlantı eklemekten ziyade doğrudan yeni karar alma yöntemleri geliştirilmesi gerektiğini vurgulamaktadır. Gerçek zamanlı dünyada veriye

ilk sahip olmanın tek başına avantaj sağlamadığı, asıl önemli olanın sürekli izlenebilirlik olduğu belirtilmektedir. Nesnelerin İnterneti, bağlamsal bilgilerin çok yoğun olduğu bir yapıyı desteklemektedir. Bu nedenle müşteri ile satıcı arasındaki işlem noktaları giderek önemini kaybederken, güven seviyelerini artıran geri bildirim mekanizmaları ön planda olacaktır. Bunun sonucunda farklı para birimlerinin, bankacılık standartlarının ve finansal araçların aynı sistemde bir arada bulunması mümkün hale gelebilir.

Etik, denetim, gözetim, rıza ve veri odaklı yaşam kavramları, IoT bağlamında giderek daha fazla tartışılmaktadır. Mark Weiser, gizliliği önemli bir mesele olarak değerlendirmiştir. Yapılan bir ankette de insanların gelecekte bağlantılı bir ortamda yaşamaya dair en büyük kaygılarının gizlilik olduğu görülmüştür. Bu kapsamda geliştirilen Gizlilik Koçu adlı mobil uygulama, kullanıcıların RFID etiketleriyle karşılaştıklarında gizlilik kararlarını vermelerine yardımcı olmayı amaçlamaktadır. Bu uygulama, müşteri tercihleri ile şirket politikaları arasında bir köprü işlevi görmektedir. Avrupa Komisyonu'ndan Gérald Santucci, gelecekte gizlilik hakkının teknoloji ve düzenlemelerle desteklenmesi gereken bir konu olduğunu, hatta bunun etik anlayışın bir alt boyutu olarak değerlendirileceğini ifade etmektedir (Akt., Wolf, 2010).

1.3. Nesnelerin İnterneti (IoT) Teknolojileri ve Akıllı Ev Otomasyon Sistemlerinde Simülasyon Tabanlı Yaklaşımlar

Nesnelerin İnterneti (IoT), çok sayıda ve farklı alanlarda gelişmeleri kapsayan bir teknoloji alanıdır. Ancak kavramın tanımı halen tartışmalı olduğu için, hangi teknolojilerin bu çerçevede değerlendirilmesi gerektiğini kesin çizgilerle belirtmek zordur. IoT'nin temelde "birbirine bağlı akıllı nesneler" düşüncesi üzerine kurulduğu kabul edilirse, özellikle iletişim teknolojilerine, bağlantı yöntemlerinin geliştirilmesine ya da enerji tasarrufu, baskılı devrelerin küçültülmesi ve plastik, metal veya ahşap gibi farklı malzemelere transistörlerin entegre edilmesi gibi konulara odaklanılabilir.

Her cihazın tek bir ağda birleştirilmesi mümkün olmasa da, hiyerarşik yapılar üzerinden düzenlenmeleriyle birlikte bağlı nesnelerin sayısının mevcut interneti birkaç kat aşması beklenmektedir. Bu nedenle, düşük kapasiteye sahip cihazlarda güvenliğin

sağlanması meselesi çözülmeli, ayrıca gizliliği gözeten teknolojik mimariler geliştirilerek gelecekteki yeniliklere temel oluşturulmalıdır. Bugünkü durum, internetin başlangıç yıllarına benzemektedir: o dönemde farklı iletişim mekanizmaları vardı ve yalnızca belirli bir referans modelinde birleşme, web'in gelişmesini mümkün kıldı. Benzer şekilde, akıllı bileşenlerin silikon dışı malzemelere entegre edilmesi, paketleme ve geri dönüşüm gibi konular da dikkate alınarak silikona bağımlılığı azaltacaktır. İnternetin gelişimini mümkün kılan "uçtan uca" ilkesi, teknolojinin merkezini basit tutarak yalnızca uç noktalarda karmaşıklığa izin vermiştir. Ancak bu yaklaşımın IoT alanında ne ölçüde uygulanabileceği tartışmalıdır. Bazı uzmanlar IP teknolojisinin sonunda tüm cihazlarda yer alacağını öngörse de (Ipso, 2011), belirli durumlarda farklı çözümlere ihtiyaç duyulmaktadır. Örneğin, otomobillerde fren sistemleri gibi gerçek zamanlı cihazlar güvensiz ve bağlantısız protokollere dayanamaz; aynı şekilde, pasif RFID gibi ucuz cihazlar da IP'nin karmaşık yapısını kaldıramaz. Dolayısıyla, farklı cihaz türlerinin birbirleriyle doğrudan iletişim kurması mümkün olmadığında, sistemler arasında köprüler veya ağ geçitleri kullanılacak ve iletişim bölümlere ayrılarak sağlanacaktır. Bu durum günümüz internetinde sorun olarak görülse de, ortak ilkelerin belirlenmesi için daha fazla araştırmaya ihtiyaç vardır.

IoT uygulamalarında yukarıdan aşağıya planlama ile aşağıdan yukarıya inovasyon arasında denge kurulması da önemlidir. Açık veri temelli ağ modelleri, doğrudan geri bildirim ve katılımcı bütçeleme yöntemleri aracılığıyla kurumların daha şeffaf hale gelmesi hedeflenmektedir (Wolf, 2010). IoT, şehir mobilyaları veya mobil uygulamalarda geri bildirimi görünür kılarak bireylerin hangi hizmetlere katkıda bulunmak istediğini belirlemesine ve toplum harcamalarının buna göre yönlendirilmesine imkan tanıyabilir. Ancak mevcut politika araçları ve araştırma mekanizmaları bu dönüşümü yeterince hızlı yönetememektedir. Özellikle iklim değişikliği gibi küresel sorunlarda acil çözüm üretilememesi, bu alanda yavaş ilerlemenin göstergesidir.

IoT'nin yaygınlaşmasıyla akıllı ev otomasyonu da hızla büyümüştür. 2025 yılı itibarıyla pazar büyüklüğünün 147,5 milyar dolara ulaşacağı, 2032'de 633 milyar dolar seviyesine çıkacağı, bazı raporlara göre ise 2035'te 1,03 trilyon dolara ulaşacağı öngörülmektedir. Ticari uygulamalara ek olarak, ev kullanıcıları da çeşitli donanımlar

kullanarak kendi çözümlerini geliştirmeye başlamıştır. Mikrodenetleyiciler (MCU) ve tek kartlı bilgisayarlar (SBC) bu süreçte yaygın olarak tercih edilmektedir. Ancak farklı türdeki çok sayıda cihazın bulunması, sistem geliştirme aşamalarında zorluk yaratmaktadır. Test süreçlerinde farklı ürünlerin denenmesi ek maliyet ve zaman kaybına neden olmakta, ayrıca büyük ölçekli prototiplerin ekonomik ve operasyonel sınırlamalar nedeniyle uygulanabilirliği azalmaktadır (Bassi vd., 2011, s. 9). Bunun yerine, simülasyon yazılımlarının kullanılması, sınırsız cihaz desteği ve test kolaylığı sağlaması sayesinde daha verimli bir yaklaşım olarak öne çıkmaktadır. IoT çözümlerinde birden fazla cihaz türü, protokol ve altyapı bulunduğu için, simülasyon yazılımları yalnızca test edilecek öğeye odaklanmayı mümkün kılarak süreci kolaylaştırmaktadır.

Günümüzde evlerde kullanılan elektronik cihazlar genellikle bağımsız şekilde çalışmaktadır. Ev otomasyon sistemlerinin amacı bu cihazların birlikte çalışabilirliğini sağlayarak daha akıllı yaşam alanları oluşturmaktır. IoT desteğiyle ev otomasyonu gelişmiş özellikler kazanmakta ve kullanıcıların yaşamını kolaylaştırmaktadır. Son yıllarda IoT tabanlı ev otomasyon sistemleri giderek daha popüler hale gelmiş ve bu alanda çok sayıda akademik araştırma yapılmıştır. IoT'nin çok disiplinli yapısı nedeniyle çalışmalar, güvenlikten mimariye, teknolojiden enerji verimliliğine kadar farklı alanları kapsamaktadır. Özellikle sağlık alanında yaşlı ve engelli bireylere yönelik çeşitli çözümler geliştirilmiş ve literatürde geniş uygulama örnekleri yer almıştır (Broenink vd., 2011, s. 9). Örneğin, bir çalışmada farklı ev otomasyon cihazlarını tek bir uygulama üzerinden entegre etmeyi amaçlayan modüler bir akıllı ev çözümü geliştirilmiştir (Nold vd., 2010, s. 9).

Güneş ve arkadaşlarının yapay zeka desteğiyle gerçekleştirdiği bir çalışmada, üç odadan oluşan bir ev ortamında termostat, priz ve aydınlatma birimleri simüle edilmiştir. Burada, farklı bileşenleri kapsayan bir simülasyon yaklaşımı önerilmiştir (Tuna vd., 2015, s. 9). Eleyan ve Fallon'un araştırmasında, özel ihtiyaçları olan bireyler için MQTT tabanlı bir otomasyon sistemi tasarlanmıştır (Daş vd., 2017, s. 9). H. Nguyen-An ve ekibinin çalışmasında ise, akıllı ev ortamlarında kullanılan çok sayıda IoT cihazının ürettiği trafiğin sistem üzerinde önemli bir etki yarattığı belirtilmiş ve bu trafiğin yeterince incelenmediği için analizinin büyük önem taşıdığı vurgulanmıştır. Ayrıca söz konusu çalışmada, bu trafiklerin sentetik olarak üretildiği

ifade edilmiştir (Patru vd., 2016, s. 9). M. Assim ve A. Al-Omary, Packet Tracer simülasyon yazılımını kullanarak bir akıllı ev ortamı tasarlamış ve sonrasında prototip geliştirmiştir. Bu çalışmadan da anlaşılacağı üzere, ev otomasyon sistemlerinde farklı sensör tipleri, MCU ve SBC donanımları kullanılmaktadır. Ancak simülasyon yazılımları sayesinde daha fazla cihaz eklenebilmekte ve büyük ölçekli uygulamalar gerçekleştirilebilmektedir (Malche vd., 2017, s. 10).

Ev otomasyon sistemleri, birbirleriyle iletişim kurabilen donanımlardan ve uzaktan erişim için web ya da mobil cihazlarla yönetilebilen bileşenlerden oluşur. Başka bir ifadeyle, bu sistemler donanım, yazılım ve ağ altyapısının birleşiminden oluşan bir IoT ekosistemini temsil eder. IoT'nin doğasında bulunan karmaşıklık nedeniyle ev otomasyon sistemlerinin doğru tasarlanması kritik öneme sahiptir. Bu sistemlerin çözdüğü sorunlar genellikle akıllı şehir ya da akıllı kampüs uygulamalarında görülen problemlerin küçük ölçekli örnekleri şeklindedir. Dolayısıyla, uygun biçimde tasarlanmış ve test edilmiş IoT tabanlı ev otomasyon sistemleri akıllı şehirlerin gelişimine katkıda bulunabilir. Bu sistemler donanım, yazılım/uygulama ve iletişim protokollerinden oluşan üç katmanlı IoT mimarisine dayanmaktadır (Singh, 2018, s. 10). Etkili bir çözüm için bu üç bileşen aynı derecede önemlidir. Tasarım aşamasında birden fazla donanım, uygulama ve protokol seçeneği değerlendirilerek en uygun sistem oluşturulmalıdır. Simülasyon yazılımlarının kullanımı, bu değerlendirme sürecinde doğru sonuçlar elde etmeyi kolaylaştırır.

IoT'nin sağladığı avantajlar, ev otomasyon sistemlerinin gelişmesini desteklemiştir. Bu sistemlerin yararlılığı doğrudan IoT bileşenlerinin kapasitesiyle ilişkilidir. Örneğin:

- Akıllı aydınlatma,
- Klima sistemleri,
- Bahçe yönetimi,
- Harekete duyarlı güvenlik çözümleri,
- Hava ve su kalitesi izleme,
- Akıllı kilit sistemleri,
- Akıllı enerji yönetimi.

Bunların yanı sıra, teknolojinin ilerlemesiyle birlikte yeni uygulama alanları da ortaya çıkmaktadır. Ancak gerçekçi bir model oluşturabilmek için akıllı ev otomasyonunda hangi temel bileşenlerin yer aldığı açıkça belirlenmelidir. IoT tabanlı ev otomasyon sistemleri, yaşam ve çalışma ortamını kişiselleştirmeye imkan veren çözümler sunar. Bu uygulamalar çoğunlukla sensörler ve aktüatörlerden oluşur. İnsan müdahalesi olmadan konfor ve güvenlik sağlayabilir (Jabbar, 2018, s. 11). Örneğin, cihazlara internet üzerinden erişimle insan-makine iletişimi (H2M) kurulabileceği gibi, duman dedektörü aracılığıyla tetiklenen bir alarmda makine-makine iletişimi (M2M) de sağlanabilir. Bu nedenle sensörler her iki iletişim biçiminde de kilit rol oynamaktadır (Yalcinkaya vd., 2020, s. 11).

IoT'nin yaygınlaşmasıyla birlikte farklı sensör tipleri ev otomasyon sistemlerinde kullanılmaya başlanmıştır. En sık kullanılanlar arasında sıcaklık, ışık yoğunluğu, su seviyesi ve çeşitli gazları algılayan sensörler vardır. Bunun yanı sıra basınç, nem, ivme, kızılötesi, titreşim, ultrasonik mesafe ve ses sensörleri de kullanılabilmektedir. Ancak bu sensörler genellikle düşük işlem kapasitesine sahip olduklarından veya doğrudan ağa bağlanamadıklarından, elde edilen verilerin aktarılması için IoT ağ geçitlerine ihtiyaç vardır (Koçyiğit vd., 2020, s. 11). IoT ağ geçidi, çevreden alınan verileri IP paketlerine dönüştürerek internet üzerinden iletir ve gerektiğinde aktüatörlere komut gönderir. Çeşitli IoT ağ geçitleri mevcut olmakla birlikte, en yaygın özellikleri kablolu ya da kablosuz bağlantı sağlayarak internet erişimi sunmalarıdır. Küçük ölçekli uygulamalarda Arduino gibi mikrodenetleyiciler veya Raspberry Pi gibi tek kartlı bilgisayarlar yaygın olarak kullanılmaktadır.

Şekil 2. Akıllı Evden Bir Görünüm

Kaynak: Balkan, N. ve Yılmaz, S. (2021). A simulation-assisted approach for IoT-based smart home automation systems. *Balkan Journal of Electrical and Computer Engineering, 9*(3), 245–256.

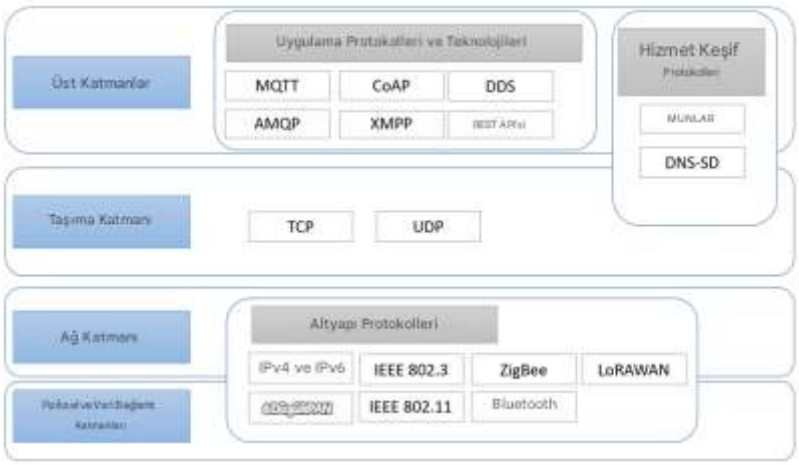
IoT iletişim protokolleri, ev otomasyon sistemlerinin geliştirilmesinde dikkate alınması gereken en temel unsurlardan biridir. Bu protokoller, verilerin ağ üzerinden IP paketleri şeklinde aktarılmasını sağlayan uygulama katmanı mekanizmalarıdır. IoT tabanlı çözümler geliştirilirken farklı iletişim yöntemleri kullanılmaktadır. Genel olarak bu protokoller iki gruba ayrılır: merkezi bir sunucu üzerinden çalışanlar (yayınla/abone ol modeli) ve herhangi bir aracı sunucuya ihtiyaç duymadan doğrudan iletişim kuranlar (istek-yanıt modeli) (Güneş, 2019, s. 12).

Ev otomasyonu için en yaygın kullanılan protokol, yayın/abone mantığıyla çalışan ve TCP tabanlı bir IoT uygulama protokolü olan MQTT'dir. Prototip aşamasında internet üzerinden erişilebilen MQTT kaynaklarından yararlanılabilir. Bu konuda hem lisanslı hem de açık kaynak çözümler bulunmaktadır. Ayrıca, SBC tabanlı cihazlarda yerel uygulamalar da tercih edilebilir. İstek/yanıt modeline dayalı bir başka önemli protokol ise CoAP'tır (Assim vd., 2020, s. 12). CoAP'ın en önemli avantajı, ek bir sunucuya gerek duymadan doğrudan IoT ağ geçidi üzerinden sorgulama

yapılabilmesidir. Böylece düzenli aralıklarla veri yayınlamaya gerek kalmaz ve bant genişliği kullanımı azaltılmış olur.

Son yıllarda yaygınlaşan bir diğer yöntem REST API kullanımıdır. CoAP'a benzer şekilde, HTTP üzerinden çalışan bu yöntem de düşük yük oluşturan istek-yanıt mantığına dayanmaktadır. REST API, HTTP protokolünün prensiplerini kullanan bir arayüzdür. IoT ağ geçidi ile doğrudan REST API aracılığıyla iletişim kurulabilir ve sensörlerden elde edilen veriler bu yolla sorgulanabilir. Hangi protokolün tercih edileceği, geliştirilen çözümün amacıyla doğrudan ilişkilidir (Öztürk vd., 2017, s. 13). Bununla birlikte veri aktarım hızı, güvenlik seviyesi, ağ topolojisi, taşınacak verinin niteliği, sorgulama sıklığı ve mesafe gibi faktörler de dikkate alınmalıdır. Simülasyon ortamında bu değerlerin kolaylıkla değiştirilebilmesi, en uygun protokolün seçilmesine yardımcı olur.

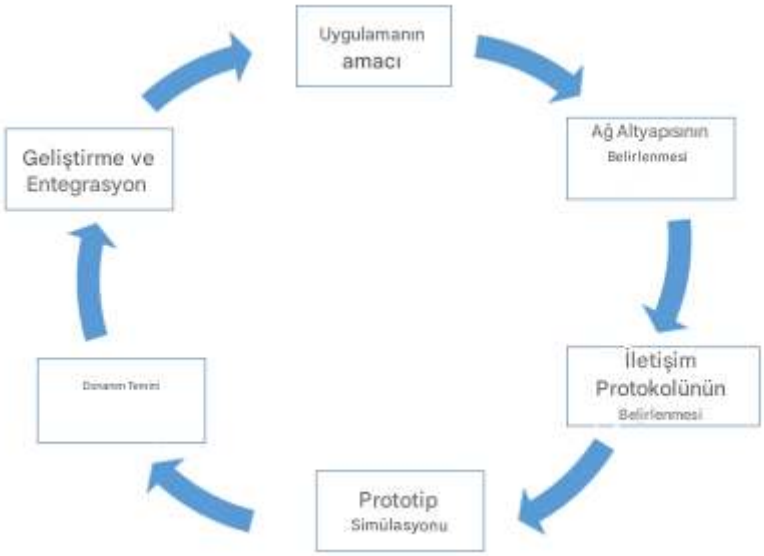
Genel olarak, Nesnelerin İnterneti protokolleri üç ana grupta toplanabilir: altyapı protokolleri, hizmet keşif protokolleri ve uygulama protokolleri. Bu protokollerin OSI katmanındaki konumları Şekil 3'te sunulmuştur.



Şekil 3. IoT Protokolleri

Kaynak: Balkan, N. ve Yılmaz, S. (2021). A simulation-assisted approach for IoT-based smart home automation systems. *Balkan Journal of Electrical and Computer Engineering, 9*(3), 245–256.

Simülasyon Destekli Ev Otomasyon Sistemi Tasarımı kapsamında, simülasyon destekli ev otomasyon sisteminin tasarımında Şekil 3'te gösterilen altı adımdan oluşan aşamalı bir yaklaşım gösterilmektedir.



Şekil 4. Simülasyon Destekli IoT Çözüm Tasarım Adımları

Kaynak: Balkan, N. ve Yılmaz, S. (2021). A simulation-assisted approach for IoT-based smart home automation systems. *Balkan Journal of Electrical and Computer Engineering, 9*(3), 245–256.

IoT tabanlı bir çözümün geliştirilme sürecinde ilk adım, uygulamanın amacının açıkça tanımlanmasıdır. Örneğin, harekete duyarlı bir ev güvenlik sistemi ya da yaşam alanlarının iklimlendirilmesine yönelik bir otomasyon çözümü bu aşamada belirlenebilir. Sonraki adımda ağ altyapısı ve gerekli teknolojiler seçilir. Burada, sistemin hedeflerine bağlı olarak kablolu veya kablosuz ağların kullanımı, sensörlerle IoT geçidi arasındaki iletişim için NFC, Bluetooth ya da ZigBee gibi teknolojilerin tercih edilip edilmeyeceği kararlaştırılır. Ayrıca, veri iletişiminin tamamen yerel mi kalacağı yoksa bulut servislerinden mi yararlanılacağı da bu aşamada belirlenir. Bulut teknolojilerinin güvenliğiyle ilgili kaygılar söz konusu olduğunda, yerel depolama ve yerel iletişim seçenekleri öne çıkabilir (Sethi vd., 2017, s. 14).

Bir sonraki adımda, kullanılacak iletişim protokolü seçilir. Eğer periyodik sorgulama ve yüksek bant genişliği gereksinimi varsa, yayınla/abone ol prensibine dayalı protokoller kullanılabilir. Bunun dışında, daha düşük bant genişliği gerektiren uygulamalarda REST-API veya CoAP gibi protokoller tercih edilebilir.

Prototip aşamasında, belirlenen hedefler ve seçilen teknolojiler doğrultusunda simülasyon yazılımları aracılığıyla sistem tasarlanır ve test edilir. Simülasyon sürecinde karşılaşılan sorunlara göre önceki adımlarda revizyon yapılabilir ya da olumlu sonuç alındığında bir sonraki aşamaya geçilebilir. Bu süreçte özellikle bant genişliği kullanımının ölçülmesi ve seçilen haberleşme protokolünün verimli çalışıp çalışmadığının değerlendirilmesi önemlidir. Son aşamada ise gerekli donanımlar temin edilir. Simülasyonlarda başarı gösteren bileşenler gerçek ortamda uygulanır. Bu uygulama, tamamen yeni bir sistemin geliştirilmesi şeklinde olabileceği gibi, mevcut bir sistemin entegrasyonu şeklinde de gerçekleştirilebilir.

1.4. IoT Akıllı Ev Sistemlerinde Siber Güvenlik Tehditleri

Bu sistemler, kullanıcıların günlük yaşamını kolaylaştırmanın yanı sıra enerji tasarrufu sağlar, konforu artırır ve güvenlik seviyesini yükseltir. Ancak bu avantajların sürdürülebilir olması, bireylerin ve ailelerin güvenliğinin korunmasına doğrudan bağlıdır. Güvenliğin sağlanması yalnızca kurulum sırasında değil, aynı zamanda düzenli güncellemeler ve sistemli kontrollerle devam eden bir süreci kapsar.

Akıllı cihazların bulunduğu ağlarda siber güvenlik açıkları ortaya çıkabilmektedir. Kötü niyetli kişiler bu açıkları kullanarak sisteme erişebilir, kişisel verileri elde edebilir veya cihazların kontrolünü ele geçirebilir. Bu tür riskleri azaltmanın en önemli yolu, kullanıcıların güvenlik bilincini artırması ve sistemleri doğru kullanım ilkelerine uygun yönetmesidir.

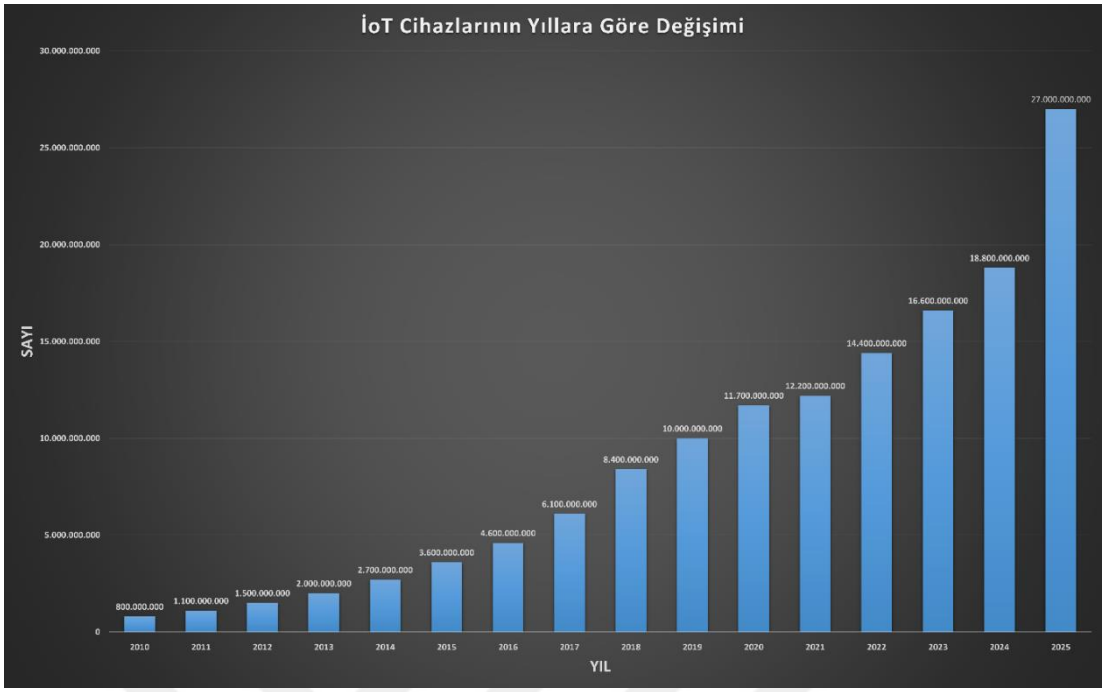
Güvenli bir kullanıcı deneyimi için güçlü ve tahmin edilmesi zor şifreler kullanılmalıdır. Varsayılan parolaların değiştirilmesi tek başına yeterli değildir; her cihaz ve hesap için farklı şifrelerin tercih edilmesi önemlidir. Buna ek olarak, iki faktörlü kimlik doğrulama yöntemi erişim güvenliğini güçlendiren etkili bir önlemdir. Bu yöntem, yalnızca parola ile değil, ikinci bir doğrulama adımıyla da erişim sağladığından yetkisiz giriş ihtimalini azaltır. Ayrıca, cihaz ve yazılımların düzenli güncellenmesi, yeni ortaya çıkan güvenlik açıklarına karşı korunmak için gereklidir. Bu noktada üreticilerin yamaları hızlı biçimde yayınlaması ve kullanıcıları zamanında bilgilendirmesi önem taşır.

Kullanıcı güvenliği yalnızca bireysel bir sorumluluk değil, aynı zamanda toplumsal bir gerekliliktir. Akıllı ev sistemleri bireylerin yaşam kalitesini artırırken daha geniş ölçekli güvenlik yapısının da parçası haline gelir. Bu nedenle kullanıcıların bilinçlendirilmesi, güvenlik standartları hakkında eğitilmesi ve bunları günlük kullanımda uygulamaları hem kişisel verilerin korunması hem de akıllı ev teknolojilerinin yaygın ve güvenli biçimde kullanılması için zorunludur.

Kullanıcı deneyimi, akıllı ev çözümlerinin başarısında belirleyici rol oynar. Bu sistemlerle sağlanan etkileşim yalnızca zaman ve enerji tasarrufu değil, aynı zamanda kullanıcıların teknolojiye bakışını da şekillendirir. Kullanıcı odaklı bir tasarım anlayışı, arayüzlerin basit, anlaşılır ve erişilebilir olmasıyla başlar.

Arayüz tasarımı bu sürecin merkezinde yer almaktadır. Sade ve minimalist bir yaklaşım, bilgi karmaşasını azaltarak gerekli özelliklere hızlı erişim sağlar. Renk, simge ve yazı tipi gibi görsel öğeler kullanıcıların sistemi algılayışını doğrudan etkiler. Ayrıca, mobil cihazlar, tabletler ve akıllı ekranlar gibi farklı platformlarla uyumluluk, erişilebilirliği artıran önemli bir faktördür.

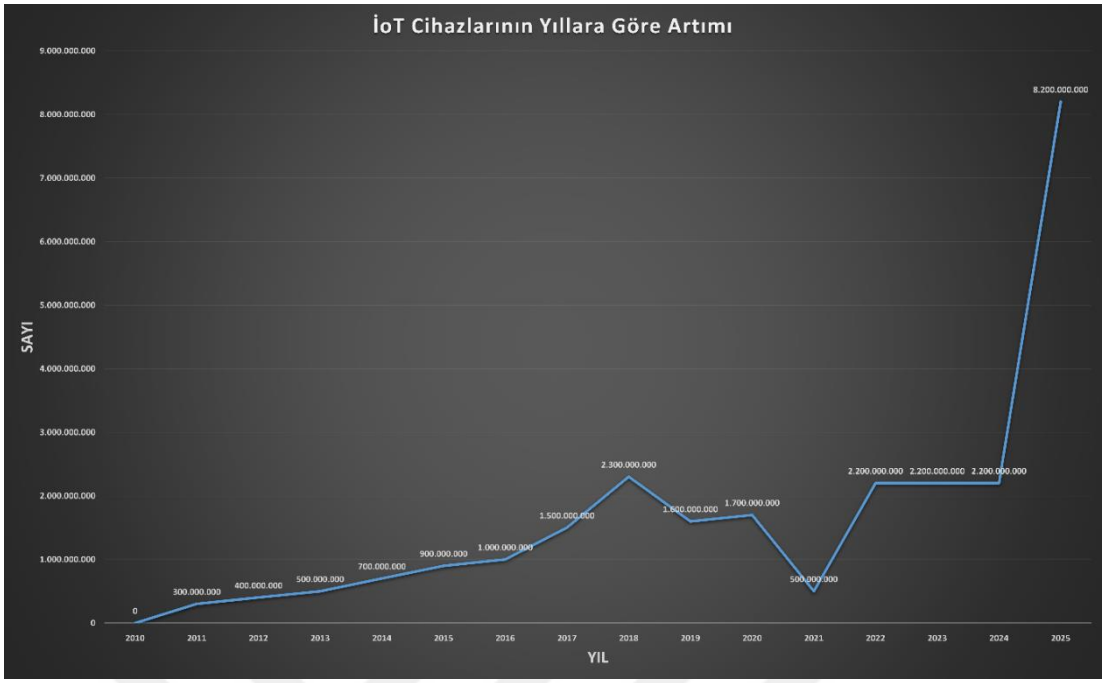
Etkileşim yöntemleri de kullanıcı deneyimini şekillendiren unsurlardandır. Dokunmatik ekranlar, sesli komutlar ve hareket algılayıcılar, kullanıcıların sistemi daha doğal ve hızlı biçimde kontrol etmesine imkan verir. Özellikle sesle kontrol ve otomatik yanıt mekanizmaları, kullanıcıların sisteme erişimini kolaylaştırarak zaman kazandırır ve konforu artırır. Bu yöntemler yalnızca bireysel kullanıcı deneyimini zenginleştirmekle kalmaz, aynı zamanda sistemin genel verimliliğini de yükseltir. Sonuç olarak, kullanıcı güvenliği ile kullanıcı deneyimi akıllı ev sistemlerinin başarısı için birbirini tamamlayan iki temel unsurdur. Güvenli, anlaşılır ve kullanıcı dostu çözümler geliştirmek, hem bireysel hem de toplumsal ölçekte sürdürülebilir bir teknoloji altyapısının oluşmasına katkı sağlar. Etkili bir kullanıcı deneyimi tasarımı yalnızca görsel ve sezgisel yönlerle sınırlı olmamalı, aynı zamanda verilere dayalı karar süreçleriyle desteklenmelidir. Kullanıcı geri bildirimleri, kullanılabilirlik testleri ve kullanıcı yolculuğu analizleri, potansiyel sorunların erken tespit edilmesine ve sistemin sürekli iyileştirilmesine olanak tanır.



Şekil 5. IoT Cihazlarının Yıllara Göre Değişimi

Kaynak: Yazar tarafından oluşturulmuştur.

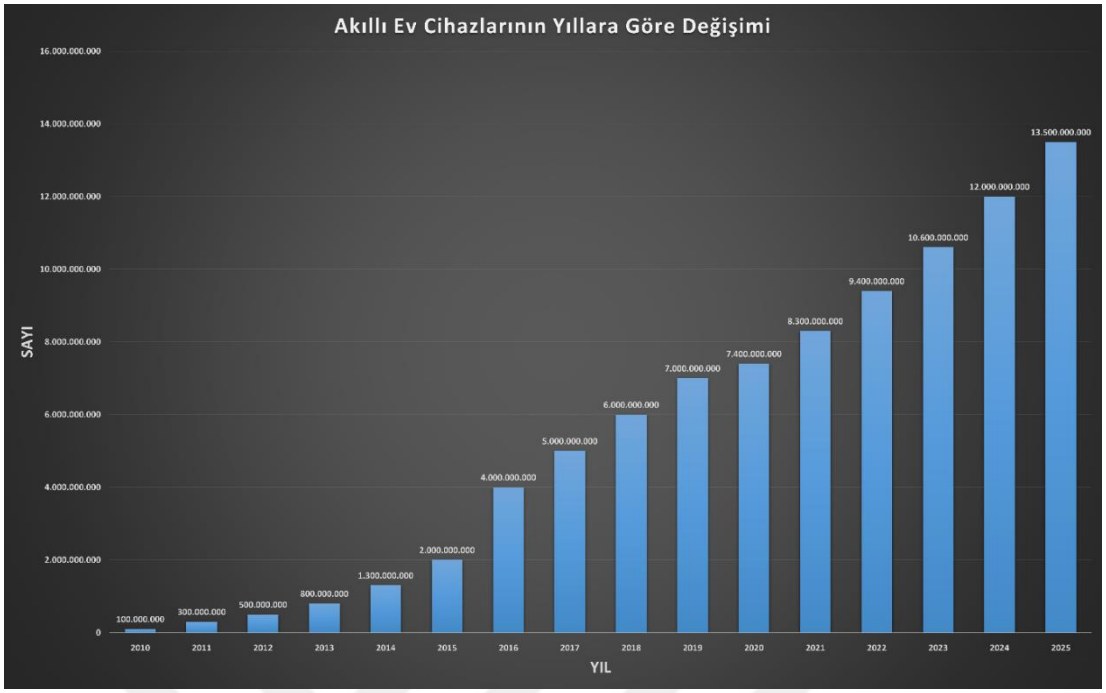
Bu grafikte, 2010 yılından 2025 yılına kadar olan IoT (Nesnelerin İnterneti) cihazlarının sayısındaki artış gösterilmektedir. 2010 yılında sadece 800 milyon olan cihaz sayısı, her yıl düzenli olarak artmış ve 2025 yılında 27 milyara ulaşması öngörülmektedir. Özellikle 2015'ten sonra büyüme daha da hızlanmıştır. Örneğin, 2015'te 3.6 milyar olan cihaz sayısı 2020'de 12.2 milyara, 2024'te ise 18.8 milyara çıkmıştır. Bu da teknolojinin hayatımıza ne kadar hızlı girdiğini gösteriyor. Özellikle son yıllarda akıllı ev cihazları, sensörler ve bağlı sistemlerin yaygınlaşması bu artışı desteklemiştir. Veriler, IoT alanındaki büyümenin gelecekte de devam edeceğini açıkça ortaya koymaktadır.



Şekil 6. IoT Cihazlarının Yıllık Artışı

Kaynak: Yazar tarafından oluşturulmuştur.

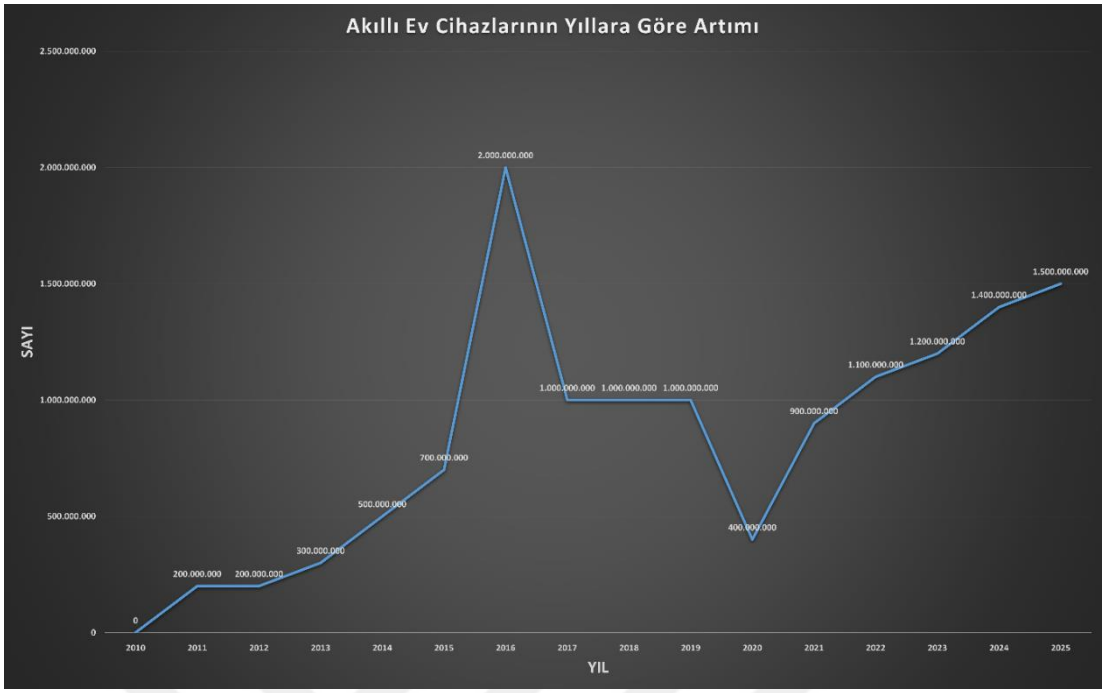
Bu grafik, yıllara göre IoT cihazlarındaki yıllık artışı göstermektedir. 2011'den 2018'e kadar artış istikrarlı bir şekilde yükselmiş, 2018 yılında 2.3 milyar cihazla zirveye ulaşmıştır. Ancak 2019 ve 2021 yılları arasında büyüme dalgalı olmuş, 2021'de sadece 500 milyonluk artışla ciddi bir yavaşlama yaşanmıştır. Bu durum, pandemi gibi küresel olayların üretim ve dağıtımı etkilemiş olabileceğini düşündürüyor. 2022'den itibaren yeniden 2.2 milyarlık sabit bir artış yaşanmış, 2025'te ise rekor kırarak 8.2 milyar cihazlık bir artış öngörülmektedir. Bu büyük sıçrama, IoT'ye olan talebin çok hızlı arttığını ve sektörün ciddi bir büyüme ivmesi kazandığını gösteriyor. Genel olarak, grafik bize teknolojik dönüşümün zamanla nasıl hızlandığını net bir şekilde yansıtıyor.



Şekil 7. Akıllı Ev Cihazlarının Yıllara Göre Değişimi

Kaynak: Yazar tarafından oluşturulmuştur.

Bu grafikte, akıllı ev cihazlarının yıllara göre sayısal değişimi gösteriliyor. 2010 yılında yalnızca 100 milyon olan cihaz sayısı, her yıl düzenli olarak artarak 2025 yılında 13.5 milyara ulaşması bekleniyor. En dikkat çeken sıçrama 2015'ten sonra başlıyor; örneğin 2015'te 2 milyar olan cihaz sayısı 2020'de 7.4 milyara çıkıyor. Bu artışın sebebi, ev otomasyonu, akıllı termostatlar, güvenlik sistemleri ve sesli asistanların yaygınlaşması olabilir. 2021 sonrası büyüme devam ediyor ama artış oranı biraz daha dengelenmiş görünüyor. 2022'de 9.4 milyar olan sayı, 2025'te 13.5 milyara çıkıyor. Bu da insanların yaşam konforuna ve güvenliğine yönelik teknolojilere olan ilgisinin giderek arttığını gösteriyor. Grafik, akıllı ev pazarının gelecekte de büyümeye devam edeceğine işaret ediyor.



Şekil 8. Akıllı Ev Cihazlarının Yıllık Artışı

Kaynak: Yazar tarafından oluşturulmuştur.

2010–2015 yılları arasında artış yavaş ve istikrarlıdır. En dikkat çeken sıçrama 2016 yılında yaşanmış ve cihaz sayısı bir yılda 2 milyar artmıştır. Bu dönem, akıllı ev teknolojilerinin hızlıca yayılmaya başladığı bir kırılma noktası olabilir. Ancak 2017–2019 arası artış sabit kalmış (1 milyar civarı), 2020'de ise büyük bir düşüş yaşanarak sadece 400 milyonluk bir artış gerçekleşmiştir. Bu düşüş, tedarik zinciri sorunları ya da ekonomik durgunlukla ilgili olabilir. 2021'den sonra sektör toparlanmış ve artış yeniden hızlanmıştır. 2025'e kadar her yıl ortalama 1–1.5 milyar arası cihaz eklenmesi beklenmektedir. Bu da insanların akıllı ev çözümlerine yeniden yöneldiğini ve sektörün istikrarlı şekilde büyümeye devam ettiğini göstermektedir.

2. KULLANICI GÜVENLİĞİ VE GİZLİLİK: STANDARTLAR, HAKLAR VE EN İYİ UYGULAMALAR

Akıllı ev sistemlerinde kullanıcı güvenliği ve gizliliği kapsamında siber tehditler, olası saldırılar, alınabilecek önlemler ve gizlilik açıkları ele alınmıştır.

2.1. IoT Destekli Akıllı Evlerin Potansiyeli ve Tehditleri

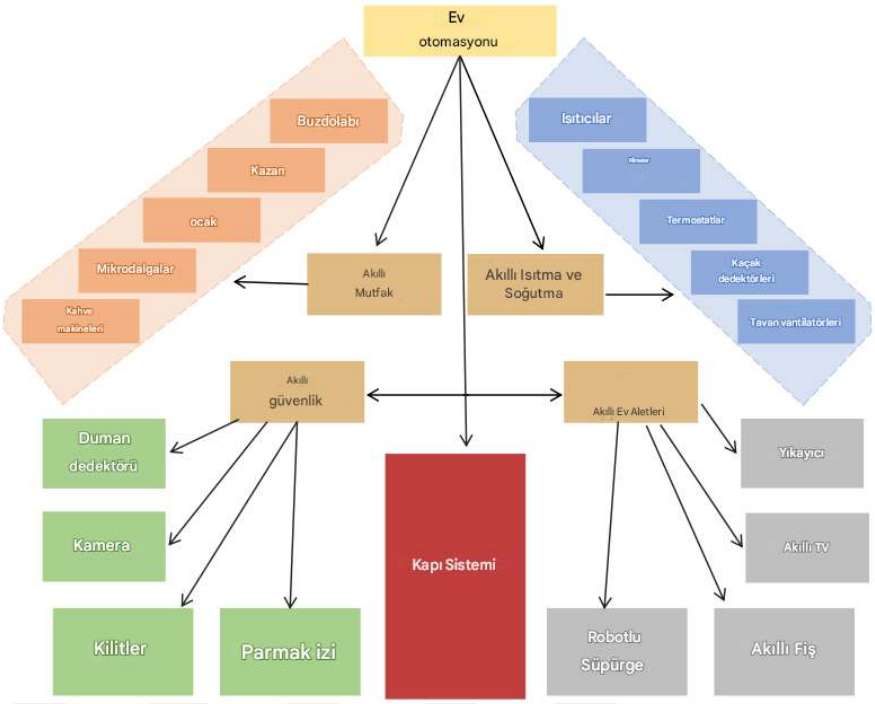
Fransa İstatistik Enstitüsü (INSEE) verilerine göre ülke nüfusunun %16,4'ü 65 yaş ve üzerindeyken, %8'i 75 yaş üstü gruptadır. Bu oranların ilerleyen yıllarda artması beklenmektedir. Buna bağlı olarak, 16-65 yaş aralığındaki bireylerin 65 yaş üstüne oranı 1990'lardaki 3:1 seviyesinden 2040 yılına kadar yaklaşık 2:1'e düşecektir. Benzer demografik eğilimler Avrupa'nın büyük kısmında, ABD'de ve Japonya'da da gözlenmektedir. Genel olarak bu durum, 2050 yılına gelindiğinde dünya nüfusunun yaklaşık %20'sinin 60 yaş ve üzerinde olacağını göstermektedir. Yaşlı bireylerin kurumlara yerleştirilmesini geciktirmek ve sağlık harcamalarını azaltmak için teknolojinin sunduğu çözümler öne çıkmaktadır. Amaç yalnızca hastalıkları tedavi etmek değil, aynı zamanda yaşamın her döneminde refahı desteklemektir. Özellikle akıllı teknolojiler, yaşlı bireylerin evlerinde bağımsız ve güven içinde yaşamalarına katkı sağlayabilir. 1980'li yılların başından itibaren ev otomasyonu, konfor ve güvenliği artırmaya yönelik bir alan olarak umut vadetmiştir. Fakat bu süreçte ev teknolojileri, telekomünikasyon ve otomotiv gibi sektörlerin gerisinde kalmıştır. Haneler gelirlerini daha çok otomobil veya bilgisayara ayırırken, ev otomasyonuna daha az yatırım yapılmıştır. Yine de belirli alanlarda önemli gelişmeler yaşanmıştır.

Nesnelerin İnterneti, "kendi kendine organize olabilen, bilgi ve kaynak paylaşımı yapabilen, çevresel değişimlere tepki veren ve hareket edebilen akıllı nesnelerden oluşan açık ve kapsamlı bir ağ" olarak tanımlanmaktadır (Madakam, 2015, s. 21). IoT, yaşam biçimimizi dönüştüren çağdaş bir teknolojidir. Otonom bir akıllı ev sistemi, ışık sensörleri, parmak izi okuyucular, gaz dedektörleri, duman ve sıcaklık sensörleri, hareket algılayıcılar ve güvenlik kameraları gibi gömülü cihazlarla donatılarak kullanıcının varlığını ve ihtiyaçlarını algılar ve bunlara yanıt verir. Bu cihazların birbirine bağlanması, enerji tasarrufu, fatura maliyetlerinde azalma ve güvenliğin artırılması gibi faydalar sağlamaktadır. Kullanıcılar bu sistemleri uzaktan

kumanda, bilgisayar veya akıllı telefon aracılığıyla kontrol edebilmektedir (Gunawan, 2018, s. 22). Günümüzde IoT tabanlı akıllı ev çözümlerinin kullanımı, dünya genelinde konforlu, kolay ve güvenli yaşam sunmak amacıyla hızla yaygınlaşmaktadır.

IoT Analytics'in 2021 yılı raporuna göre, aktif bağlantıya sahip cihaz sayısı 12,3 milyara ulaşmıştır. Transforma Insights verilerine göre ise bu sayı 2025'te 19,8 milyara, 2026'da 21,1 milyara, 2027'de 23,1 milyara ve 2030'da 31,2 milyara çıkacaktır. Cihaz sayısındaki bu hızlı artış, saldırı yüzeyini de genişletmekte ve herhangi bir güvenlik açığı potansiyel tehdit noktası haline gelebilmektedir. Ayrıca bu cihazlar Bluetooth, Wi-Fi, ZigBee gibi çeşitli iletişim protokollerini kullanarak doğrudan ya da dolaylı bağlantı kurmakta ve ev internetine entegre olmaktadır. Bu iletişimi ve cihazları güvenli hale getirmek, son yıllarda IoT sistem tasarımcıları için daha karmaşık bir sorun haline gelmiştir (Heartfield vd., 2018, s. 22).

Akıllı evler, birbirine bağlı sensörler ve cihazların tek bir merkezden yönetilmesine imkan tanır. Bu merkez akıllı telefon, tablet veya bilgisayar olabilir. Evde kontrol edilebilen nesneler arasında kapılar, kilitler, klimalar, ev aletleri, termostatlar, ekranlar, aydınlatma sistemleri, kameralar ve buzdolapları bulunmaktadır. Bu cihazların büyük çoğunluğu çevrimiçi bağlanarak bulut veya mobil uygulamalar üzerinden uzaktan kontrol edilebilir. Bu durum, kullanıcıya yüksek konfor ve ölçeklenebilir kullanım avantajı sunarken, bazı riskleri de beraberinde getirmektedir (Kopetz vd., 2011, s. 22). Kullanıcılar genellikle cihazların güvenlik yönetimini bilgisayar veya mobil uygulamalar aracılığıyla yapmaktadır. Bununla birlikte, sağlık verileri veya kredi kartı bilgileri gibi hassas verilere erişim imkanı sağlayan kötü niyetli saldırılar, ciddi endişelere yol açmaktadır. Örneğin, bir klimayı devreye sokarak hasar vermek veya buzdolabının sıcaklığını düşürmek gibi siber tehditler mümkündür.



Şekil 9. Akıllı Ev Cihazlarının İletişimi

Kaynak: Heartfield, R., Loukas, G. ve Gan, D. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers ve Security, 78*, 398–428.

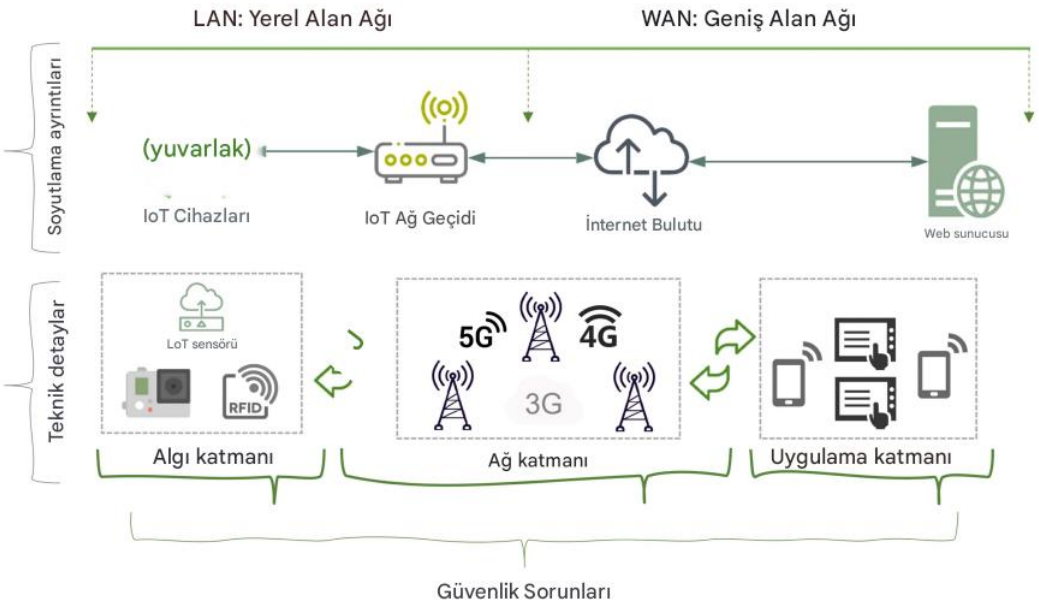
Son birkaç on yılda internet büyük bir gelişim göstermiş ve vazgeçilmez bir unsur haline gelmiştir. İnternetin yaygınlaşmasında ve Dünya Çapında Ağ'ın şekillenmesinde Berners-Lee önemli katkılar sağlamıştır. Berners-Lee'ye göre Nesnelerin İnterneti (IoT), herkesin erişimine açık, ücretsiz ve şeffaf bir yapıda olmalıdır. Transforma Insights verilerine göre, 2025 yılı itibarıyla dünya genelinde yaklaşık 19,8 milyar IoT cihazı çevrimiçi durumda olacaktır (Transforma Insights, 2025, s. 23). Ancak bu hızlı büyüme ciddi güvenlik sorunlarını da beraberinde getirmektedir.

IoT cihazları, kullanıcıların ad, doğum tarihi, adres ve kredi kartı bilgileri gibi birçok kişisel verisini toplayabilmektedir. Bu durum, milyonlarca dolarlık kayıplara ve müşteri güveni ile marka değerinde azalmaya neden olabilmektedir (Arora vd., 2018, s. 23). Özellikle fidye yazılımları giderek yaygınlaşmaktadır. 2021'de ABD'deki şirketlerin yaklaşık %11'i fidye taleplerine karşı 1 milyon dolar ödeme yapmıştır. Daha düşük miktarlar ödeyenlerin oranı ise %34'ten %21'e gerilemiştir. 2025 yılına gelindiğinde, fidye yazılımı saldırılarında ödeme yapan şirketlerin oranı %49'a

yükselmiş, ortalama fidye miktarı 2 milyon dolardan 1 milyon dolara düşmüş, ayrıca şirketlerin %53'ü talep edilen tutardan daha az ödeme yapabilmiştir.

Bu tür saldırılar hassas bilgilerin yetkisiz şekilde açığa çıkmasına yol açmaktadır. Örneğin, akıllı ev sistemlerinde yaşanan bir güvenlik ihlali, kullanıcıların sağlık verilerinin ifşa edilmesine neden olabilir. Bunun yanı sıra, sistem yöneticisi düzeyinde yetkisiz erişimler de tüm sistemi savunmasız hale getirmektedir (Lin vd., 2016). Ayrıca, bağlı cihazların çok sayıda saldırı yüzeyi bulunmakta ve farklı güvenlik açıkları ortaya çıkabilmektedir. Bu saldırılar uzaktan erişim, kontrol arayüzlerinin ele geçirilmesi ya da kötü amaçlı yazılımların yüklenmesi yoluyla gerçekleştirilebilmektedir.

Akıllı evlere yönelik güvenlik sorunları günümüzde daha belirgin hale gelmiştir. İnsanların teknoloji ve yeniliklere olan ilgisi, akıllı cihazlarla desteklenen konforlu bir yaşam tarzını teşvik etmektedir. Ancak bu cihazlar kullanım kolaylığı ve güvenlik avantajları sunsalar da, aynı zamanda siber tehditlere açıktır. Kullanıcı ihmalleri ve cihazlardaki zafiyetler nedeniyle, akıllı ev sistemlerinin pek çok kez saldırıya uğradığı çeşitli olaylarla kanıtlanmıştır (Siddhanti vd., 2019, s. 24).



Şekil 10. IoT Sisteminin Mimarisi

Kaynak: Meng, Y., Zhang, W., Zhu, H. ve Shen, X. S. (2018). Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. *IEEE Wireless Communications, 25*(6), 53–59.

2.2. Akıllı Ev Sistemlerine Saldırılar

Akıllı ev teknolojilerinin yaygınlaşması, kullanıcıların yaşamlarının pek çok yönünü doğrudan etkilemektedir. Kameralar, mikrofonlar, hareket sensörleri ve aktivite kayıt sistemleri gibi çeşitli sensörler, bu ortamları sürekli olarak izlemektedir. Sesle kontrol edilen aydınlatmalar veya uzaktan yönetilebilen kapı kilitleri gibi işlevsel özellikler sağlansa da, güvenlik uzmanları akıllı evlerde kullanılan internete bağlı cihazların beraberinde getirdiği gizlilik ve güvenlik risklerine dikkat çekmektedir. Yetersiz koruma önlemleri nedeniyle ev sakinlerine dair özel bilgilerin sızdırılması, ya da mevcut güvenlik açıklarının saldırganlar tarafından kullanılarak bireylerin yaşamlarının uzaktan izlenmesi veya manipüle edilmesi mümkün olabilmektedir (Zeng vd., 2017, s. 25). Bu sistemler, yaşam kalitesini artırmaya yönelik hizmetler sunsa da, veri sızıntısı ihtimali ciddi gizlilik sorunlarını beraberinde getirmektedir. Akıllı bir ev altyapısının oluşturulabilmesi için dört katmanlı otomasyon yapısı dikkate alınmalıdır: taşıma katmanı, algı katmanı, uygulama katmanı ve ağ katmanı. Şekil 11'de bu katmanlarda kullanılan IoT cihazları ve akıllı evlere yönelik saldırı türleri gösterilmektedir.

Taşıma katmanı: IoT ve makineden makineye (M2M) veri aktarımında en sık kullanılan protokollerden biri MQTT'dir. Bu protokol, TCP üzerinden çalışır ve bağlantının güvenliğini sağlamak amacıyla Taşıma Katmanı Güvenliği (TLS) kullanır. MQTT, olay tabanlı veri aktarımı ve sürekli veri akışlarında önemli bir rol üstlenir. Kısıtlı kaynaklara sahip uygulamalarda düşük yükle çalışabilmesi, onu birçok IoT çözümünde yaygın hale getirmiştir. Diğer bir protokol olan CoAP ise UDP üzerinde çalışmakta ve güvenlik için Datagram TLS'den yararlanmaktadır. HTTP protokolü TCP üzerinde TLS kullanırken, CoAP UDP üzerinden güvenlik sağlamaktadır.

Taşıma katmanına yönelik başlıca saldırı türleri şunlardır:

- Tekrar saldırısı: Bu yöntemde saldırgan, iki güvenilir taraf arasındaki veri akışını dinler, kopyalar ve sonrasında bu verileri kendisinden gönderilmiş gibi yeniden iletir. Böylece meşru bir hizmet isteğini taklit ederek kullanıcının erişim hakkına sahip olduğu hizmete izinsiz biçimde ulaşabilir.

- Mesaj değişikliği: Saldırgan, taraflar arasındaki iletişime müdahale ederek mesaj içeriklerini manipüle edebilir. Bu değişiklikler yazılımın kötü amaçlı çalışmasına veya veri değerlerinin değiştirilmesine yol açabilir.
- Hizmet reddi saldırıları (DoS): Bu saldırılarda amaç, meşru kullanıcıların ağ hizmetlerine erişimini engellemektir. Saldırgan, ağ kaynaklarını tüketmek için kesintisiz mesaj akışı gönderebilir. Sonuç olarak, yetkili kullanıcılar sistemin sağladığı hizmetlerden yararlanamaz. Ayrıca, sunuculara ve internete bağlı diğer cihazlara yoğun mesaj gönderimiyle akıllı evlerdeki kablolu ya da kablosuz ağ trafiği kısıtlanabilir.

Katman	IoT cihazı/Uygulama	Amaç	Saldırı nesnesi
Algı	Fiziksel nesneler, Sensörler, Aktüatörler	bilgi toplayın itibaren hakkında	Fiziksel hasar, Dinleme, Düğüm yakalama, Tekrar saldırısı, Zamanlama saldırısı
Ağ/Ulaşım	Yönlendirici, Ağ Geçitleri, LoraWAN, 3G, 4G	Cihazları kablolu/kablosuz ortam aracılığıyla birbirine ve daha üst katmana bağlayın	Tam kontrol, Dinleme, Trafik analizi, DoS saldırısı, Ortadaki adam, DDoS
Başvuru	Ev aletleri	Sensörlere özgü hizmeti uygulamaya/istemcilere genişletme sorumluluğuna sahiptir	Kontrolü ele alın, Konuşmacıları tanımlayın, Siteler arası betik çalıştırma, Kötü amaçlı canlı taşması

Şekil 11. Farklı Katman Seviyelerindeki Akıllı Ev Saldırıları

Kaynak: Zeng, E., Mare, S. ve Roesner, F. (2017). End user security and privacy concerns with smart homes. *Proceedings of the 13th Symposium on Usable Privacy and Security*, Paul G. Allen School of Computer Science and Engineering University of Washington, Washington.

Algılama katman

Bu seviyedeki tehditlerin büyük kısmı doğrudan sensörlere yöneliktir. En yaygın güvenlik sorunları arasında dinleme, düğüm yakalama, tekrar saldırısı ve zamanlama saldırıları yer almaktadır. Dinleme saldırılarında, saldırgan telefon görüşmeleri, mesajlar veya görüntülü konferanslar gibi özel iletişimleri ele geçirir ve güvenli olmayan kanallardan faydalanarak bu verilere erişir. Düğüm yakalama saldırısı ise kablosuz sensör ağlarında kritik bir risktir; saldırgan, sistemdeki konuşmaları, paylaşılan şifreleri ve kriptografik anahtarları ele geçirerek tüm ağı tehlikeye atabilir. Tekrar saldırılarında (Aarika, 2020, s. 26), saldırgan meşru iletişimi dinler, bilgileri kopyalar ve kurbana yeniden göndererek bunun geçerli bir iletişim olduğuna inandırır. Zamanlama saldırıları ise sınırlı işlem gücüne sahip cihazlarda görülür; saldırgan,

sistemin farklı girdilere yanıt verme sürelerini gözlemleyerek gizli bilgileri ele geçirebilir.

Uygulama katman

Bu katman, heterojen IoT ortamlarında cihazlarla ağ arasındaki iletişimi tanımlar. Uygulama düzeyinde oluşabilecek bir açık, tüm ağı tehlikeye atarak kişisel verilerin ifşasına yol açabilir. Bu seviyede sık rastlanan güvenlik tehditlerinden biri siteler arası komut dosyası saldırısıdır. Web tabanlı bir enjeksiyon saldırısı olan bu yöntem, genellikle kullanıcı taraflı uygulamaları hedef alır. Kötü amaçlı bir komut dosyası aracılığıyla tarayıcıya enjekte edilen kod, saldırgana çerez bilgilerine erişim veya cihazlar üzerinde kontrol sağlama imkanı verir (Pranathi vd., 2018; Rodríguez, 2020, s. 27). Diğer bir tehdit, sisteme zarar vermeyi amaçlayan kötü amaçlı kod saldırılarıdır. Bu tür saldırılar antivirüs yazılımlarıyla tamamen engellenemeyebilir. Ayrıca, IoT cihazları yazılım ve donanım açıkları sebebiyle arabellek taşması saldırılarına da maruz kalabilmektedir.

Ağ katmanı: Akıllı ev cihazları, Bluetooth, WiFi, ZigBee, RFID, NFC, Wireless Hart gibi farklı iletişim teknolojileri aracılığıyla bağlanmaktadır. Kablosuz ağların güvenli olmaması, saldırganların ağ koklama veya gözetleme saldırıları başlatmasına zemin hazırlar. Bu seviyedeki başlıca saldırılar şunlardır:

DoS saldırıları: Meşru kullanıcıların sisteme erişimini engellemek amacıyla ağ kaynaklarının aşırı yüklenmesidir. Saldırgan, sürekli istek göndererek cihazların veya ağların hizmet veremez hale gelmesine neden olur.

Aracı (MiTM) saldırıları: İki taraf arasındaki iletişim saldırgan tarafından gizlice dinlenir ve değiştirilir. Taraflar doğrudan konuştuklarını sanırken, saldırgan iletişimi manipüle ederek kendi çıkarına yönlendirebilir. Örneğin, bir Samsung akıllı buzdolabında SSL sertifikalarının kontrol edilmediği tespit edilmiş, bu zafiyet üzerinden Gmail kullanıcılarının oturum bilgileri ele geçirilmiştir.

DDoS saldırıları: İnternete yönelik en önemli tehditlerden biri dağıtılmış hizmet reddi saldırılarıdır. Bu saldırılarda yansıma ve trafik yükseltme yöntemleriyle hedef sistemlere çok sayıda paket gönderilir. TCP Syn Flood, UDP Flood veya ICMP

Flood gibi farklı teknikler kullanılarak TCP/IP protokolündeki zayıflıklar istismar edilir (Džaferovic vd., 2019, s. 27).

Klasik brute force yöntemlerinden farklı olarak bu saldırılarda, dil modelleri ve ele geçirilmiş veri kümeleri kullanılır. Böylece parolalar rastgele denenmez, kullanıcıya özgü tahmin dizileri oluşturulur. Örneğin, akıllı kilitler veya Wi-Fi yönlendiricileri için yapılan denemelerde, kullanıcının sosyal medya hesaplarından elde edilen doğum tarihi, evcil hayvan adı gibi ipuçları önceliklendirilir. Bu yöntem, parola kırma süresini önemli ölçüde kısaltır. Zararlı yazılım, ev ağındaki tüm IoT cihazlarını pasif şekilde tarayarak haritalandırır. CPU gücü düşük bir akıllı süpürge dahi ağ topolojisini analiz ederek en zayıf güvenlik önlemine sahip cihaza yönlenebilir. İnsan müdahalesine gerek kalmadan "en kolay ele geçirilecek hedef" belirlenir ve saldırının kapsamı hızla büyür. Kamera, hareket sensörü veya akıllı hoparlör gibi yapay zeka tabanlı modüller, insan gözüyle fark edilmeyen özel gürültü ve örüntülerle yanıltılabilir. Bu sayede cihaz yanlış sınıflandırma yapar; örneğin, hırsızlık olayını "normal durum" olarak algılar. Böylece fiziksel hasar olmadan algı katmanı işlevsiz hale gelir.

Edge AI destekli saldırılar, ağ trafiğini normal akışlara benzeterek güvenlik yazılımlarının imza ve davranış tabanlı tespit mekanizmalarını aşar. Ayrıca log kayıtlarını otomatik olarak silerek uzun süre fark edilmeden çalışır. Bu yöntemle saldırgan, cihazı kalıcı bir komuta-kontrol merkezine dönüştürebilir. Cihaz içindeki yerel yapay zeka modeli kopyalanabilir, değiştirilebilir veya yanına izinsiz ikinci bir "gölge model" yüklenebilir. Manipüle edilen model, örneğin güvenlik kamerasının tüm görüntüleri "tehlikesiz" olarak etiketlemesine neden olur. Kullanıcı, arayüzde herhangi bir anormallik fark etmeden sistemi kullanmaya devam eder.

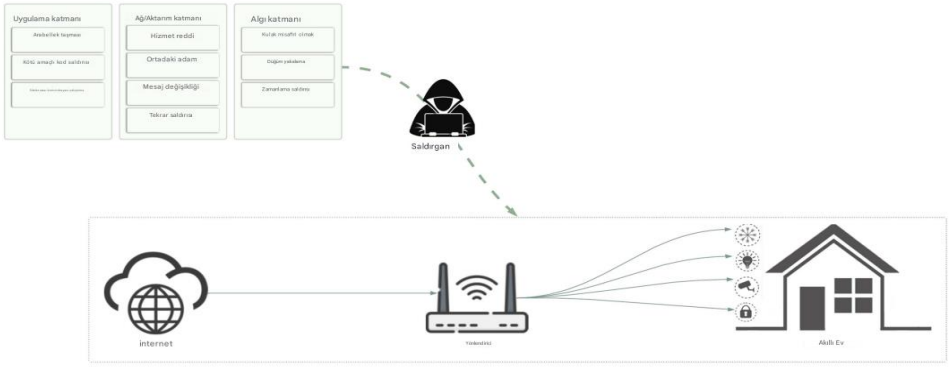
2.3. Saldırıları Önlemek İçin Güvenlik Önlemleri

Siber güvenlik riskleri, aydınlatma, ev aletleri ve kilitler gibi normalde bağımsız çalışan akıllı cihazların birbirine bağlanmasıyla daha net şekilde ortaya çıkmaktadır. Nitekim bazı ebeveynler, bilgisayar korsanlarının ele geçirilen bebek monitörleri aracılığıyla küçük çocuklarıyla iletişim kurabildiğini gördüklerinde büyük bir şok yaşamıştır. Şekil 12'de akıllı ev cihazlarını hedef alan en yaygın siber güvenlik

tehditleri ve saldırı türlerine örnekler sunulmaktadır. Bu tür saldırıların önlenebilmesi için çeşitli güvenlik önlemlerinin alınması gerekir.

Ağ katmanında, ev ağları genellikle kısıtlı kaynaklara sahip bir ağ geçidi aracılığıyla internete bağlanan heterojen yapılardan oluşmaktadır (Camphouse, 2019). Akıllı ev bağlamında düşünüldüğünde, Wi-Fi yönlendirici birincil ağ geçidi rolünü üstlenmektedir. Bu noktada, yönlendiriciye bağlı cihaz çeşitliliği ve güvenlik açıklarından kaynaklanan trafik sorunları önemli tehditler oluşturmaktadır. TR-069 protokolü, yani CPE WAN Yönetim Protokolü (CWMP), çevrimiçi tüm cihazların uzaktan izlenmesini kolaylaştırmakta ve hizmet kalitesini artırmaktadır. Ancak aynı zamanda, kötü niyetli bir aktör tüm yönlendiriciyi ve ağı ele geçirerek sistemi bozabilir. Bu nedenle yönlendiricinin güçlendirilmesi, akıllı ev güvenliğinin sağlanmasında ilk kritik adım olarak görülmektedir. Yönlendirici, IoT cihazlarını birbirine bağlayan yapıştırıcı işlevi görür ve sistemin işlevselliğinde temel role sahiptir. Daha güvenli bir yönlendirici kurulumu için aşağıdaki hususlara dikkat edilmelidir:

- **Yönlendiricinin varsayılan adını kullanmamak:** Yönlendiricinin marka veya model bilgisini içermeyen yeni bir ad belirlenmelidir. Eğer cihazın marka ve modeli biliniyorsa, dışarıdan kişiler akıllı ev ağına daha kolay erişebilir. Bu nedenle cihaz adı, kullanıcının kimliği veya adresi gibi kişisel bilgilerle ilişkilendirilmeyecek şekilde değiştirilmelidir.
- **Ev sahibinin adından farklı ve güçlü bir parola belirlemek:** Yönlendirici parolası, harf, sayı ve sembol kombinasyonlarından oluşan, tahmin edilmesi güç bir yapı ile ayarlanmalıdır. Rastgele parola üreteçleri kullanılarak kırılması neredeyse imkansız şifreler oluşturmak mümkündür.



Şekil 12. Akıllı Evlerdeki Güvenlik Saldırıları

Kaynak: Camphouse, A. ve Ngalamou, L. (2019, 10-12 Ekim). *Securing a connected home*. Proceedings of the 10th Annual Ubiquitous Computing, Electronics ve Mobile Communication Conference, Columbia University, New York.

- **Veri Şifreleme:** Kablosuz ağ güvenliği için en gelişmiş yöntem WPA3 protokolüdür. WPA2'nin yerine geçmeye başlayan bu standart, daha güçlü güvenlik özellikleri sunmaktadır. WPA3 kullanıldığında, IoT ortamındaki kablosuz iletişimler kırılma, gizlice dinleme ve yetkisiz erişim girişimlerine karşı korunur. WPA3'ün sunduğu bireysel şifreleme özelliği sayesinde, aynı ağa bağlı cihazların birbirlerinin verilerine erişmesi mümkün olmaz. Bilgisayar korsanlarının öncelikli hedefi genellikle ev yönlendiricileridir; bu nedenle güvenli bir yönlendirici, akıllı ev güvenliği için temel bir gerekliliktir (Vlajic, 2018, s. 30).

Yapay zeka tabanlı güvenlik kameraları, yüz tanıma özelliği sayesinde geleneksel kamera sistemlerinden ayrılır. Bu sayede ev sahipleri eve giren kişileri ve izinsiz giriş zamanlarını kolayca görebilmektedir. Edge AI cihazları, verileri doğrudan yerel ortamda işlediğinden internet bağlantısına gerek duymaz; böylece veri gecikmesi ortadan kalkar ve gerçek zamanlı analiz mümkün olur. Edge AI sistemleri hızlı işlem, düşük gecikme, maliyet avantajı, daha az bant genişliği kullanımı, artırılmış güvenlik ve enerji verimliliği gibi avantajlar sağlamaktadır. Bununla birlikte, yapay zeka modellerinde karşılaşılan bazı teknik sorunlar dikkate alınmalıdır. IoT cihazları, akıllı evlerde veri toplayıp işleyerek güvenlik tehditlerinin analiz edilmesine yardımcı olur. Manuel işlem gerektirmeden tehdit algılama ve yüz tanıma işlevleri otomatik olarak gerçekleştirilir. Gelişmiş sistemler aile üyelerini, arkadaşları ve evcil hayvanları

tanıyabilir; yapay zeka destekli duman dedektörleri ise dumanı algılayarak mobil cihazlara bildirim gönderebilir, yangının yeri hakkında bilgi sağlayabilir. Ayrıca, Google Asistan, Siri ve Alexa gibi sesli asistanlar yapay zeka ile desteklenmekte ve kullanıcıların evlerini ses komutlarıyla kontrol etmesini sağlamaktadır.

Akıllı ev otomasyon sistemleri, alarmlarla entegre edilmiş güvenlik stratejileri aracılığıyla konutların korunmasına katkıda bulunur. Hareket sensörleri yanlış alarmları en aza indirirken, izinsiz girişleri tespit eder. Yürüyüş kalıpları her birey için farklı olduğundan, IoT sensörleri biyometrik doğrulama için kullanılabilir. Bu sistemlerde hareket algılama ve tanıma temelli güvenlik çözümleri önerilmektedir. Ayrıca yüz tanıma algoritmaları, göz rengi ve cilt tonu gibi farklı özellikleri de değerlendirerek güvenliği artırmaktadır.

Yeni Saldırılara Karşı Güvenlik Önlemleri:

- **Mikro Segmentasyon ve Yapay Zeka Tabanlı Yönlendirici Koruması:** VLAN tabanlı segmentasyon sayesinde cihazlar farklı alt ağlara ayrılır; Netgear Orbi 770/970 serisi gibi yeni nesil yönlendiriciler, şüpheli veri akışlarını tespit ederek cihazları otomatik karantinaya alabilir.
- **Model Sertleştirme ve İmzalı Dağıtım:** Adversarial saldırılara karşı güçlendirilmiş yapay zeka modelleri TPM veya TrustZone gibi güvenli alanlarda saklanır. Modeller kriptografik olarak imzalanır; doğrulama yapılmadan yükleme mümkün değildir.
- **Secure Boot ve İmzalı OTA Güncellemeler:** Yalnızca üretici imzasına sahip yazılımlar çalıştırılabilir. Firmware bütünlüğü başlangıçta kontrol edilir; imzasız kod çalıştırılmaz.
- **PUF Tabanlı Kimlik ve Model Koruma:** Donanım seviyesinde benzersiz kimlik üreten Physically Unclonable Function (PUF) sayesinde modeller yalnızca ilgili cihazda çalışabilir. AWS Device Defender benzeri sistemler sertifika yaşam döngüsünü denetler.
- **AI Destekli Ağ Anomali Tespiti ve DNS Koruması:** Kaspersky Smart Home Monitor, olağan dışı trafik davranışlarını izleyerek saldırıları erkenden durdurur. Palo Alto Networks Advanced DNS Security ise kötü amaçlı alan adlarını filtreleyerek komuta-kontrol bağlantılarını engeller.

- **Güçlü Şifre Kullanımı:** Güçlü şifreler yalnızca Wi-Fi ağları için değil, aynı zamanda IoT cihaz hesapları ve mobil uygulamalar için de zorunludur. Her cihazın farklı giriş bilgilerine sahip olması gerekir. Böylece bir cihazın parolası ele geçirilse bile diğer cihazlar güvende kalır. Çok sayıda şifreyi yönetmek için parola yöneticilerinden yararlanılmalıdır. Bu yazılımlar, güvenli parola oluşturma, kaydetme ve farklı cihazlarla senkronizasyon imkanı sunarak kullanıcıların güvenlik düzeyini artırır.

Ev güvenliğinde hareket algılama ve izleme için konvolüsyonel sinir ağları önemli rol oynamaktadır. Bu modeller gözetim kameralarından elde edilen görüntüleri işleyerek alanları tanıyabilir. Derin öğrenme tabanlı akıllı algılama sayesinde, ev otomasyon sistemi tarafından tespit edilen hareketler, alarm tetiklenmeden önce ev sakinleri ya da izinsiz giriş yapan kişiler olarak sınıflandırılabilir (Kishore vd., 2018, s. 32). Bununla birlikte, verimli çalışan bir ev otomasyon sistemi, su ve elektrik gibi kaynakların daha bilinçli kullanılmasına imkan vererek enerji tasarrufu sağlar. Ortam zekası ışıkları, iklimlendirme sistemlerini, eğlence araçlarını ve ev aletlerini düzenleyebilir.

Modern yönlendiricilerde misafir ya da ikincil ağ oluşturma özelliği bulunmaktadır. Akıllı ev kullanıcıları, IoT cihazları için ayrı bir ağ kurarak birincil ağı siber tehditlerden koruyabilir. Bu sayede misafirler, aile üyeleri veya arkadaşlar IoT cihazlarının bağlı olmadığı bir ağa erişir. Böylece yalnızca ev sahibi ve ailesi akıllı ev ağına erişebilir. IoT cihazlarının ayrı bir ağda çalışması durumunda, bilgisayar korsanlarının dizüstü bilgisayar veya akıllı telefon gibi kritik cihazlara erişmesi engellenmiş olur.

Birçok IoT cihazı uzaktan erişim özelliği ile donatılmıştır. Ancak güvenlik gerekçesiyle kullanılmayan uzaktan erişim özelliklerinin devre dışı bırakılması önerilir. Örneğin, akıllı hoparlörler Wi-Fi'ye ek olarak Bluetooth bağlantısı da içerir; kullanılmayan bu hizmetlerin kapatılması güvenliği artırır. Benzer şekilde, akıllı televizyonlarda sesli komut özellikleri devre dışı bırakılabilir. Mikrofonlar saldırılar için giriş noktası oluşturabileceğinden, bu özelliklerin kapatılması güvenliği artırır. IoT cihazlarının her biri incelenmeli, gerekli ve gereksiz özellikler ayırt edilmelidir. Özellikle, IP tabanlı endüstriyel sensörler daha az özelliğe sahipken, son kullanıcı

cihazlarında daha fazla özellik yer alabilmektedir. Gereksiz bir özelliğin kapatılması dahi güvenlik düzeyini yükseltebilir. Örneğin, Wi-Fi özellikli bir termostatın uzaktan erişim özelliği devre dışı bırakıldığında, bilgisayar korsanının bu cihazı diğerlerine saldırı için bir araç olarak kullanma ihtimali ortadan kaldırılır.

Uzaktan hizmetler, akıllı ev sistemine ek işlevler kazandırmak amacıyla toplanan verileri analiz eder ve raporlar. Ancak gizlilik ihlallerini önlemek için, sistemde özelleştirilebilir zaman çözünürlüğü kısıtlamalarının uygulanması tavsiye edilmektedir. Örneğin, veri toplama çözünürlüğü 15 dakikanın altına düşürülemez; bu yöntem gizliliği artırırken kullanılabilirlik üzerinde minimal etki yaratır (Brauchli vd., 2015, s. 33). Ayrıca, API erişimlerinin ve tüm işlemlerin kayıt altına alınması, güvenliği artıracak ve üçüncü taraf hizmetlerden kaynaklı riskleri azaltacaktır. Otomatik log denetimleriyle anormal durumlar erkenden tespit edilebilir. Kullanıcılar, uygulama özelliklerini yüklemeden önce onaylama veya reddetme hakkına sahip olmalıdır. Bu nedenle, uygulamaların veri işleme süreçleri açıkça belgelenmeli ve kod yollarıyla karşılaştırılarak doğrulanmalıdır.

GDPR (Genel Veri Koruma Yönetmeliği), hizmet sağlayıcıların kullanıcıların gizliliğini korumak için gerekli önlemleri almasını zorunlu kılmaktadır. Bu kapsamda üç farklı yaklaşım uygulanabilir:

- **Satıcı tabanlı anonimleştirme:** Kullanıcı verileri üçüncü taraf hizmetlere aktarılmadan önce üretici tarafından anonimleştirilir.
- **Hizmet olarak anonimleştirme:** Anonimleştirme işlemi üçüncü taraf hizmet tarafından gerçekleştirilir ve yalnızca anonim veriler üreticiye aktarılır.
- **Yerel anonimleştirme:** Kullanıcıların hem satıcıya hem de üçüncü taraf hizmetlere güvenmediği durumlarda anonimleştirme, uç yönlendiricide yerel olarak yapılır. Böylece bilgiler üreticiye iletilmeden önce gizlilik korunur.

Wi-Fi yönlendiricilerinde aygıt yazılımı güncellemeleri genellikle otomatik olarak yapılmamaktadır. Oysa güvenlik açıklarına yönelik yamalar çoğunlukla bu sürümlere eklenir. Bu nedenle birkaç ayda bir manuel olarak güncelleme kontrolü yapılmalı, mevcutsa indirilip hemen kurulmalıdır. IoT cihazları ve uygulamaları da çoğu zaman otomatik güncellenmez; yeni sürümler çıktığında kullanıcıya yalnızca bildirim gönderilir (McIlroy vd., 2016, s. 33). Kablosuz aygıt yazılımı veya FOTA,

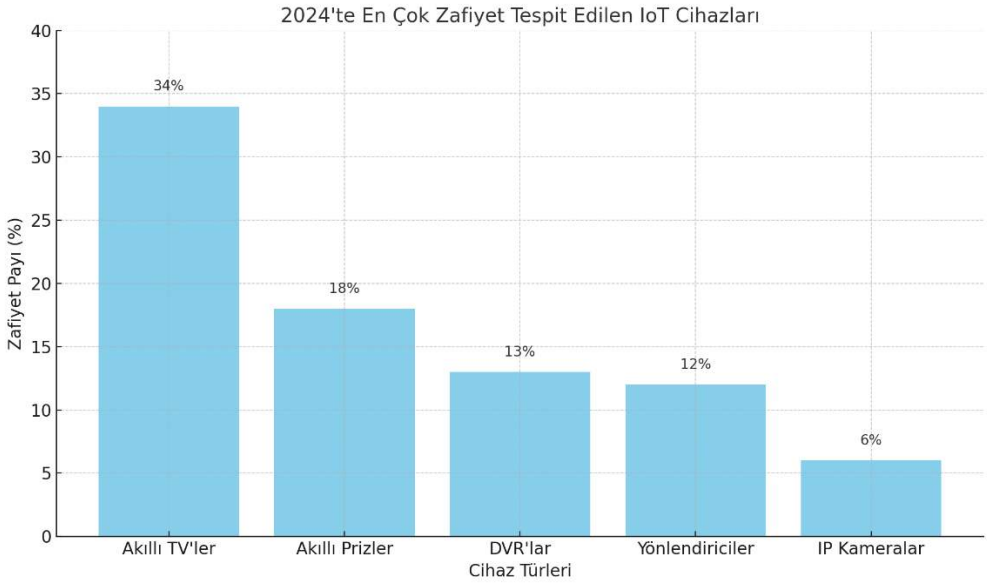
cihazlara fiziksel erişim gerektirmeden uzaktan güncelleme yapmayı sağlayarak ölçeklenebilirlik ve güvenilirliği artırır. Ancak güncellemeler sırasında güvenlik önlemleri kritik öneme sahiptir; çünkü akıllı evlerde yeterli güvenlik sağlanmadığında güncellemeler saldırganlar tarafından değiştirilebilir. Bu sebeple güvenli JavaScript Nesne Gösterimine dayalı FOTA nesneleri kullanılmalı ve Gelişmiş Şifreleme Standartları ile simetrik şifrelemeye dayalı güvenli kablosuz programlama çerçeveleri benimsenmelidir.

Çok faktörlü kimlik doğrulama (2FA), yalnızca parolayla sınırlı kalmayan ek bir güvenlik katmanı sağlar. Böylece IoT cihazına giriş yapmaya çalışan kişi, kimliğini doğrulamak için ek kanıt sunmak zorunda kalır. Varsayılan olarak bu özelliği bulunmayan cihazlarda üçüncü taraf kimlik doğrulama çözümleri (bulut tabanlı) kullanılabilir. Güvenilir hizmet sağlayıcıları tarafından sunulan bu ek koruma, cihazların eşlik eden mobil uygulamalarında dahi güvenliği artırarak kullanıcıya daha fazla güvenlik garantisi sağlar (Adat vd., 2018, s. 34).

Kablosuz ve kablolu ağlarda makineden makineye (M2M) iletişim giderek daha kritik hale gelmektedir. Akıllı evlerde M2M, kullanıcıların evlerini uzaktan ve otomatik olarak yönetmelerini sağlar. Yangın ve gaz algılama, aydınlatma, otomatik kapılar, alarm sistemleri ve sıcaklık kontrolü gibi özellikler buna dahildir. Bu sistemler, Arduino UNO'nun merkezi işlemci rolü üstlendiği Android/Arduino UNO tabanlı platformlarla desteklenebilir (Jiang vd., 2015, s. 34). Böylece kullanıcılar yalnızca akıllı telefon üzerinden evi kontrol ederek konfor ve güvenlik sağlayabilir. Endüstriyel IoT ortamında uzmanlar, XOR ve hash temelli hafif kimlik doğrulama mekanizmaları önermektedir. Bu mekanizmalar düşük işlem yükü ve iletişim maliyeti ile çalışırken, kimlik gizliliğini korur ve tekrar, aracı ya da kimliğe bürünme gibi saldırılara karşı direnç sağlar. Sensörlerin kayıt prosedürü güvenli kanallar üzerinden yapılmalı, ardından yönlendirici ile sunucu arasında karşılıklı kimlik doğrulaması gerçekleştirilmelidir. Ayrıca sensörlerin doğrulama sürecinde gerçek kimliklerini paylaşmadığı unutulmamalıdır. Bu yöntem, kötü niyetli aktörlerin sensör kimliklerini ele geçirmesini engeller.

Yönlendiricilerde bulunan standart güvenlik duvarları, kötü amaçlı yazılım koruması, içerik filtreleme, SSL/SSH engelleme, QoS yönetimi ve VPN denetimi gibi

ek özelliklerden yoksundur. Yeni nesil güvenlik duvarları ise bu eksiklikleri gidererek siber saldırıları tespit edip engelleyebilir. NGFW'ler maliyet açısından yüksek olsa da, akıllı ev güvenliği için önemli katkılar sağlar. Son dönemde araştırmacılar, yazılım tanımlı ağlar (SDN) üzerinden ev kullanıcılarına güvenlik duvarı işlevi sunulmasını önermektedir. Gordon ve çalışma arkadaşları, K-En Yakın Komşu (KNN) tabanlı cihaz sınıflandırmaları ve FPGA destekli trafik analiziyle akıllı evlerin korunması için SDN-FPGA tabanlı bir mimari geliştirmiştir. Ayrıca, ağ güvenliğini artırmak amacıyla NFV teknolojileri uygulanmaktadır. Örneğin, bir TP-Link kamerasından elde edilen gerçek zamanlı trafikle eğitilen kenar analizi VNF'si, tehditleri bir saniyeden kısa sürede yaklaşık %95 doğrulukla tespit edebilmektedir. Doğru VNF çözümleriyle bilinen saldırılar etkisiz hale getirilebilmektedir.



Şekil 13. En Çok Zafiyet Tespit Edilen IoT Cihazları 2024

Kaynak: Yazar tarafından oluşturulmuştur.

Grafikte 2024 yılında en çok güvenlik zafiyeti tespit edilen IoT cihaz türleri gösterilmektedir. Verilere göre en yüksek oran %34 ile akıllı televizyonlardadır. Bu sonuç, akıllı TV'lerin hem yaygın kullanımından hem de çoğu zaman güncellemelerinin ihmal edilmesinden kaynaklanmaktadır. İkinci sırada %18 ile akıllı prizler gelmektedir. Bu cihazların basit yapıda olması, güvenlik önlemlerinin yetersiz kalmasına yol açmaktadır. DVR cihazları %13 oranında zafiyet göstermektedir; genellikle kamera sistemlerinde kullanıldıkları için saldırganlar için cazip hedeflerdir.

Yönlendiriciler %12 oranıyla dikkat çekmektedir. İnternetin ana giriş noktası olduklarından, burada yaşanan bir açık tüm ağa zarar verebilir. IP kameralar ise %6 ile en düşük orana sahiptir. Ancak düşük oran riskin önemsiz olduğu anlamına gelmez; çünkü kameralar doğrudan mahremiyet ihlallerine sebep olabilir. Genel tabloya bakıldığında, akıllı cihazların sağladığı kolaylıkların yanında ciddi güvenlik riskleri taşıdığı görülmektedir. Kullanıcıların yazılım güncellemelerini aksatmaması, güçlü şifreler kullanması ve üreticilerin daha güvenli sistemler geliştirmesi büyük önem taşımaktadır. Böylece hem bireysel gizlilik hem de genel siber güvenlik korunabilir.

2.4. Kullanıcı Gizliliği ve Siber Güvenlik Zafiyetleri

IoT tabanlı akıllı ev sistemlerinde güvenlik bilinci, hem sistemlerin etkinliği hem de güvenlik düzeyleri açısından belirleyici bir rol oynamaktadır. Bu sistemler günlük yaşamı kolaylaştıran pek çok avantaj sunsa da, kullanıcıların veri güvenliği ve mahremiyetine yönelik tehditler barındırdığı unutulmamalıdır. Günümüzde bireylerin bu tehditlerin farkında olması ve sorumluluk alması, akıllı ev sistemlerinin daha güvenli hale gelmesine katkı sağlamaktadır. Kullanıcılar yalnızca teknolojinin faydalarından yararlanmakla kalmamalı, aynı zamanda potansiyel riskler konusunda da bilinçli olmalıdır (Singh vd., 2019, s. 36).

Güvenlik bilinci, kullanıcıların çevrimiçi ortamda kişisel verilerini koruma alışkanlıklarını ve bunun için atılacak adımları kapsar. Bu noktada siber güvenlik eğitimleri ve farkındalık programları, güvenli davranışların teşvik edilmesi açısından önemlidir. Örneğin, güçlü ve karmaşık şifreler oluşturmak, düzenli yazılım güncellemeleri yapmak ve ağ güvenliğini sağlamak temel adımlardandır. Ayrıca, cihaz ayarlarının ve gizlilik politikalarının dikkatle incelenmesi, veri paylaşımı izinlerinin yönetilmesi ve güvenlik açıkları hakkında bilgi edinilmesi, kullanıcıların genel güvenlik bilincini artırmaktadır. Sonuç olarak, akıllı evler yalnızca teknik yenilikler değil, aynı zamanda kullanıcıların güvenlik farkındalığıyla desteklenen dinamik bir çerçevedir (Jyothi vd., 2017, s. 36). Kullanıcılar sadece kendi verilerini korumakla kalmamalı, aynı zamanda güvenli bir dijital yaşam alanının oluşturulmasına da katkıda bulunmalıdır.

Akıllı ev sistemlerinde güvenliği ve kullanıcı mahremiyetini sağlamak için gizlilik politikaları ve yasal düzenlemeler büyük önem taşımaktadır. Bu düzenlemeler, kullanıcıların kişisel verileri üzerindeki haklarını ve bu verilerin nasıl işlendiğine dair bilgilendirilmesi gereken hukuki çerçeveyi oluşturur. Genel Veri Koruma Yönetmeliği (GDPR) gibi düzenlemeler, verilerin toplanması, saklanması ve işlenmesinde şeffaflık sağlamak amacıyla bireylere çeşitli haklar tanımaktadır. GDPR'ye göre kullanıcıların kişisel verilerinin işlenmesi için meşru bir zemin bulunmalı ve kullanıcılar hangi amaçla kullanılacağını bilerek onay vermelidir.

Akıllı ev sistemleri enerji kullanımı, güvenlik kameraları ve sıcaklık ayarları gibi pek çok hassas veri toplayabilmektedir. Bu nedenle, firmaların kapsamlı gizlilik politikaları geliştirmesi hem kullanıcı mahremiyetini korumak hem de yasal yükümlülüklerini yerine getirmek açısından gereklidir. Açık ve anlaşılır gizlilik politikaları, kullanıcıların sisteme olan güvenini artırırken, yasal düzenlemeler üreticilere uyum zorunluluğu, kullanıcılara ise koruma sağlamaktadır. Ancak gizlilik yasaları ülkeler arasında farklılık gösterebilir. Örneğin ABD'de federal düzeyde bir gizlilik yasası yoktur, düzenlemeler eyalet bazında yapılmaktadır (Davis vd., 2020, s. 37). Bu durum IoT şirketleri için zorluk yaratabilir. Bununla birlikte, tüketici koruma yasaları kullanıcıların gizlilik haklarını güvence altına almakta ve satın alma kararlarını daha bilinçli vermelerine katkıda bulunmaktadır.

IoT cihazları, günlük yaşamda büyük kolaylık sağlamakla birlikte, ağ bağlantılı yapıları nedeniyle ciddi güvenlik riskleri taşımaktadır. Zayıf şifreleme, güncellenmeyen yazılımlar ve kullanıcıların bilinç eksikliği bu cihazları siber saldırılara karşı savunmasız bırakmaktadır. Bu nedenle IoT güvenliği yalnızca teknik bir konu değil, aynı zamanda üretici, geliştirici ve kullanıcıların ortak sorumluluk almasını gerektiren çok boyutlu bir meseledir.

Bu noktada güvenlik standartları, IoT cihazlarının korunmasında kritik öneme sahiptir. Cihazların tasarımından kullanımına kadar tüm aşamalarda güvenliği merkeze alan bu standartlar, veri aktarımı, kimlik doğrulama ve şifreleme gibi unsurları düzenler. Örneğin, IEEE 802.15.4 protokolü cihazlar arası güvenli iletişim sağlarken, NIST tarafından yayımlanan çerçeveler olası zafiyetleri en aza indirmek için kapsamlı rehberlik sunar.

Cihaz güvenliğini sürdürmenin en önemli adımlarından biri düzenli yazılım güncellemeleridir. Güncellemeler bilinen güvenlik açıklarını kapatır ve yeni tehditlere karşı savunma sağlar. Üreticilerin bu süreçte şeffaf olması, kullanıcıların ise aktif şekilde yazılımlarını güncellemesi gerekir. Bunun yanı sıra, güvenlik standartları yalnızca teknik önlemlerle sınırlı değildir; üreticiler, yazılım geliştiriciler ve kullanıcılar arasında ortak bir güvenlik anlayışının geliştirilmesini de içerir. Güçlü şifreleme, çok faktörlü kimlik doğrulama ve kullanıcı farkındalığına dayalı politikalar, akıllı ev güvenliğini bütüncül bir yaklaşım çerçevesinde destekleyen temel araçlardır.

IoT tabanlı akıllı ev sistemlerinde yazılım güncellemeleri, güvenliğin sağlanması açısından temel unsurlardan biridir. Bu sistemlerin sürekli internete bağlı olması, onları potansiyel siber saldırılara açık hale getirmektedir. Saldırganlar çoğunlukla kötü amaçlı yazılımlar veya mevcut güvenlik açıkları üzerinden cihazlara erişmeye çalışır. Bu nedenle güncellemeler, tehditlerin önlenmesi ve sistem güvenliğinin artırılması için vazgeçilmezdir. Yazılımların güncel tutulması yalnızca yeni özelliklerin eklenmesi anlamına gelmez; aynı zamanda bilinmeyen zafiyetlerin kapatılması yoluyla kullanıcı verilerinin gizliliğini doğrudan etkiler.

Güncellemelerin etkinliği, kullanıcıların farkındalık düzeyi ve sistem yönetim becerileriyle yakından ilişkilidir. Zamanında yapılmayan güncellemeler, cihazların kontrolünün kaybedilmesine ve kullanıcı verilerinin riske girmesine yol açabilir. Örneğin, bir akıllı termostatın güncellenmemesi, saldırganın cihazı ele geçirerek ev güvenlik sistemine erişmesine neden olabilir. Bu tür durumlar hem maddi kayıplara hem de kullanıcı mahremiyetinin ihlal edilmesine yol açarak genel güvenlik algısını olumsuz etkiler. Dolayısıyla güncellemelerin ihmal edilmesi, siber güvenlik açıklarını artırır ve sistemin bütünlüğünü tehdit eder (Zhang vd., 2017, s. 38). Kullanıcıların bilinçli olarak güncellemeleri takip etmesi ve zamanında uygulaması, yalnızca bireysel güvenlik için değil, aynı zamanda IoT ekosisteminin sağlığı için kritik öneme sahiptir. Akıllı evlerde güncellemeler, teknik bir zorunluluk olmanın ötesinde, güvenli dijital yaşam alanı oluşturmanın da ayrılmaz parçasıdır.

IoT tabanlı akıllı ev çözümleri, yaşam konforunu artırsa da beraberinde ciddi gizlilik ve veri koruma sorunlarını getirmektedir. Bu sistemler; sensörler, kameralar ve kullanım verileri aracılığıyla bireylerin davranışlarını takip edebilmekte ve

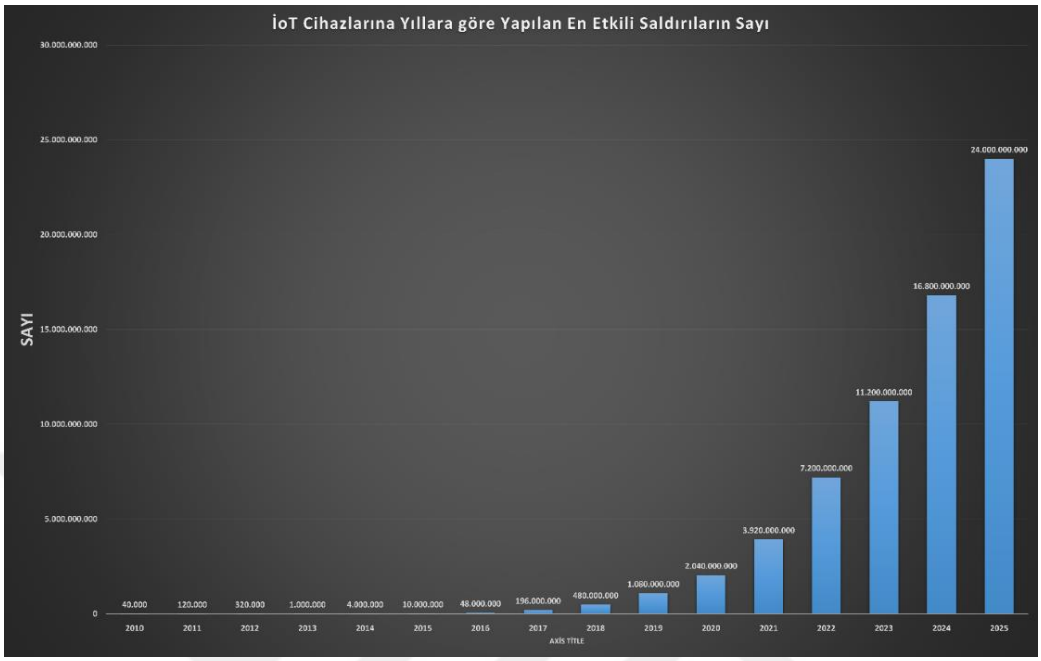
mahremiyet riskleri yaratmaktadır. Kullanıcıların kişisel verileri üzerindeki hakları, yalnızca korunma ile sınırlı değildir; aynı zamanda verilerin hangi amaçlarla işlendiği, kimlerle paylaşıldığı ve ne kadar süre saklandığı konularını da kapsar. Bu noktada veri koruma düzenlemeleri, kullanıcı gizliliğinin sağlanmasında kritik rol üstlenmektedir. Avrupa Birliği'nin GDPR düzenlemesi, verilerin işlenmesinde açık rıza şartı getirerek kullanıcıların verileri üzerindeki denetimini güçlendirmiştir (Somasundaram vd., 2018, s. 38).

Hukuki düzenlemelere göre, akıllı ev sistemleri kullanıcı onayı olmadan veri toplayamaz veya işleyemez. Dolayısıyla, sistem geliştiricilerin veri toplama süreçlerini şeffaf biçimde kullanıcıya sunması ve rıza alması yasal zorunluluktur. Ayrıca, kullanıcıların verileri üzerinde bilgilendirilme, düzeltme ve sildirme gibi haklara sahip olması dijital mahremiyetin korunmasında güvence sağlamaktadır. Bu nedenle gizlilik, akıllı ev tasarımlarında temel bir kriter olarak ele alınmalıdır. Aksi takdirde, yalnızca yasal yaptırımlarla değil, kullanıcı güveninin kaybıyla da karşılaşılabilir. Şeffaf veri işleme politikaları oluşturmak ve bunları kullanıcılara açıkça sunmak, firmaların güvenilirliğini artıran önemli bir faktördür.

Akıllı evlerde güvenlik ve mahremiyetin sağlanması için siber güvenlik uygulamaları kritik öneme sahiptir. Bu uygulamalar, kullanıcılar ve sistem geliştiricileri için yol gösterici niteliktedir. Kullanıcıların güçlü ve karmaşık parolalar oluşturması, bunları düzenli aralıklarla değiştirmesi siber saldırılara karşı ilk savunma hattıdır (Mann vd., 2020, s. 39). Çok faktörlü kimlik doğrulama yöntemleri ek bir güvenlik katmanı sağlayarak parola temelli riskleri azaltır. Ayrıca, cihaz yazılımlarının ve işletim sistemlerinin güncel tutulması büyük önem taşır; zira güncellemeler yeni tehditlere karşı koruma sağlayan yamaları içerir. Sistem geliştiriciler ise düzenli sızma testleri ve güvenlik denetimleriyle zafiyetleri en aza indirmelidir.

Veri iletiminde şifreleme yöntemlerinin kullanılması, bilgilerin kötüye kullanımını engeller. Böylece izinsiz erişim ve veri hırsızlığı riski azaltılabilir. Kullanıcı eğitimi de güvenlikte önemli bir faktördür. Farkındalık kampanyaları, kullanıcıların sosyal mühendislik gibi yaygın tehditlere karşı bilinçlenmesini sağlar. Ayrıca, ev ağında ayrı bir misafir ağı oluşturmak, zararlı yazılımların ana ağa sızma

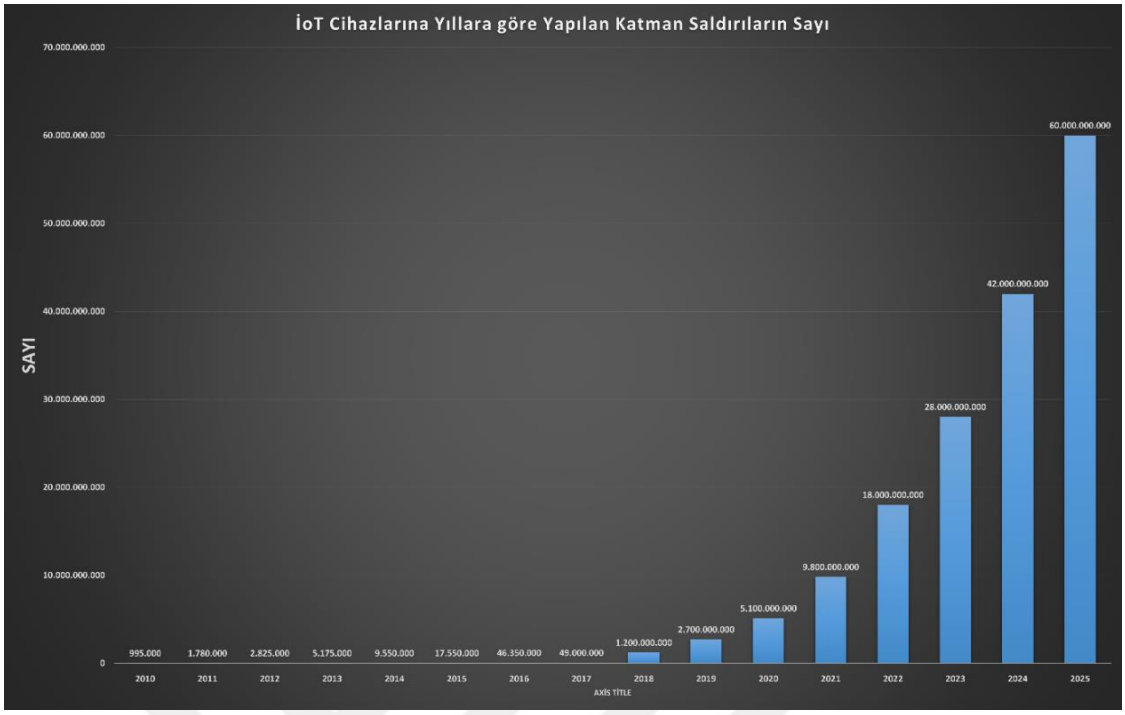
ihtimalini düşürür. Bütün bu stratejiler, hem kullanıcı güvenliğini artırır hem de akıllı ev sistemlerinin güvenilirliğini güçlendirir.



Şekil 14. IoT Cihazlarının Yıllara Göre Yapılan En Etkili Saldırıları

Kaynak: Yazar tarafından oluşturulmuştur.

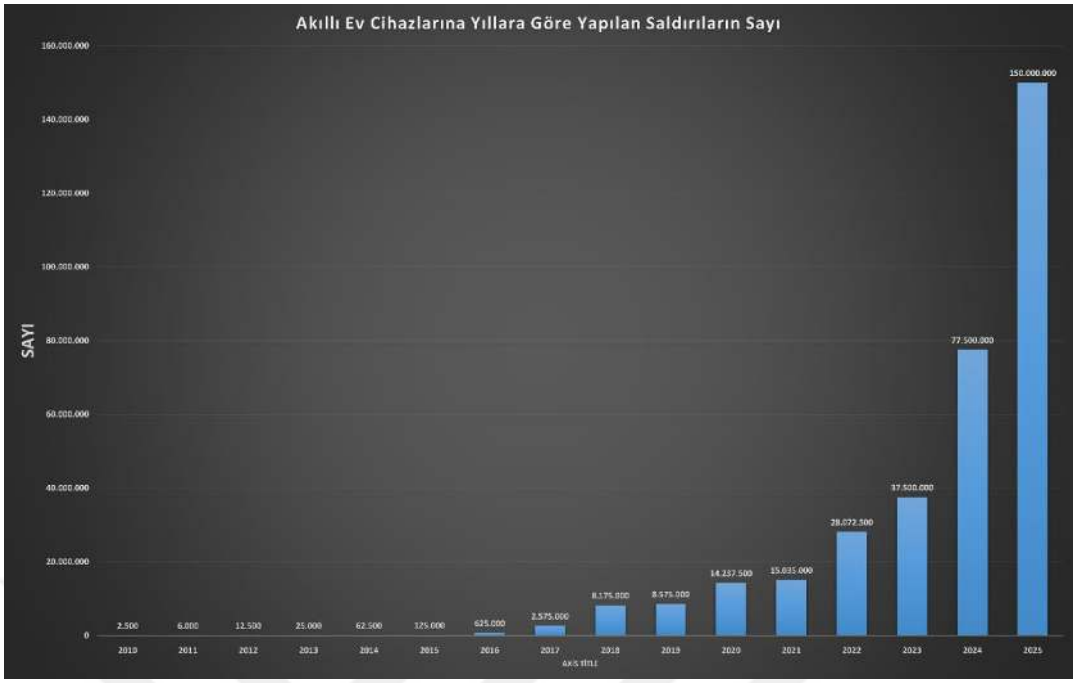
Bu grafik, IoT cihazlarına yıllara göre yapılan en etkili siber saldırıların sayısını göstermektedir. 2010'da sadece 40 bin olan saldırı sayısı, özellikle 2017'den itibaren hızla artmış ve 2025 yılında 24 milyara ulaşması beklenmektedir. Bu dramatik artış, IoT cihazlarının yaygınlaşmasıyla saldırı yüzeyinin de genişlediğini gösteriyor. 2017 yılına kadar saldırı sayıları milyon seviyesindeyken, 2018'den itibaren milyarlarla ifade edilen büyümeler yaşanmıştır. Örneğin, 2020'de 2 milyar olan saldırı sayısı 2022'de 7.2 milyara, 2024'te ise 16.8 milyara yükselmiştir. Bu veriler, IoT güvenliğinin ciddi bir sorun haline geldiğini açıkça ortaya koyuyor. Her geçen yıl daha fazla cihaz hedef alınıyor ve daha büyük zararlar meydana geliyor. Bu nedenle hem bireylerin hem de kurumların IoT güvenliğine yatırım yapmaları artık bir zorunluluk halini almıştır.



Şekil 15. IoT Cihazlarına Katmanlara Göre Yapılan Saldırı Sayı

Kaynak: Yazar tarafından oluşturulmuştur.

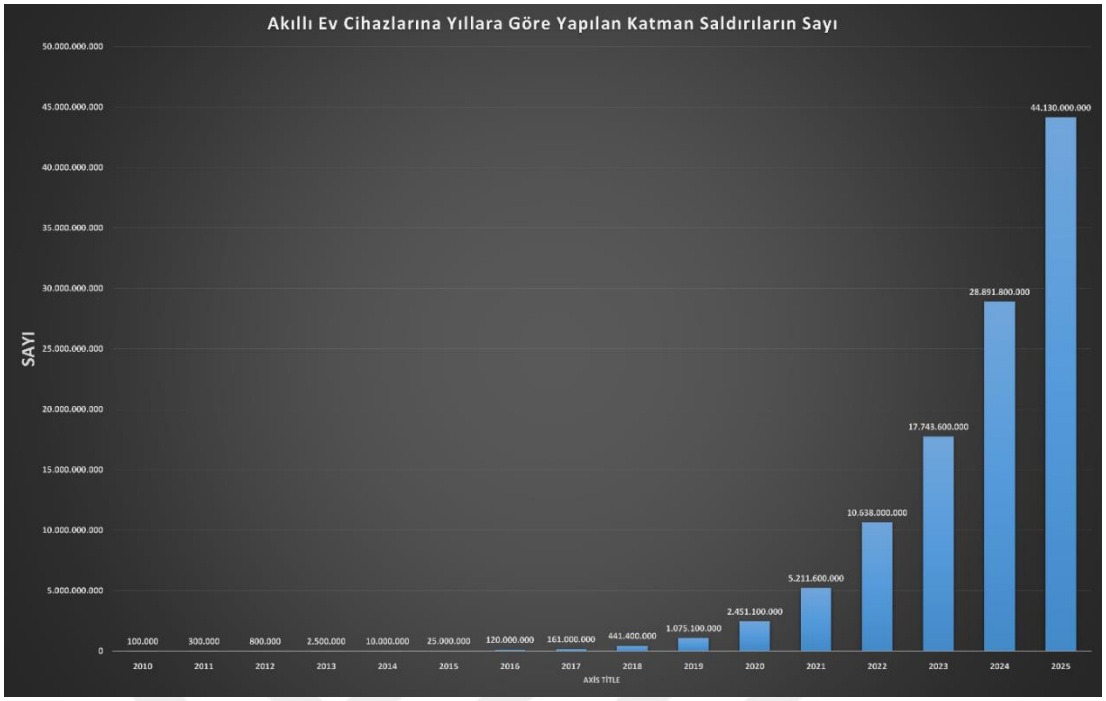
Bu grafik, IoT cihazlarına katmanlara göre yapılan saldırı sayısını yıllara göre göstermektedir. 2010–2016 yılları arasında saldırı sayıları çok düşüktür ve milyon seviyesindedir. Ancak 2017 yılından sonra ciddi bir artış başlıyor. Örneğin 2017'de yaklaşık 49 milyon saldırı varken, 2020'de bu sayı 5.1 milyara, 2023'te 28 milyara ve 2025'te ise 60 milyara ulaşmıştır. Bu büyük artış, hem IoT cihazlarının daha karmaşık hale geldiğini hem de saldırıların artık sadece tek bir noktaya değil, cihazların farklı katmanlarına (uygulama, ağ, fiziksel vd.) yönelik olarak yapıldığını gösteriyor. Saldırı yüzeyinin genişlemesiyle, tehditler daha etkili ve yıkıcı hale gelmektedir.



Şekil 16. Akıllı Ev Cihazlarına Yapılan Saldırıların Sayı

Kaynak: Yazar tarafından oluşturulmuştur.

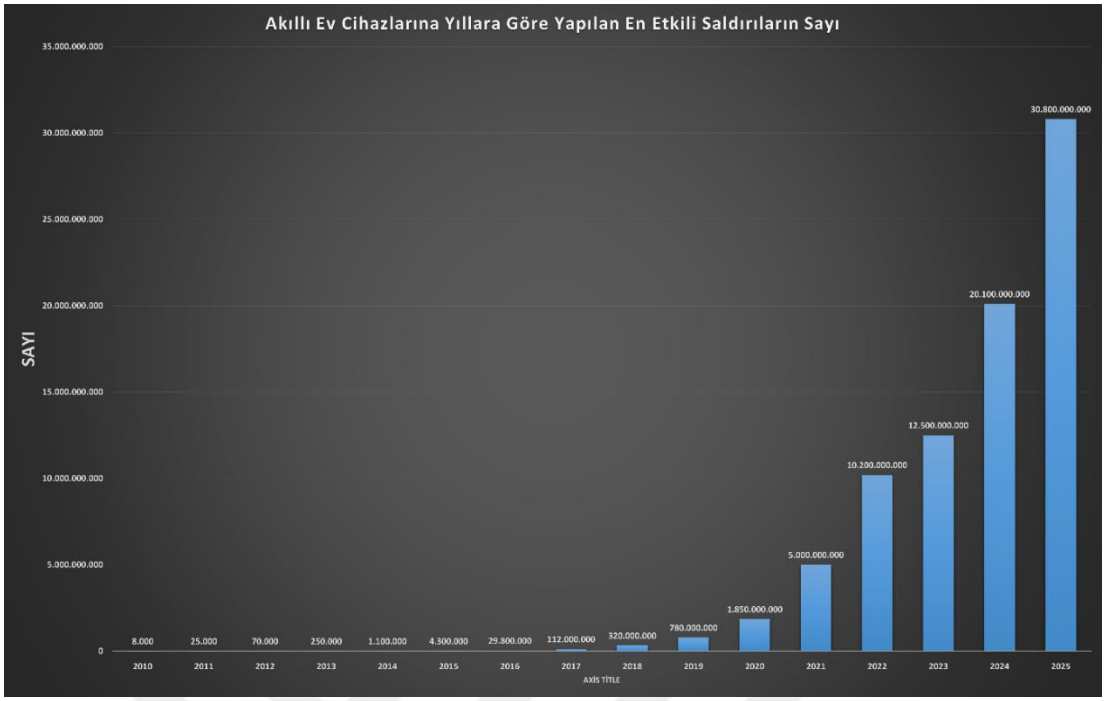
Bu grafikte, akıllı ev cihazlarına yapılan saldırıların yıllara göre sayısı gösterilmektedir. 2010–2016 yılları arasında saldırılar çok düşük seviyelerde kalmış; binlerle ifade edilmiştir. Ancak 2017 itibarıyla hızlı bir artış başlamıştır. Örneğin 2017'de yaklaşık 2.5 milyon, 2020'de 14 milyon, 2022'de ise 28 milyon saldırı kaydedilmiştir. En dikkat çekici artış ise 2024 ve 2025 yıllarında yaşanmış; 2024'te 77.5 milyon, 2025'te ise 150 milyon saldırı yapılmıştır. Bu, hem cihaz sayısının hem de tehditlerin ciddi şekilde arttığını gösteriyor. Özellikle güvenlik kameraları, akıllı kapı zilleri gibi cihazlar bu saldırıların başlıca hedefidir. Sonuç olarak, akıllı ev teknolojileri yaygınlaştıkça siber güvenlik riski de büyümekte, bu da kullanıcıların daha güçlü şifreler, güncel yazılımlar ve güvenli ağ kullanımı gibi önlemleri ciddiye alması gerektiğini ortaya koymaktadır.



Şekil 17. Akıllı Ev Cihazlarının Katmanlarına Göre Yapılan Saldırıların Sayı

Kaynak: Yazar tarafından oluşturulmuştur.

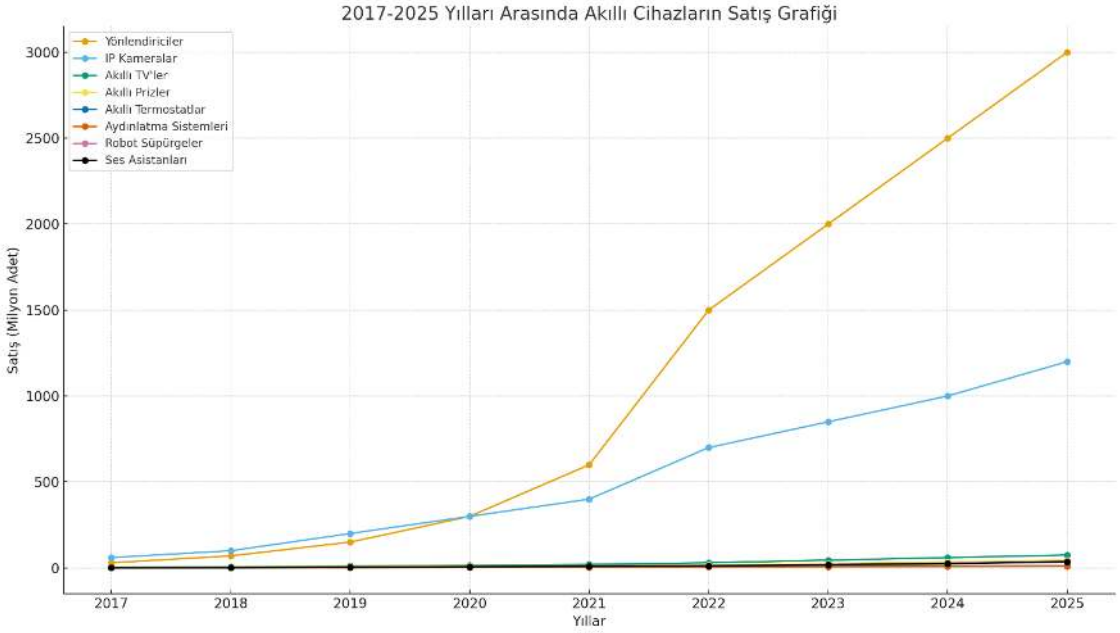
Bu grafikte, akıllı ev cihazlarının katmanlarına yapılan saldırıların yıllara göre artışı gösterilmektedir. 2010'dan 2016'ya kadar saldırı sayısı oldukça düşüktür. Ancak 2017'den sonra hızlı bir yükseliş başlamıştır. 2019'da saldırı sayısı 1 milyarı geçmiş, 2021'de 5 milyarı, 2023'te 17 milyarı ve 2025'te tam 44 milyar saldırıya ulaşması beklenmektedir. Bu büyük artış, saldırıların sadece cihazlara değil, cihazların içindeki katmanlara (ağ, yazılım, donanım gibi) yapıldığını gösteriyor. Yani saldırılar artık daha hedefli ve etkili hale gelmiştir. Akıllı ev sistemleri ne kadar yaygınlaşırsa, güvenlik açıkları da o kadar büyüyor. Sadece cihazları değil, iç yapısını da korumak gerekiyor. Bu nedenle çok katmanlı güvenlik önlemleri almak, güncel yazılımlar kullanmak ve güçlü şifrelerle sistemi korumak günümüzde çok daha önemlidir.



Şekil 18. Akıllı Ev Cihazlarına Yapılan En Etkili Saldırıların Sayı

Kaynak: Yazar tarafından oluşturulmuştur.

Bu grafikte, akıllı ev cihazlarına yapılan en etkili saldırıların yıllara göre sayısı gösterilmektedir. 2010–2016 arasında saldırılar çok düşük seviyelerde kalmıştır. Ancak 2017'den sonra hızlı bir artış başlar. 2019'da 78 milyon olan saldırı sayısı, 2021'de 500 milyon, 2022'de 1 milyar, 2024'te 2 milyar ve 2025'te 3.08 milyar seviyesine çıkar. Bu artış, saldırıların yalnızca çoğaldığını değil, aynı zamanda daha etkili ve yıkıcı hale geldiğini gösteriyor. Akıllı ev cihazları artık siber suçlular için ciddi bir hedef haline gelmiş durumda. Kamera sistemleri, akıllı kilitler ve sesli asistanlar bu saldırıların başlıca hedefleri olabilir. Akıllı ev teknolojileri büyüdükçe güvenlik önlemleri de aynı hızda geliştirilmelidir. Aksi takdirde, bu cihazlar evler için kolayca ele geçirilebilir açık kapılara dönüşebilir.



Şekil 19. 2017-2025 Yılları Arasında Akıllı Cihazların Satış Grafiği

Kaynak: Yazar tarafından oluşturulmuştur.

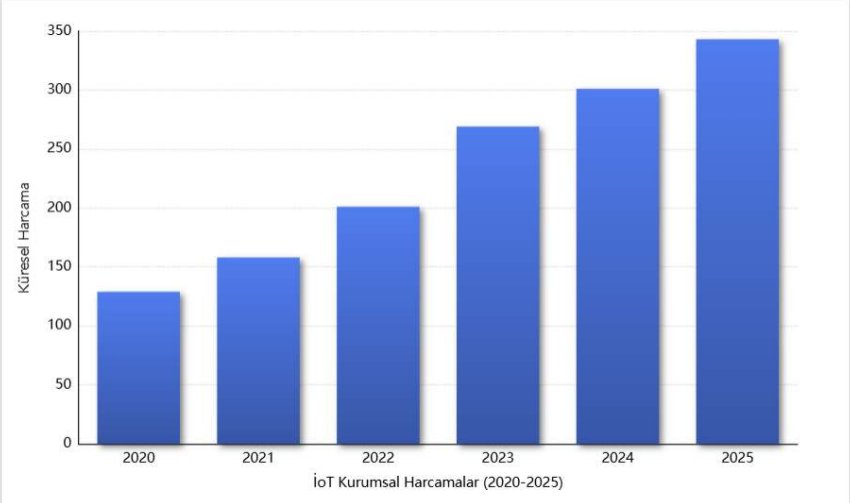
Grafikte 2025 yılında akıllı ev cihazlarına yapılan saldırıların cihaz türlerine göre dağılımı görülmektedir. En çok saldırıya uğrayan cihaz türü 3 milyar saldırı ile yönlendiriciler olmuştur. Yönlendiricileri 1.2 milyar saldırı ile IP kameralar takip etmektedir. Bu iki cihaz diğerlerine göre açık ara farkla daha fazla hedef alınmıştır. Bunun nedeni bu cihazların doğrudan internete bağlı olması ve ağ trafiğini kontrol etmeleridir. Akıllı TV'ler 75 milyon, akıllı prizler 45 milyon, robot süpürgeler 40 milyon, ses asistanları 35 milyon, akıllı termostatlar 12 milyon ve aydınlatma sistemleri ise 9 milyon saldırıya maruz kalmıştır. Bu rakamlar bize saldırganların en çok ağ ve güvenlik zafiyetlerinden faydalandığını göstermektedir. Özellikle yönlendiriciler ve IP kameralar gibi cihazlarda güçlü şifreler kullanılmaması, yazılım güncellemelerinin ihmal edilmesi büyük risk yaratmaktadır. Kullanıcıların cihaz seçiminde güvenlik kriterlerini ön planda tutmaları ve düzenli güvenlik önlemleri almaları büyük önem taşımaktadır. Aksi takdirde bu cihazlar evdeki zayıf halka haline gelebilir.

3. IoT TABANLI AKILLI EV SİSTEMLERİNDE SON TEKNOLOJİK GELİŞMELER

IoT tabanlı akıllı ev sistemlerinde son teknolojik gelişmeler, veri güvenliği, yönetimsel riskler, katmanlı mimaride bilgi güvenliği ve yangınlara karşı alınabilecek önlemler değerlendirilmiştir.

3.1. IoT akıllı ev sistemlerinde güncel gelişmeler

Son on yılda, İnternet'e bağlanabilen ve uygulamaları kullanarak uzaktan kontrol edilebilen yeni "akıllı" cihazların yaratılmasında bir artış oldu. Sensörler, yazılımlar ve cihazların birbirine bağlanması Nesnelerin İnterneti (IoT) ağını oluşturur. Nesnelerin İnterneti (IoT), bilgi devriminin bir sonraki aşaması olacak ve beraberinde internet ile aynı seviyede toplumsal değişim getirecek. IoT'nin muazzam olması öngörülüyor: 2020 yılında dünya genelinde yaklaşık 11,3 milyar IoT cihazı bağlıydı ve IoT harcamaları yaklaşık 749 milyar ABD doları seviyesine ulaşmıştı (IoT Analytics 2022). Bu sayı 2025 yılına gelindiğinde 27,1 milyara yükselmiştir ve aynı yıl küresel IoT alanına yapılan toplam yatırım yaklaşık 1,35 trilyon ABD doları seviyesine çıkmıştır (Mordor Intelligence 2025). Sonuç olarak, tüm dünyadaki işletmelerin, hükümetlerin ve vatandaşların ilgisini çekmiş ve hem endüstride hem de akademide araştırmaları ateşlemiştir.

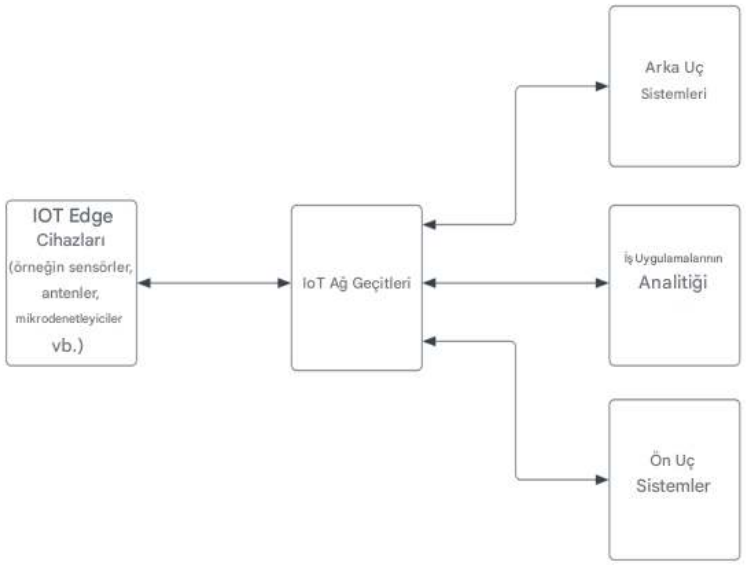


Şekil 20. IoT Kurumsal Harcamaları 2020-2025

Kaynak: Chan, M., Estève, D., Escriba, C. ve Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55–81.

Bu görselde gösterilen diyagram, 2020-2025 yılları arasında sadece işletmelerin IoT (Nesnelerin İnterneti) teknolojilerine yaptığı küresel harcamaları göstermektedir. Büyüme istikrarlı ve istikrarlı bir şekilde devam ediyor. Bu, işletmelerin giderek daha fazla Nesnelerin İnterneti teknolojilerine güvendiği ve bunların iş süreçlerine fayda sağlayacağına inandığı anlamına geliyor. Bu büyüme hem teknolojiye olan ilginin arttığını hem de dijital dönüşümün yaygınlaştığını gösteriyor. Genel olarak IoT harcamalarının 6 yıl içinde üç katına çıkması bekleniyor. Bu durum gelecekte daha akıllı sistemlerin, otomatik yönetimin ve veriye dayalı kararların yaygınlaşacağını gösteriyor. Dolayısıyla bu istatistiksel artış, işletmelerin rekabet güçlerini ve verimliliklerini artırmak amacıyla teknolojik yatırımlara öncelik verdiklerini kanıtlıyor.

Nesnelerin İnterneti (IoT), çeşitli iletişim yöntemleriyle bağlanan ve mikrodenetleyici birimi (MCU) tabanlı sistemlerle entegre edilmiş cihazlardan oluşur. Çevrelerinden veri toplayan, gönderen ve bu veriler üzerinde işlem yapan web özellikli akıllı cihazlar bir IoT ekosistemi oluşturur. Uç cihazlar ve ağ geçitleri, işletim sistemlerine gömülü iki tür IoT bileşenidir. Sensörler, cihazlar ve anahtarlar, yalnızca sınırlı bir dizi eylem gerçekleştirebilen uç cihazlara örnektir. Bu cihazlar genellikle küçüktür, son derece enerji verimli olan kaynak kısıtlı bir MCU'ya (enerji, ROM ve RAM) sahiptir ve kısa menzilli düşük güçlü iletişim protokollerini destekler. Bu uç cihazlardan (sensörler) veri toplamak veya bir olaya (cihazlar) dayalı olarak yürütülecek bir komut iletmek için daha güçlü bir cihaz - ağ geçidi - gereklidir. IoT sensörleri, IoT ağ geçidine veya sistemdeki diğer uç cihazlara bağlandığında, verilerini bulut ortamıyla veya yerel veri yönetim araçlarıyla paylaşabilirler. Bu sensörler, aldıklarına yanıt verebilir ve birbirleriyle iletişim kurabilir. İnsanlar IoT cihazlarının yapılandırması üzerinde çalışır ve mevcut sisteme talimatlar verir. Daha sonra cihazlar insan etkileşimi olmadan çalışır.

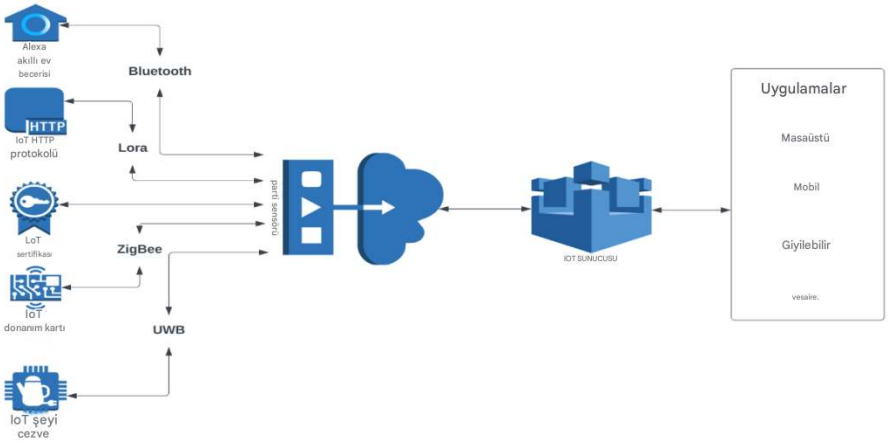


Şekil 21. IoT Bileşenlerinin İletişim Grafiği

Kaynak: Chan, M., Estève, D., Escriba, C. ve Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55–81.

Bu diyagram, IoT mimarisinde veri akışını açıklamaktadır. İlk aşamada IoT Edge cihazları yer alır. Bunlar sensörler, antenler, mikrodenetleyiciler gibi donanımlardır. Çevreden sıcaklık, nem, hareket veya ışık gibi verileri toplar. Ancak bu cihazların tek başına işlevi sınırlıdır. Bu nedenle veriler IoT ağ geçitlerine aktarılır. Ağ geçitleri, edge cihazlardan gelen ham verileri bir araya getirir, ön işlemden geçirir ve daha güvenli biçimde sonraki aşamalara iletir. Ayrıca iletişim protokollerini uyumlu hale getirerek farklı cihazların birlikte çalışmasını sağlar.

Sonraki adımda veriler üç farklı yönde kullanılabilir. Arka uç sistemleri, genellikle büyük veri tabanları ve bulut servislerinden oluşur. Burada veriler depolanır, uzun vadeli analiz ve raporlama yapılır. İş uygulamalarının analitiği, gelen verileri gerçek zamanlı yorumlar. Örneğin, enerji tüketimi fazlaysa kullanıcıya bildirim gönderilebilir. Ön uç sistemler ise doğrudan kullanıcıyla etkileşimde bulunur; mobil uygulamalar veya akıllı ev panelleri aracılığıyla bilgileri kullanıcıya sunar. 15Bu yapı sayesinde IoT ekosistemi, verilerin sensörden kullanıcıya kadar düzenli ve güvenli şekilde aktarılmasını sağlar. Böylece akıllı sistemler hem işlevsel hem de yönetilebilir hale gelir.



Şekil 22. Genel IoT Sistemleri İçin İş Akışı

Kaynak: Devalal, S. ve Karthikeyan, A. (2018, 29-31 Mart). *LoRa technology – an overview.* 2018 Second International Conference on Electronics, Communication and Aerospace Technology. RVS Technical Campus, Coimbatore, India.

IoT cihazları, düşük maliyetli bilgisayarlar, insan tepkilerinden veri oluşturabilir. Bu veriler mobil uygulamaların, büyük veri teknolojilerinin ve bulut bilişimin bir parçası olarak toplanabilir ve paylaşılabilir. Cihazdan cihaza veya insandan cihaza her etkileşim, hiper bağlantılı bir ortam sayesinde kaydedilir, izlenir veya değiştirilir. Dijital ve fiziksel dünyalar çarpışsa da, herhangi bir sorun yaratmadan birlikte çalışırlar. Son yıllarda, IoT akıllı sistemlerin yenilikçi bir teknolojisi olarak kabul edilir. Gömülü IoT teknolojilerinin yardımıyla cihazlar, insanlar ve süreçler arasındaki iletişim ve bağlantı kolaylaşıyor. İnternet Protokolü (IP) adresini kullanabilen veya ağa veri aktarabilen doğal veya insan yapımı nesneler IoT akıllı cihazlarına örnektir. Lastik basıncı düşük olduğunda sürücüyü uyarmak için yerleşik sensörlere sahip akıllı arabalar, kalp monitörü implantları gibi sağlık uygulamaları ve Amazon Echo ve Google Hub gibi sesli asistanlar gerçek dünya IoT uygulamalarına örnektir. Nesnelerin İnterneti'ndeki heterojenlik, geniş bir donanım yetenekleri (örneğin CPU hesaplama ve bellek izi) ve protokoller, platformlar ve kurallar yelpazesini ifade eder (Şekil 22) (Devalal ve Karthikeyan, 2018, s. 49).

Birkaç Nesnelerin İnterneti iş uygulaması vardır. Pratikte, akıllı cihazların mevcut endüstrinin iş akışını değiştirmesiyle ilgili olarak endüstride birkaç işaret vardır. Bu teknolojideki geniş uygulama yelpazesi, diğer teknolojilere kolayca

uyarlanabilmesi ve sistem içinde doğru bilgileri aktarabilmesi özelliklerinden kaynaklanmaktadır. Her senaryoyu kullanmaya uygun görünse de, geliştiriciler bir etkinliğin performansını dikkate almalı, çevresel koşullar açısından uzaktan izlemeli ve düzenlemelidir. Çoğu teknoloji firması, çalışma süreçlerini daha otomatik, daha basit ve kontrolü kolay hale getirmek için Nesnelerin İnterneti teknolojilerini kullanır. Enerji şirketleri, bilgi ve iletişim teknolojisi (BİT) tarafından etkinleştirilen akıllı enerji uygulamalarının potansiyeli olduğunu düşünmektedir. Sağlık hizmeti sağlayıcıları, yaşlıların ve kronik hastalığı olan bireylerin tıbbi ve sağlık harcamalarını düşürme amacıyla daha uzun süre evlerinde kalmalarını sağlayan akıllı cihazlara bağlı sensör ağları için umutlar görmektedir. Telekom, kablo ve medya şirketleri, donanım ve içerik tedarikçileri, evi eğlence ve oyun merkezi haline getirme konusunda umutlar görüyor. Erişim sağlayıcılarına göre, evde yönetilen BİT hizmetleri giderek daha popüler hale geliyor. Güvenlik şirketleri, uzaktan gözetim, kontrol ve güvenlik cihazlarını yeni bir iş fırsatı olarak görüyor. Dahası, bu alanın çeşitli disiplinleri ve çeşitli sorunları belirlemek ve incelemek için farklı bakış açılarını (ör. kullanıcılar, sistem, organizasyon) içerdiğini söylemeye gerek yok. Sesli asistanlar (Siri ve Alexa), giyilebilir fitness ve izleyiciler (akıllı saatler gibi), IoT sağlık uygulamaları, akıllı arabalar ve akıllı ev uygulamaları IoT'nin gerçek dünyadaki bazı örnekleridir.

	Kablosuz 802.11n	Bluetooth	Bluetooth LE	ZigBee	Z-Dalga	6DüşükPAN
Sıklık	2,4-5,8 GHz	2.402–2.48 GHz	2.402–2.48 GHz	868/915 MHz, 2,4 GHz	868/915 MHz	868/921 MHz, 2,4-5 Ghz
Veri hızı	450 Mb/sn	0,7-2,1 Mb/sn	2 Mb/sn	20/40 kbps, 250 kbps	10–100 kbps	10–40 kbps, 250 kbps
Menzil	10-100 metre	15-20m	10-15m	10-100 metre	30-50 metre	10-100 metre
Ağ boyutu	Binlerce (örgü)	8	Yok	65.536	232	250
Ağ Topolojisi	Yıldız, ağaç, P2P, ağ	Yıldız	Yıldız	Yıldız, ağ, küme ağacı	ağ	Yıldız, örgü, P2P
Şifreleme	WPA2	AES-128	AES-128	AES-128	AES-128	AES-128

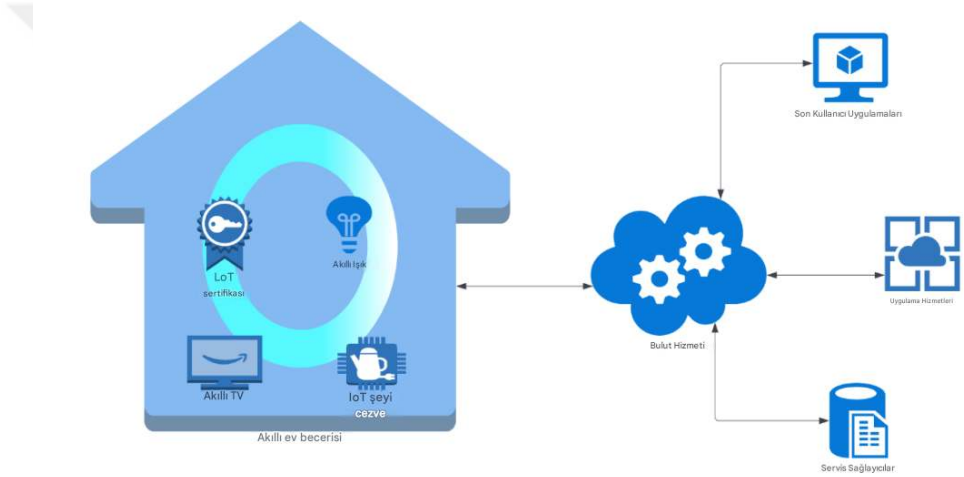
Şekil 23. Akıllı Ev Uygulamalarında Kullanılan Kablosuz İletişim Protokolleri

Kaynak: Chan, M., Estève, D., Escriba, C. ve Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55–81.

Akıllı evlerde genellikle sensörler, cihazlar veya aygıtlar gibi tek başına "akıllı" özelliğe sahip olmayan birkaç temel bileşen bulunur. Ancak otomasyonun kapsamı sınırlı olduğunda, sistem yalnızca belirli görevleri yerine getirir ve genel tabloyu göremez. Örneğin, bir sensör veri üretebilir fakat bu verinin tek başına akıllı ev sistemleri için anlamı yoktur. Buna karşılık, asıl "zeka", tüm sensörler ve bağlı cihazlardan elde edilen bilgilerin bütüncül bir bakış açısıyla değerlendirilmesiyle

ortaya çıkar. Bu durumda sistem, ortamın genel durumunu daha doğru analiz edebilir, kullanıcılar hakkındaki geçmiş verilere dayanarak uyum sağlayabilir ve öngörülerde bulunabilir.

Bir ortam ancak verilerin topluca saklandığı, analiz edildiği, düzenli kalıpların çıkarıldığı ve kullanıcı müdahalesi olmaksızın kararların verildiği noktada gerçekten akıllı olarak nitelendirilebilir. Akıllı evin yapısını belirleyen temel unsur ise cihazların nasıl kimliklendirildiği, sensörlerden elde edilen verilerin nerede ve nasıl kaydedildiği, bu bilgilerin hangi yöntemlerle incelendiği, kullanıcıların cihazlarla nasıl etkileşim kurduğu ve aynı zamanda cihazların kullanıcıya nasıl yanıt verdiğidir.



Şekil 24. Geleneksel Akıllı Ev Mimarisi

Kaynak: Chan, M., Estève, D., Escriba, C. ve Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55–81.

Zhou ve çalışma arkadaşları, IoT uygulamalarının geliştirilmesi ve bakım süreçlerini hızlandırmayı amaçlayan bulut tabanlı bir mimari olan CloudThings'i tanıtmıştır (Zhang vd., 2015, s. 51). Bu sistemde uç cihazlar (Things), 6LowPAN ile birlikte CoAP protokolünü kullanarak doğrudan internete bağlanabilmektedir. CloudThings, IoT uygulamaları ve hizmetlerinin tasarlanması, dağıtılması, sürdürülmesi ve entegrasyonunu destekleyen çevrimiçi bir platform niteliği taşımaktadır.

3.2. IoT Ortamlarında Veri Güvenliği ve Yönetimsel Riskler

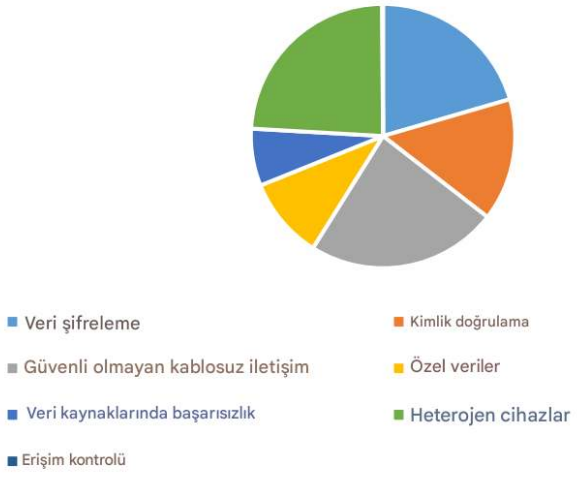
Nesnelerin İnterneti (IoT) günümüzde insan deneyiminin ayrılmaz bir parçası haline gelmiştir. "Her şey, her yerde, her zaman" mottosuyla tanımlanabilecek bu yapı; birbirleriyle iletişim kuran akıllı araçlardan, ev planlarını çıkarabilen robot süpürgelere, yakılan kaloriyi ölçen giyilebilir cihazlardan, internet üzerinden kontrol edilebilen ampullere kadar geniş bir yelpazede yaşamın içine girmiştir. IoT'nin yaygınlaşması, cihazların topladığı veya işlediği verilerin doğrudan ya da dolaylı olarak insan davranış ve tercihlerine dair çıkarımlar yapılabilmesini mümkün kılmaktadır. Bazı kullanıcılar bu durumun sunduğu kişiselleştirilmiş hizmetleri faydalı bulurken, diğerleri kişisel verilerin toplanması ve işlenmesi sebebiyle kaygı duymaktadır. Akıllı evlerdeki veriler üç kaynaktan elde edilebilmektedir: kullanıcıyla pasif etkileşim (örneğin giyilebilir sensörler, hareket dedektörleri, RFID etiketleri, akıllı zemin sensörleri, derinlik kameraları ve video kayıtları), kullanıcıyla aktif etkileşim (jest tanıma, sesli komut, dokunmatik ekran kullanımı veya butonlar aracılığıyla eylem algılama) ve kullanıcı dışı kaynaklar (örneğin termostat verileri, hava akışı sensörleri).

Chan ve çalışma arkadaşları, akıllı şebeke ortamını tanımlayarak CCTV sistemlerinin şehir genelinde kurulacağını ve sensörlerden elde edilen tüm verilerin ağa aktarılacağını belirtmiştir (Bourobou vd., 2015, s. 52). Büyük veri, mevcut bilgi türlerini çeşitlendirerek toplam veri hacmini artıracak ve bu bağlamda gizlilik korumasının önemi daha da artacaktır. Araştırmacılar, IoT'nin yapısal özellikleri ve güvenlik ihtiyaçlarını dikkate alarak gizlilik konusunda yeni güvenlik stratejileri geliştirmelidir.

Akıllı evlerde IoT'nin kullanımı, kötü niyetli aktörlerin doğrudan kullanıcıları hedef alan saldırılar gerçekleştirmesine de imkân tanımaktadır. Koklama (sniffing), CCTV sistemlerinin kötüye kullanımı ve DoS saldırıları en sık karşılaşılan güvenlik tehditlerindendir (Jiang vd., 2016, s. 52). Güvenlik zafiyetleri ve tepki süresindeki hatalar, internet üzerinde felaketle sonuçlanabilecek arızalara yol açabilmekte, ağ iletişimini bozarak yavaşlamaya neden olabilmektedir (Hasibuan vd., 2015, s. 52). Han ve arkadaşları, veri sızıntısının akıllı evlerde ciddi sorunlara yol açabileceğini ortaya koymuştur (Kailas vd., 2012, s. 52). Sonuç olarak, IoT bağlamında güvenlik

açıklarının mutlaka göz önünde bulundurulması gerekmektedir. Çünkü bazı akıllı ev cihazları yeterli şifreleme ve kimlik doğrulama mekanizmalarına sahip değildir; bu durum onları DoS saldırılarına, aracı saldırılarına ve kullanıcıların bağlantı ile fiziksel güvenliğini tehdit eden diğer siber risklere karşı savunmasız hale getirmektedir. Örneğin, Londra'daki Wi-Fi ağlarının yaklaşık %27'sinin yetersiz korunması veya hiç güvenlik önlemine sahip olmaması bu duruma işaret etmektedir (Kramp vd., 2013, s. 53).

Akıllı mobil ev sistemleri, mobil telefonlar üzerinden cihazların kablosuz bağlantılarla kontrol edilmesini mümkün kılmaktadır. Ancak bu durum, bilgisayar korsanlarının yetkisiz erişim sağlaması gibi tehditleri beraberinde getirmektedir. Bao ve çalışma arkadaşları, siber güvenlik sorunlarının gizlilik kaygılarıyla doğrudan bağlantılı olabileceğini ortaya koymuştur; örneğin saldırganlar ev sakinlerinin konuşmalarını dinleyebilmektedir (Amadeo vd., 2015, s. 53). Ayrıca IoT cihazlarının kullandığı paket yönlendirme mekanizması bağlantısız çalışmakta, bu da güvenlik mekanizmalarının eksikliği sebebiyle hatalara yol açabilmektedir. Yanlış yönlendirmeler, korumasız kablosuz kanallar, çarpışmalar ve gecikmeler paket kayıplarına neden olabilmektedir (Jacobsson vd., 2016, s. 53).



Şekil 25. Akıllı Ev IoT'sindeki Veri Güvenliği Sorunları

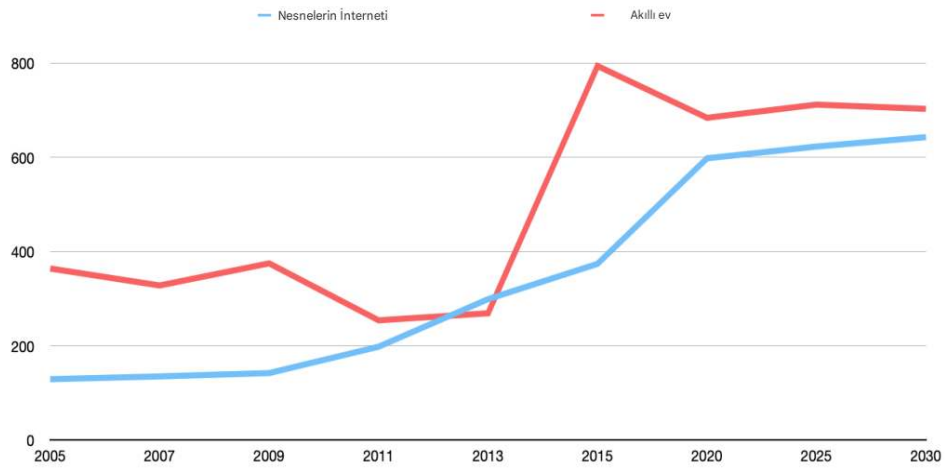
Kaynak: Chan, M., Estève, D., Escriba, C. ve Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55–81.

Diyagramda öne çıkan en büyük sorunlardan birinin “güvenli olmayan kablosuz iletişim” olduğu görülmektedir. Bu durum, veri aktarımı sırasında güvenlik açıklarının ortaya çıkmasına neden olmaktadır. İkinci kritik başlık ise “heterojen cihazlar”, yani farklı türde cihazların aynı sisteme entegre edilmesidir. Bu çeşitlilik, teknolojilerin birlikte çalışabilirliği konusunda uyumluluk sorunları yaratmakta ve güvenlik risklerini artırmaktadır. Bunun ardından, “kimlik doğrulama” meselesi öne çıkmaktadır. Kullanıcı kimliklerinin doğru şekilde doğrulanmaması, sistemlere yetkisiz erişim ihtimalini doğurur.

“Özel verilerin korunması” da temel bir güvenlik alanıdır. Kişisel bilgilerin üçüncü kişilerin eline geçmemesi, kullanıcı mahremiyetinin korunması açısından kritik öneme sahiptir. “Veri şifreleme”, diyagramda daha küçük bir paya sahip görünse de, sistem güvenliği için kilit rol oynamaktadır. Verilerin şifrelenmeden saklanması, bu bilgilerin kolayca çalınmasına yol açabilmektedir. Ayrıca, “veri kaynaklarında arıza” oluşması da önemli bir tehdit unsurudur ve bu durum sistemin kararlılığını azaltarak güvenlik zafiyetlerini tetikleyebilir.

Bunlara ek olarak, “erişim kontrolü” konusu da dikkat çekmektedir. Kullanıcıların sistem içinde sahip oldukları yetki ve izinlerin doğru şekilde yönetilmesi, yetkisiz erişimlerin önlenmesi açısından önemlidir. Genel olarak bakıldığında, bu diyagram bilgi güvenliğinin karmaşık bir mesele olduğunu ve tek bir çözüm yoluyla giderilemeyeceğini göstermektedir. Riskler birbirleriyle bağlantılıdır ve her biri sistem güvenliğini doğrudan etkilemektedir. Bu nedenle, şirketlerin bu sorunları sistematik olarak analiz etmesi ve uygun teknolojik çözümler ile prosedürler geliştirmesi gerekmektedir (Krishna vd., 2017; Arunvivek vd., 2015, s. 54).

Ayrıca, Şekil 26, 2004 yılından itibaren Nesnelerin İnterneti, akıllı şebeke ve akıllı ev güvenlik sorunlarına yönelik web aramalarının artışını göstermektedir (Stojkoska vd., 2017, s. 54).



Şekil 26. Nesnelerin İnterneti, Akıllı Şebeke ve Akıllı Ev Güvenlik Sorunları İfadelerine Dikkat

Kaynak: Stojkoska, B. L. R. ve Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production, 140*, 1454–1464.

Grafikte 2005–2030 dönemi için Nesnelerin İnterneti (IoT) ve akıllı ev teknolojilerinin gelişim eğrileri gösterilmektedir. Mavi çizgi IoT'yi, kırmızı çizgi ise akıllı ev uygulamalarını temsil etmektedir. 2005 yılında IoT düşük seviyede, yaklaşık 120 civarında başlamıştır. Bu dönemden 2010'a kadar yavaş ama istikrarlı bir artış gözlenmiştir. 2010 sonrasında IoT daha hızlı bir ivme yakalamış, özellikle 2015'ten sonra güçlü bir yükseliş göstermiştir. 2020'ye gelindiğinde IoT yaklaşık 600 seviyesine ulaşmış, 2030'a kadar ise büyümesini koruyarak 650'nin üzerine çıkmıştır.

Akıllı evler tarafında ise farklı bir tablo vardır. 2005'te 350 seviyesinde olan akıllı ev uygulamaları, 2010'a kadar dalgalı bir seyir izlemiş, hatta 2011'de belirgin bir düşüş yaşamıştır. Ancak 2013'ten sonra çok hızlı bir artış olmuş, 2015 yılında 800 ile zirveye ulaşmıştır. Bu tarihten sonra bir miktar gerileme görülse de 2020'den sonra nispeten dengelenmiş ve 700 civarında sabitlenmiştir. Genel değerlendirmede, IoT sürekli yükselen bir grafik sergilerken, akıllı evler hızlı bir sıçrama yapıp daha sonra durağan bir seyre girmiştir. Bu durum, IoT'nin daha geniş alanlarda kullanılmaya devam ettiğini, akıllı evlerin ise belli bir doygunluk noktasına ulaştığını göstermektedir.

Araştırmacılar, ağların siber güvenliğini incelemek amacıyla ISO 15408 temelli Ortak Kriterler (Common Criteria, 2017) sertifikasına dayalı Değerlendirme Güvence Düzeyi ile IEC 62443 standardından türetilen EDSA (Gömülü Cihaz Güvenlik Güvencesi) sertifikasına yönelik çeşitli teknikler geliştirmiştir. IEC 62443 özellikle endüstriyel kontrol sistemlerinde kritik altyapılar için hazırlanmışken, ISO 15408 daha çok güvence standartlarına odaklanmakta ve hangi somut adımların uygulanacağını açıkça belirtmemektedir. Ancak her iki yaklaşım da tedarikçiler ya da güvenlik alanında yeterli bilgiye sahip olmayan kullanıcılar için IoT ürünlerindeki siber güvenlik seviyesini kolayca belirleyecek pratik bir yöntem sunmamaktadır.

Bağlam farkındalığına sahip bir ev otomasyon sistemi, kullanıcının verdiği kararları anlayabilmeyi hedeflemektedir. Örneğin, bir kullanıcının ev içerisindeki konumunun tahmin edilmesi bağlamın tanımlanmasına yardımcı olur. Schilit ve arkadaşları (ISO, 2021), kullanıcının evdeki konumunu tespit etmenin çeşitli yollarını özetlemektedir. Çalışmalar, kızılötesi ağların bu amaçla kullanılabileceğini ve bunun güvenliği önemli ölçüde artırabileceğini belirtmektedir; ancak bu yöntem kullanıcı açısından zahmetli olabilir. Schilit ve arkadaşları ayrıca, sistemlerin tamamen kendi başlarına bağlam odaklı kararlar alması yerine, akıllı ev teknolojilerinin kullanıcılara fırsat ortaya çıktığında hatırlatmalar yaparak onların güvenlik ve enerji tasarrufu konusunda bilinçli seçimler yapmalarını desteklemesi gerektiğini vurgulamıştır. Buna ek olarak, Yin ve arkadaşları akıllı evlerde IoT güvenliği için IoT merkezli bir yönetim yaklaşımı geliştirmiştir. Bao ve arkadaşları (Cebrat, 2014, s. 56) ise mobil akıllı ev konseptini tasarlayıp uygulamaya koymuştur. Ayrıca, akıllı ev uygulamalarında insan etkileşimlerini daha verimli hale getirmek amacıyla matematiksel temele dayalı bir model oluşturulmuş ve dağıtılmıştır.

3.3. IoT Mimarisi Üzerinde Katmanlara Göre Bilgi Güvenliği Analizi

Güvenli bir IoT ortamı için Santhosh Krishna ve Gnanasekaran en yaygın güvenli IoT mimarisini sağlar. Diğer araştırmalar genellikle bu mimarinin yalnızca bir kısmına odaklanır.

Şekil 27. Güvenli IoT Mimarisi

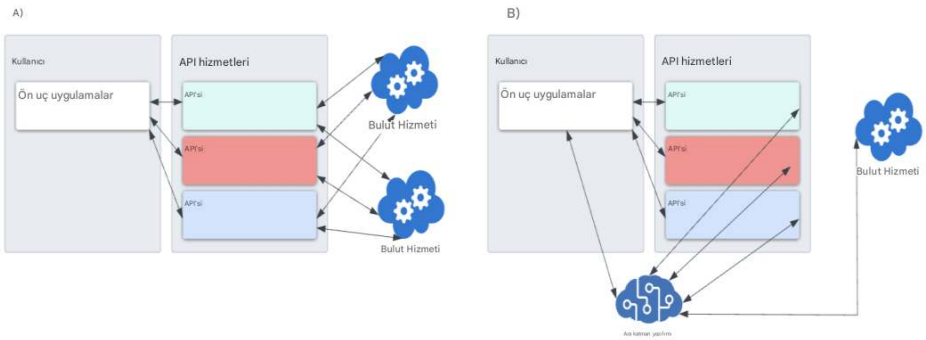
Kaynak: Chan, M., Estève, D., Escriba, C. ve Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55–81.

IoT cihazlarının fiziksel güvenliği, öncelikle algılama katmanında sağlanmalıdır. Sensör ağlarında karşılaşılan mimari sınırlamalar arasında DoS saldırıları, sensör ve ağ geçidi düğümlerinin fiziksel ele geçirilmesi, veri dinleme, bütünlük ihlalleri, ağ tıkanıklığı ve düğüm çoğaltma saldırıları yer almaktadır. Ayrıca, yetkisiz erişim girişimleri, kişisel bilgilerin kaybolması veya silinmesi, SIM kart bilgilerinin kopyalanması ve hava arayüzü verilerinin sahte olarak üretilmesi, IoT sensör düğümlerine yönelik en kritik güvenlik riskleri arasında sayılmaktadır. Bu tehditlere karşı, şifreleme algoritmaları, anahtar dağıtım mekanizmaları ve saldırı tespit sistemleri gibi güvenlik önlemleri uygulanarak sensör ağları için güçlü bir güvenlik mimarisi oluşturulmalıdır (Cho vd., 2015). Günümüzde kullanılan güvenlik protokolleri arasında TinySec ve LEAP öne çıkmaktadır. Verilerin korunmasında en yaygın yöntemler simetrik ve asimetrik anahtar tabanlı şifreleme teknikleridir. Ancak bu teknikler, sınırlı enerji kapasitesine ve işlem gücüne sahip taşınabilir cihazlar için ek zorluklar yaratmaktadır. Bu nedenle enerji verimliliği ve işlem yükü söz konusu yaklaşımların temel sınırlamalarını oluşturmaktadır. Alternatif olarak, sinir sistemi uyarı aralıkları veya damar içi kan hacmi gibi biyometrik özelliklerden yararlanılarak giyilebilir algılama cihazları arasında veri şifreleme yöntemleri geliştirilmektedir. Özetle, akıllı ev ortamlarında karşılaşılan tehditler hem dahili hem de harici kaynaklardan gelebilmektedir (Hejazi vd., 2018, s. 57).

Winter vee arkadaşları, IoT düşük güç kaynakları için Düşük Güç ve Kayıplı Ağlar için Yönlendirme Protokolü (RPL) yöntemini önerdi (Li vd., 2012, s. 57). Bu

önerilen yöntem, IoT öğelerinin sınırlı kaynak yapısı nedeniyle çeşitli saldırılara karşı savunulamazdır. RPL standardının kontrol iletişimlerini şifrelemeyle korumasına rağmen, RPL yine de dâhili saldırganlara ve bencil davranışlara karşı savunmasızdır. Duan ve arkadaşları, güvenlik açığı ölçümlerini tahmin etmeden önce makine öğrenimi ve doğal dil işleme kullanarak veri güvenlik açığı açıklamalarını analiz eden bir çerçeve sundu (Duan vd., 2021, s. 58). Beklenen ölçümler daha sonra iki katmanlı bir grafiksel güvenlik modeline beslenir. Bu model, ağdaki her düğümden güvenlik açığı sorunlarıyla ilgili bilgileri toplamak için alttan ilk katmanında bir saldırı ağacı içerir ve saldırı grafiğine sahip üst katman ağ bağlantısını gösterir. Bu güvenlik modeli, olası saldırı yollarını toplayarak IoT ağının güvenliğini otomatik olarak analiz eder. Gerçek dünyadaki IoT cihazlarından ve olası güvenlik açığı bilgisinden, yöntemlerinin yararlılığını değerlendirmek için bir kavram kanıtı istihbarat yapıları türü kullanılır. Önerilen çerçevenin sonuçları, yeni güvenlik açıklarının güvenlik açığı ölçümlerini %90'ın üzerinde ortalama doğrulukla doğru bir şekilde tahmin edebileceğini ve bir IoT ağı içindeki en savunmasız saldırı vektörlerini bulabileceğini göstermektedir. Değerlendirme bulguları, siber güvenlik uzmanlarının ek adımlar atması ve tehditleri mümkün olan en kısa sürede en aza indirmesi için bir referans olarak kullanılabilir.

Veri erişim ara yazılım yaklaşımı bu fikrin etkili örneklerinden biridir. Verileri doğrudan kaynaktan çevirmeden önce, kimlik doğrulama güvenlik protokolünü ve erişim kontrol protokollerini kullanır. Daha sonra verileri evrensel bir dile çevirir. Her durumda tek bir ara yazılım parçası kullanılamayacağından, genellikle belirli bir koşul kümesi için oluşturulurlar.



Şekil 28. (a) Ara Yazılım Olmadan ve (b) Ara Yazılımla İletişimin Gösterimi

Kaynak: Chan, M., Estève, D., Escriba, C. ve Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55–81.

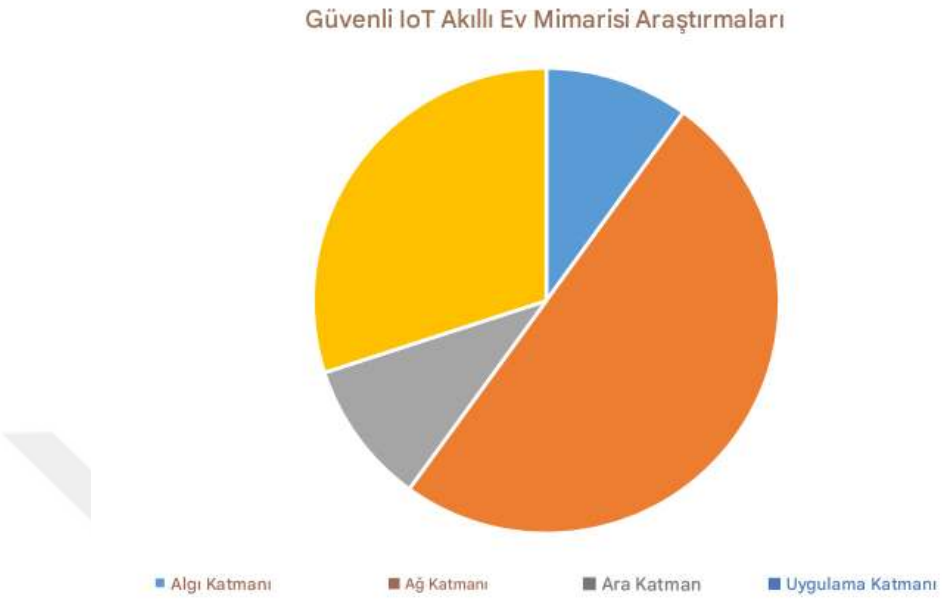
Uygulama katmanı güvenliği, yasa dışı veri erişimini ve kullanımını önlemek için kritik bir öneme sahiptir. Bu bağlamda, erişim kontrollerinin doğru bir şekilde uygulanması gerekir. Veritabanı gizliliğini korumak için kullanılan başlıca teknikler arasında veri maskeleme ve veri şifreleme teknolojileri öne çıkmaktadır. Ayrıca veri güvenliğini desteklemek için yedekleme ve kurtarma mekanizmalarının etkin şekilde uygulanması zorunludur. TLS, SSL ve DNS gibi gizlilik protokolleri bu kapsamda örnek gösterilebilir.

2014 yılından itibaren IoT için oyun tabanlı güvenlik modellemeleri üzerine çeşitli çalışmalar yapılmıştır. Ancak bu çalışmalar çoğunlukla belirli tehditlerin etkilerini sınırlamaya veya yalnızca belirli alanlara yönelik model çözümlerine odaklanmıştır. Örneğin Chen ve arkadaşları, kasıtlı saldırıların etkilerini azaltmak amacıyla füzyon tabanlı bir koruma mekanizması geliştirmiştir (Bourobou vd., 2015, s. 59). Araştırmacılar bu yaklaşımda, saldırganın ağ topolojisine dair ön bilgiye sahip olduğu ve tüm düğümleri aynı anda hedef alabildiği en kötü senaryoyu ele almışlardır. Bu durumda savunma stratejisi ile saldırgan arasında sıfır toplamlı bir oyun kurulmakta, sonuçlar ise önerilen yöntemin IoT sistemlerinin dayanıklılığını belirgin ölçüde artırdığını göstermektedir.

Benzer şekilde, Kim ve Lee IoT cihazları, ağları ve operasyonel süreçleri arasındaki etkileşimleri yönetmeye yönelik bir öneri sistemi tasarlamıştır. Bu sistem, uygun güvenlik politikalarının uygulanmasına yardımcı olmakta, akıllı evlerde veri güvenliği açıklarının tespit edilmesini kolaylaştırmakta ve ev cihazlarının kullanımına ilişkin öneriler sunmaktadır (Jacobsson vd., 2016, s. 59). Ayrıca, cihaz güvenliğini geliştirmek ve veri aktarım verimliliğini korumak amacıyla akıllı evlerde donanım güvenlik modüllerinin kullanılması önerilmektedir (Hejazi vd., 2018, s. 59).

Akıllı ev mimarilerinde güvenli veri iletimini sağlamak ve ağ içi aktarım sırasında veri kayıplarını önlemek için kapsamlı koruma mekanizmaları tasarlanmıştır. Bazı senaryolarda, yalnızca akıllı evlere uyarlanmış öneri sistemleri yönlendirme ve tahminler için kullanılmaktadır. Örneğin, aynı anda bir müzik çalar ve DVD oynatıcı kullanılan bir durumda, öneri sistemi kullanıcı eylemlerinden oluşan kalıpları analiz ederek tavsiyelerde bulunur. Bhole ve çalışma arkadaşları, geliştirdikleri çözümde veri güvenliği için öneri sistemi mimarisinden yararlanmıştır. Ancak Cebrat, öneri

sistemlerinin kullanıcı davranışlarından öğrenmeye dayalı olduğu için yalnızca güvenlik amacıyla yeterli olmayabileceğini vurgulamaktadır.



Şekil 29. Güvenli IoT Akıllı Ev Mimarisi Araştırmalarının Dağılımı

Kaynak: Chan, M., Estève, D., Escriba, C. ve Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55–81.

3.4. Ev Yangınlarına Yönelik Veri Analizi ve Güvenlik Önlemleri

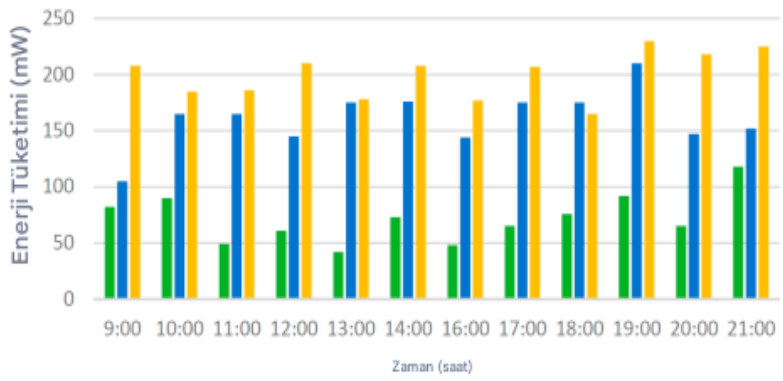
Yangın kaynaklı can ve mal kayıpları; alarm sistemlerindeki arızalar, yanlış alarmlar, müdahale edilmemesi ya da farklı nedenlerden meydana gelebilmektedir. Bu kapsamda, yangın algılama sistemlerinin kurulu olduğu ortamlarda yangın hasarlarının nedenleri üzerine bir analiz yapılmıştır. Çalışmada, 2010–2016 yılları arasında İngiltere'den elde edilen veriler değerlendirilmiştir. İnceleme, özellikle şu başlıklar altında yürütülmüştür:

- Yanlış alarmlardan doğan yangın hasarları,
- Herhangi bir müdahalenin yapılmaması sonucu ortaya çıkan kayıplar,
- Diğer ya da belirtilmeyen nedenlerden kaynaklanan zararlar.

Sonuçlar, kayıpların önemli bir kısmının yanlış alarmlardan ileri geldiğini ortaya koymuştur. İncelenen evlerin büyük çoğunluğunda WSN tabanlı yangın alarm sistemleri bulunmaktadır. Dört odalı bir ev planı (mutfak, televizyon bölümü, oturma

alanı ve yatak odası) üzerinden yapılan deneyde, ZigBee tabanlı sensörlerin 12 saatlik çalışma süresi içinde %50 ve %100 görev çevrimlerinde ortalama enerji tüketimi ölçülmüştür. Görev çevrimi, radyo biriminin aktif kaldığı süreyi ifade etmektedir. Enerji açısından verimli bir iletişim katmanında bu oran %1'in altında olmalıdır.

Her odada kullanılan sensörler, 3000 mAh kapasiteli ikili AA pillerle çalıştırılmıştır. Ölçümler sonucunda, %50 ve %100 görev çevrimlerinde 12 saatlik enerji tüketimi hesaplanmış ve Şekil 31'de sunulmuştur. Elde edilen bulgular, ZigBee sensörlerinin enerji tüketiminin kabul edilebilir sınırlar içerisinde kaldığını göstermektedir. Tüm odalara üçlü sensör seti (sıcaklık, gaz ve duman algılayıcıları) yerleştirilmiştir. Özellikle mutfaktaki enerji harcamasının diğer odalara kıyasla daha yüksek olduğu görülmüştür. Sabah, öğle sonrası ve akşam saatlerinde tüketimde artış kaydedilmiştir. Ayrıca, Şekil 22'de yangın senaryosu için bir saatlik enerji kullanımı verilmiş ve yangın anında sensörlerin tüketiminin belirgin şekilde yükseldiği saptanmıştır. Sonuç olarak, ZigBee tabanlı sensörlerin enerji kullanımı önerilen sistem bağlamında değerlendirildiğinde makul düzeyde kalmıştır ve akıllı yangın algılama uygulamaları için uygun bir çözüm sunmaktadır.

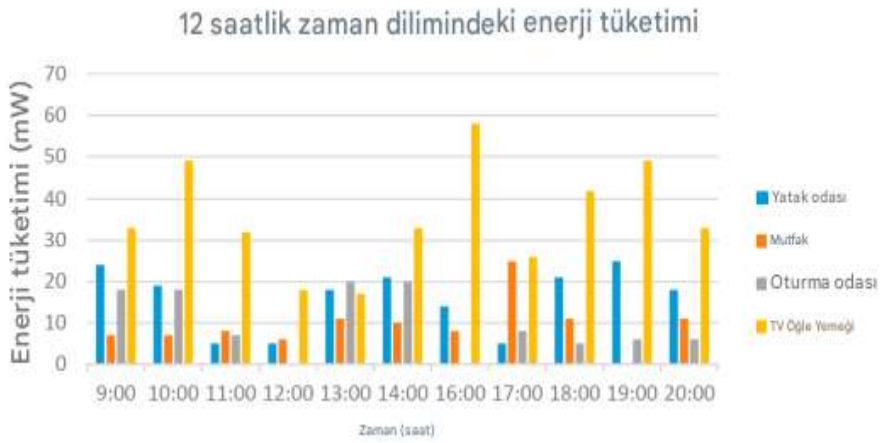


Şekil 30. Sensörler 50% ve 100% Görev Döngüsünde Çalışırken Enerji Tüketimi

Kaynak: Saeed, F., Paul, A., Rehman, A., Hong, W. H. ve Seo, H. (2018). IoT-based intelligent modeling of smart home environment for fire prevention and safety. *Sensor and Actuator Networks, 10*(2), 45-59.

Günlük enerji tüketimi, zaman dilimlerine göre farklılık göstermektedir. Özellikle sabah saat 09:00'dan itibaren sensörlerin enerji harcaması kademeli olarak yükselmekte ve günün belirli aralıklarında en yüksek seviyelere ulaşmaktadır. Bu

eğilim, hem kullanıcı faaliyetlerinin artışı hem de çevresel koşulların değişmesi ile bağlantılıdır. Sensörler %50 görev döngüsünde çalıştırıldığında enerji kullanımı daha sınırlı kalmaktadır; çünkü radyo birimi daha kısa süre aktif durumda olur. Ancak %100 görev döngüsünde sürekli açık kalmaları, tüketimin belirgin biçimde yükselmesine yol açmaktadır. Bu farklılık, esasen sensörlerin çalışma sıklığı ve veri iletim yoğunluğundan kaynaklanmaktadır. Sonuçlar göstermektedir ki enerji kullanımı günün farklı saatlerinde değişkenlik arz etmektedir. Özellikle yoğun kullanım zamanlarında yaşanan artışlar, sistem tasarımında enerji tasarrufunu ön plana çıkarmayı gerekli kılmaktadır. Görev döngüsünün optimize edilmesi, sensörlerin gereksiz yere sürekli çalışmasının engellenmesi ve düşük enerji tüketimli iletişim protokollerinin uygulanması, hem pil ömrünü uzatacak hem de maliyetleri azaltacaktır. Bu nedenle yapılan bu tür analizler, akıllı ev sistemlerinde daha verimli, güvenli ve sürdürülebilir çözümler üretmek açısından kritik bir rol oynamaktadır.



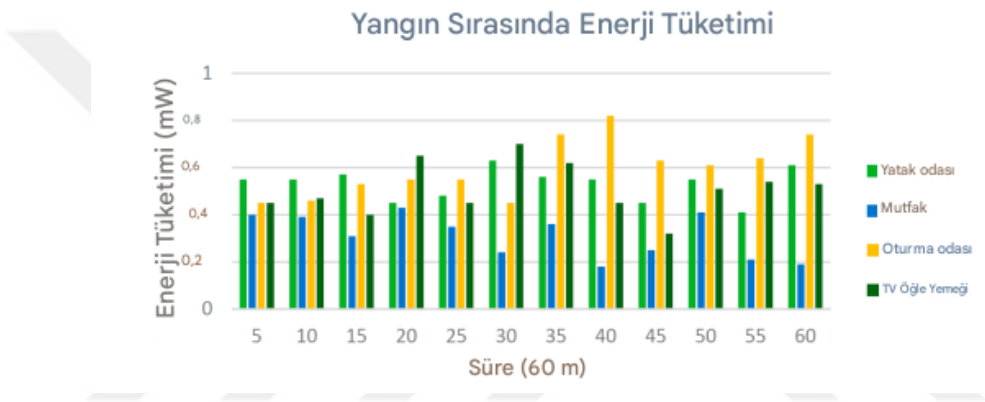
Şekil 31. Sensörlerin 12 Saatlik Enerji Tüketimi

Kaynak: Saeed, F., Paul, A., Rehman, A., Hong, W. H. ve Seo, H. (2018). IoT-based intelligent modeling of smart home environment for fire prevention and safety. *Sensor and Actuator Networks, 10*(2), 45-59.

Evdeki farklı odaların enerji tüketiminde belirgin farklılıklar bulunmaktadır. Yatak odasında enerji kullanımı genellikle daha düşüktür; bunun temel nedeni, bu alanın gün içinde daha az tercih edilmesidir. Mutfakta ise tüketim özellikle 13:00 ile 17:00 saatleri arasında artış göstermektedir. Bu durum, yemek hazırlama ve pişirme süreçlerinin yoğunlaştığı zaman dilimlerinden kaynaklanmaktadır. Oturma odasında

ise enerji kullanımı daha dengeli bir seyir izlemekte, ancak bazı saatlerde kısa süreli artışlar meydana gelebilmektedir.

Yapılan bu değerlendirme, odalara göre değişen enerji tüketim alışkanlıklarını ortaya koymaktadır. Bu farklılıkların belirlenmesi, enerji yönetiminde verimliliği artırmak için önemli ipuçları sağlamaktadır. Özellikle mutfak gibi yoğun kullanım alanlarında enerji tasarrufu sağlayacak cihazların tercih edilmesi, akıllı kontrol sistemleriyle tüketimin dengelenmesi ve düşük kullanım alanlarında sensörlerin daha düşük görev çevriminde çalıştırılması, toplam enerji harcamasını azaltmaya yardımcı olabilir.



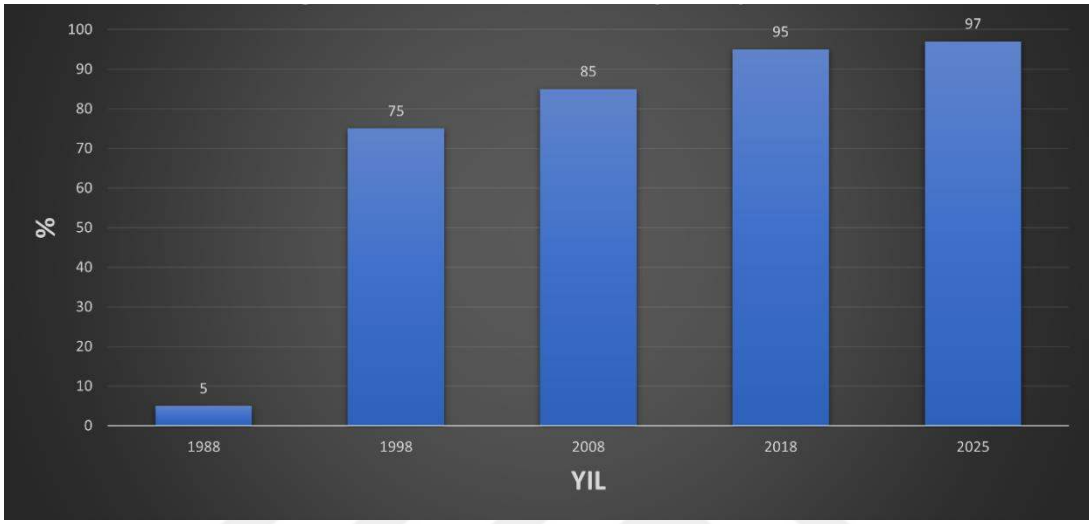
Şekil 32. 1 Saatlik Yangın Simülasyonu Sırasında Sensörlerin Enerji Tüketimi

Kaynak: Saeed, F., Paul, A., Rehman, A., Hong, W. H. ve Seo, H. (2018). IoT-based intelligent modeling of smart home environment for fire prevention and safety. *Sensor and Actuator Networks, 10*(2), 45-59.

Şekil 32'de yer alan simülasyon, bir saatlik yangın senaryosu sırasında farklı odaların enerji tüketim düzeylerini ortaya koymaktadır. Yatak odasında tüketim sabit kalırken, mutfak ve oturma odasında özellikle 10–20. dakikalar arasında belirgin bir artış gözlenmektedir. Televizyon bölümü ile oturma odasında ise belirli zaman aralıklarında tüketimin daha yüksek olduğu dikkat çekmektedir. Bu tür bulgular, yangın gibi acil durum senaryolarında sensörlerin enerji kullanımını izlemek ve daha verimli hale getirmek için önemli bilgiler sağlamaktadır.

Yangın algılama sistemlerinde karşılaşılan alarm arızalarının çoğu, WSN (Kablosuz Sensör Ağları) üzerindeki bozulmalardan kaynaklanmaktadır. WSN'nin temelinde sensörler arasındaki iletişim yatmaktadır. Bu nedenle, ağ bağlantısının

kopması durumunda sensörler birbirleriyle veri paylaşamaz. Tek bir sensörün işlevsiz hale gelmesi bile zincirleme etki oluşturarak ciddi problemlere yol açabilir. Sensörlerin büyük kısmı pille çalıştığından, yeniden şarj imkânı bulunmayabilir. Ayrıca, enerji tüketiminin en yoğun olduğu alan iletişim sürecidir; bu sırada batarya tükenirse sensör arızalanabilir ve bu durum tüm ağın çalışmasını aksatabilir.



Şekil 33. Yangın Alarmı Olan Evlerin Yıllık Yüzdesi

Kaynak: Yazar tarafından oluşturulmuştur.

Şekil 33 de yangın alarmı bulunan evlerin yüzdesinin 1988'den 2025'e nasıl değiştiğini göstermektedir. 1988 yılında yangın alarmı bulunan evlerin oranı oldukça düşüktü. O dönemde yangın alarmı sistemleri hem pahalıydı hem de yaygın değildi. Evlerde yangın güvenliğine dair ciddi bir farkındalık eksikliği söz konusuydu. Bu nedenle alarm bulunan ev oranı 5%'in bile altındaydı. Yangın sonucu can ve mal kaybı haberleri sonrasında kamuoyunda dikkat oluşmaya başlamıştı, ancak henüz yaygın bir politika geliştirilememişti. Toplumda alarm taktırmak bir lüks olarak görülüyordu.

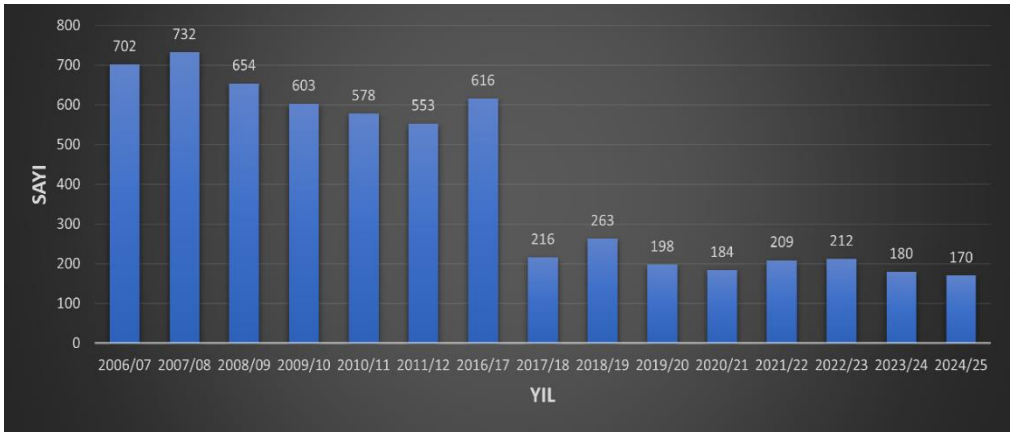
1998 yılına gelindiğinde tablo ciddi şekilde değişmeye başlamıştı. Özellikle 1990'ların başından itibaren başlatılan kamu spotları, yangın tatbikatları ve yerel yönetimlerin destek programları sayesinde halkta yangın güvenliği bilinci artmıştı. Bu yıllarda yangın alarmı sistemlerinin maliyeti düşmeye başlamış, kurulumu daha erişilebilir hale gelmişti. 1998 yılı itibarıyla yangın alarmı bulunan evlerin oranı 75%'in üzerine çıkmıştı. Artık yeni yapılan konutların büyük bir kısmında alarm

sistemleri standart olarak yer alıyor, eski evlerde ise bireysel kurulumlar hızla yaygınlaşıyordu.

2008 yılına gelindiğinde, yangın alarmı bulunan ev oranı 85% seviyesini geçmişti. Bu yıllarda yangın güvenliğiyle ilgili düzenlemeler daha sıkı hale gelmiş, bazı bölgelerde alarm zorunluluğu getirilmişti. Hükümetin desteklediği projelerle sosyal konutlara ücretsiz ya da düşük maliyetli dedektörler yerleştirilmişti. Alarm kurulum oranı düzenli şekilde artmaya devam etmişti, ancak artık artış hızı ilk yıllara kıyasla biraz daha yavaşlamıştı. Çünkü büyük çoğunluk zaten bu sistemlere erişmişti. Yine de alarmı olmayan evlerin varlığı dikkat çekmeye devam ediyordu.

2018 yılı itibarıyla yangın alarmı bulunan evlerin oranı 95%'e ulaşmıştı. Bu dönemde hem mevzuatlar hem de kamu bilinci daha da gelişmişti. Özellikle sosyal konutlarda oran 97%'lere çıkarken, özel kiralık evlerde ise 2015'te yürürlüğe giren zorunlu alarm düzenlemeleri sayesinde hızlı bir yükseliş yaşanmıştı. Artık yangın alarmı olmayan evler istisna haline gelmişti. Ancak buna rağmen bazı evlerde alarm sistemleri bulunsa bile, pillerinin bitmiş olması veya bakım yapılmaması gibi nedenlerle işlevsiz hale geldiği görülüyordu. Dolayısıyla alarm varlığı ile çalışır durumda olması arasında fark olduğu anlaşılmıştı.

2025 yılına gelindiğinde yangın alarmı bulunan evlerin oranının 97% seviyesinde sabit kaldığı görülmektedir. Artık evlerin neredeyse tamamında alarm sistemi bulunmaktadır. Ancak oranın 100%'e ulaşamamasının temel nedeni, hala bazı evlerde alarm sistemlerinin hiç bulunmaması ya da çalışmaması, bazı kullanıcıların sistemleri sökmesi veya bilinç eksikliği nedeniyle kullanmaması gibi durumlardır. Bu dönemde artış hızı tamamen yavaşlamış ve eğilim plato çizmiştir. Politikalar, yeni kurulumdan çok mevcut sistemlerin bakımına, sürekliliğine ve çalışır durumda tutulmasına odaklanmaya başlamıştır.



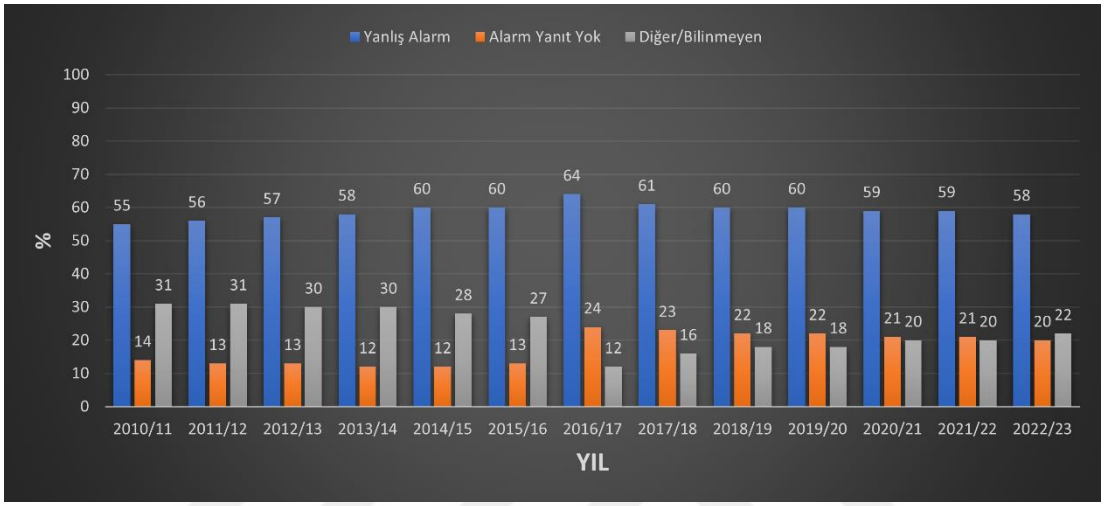
Şekil 34. Yangın Kaynaklı Ölümler

Kaynak: Yazar tarafından oluşturulmuştur.

Şekil 34, 2006–2025 yılları arasında İngiltere ve Galler'de milyon kişi başına düşen yangın kaynaklı ölümleri göstermektedir. 2006 yılında bu oran yaklaşık 702 kişi olarak kaydedilmiş, 2007'de ise 732 kişiyle en yüksek seviyesine ulaşmıştır. Ancak bu zirvenin ardından yangına bağlı ölümler genel olarak düşüş trendine girmiştir. 2008'de oran 654, 2009'da 603, 2010'da ise 578 kişi düzeyine gerilemiştir. Bu dönemdeki istikrarlı azalma, toplumsal ölçekte yangın risklerinin giderek azaldığını ortaya koymaktadır. 2011–2016 yılları arasındaki beş yıllık süreçte ölüm oranları 553 ile 616 kişi arasında dalgalı bir seyir izlemiştir. 2016 yılı itibarıyla oran yaklaşık 616 kişi olarak tespit edilmiştir. Bu dönem, düşüş eğiliminin sürdüğü ancak belirli bir seviyede yatay hareket ettiği bir zaman dilimi olmuştur.

2016/17 döneminde yangına bağlı toplam ölüm sayısı 216 kişi olarak kaydedilmiştir. Bu değer, önceki yıllarla benzer seviyede seyretmiş olsa da 2017/18 döneminde belirgin bir artış yaşanmıştır. Özellikle Grenfell Tower faciası bu artışın başlıca nedeni olmuş ve ölüm sayısını 263'e çıkarmıştır. Bu durum, tek bir büyük olayın yıllık ölüm istatistikleri üzerinde doğrudan ve önemli bir etkiye sahip olabileceğini göstermesi bakımından dikkat çekicidir.2018/19 ve 2019/20 yıllarında yangına bağlı ölümler 198 kişi olarak kaydedilmiştir. 2020/21'de bu sayı 184'e gerilemiş, ancak 2021/22 döneminde 209'a, 2022/23 yılında ise 212'ye yükselmiştir. Buna rağmen Home Office'in 2022/23 raporunda, ölüm oranlarında bir önceki yıla kıyasla %5,1'lik bir düşüş yaşandığı belirtilmiştir. Bu da toplam ölüm sayısındaki artışa rağmen, nüfusa oranla göreli bir iyileşme olduğunu göstermektedir.

2023/24 yılında ölümler tekrar azalarak yaklaşık 180 kişi olarak açıklanmıştır. 2025 yılı tahminlerine göre, ölüm sayısının 170–180 aralığında olacağı öngörülmektedir. Bu, 2006 yılına kıyasla önemli bir düşüşe işaret etmekte ve son 20 yılda genel olarak azalan bir eğilim olduğunu göstermektedir. Ancak yaşlılar ve erkekler arasında ölüm oranları hala yüksektir, bu nedenle bu gruplara yönelik daha hedefli önlemler alınması gerekmektedir.



Şekil 35. Nedene Göre Yangın Kayıp Oranı

Kaynak: Yazar tarafından oluşturulmuştur.

Şekil 35, yangın nedenlerine göre oluşan kayıpların yıllar içindeki dağılımını göstermektedir. Grafik incelendiğinde, her yıl en yüksek oranın yanlış alarmlara ait olduğu, buna karşılık alarmlara yanıt verilmemesi ve diğer/bilinmeyen nedenlerin daha düşük oranlarda kaldığı görülmektedir. Bu durum, sadece alarm sistemine sahip olmanın yeterli olmadığını; sistemlerin düzgün çalışması ve kullanıcıların doğru tepki verebilmesinin kritik olduğunu ortaya koymaktadır. 2010/11 yılında kayıtlar daha düzenli şekilde toplanmaya başlanmış, olayların %55'i yanlış alarm olarak sınıflandırılmıştır. Aynı dönemde alarmlara yanıt verilmemesi %14, diğer nedenler %31 oranında kaydedilmiştir. Bu, teknolojik sistemlerin yanında insan davranışlarının ve bakım süreçlerinin de yangın güvenliğinde belirleyici olduğunu göstermektedir. 2011/12 ve 2012/13 yıllarında yanlış alarm oranı sırasıyla %56 ve %57'ye yükselmiş, alarmlara yanıt verilmemesi %13 seviyesinde kalmış, diğer nedenler ise sırasıyla %31 ve %30 olarak ölçülmüştür. Bu yıllarda alarm sistemlerine güvenin sınırlı olduğu ve kullanıcı alışkanlıklarının yeterince gelişmediği anlaşılmaktadır. 2013/14 döneminde

yanlış alarmlar %58'e çıkmış, alarm tepkisizliği %12'ye düşmüş, diğer nedenler ise %30 olmuştur. 2014/15 yılı ise yanlış alarmların %60'a ulaştığı kritik bir döneme işaret etmektedir. Bu durum, teknolojinin yaygınlaşmasına rağmen sistemin gereğinden fazla tetiklendiğini göstermektedir.

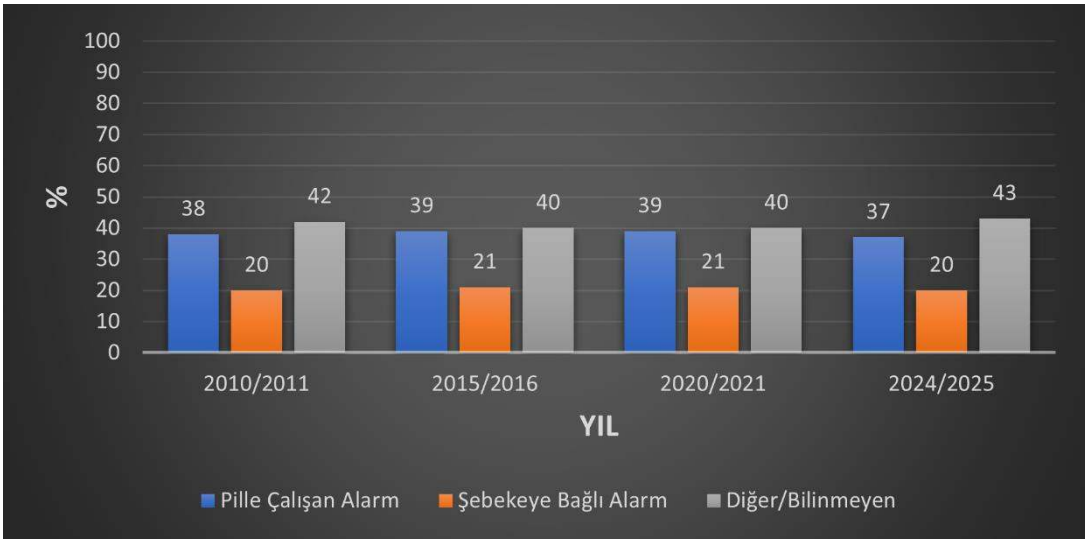
2015/16 yılında oranlar sabit kalmış; yanlış alarm %60, yanıt verilmemesi %13, diğer nedenler %27 olarak ölçülmüştür. Bu da mevcut farkındalık çalışmalarının yeterince etkili olmadığını düşündürmektedir. 2016/17 yılı dikkat çekicidir: yanlış alarm oranı %64, alarm tepkisizliği %24'e yükselmiş, diğer nedenler %12'ye düşmüştür. Bu dönemde yaşanan Grenfell Tower faciası, kayıtlarda artışa ve toplumsal farkındalığa yol açmıştır. 2017/18 sonrası göreli bir iyileşme gözlemlenmiş; yanlış alarmlar %61, tepkisizlik %23, diğer nedenler %16 olmuştur. Ancak yapısal eksiklikler devam etmektedir. 2018/19 ve 2019/20 dönemlerinde oranlar sabitlenmiş; yanlış alarm %60, tepkisizlik %22, diğer nedenler %18 seviyesinde kalmıştır.

2022/23 yılında da benzer bir tablo görülmüş; yanlış alarm %58, alarm tepkisizliği %20, diğer nedenler %22 olarak raporlanmıştır. Her ne kadar toplam ölüm sayısı artsa da Home Office verilerine göre ölüm oranı bir önceki yıla göre %5,1 azalmıştır. Bu da nüfus oranına göre göreli bir iyileşmeye işaret etmektedir.

Aynı yıl yangına bağlı ölümlerin başlıca nedenleri şunlardır:

- %28: sigara içme materyalleri (özellikle yatakta sigara)
- %9: ısıtıcı cihazlar
- %7: elektrik arızaları
- %7: pişirme ekipmanları
- %6: mum ve açık alevli araçlar
- %15: kasıtsız diğer nedenler
- %28: belirlenemeyen veya eksik raporlanmış vakalar

Sonuç olarak, 2010–2023 döneminde yangınla ilgili kayıplarda en büyük pay yanlış alarmlara aittir. Alarmlara yanıt verilmemesi ve rapor eksiklikleri de önemli yer tutmaktadır. Ayrıca ölümlerin başlıca nedenlerinin sigara, pişirme hataları ve elektrik arızaları olması, yangın güvenliği stratejilerinin hem teknolojik altyapıyı hem de kullanıcı farkındalığını kapsaması gerektiğini açıkça ortaya koymaktadır.



Şekil 36. Türlere Göre Yangın Arıza Oranları

Kaynak: Yazar tarafından oluşturulmuştur.

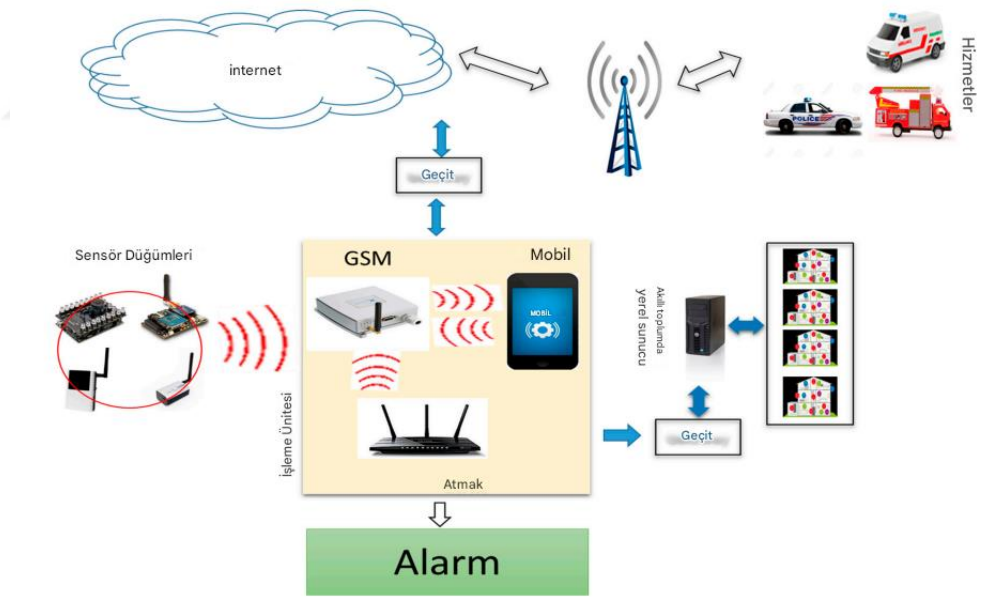
Şekil 36, farklı yangın alarmı türlerine ait arıza oranlarını göstermektedir. Verilere göre, pille çalışan sistemlerin arıza oranı 2010/11'de yaklaşık %38 iken sonraki yıllarda %40 seviyelerine kadar yükselmiş, 2016/17 itibarıyla yeniden %39'a gerilemiştir. Bu tür sistemlerdeki arızalar genellikle pilin zamanında değiştirilmemesi, kullanıcının pili çıkarması veya cihazın hiç test edilmemesi gibi bakım eksikliklerinden kaynaklanmaktadır. 2017–2025 döneminde, pilli alarmların arıza oranı %38–40 aralığında sabit kalmıştır. Bu da uzun vadede anlamlı bir gelişme yaşanmadığını, mevcut sorunların yapısal nitelik taşıdığını göstermektedir. Öte yandan, şebeke elektriğine bağlı alarmlar bu süre boyunca daha güvenilir bir performans sergilemiştir. Bu sistemlerin arıza oranı genellikle %20–22 bandında sabit kalmış, düşük bakım gereksinimi ve doğrudan elektrik altyapısına bağlı olmalarıyla öne çıkmıştır.

Grafikte ayrıca, "diğer" veya kaynağı tanımlanmamış sistemlerin arıza oranlarında da dikkat çeken bir artış görülmektedir. Özellikle 2013/14'ten itibaren bu oran %30'un üzerine çıkmış, 2016/17'de %36 ile zirve yapmıştır. Bu grup; eski tip dedektörler, bağlantısı belirsiz cihazlar gibi çeşitli sistemleri kapsamaktadır. 2017–2025 arasında bu türlerin arıza oranı %39–42 aralığında dalgalanmış, daha önce belirtilen %30–36 düzeyi güncelliğini yitirmiştir. Bu veriler, sadece alarm sistemine sahip olmanın yeterli olmadığını; seçilen alarm türünün güvenilirliğinin de yangın

güvenliği açısından kritik olduğunu ortaya koymaktadır. Özellikle pille çalışan sistemlerde, üç yangından birinde alarmın çalışmaması hala ciddi bir güvenlik açığı yaratmaktadır.

Amerikan Ulusal Yangın Koruma Birliği (NFPA)'nin 2018–2022 verileri de bu tabloyu desteklemektedir. Buna göre, büyük yangınlarda şebeke bağlantılı alarmların %94'ü çalışırken, pilli alarmlarda bu oran %85'tir. Ayrıca, yangın ölümlerinin %66'sı pilli alarm bulunan evlerde; yalnızca %29'u şebekeye bağlı alarm bulunan evlerde yaşanmıştır. Bu fark, sadece sistemin varlığı değil, seçiminin ve bakımının da hayati rol oynadığını göstermektedir.

Sonuç olarak, alarm tipi yangın güvenliğinde belirleyici bir unsurdur. Şebekeye bağlı sistemler düşük arıza oranlarıyla öne çıkarken; pilli ve tanımlanamayan sistemlerdeki sorunlar 2025'e kadar varlığını sürdürmüştür. Bu durum, yalnızca alarm kurulumunun değil, doğru sistem seçimi ve düzenli kontrollerin de güvenlik stratejilerinde öncelik haline gelmesi gerektiğini göstermektedir.



Şekil 37. IoT Tabanlı Yangın Önleme İçin Akıllı Ev Modellemesi

Kaynak: Saeed, F., Paul, A., Rehman, A., Hong, W. H. ve Seo, H. (2018). IoT-based intelligent modeling of smart home environment for fire prevention and safety. *Sensor and Actuator Networks, 10*(2), 45-59.

Mevcut sistemlerin eksiklikleri: Geleneksel akıllı ev yangın algılama sistemleri, her bölümde yalnızca tek bir sensörün bulunması nedeniyle bazı yetersizliklere sahiptir. Örneğin, belirli bir noktada olay meydana geldiğinde ilgili sensör çalışmazsa, yangının başlangıç aşamasında tespit edilmesi düşük bir olasılıktır. Bir diğer önemli sorun ise sıkça ortaya çıkan **yanlış alarmlardır**. Bu eksikleri gidermek amacıyla önerilen akıllı ev yangın algılama sistemi dört ana bileşenden oluşmaktadır:

1. Sensörler,
2. Ana ev alıcısı ve işleme birimi,
3. GSM iletişimmodülü,
4. Alarm sistemi.

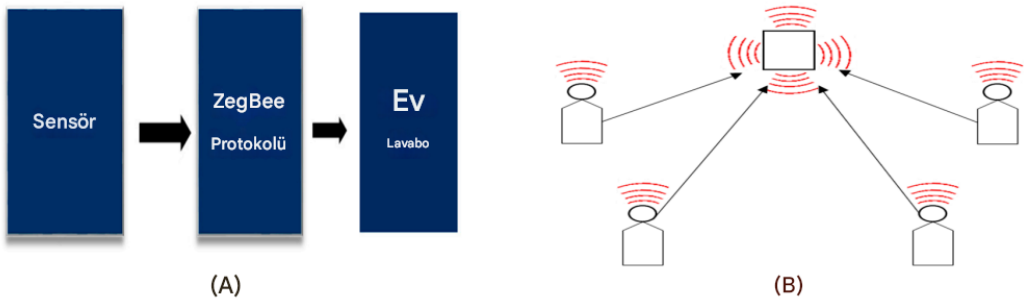
Sensörler, her bir ev bölümüne çoklu yerleştirilmiştir; yani duman, gaz ve ısı sensörleri birlikte kullanılmıştır. Tüm sensörlerin kendi olay algılama mekanizması vardır. Şekil 38'de çalışmanın genel modeli sunulmaktadır. İşleme birimi, sensörlerle ZigBee protokolü üzerinden iletişim kuran bir ev alıcısı içermektedir. Yangın tespiti kararı, sensörlerden gelen bilgiler ve kullanıcının tepkisi doğrultusunda alınır. Tek bir sensörden uyarı geldiğinde sistem GSM modülünü devreye sokar ve kullanıcıya bildirim gönderir. Kullanıcı veya diğer sensörlerden gelen onayla birlikte iki veya daha fazla doğrulama sağlanırsa, alarm tetiklenir. Aynı zamanda olay bilgileri hem buluta hem de yerel sunucuya aktarılır. Yerel sunucu, çevredeki evlerle bağlantılı olduğundan durumun paylaşılmasına olanak tanır.

Yangın sırasında açığa çıkan temel göstergeler ısı, duman, gaz veya kızılötesi/ultraviyole radyasyondur. Bu modelde duman, gaz ve sıcaklık sensörleri birlikte kullanılmıştır. Sıcaklık sensörleri, ortam ısısındaki değişiklikleri tespit eder. İki tip sıcaklık algılama yöntemi vardır: (i) ısının yükselme hızı, (ii) sabit sıcaklık. LM35 (Texas Instruments, Çin), düşük enerji tüketimi ve yüksek doğrulukla kalibre edilmiş bir sensör olup 4V–30V aralığında çalışabilmektedir (Texas Instruments, 2017).

Duman sensörleri, yangında ortaya çıkan duman partiküllerini algılar. Çoğunlukla disk formunda plastik kafes içerisine yerleştirilir. MQ9 (Henan Hanwei Electronics, Zhengzhou, Çin), karbon monoksit hassasiyeti ve oksit tabakası ile

dumanı yüksek doğrulukla algılayan bir modeldir (Henan Hanwei Electronics, 2017). Gaz sensörleri, yangın esnasında üretilen karbon monoksit (CO), karbondioksit (CO_2) gibi zararlı gazları algılar. MH-Z19 NDIR (Zhengzhou Winsen Electronics, Çin), dağılmayan kızılötesi (NDIR) teknolojisiyle çalışan küçük ve uzun ömürlü bir CO_2 dedektörüdür.

Kablosuz sensör ağlarının kurulmasında farklı topolojiler (eşler arası, ağ, ağaç ve yıldız) tercih edilebilir (Kosmerchock, 2017). Bu sistemde yıldız topolojisi benimsenmiştir; kurulumu basit ve işlevseldir. Şekil 38, yıldız ağı topolojisini göstermektedir. Sensörler ile alıcı arasındaki iletişim ZigBee protokolüyle sağlanmaktadır. ZigBee, IEEE 802.15.4 standardına dayalıdır ve küçük, düşük güçlü dijital radyo cihazlarıyla 10–100 metre mesafede veri aktarımı yapabilmektedir. Mesafe çevresel koşullara bağlı olarak değişmektedir. Enerji tüketiminin düşük olması, ZigBee'yi akıllı evler için uygun bir iletişim protokolü haline getirmektedir.



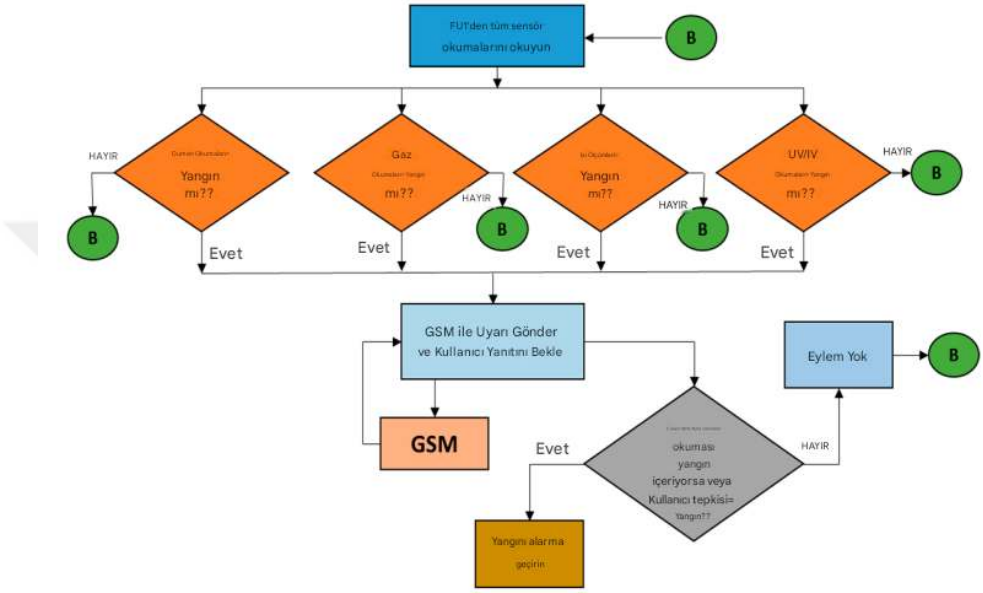
Şekil 38. (a) Kablosuz Sensör Düğümüne Ait Akış Diyagramı (b) Yıldız Topolojisi

Kaynak: Saeed, F., Paul, A., Rehman, A., Hong, W. H. ve Seo, H. (2018). IoT-based intelligent modeling of smart home environment for fire prevention and safety. *Sensor and Actuator Networks, 10*(2), 45-59.

Sensörlerden elde edilen veriler, kablosuz bağlantı aracılığıyla merkezi işlem merkezine ya da ana ev alıcısına iletilmektedir. Günümüzde yaygın olarak kullanılan Raspberry Pi (RPI), esnek işlevleri ve popülerliği nedeniyle birincil işlem birimi olarak tercih edilmektedir. Bu cihaz, sensörlerden gelen bilgileri değerlendirerek alarmın devreye girip girmeyeceğine karar veren bir işlemci görevi üstlenmektedir.

RPI, sensör düğümlerinden gelen verileri işlemek için gerekli modülleri aktif hale getirir. Örneğin, önerilen sistemde GSM tabanlı kısa mesaj (SMS) bildirim

modülü ve GPIO (genel amaçlı giriş-çıkış) modülü kullanılmıştır. Eğer sensörlerden gelen ölçümler yangın tehlikesi işaret ediyorsa, GSM modülü devreye girer ve kullanıcının telefonuna otomatik olarak uyarı mesajı gönderilir. GPIO modülünün temel işlevi ise kullanıcının yangına verdiği yanıtı kontrol etmektir. Yanıt "evet" olduğunda yangın doğrulanmış sayılırken, "hayır" yanıtı durumun yanlış alarm olduğunu göstermektedir.



Şekil 39. Önerilen Şemanın Akış Şeması

Kaynak: Saeed, F., Paul, A., Rehman, A., Hong, W. H. ve Seo, H. (2018). IoT-based intelligent modeling of smart home environment for fire prevention and safety. *Sensor and Actuator Networks, 10*(2), 45-59.

GSM Modülü

Yanlış alarmların maliyeti oldukça yüksek olduğundan, bu sorunu engellemek amacıyla bir bileşen, yani GSM tercih edilmiştir. Mutfak ortamında hata ihtimali daha fazladır; sıcaklık, gaz, duman ve UV ya da IR ışınları genellikle havada bulunur. Günümüzde WaveCom ve Multitech gibi GSM modemleri, SMS modunu destekleyen özelliklere sahiptir. Mesajların ikili PDU biçiminde kodlanması yerine, bu metin modu, ev içi sensörün AT komutlarını kullanarak kullanıcıya erken bir uyarı iletisi göndermesine imkan sağlamaktadır. GSM modülüne ait sahte kod aşağıda sunulmaktadır:

- RPi cihazının seri portunu açın ve 3G modemi bağlayın.
- Telefon numarasını ve mesaj içeriğini ayarlayın.
- SMS gönderilmesi için “AT” komutları gönderin.
- Telefonun bağlantısını kesin.

Diyagramın başlangıç noktası, evin farklı bölümlerine yerleştirilmiş olan sensörlerin verilerinin okunması sürecidir. Burada amaç, yangına sebep olabilecek herhangi bir işaretin erken dönemde yakalanmasıdır. Sensörler; sıcaklık, duman, gaz, ultraviyole (UV) ve kızılötesi (IR) ışınlar gibi çeşitli parametreleri ölçmektedir. Sistem, bu sensörlerden gelen tüm bilgileri periyodik olarak toplar ve merkezi işleme birimine gönderir. Bu aşamanın önemi, erken tespit imkanı sağlamasıdır. Yangın gibi tehlikeli olaylar genellikle küçük işaretlerle başlar. Örneğin, sıcaklığın anormal şekilde artması, odada duman oluşması veya yanıcı gazların yoğunluğu gibi durumlar tehlikenin habercisi olabilir. Eğer sistem, bu verileri sürekli okur ve kaydederse, olası bir yangın daha başlangıçta fark edilebilir.

Sensör verilerinin okunması sırasında dikkat edilmesi gereken bazı noktalar vardır. Öncelikle sensörlerin düzenli olarak kalibre edilmesi gerekir. Kalibre edilmeyen sensörler yanlış değerler üretebilir, bu da sistemin doğru çalışmasını engeller. İkinci olarak, sensörlerin bulunduğu ortam koşulları ölçümleri doğrudan etkileyebilir. Örneğin, mutfakta kullanılan bir gaz sensörü pişirme sırasında yanlış alarm verebilir. Bu tür hataları azaltmak için sistem, birden fazla sensörün verilerini karşılaştırmalı şekilde analiz etmelidir. Bir diğer önemli nokta ise sensörlerin enerji tüketimidir. Akıllı evlerde genellikle düşük güçlü cihazlar kullanılır. Bu nedenle, sensörlerin hem sürekli çalışabilmesi hem de pil ömrünü koruyabilmesi için enerji verimliliği önemlidir. ZigBee veya benzeri düşük enerji harcayan iletişim protokolleri bu aşamada avantaj sağlar.

Özetle, ilk aşama olan sensör okumaları, sistemin bel kemiğini oluşturur. Çünkü yanlış veya eksik veri toplanırsa, sonraki aşamalarda alınan kararlar da hatalı olabilir. Bu yüzden, doğru çalışan sensörler, güvenilir veri aktarımı ve düzenli bakım, akıllı ev yangın algılama sisteminin güvenilirliği için kritik önemdedir. İkinci adımda gaz sensörleri devreye girer. Yangın sırasında ortaya çıkan en tehlikeli unsurlardan biri karbonmonoksit ve karbondioksit gibi gazlardır. Gazların sızıntısı, bazen yangın

çıkmadan da tehlike yaratabilir. Bu nedenle gaz sensörlerinin sürekli ölçüm yapması ve değerleri merkezî sisteme göndermesi kritik önemdedir.

Eğer gaz sensöründen gelen veriler olağan dışı bir yoğunluğu işaret ediyorsa sistem "yangın ihtimali var" sonucuna yaklaşır. Ancak tek bir sensörden gelen bilgi yeterli değildir. Yanlış alarm ihtimalini azaltmak için gaz sensörünün verisi, diğer sensörlerden gelen bilgilerle karşılaştırılır. Gaz sensörleri, genellikle MQ9 gibi hassas modellerden seçilir. Bu tür sensörler karbonmonoksit gibi gazlara karşı yüksek duyarlılığa sahiptir. Ayrıca gazın türüne göre farklı dedektörler de kullanılabilir: kızılötesi, katalitik veya fotoiyonizasyon tipleri. Bu aşama, kullanıcı güvenliği açısından kritik bir basamaktır. Çünkü gaz kaçağı ve yangın riski yalnızca mal kaybına değil, doğrudan can kaybına da yol açabilir.

Üçüncü bölümde sıcaklık sensörlerinden gelen veriler kontrol edilir. Yangınların erken evrelerinde sıcaklık hızla yükselir. Bu nedenle sistem, ortam sıcaklığını sürekli takip eder. Sıcaklık sensörleri genellikle iki farklı şekilde çalışır: sabit sıcaklık ölçümü ve ısının yükselme hızı ölçümü. LM35 gibi sensörler düşük enerji tüketimi, yüksek doğruluk ve geniş çalışma voltajı sayesinde tercih edilmektedir.

Bu sensörler sayesinde, yangın başlamadan önce bile sıcaklıktaki anormal artış fark edilebilir. Ancak tek başına sıcaklık ölçümü yeterli değildir. Çünkü bazı durumlarda güneş ışığı veya elektrikli cihazlar ortamı geçici olarak ısıtabilir. Bu yüzden sıcaklık verileri duman ve gaz sensörleriyle birlikte değerlendirilir. Bu aşama, yanlış alarmların azaltılmasına yardımcı olur ve yangın tehlikesini daha kesin şekilde tespit etmeyi sağlar. Yangın sırasında ortaya çıkan en belirgin işaretlerden biri dumandır. Duman sensörleri, havadaki partikülleri algılayarak sistemin yangını fark etmesine katkı sağlar. MQ9 gibi sensörler bu işlev için yaygın olarak kullanılmaktadır.

Ayrıca UV (ultraviyole) ve IR (kızılötesi) sensörleri de alevin yaydığı ışınları algılayarak sistemin doğrulama yapmasını sağlar. Bu sensörlerin avantajı, duman oluşmadan da alevi fark edebilmesidir. Duman ve ışık sensörlerinden gelen veriler, sıcaklık ve gaz ölçümleriyle birlikte incelendiğinde yangın ihtimali daha yüksek doğrulukla belirlenir. Eğer sensörlerden gelen veriler yangın olasılığını gösteriyorsa,

sistem otomatik olarak GSM modülünü devreye alır. GSM sayesinde kullanıcıya SMS yoluyla uyarı gönderilir.

Bu aşama çok önemlidir çünkü kullanıcı evde olmasa bile sistem, acil durumu haber verir. Böylece hızlı bir şekilde önlem alınabilir. Kullanıcıya gelen mesaj, sistemin güvenilirliğini artırır ve olaylara zamanında müdahale imkanı sunar. GSM modülünün temel avantajı, internet bağlantısına ihtiyaç duymadan çalışabilmesidir. Bu da acil durumlarda kesintisiz haberleşme sağlar. GSM üzerinden gönderilen mesajı alan kullanıcıdan yanıt beklenir. Kullanıcının vereceği yanıt iki seçeneklidir: "Evet" veya "Hayır". Eğer kullanıcı "Evet" cevabını verirse, yangın durumu doğrulanmış kabul edilir. Kullanıcı "Hayır" derse, alarm iptal edilir.

Bu yöntem yanlış alarmları azaltmak için tasarlanmıştır. Çünkü bazı durumlarda sensörler yanlış pozitif sonuç verebilir. Kullanıcının olaya müdahale ederek doğrulama yapması sistemin esnekliğini artırır. Eğer birden fazla sensörden gelen veri yangını işaret ediyorsa ve kullanıcı da "Evet" yanıtı vermişse, sistem otomatik olarak alarmı devreye sokar. Bu alarm, hem ev sakinlerini uyarır hem de çevredeki kişilerin durumu fark etmesini sağlar. Alarm devreye girdiğinde sistem aynı zamanda bulut sunucusuna ve yerel ağa da bilgi gönderir. Böylece diğer evler ve servis birimleri durumdan haberdar edilir.

Son aşamada, yangın olayıyla ilgili bilgiler hem bulut sistemine hem de yerel sunucuya aktarılır. Bulut sistemi, acil durum verilerinin daha geniş çapta paylaşılmasına olanak tanır. Yerel sunucu ise çevredeki evlerle iletişim kurarak topluluk bazında güvenliği artırır. Bu entegrasyon, yalnızca yangının hızlı tespit edilmesini değil, aynı zamanda yayılmasının önlenmesini de destekler. Çünkü sistemden gelen uyarılar komşu evlere ulaştığında, onların da önlem alması sağlanır.

SONUÇ

Nesnelerin İnterneti sayesinde insanlar daha akıllıca çalışıp yaşayabilir ve günlük yaşamları üzerinde daha fazla kontrole sahip olabilirler. Akıllı ev sistemlerini daha otomatik hale getirmenin, bağımsız olarak çalışmasının kritik konusu IoT cihazları tarafından sağlanır. Nesnelerin İnterneti, insanların günlük yaşamları için son yıllardaki en önemli gelişmelerden biridir ve daha fazla kuruluş rekabetçi kalmada bağlı cihazların önemini gördükçe ivme kazanmaya devam edecektir. Sistemlerin hem kablosuz hem de kablolu unsurları için siber güvenlik, akıllı şebeke gelişiminin karşı karşıya olduğu ortaya çıkan gereksinimlerin en ciddi endişelerinden biridir. Ağ bağlantıları aracılığıyla, IoT cihazları her seferinde büyük miktarda veri gönderip alabilir. Bu, saldırganların IoT ağlarına erişmesini ve değerli verilerini çalmasını sağladı. Siber teröristler, sistem tasarımcıları için ciddi bir endişe olan akıllı şebekeyi hedef alabilir.

Akıllı ev sistemlerinde kullanılan veri aktarım protokollerindeki açıklıklar, zayıf parola politikaları, güncellenmeyen yazılımlar ve şeffaf olmayan veri işleme yöntemleri, kullanıcı mahremiyetini ciddi şekilde tehdit etmektedir. Konuyla ilgili birkaç öneri paylaşılabilir:

- IoT cihazlarının güvenlik ve gizlilik ilkeleri için evrensel standartlar oluşturulmalı ve üreticilerin bu kurallara yasal zorunlulukla uyması sağlanmalıdır.
- Güvenlik açıklarını kapatmak amacıyla cihazlara otomatik yazılım güncellemeleri yapılmalı, üreticiler ürünleri için düzenli destek vermekten sorumlu tutulmalıdır.
- Kullanıcı verileri hem cihaz üzerinde hem de bulut ortamında şifrelenmeli, ayrıca kişisel bilgilerin gizliliği için anonimleştirme yöntemleri kullanılmalıdır.
- Yeni akıllı ev sistemleri piyasaya sürülmeden önce, olası güvenlik risklerine karşı test edilmeli, zayıflıklar belirlenip giderilmelidir.
- Akıllı ev çözümleri, yangın, gaz sızıntısı veya su taşkını gibi acil durumlara kendi kendine müdahale edebilecek şekilde tasarlanmalı, böylece insan müdahalesine gerek kalmadan güvenlik sağlanmalıdır.

KAYNAKÇA

Aarika, K., Bouhlal, M., Abdelouahid, R. A., Elfilali, S. ve Benlahmar, E. (2020). Perception layer security in the Internet of Things. *Procedia Computer Science*, *175*, 591–596.

Abdullah, T. A., Ali, W., Malebary, S. ve Ahmed, A. A. (2019). A review of cybersecurity challenges, attacks and solutions for Internet of Things based smart home. *International Journal of Computer Science and Network Security*, *19*(9), 139–146.

Adat, V. ve Gupta, B. B. (2018). Security in Internet of Things: Issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*(3), 423–441.

Akanksha, E., Debnath, A. ve Dey, B. (2021). *Extensive review of cloud-based Internet of Things architecture and current trends*. Proceedings of the IEEE 6th International Conference on Inventive Computation Technologies.

Ali, B. ve Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors*, *18*(3), 817.

Amadeo, M., Campolo, C., Iera, A. ve Molinaro, A. (2015). *Information centric networking in IoT scenarios: The case of a smart home*. Proceedings of the 2015 International Conference on Communications.

Anzelmo, E., Bassi, A., Caprio, D., Dodson, S. ve van Kranenburg, R. (2011, 26-28 Ekim). *Internet of Things*, Discussion/position paper prepared for the 1st Berlin Symposium on Internet and Society. Institute for Internet and Society, Berlin.

Arora, A., Kaur, A., Bhushan, B. ve Saini, H. (2019). *Security concerns and future trends of Internet of Things*. Proceedings of the 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies.

Arunvivek, J., Srinath, S. ve Balamurugan, M. S. (2015). Framework development in home automation to provide control and security for home automated devices. *Indian Journal of Science and Technology*, *8*(19), 14-17.

Assim, M. ve Al-Omary, A. (2020). *Design and implementation of smart home using WSN and IoT technologies*. 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies.

Atzori, L., Iera, A. ve Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.

Balkan, N. ve Yılmaz, S. (2021). A simulation-assisted approach for IoT-based smart home automation systems. *Balkan Journal of Electrical and Computer Engineering*, *9*(3), 245–256.

Bourobou, S. T. M. ve Yoo, Y. (2015). User activity recognition in smart homes using pattern clustering applied to temporal ANN algorithm. *Sensors*, *15*(5), 11953–11971.

Brauchli, A. ve Li, D. (2015). *A solution-based analysis of attack vectors on smart home systems.* Proceedings of the International Conference on Cyber Security for Smart Cities, Industrial Control Systems and Communications.

Broenink, G., Hoepman, J. H., Hof, C. V. T., Van Kranenburg, R., Smits, D., and Wisman, T. (2010). The privacy coach: Supporting customer privacy in the internet of things. *arXiv preprint arXiv:1001.4459, 7-9*.

Camphouse, A. ve Ngalamou, L. (2019). *Securing a connected home*. Proceedings of the IEEE 10th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, Columbia University, New York.

Cebrat, G. (2014). *Secure web-based home automation: Application layer-based security using embedded programmable logic controller*. Proceedings of the 2014 2nd International Conference on Information and Communication Technology.

Chan, M., Estève, D., Escriba, C. ve Campo, E. (2008). A review of smart homes: Present state and future challenges. *Computer Methods and Programs in Biomedicine*, *91*(1), 55–81.

Chernyshev, M., Baig, Z., Bello, O. ve Zeadally, S. (2018). Internet of Things (IoT): Research, simulators, and testbeds. *IEEE Internet of Things Journal*, *5*(3), 1637–1647.

Cho, H., Ji, J., Chen, Z., Park, H. ve Lee, W. (2015). Measuring distance between things with improved accuracy. *Procedia Computer Science*, *52*, 1083–1088.

Daş, R., Tuna, A., Demirel, S. ve Yurdakul, M. K. (2017). A survey on the Internet of Things solutions for the elderly and disabled: Applications, prospects, and challenges. *International Journal of Computer Networks and Applications*, *4*(3), 84–92.

Daş, R., Tuna, G. ve Tuna, A. (2015). Design and implementation of a smart home for the elderly and disabled. *International Journal of Computer Networks and Applications*, *2*(6), 242–246.

Datta, S. K. (2016). *Towards securing discovery services on the Internet of Things*. Proceedings of the 2016 International Conference on Consumer Electronics.

Davis, B. D., Mason, J. C. ve Anwar, M. (2020). Vulnerability studies and security postures of IoT devices: A smart home case study. *Internet of Things Journal*, *7*(10), 10102–10110.

Devalal, S. ve Karthikeyan, A. (2018, 29-31 Mart). *LoRa technology – an overview*. Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology. RVS Technical Campus, Coimbatore, India.

Duan, X., Ge, M., Le, T. H. M., Ullah, F., Gao, S., Lu, X. ve Babar, M. A. (2021). Automated security assessment for the Internet of Things. *Proceedings of the 2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing*.

Džaferovic, E., Sokol, A., Almisreb, A. A. ve Norzeli, S. M. (2019). Dos and DDoS vulnerability of IoT: A review. *Sustainable Engineering and Innovation*, *1*(1), 43–48.

Eleyan, A. ve Fallon, J. (2020). IoT-based home automation using Android application. *Proceedings of the 2020 International Symposium on Networks, Computers and Communications*.

Ghirardello, K., Maple, C., Ng, D. ve Kearney, P. (2018). Cybersecurity of smart homes: Development of a reference architecture for attack surface analysis. *Proceedings of Living on the Internet of Things: Cybersecurity of the IoT*.

Gordon, H., Park, C., Tushir, B., Liu, Y. ve Dezfouli, B. (2021). An efficient SDN architecture for smart home security accelerated by FPGA. *Proceedings of the International Symposium on Local and Metropolitan Area Networks*.

Gunawan, T. S., Yaldi, I. R. H., Kartiwi, M. ve Mansor, H. (2018). Performance evaluation of smart home system using Internet of Things. *International Journal of Electrical and Computer Engineering*, *8*(1), 400–411.

Güneş, H., Bıçakcı, S., Orta, E. ve Akdaş, D. (2019). Akıllı evlerde kullanılan yapay zeka teknikleri için simülasyon geliştirilmesi. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, *7*(3), 554–563.

Hall, F., Maglaras, L., Aivaliotis, T., Xagoraris, L. ve Kantzavelou, I. (2020). Smart homes: Security challenges and privacy concerns. *arXiv preprint arXiv:2010.15394,* 3-4.

Hasibuan, A., Mustadi, M., Syamsuddin, I. E. Y. ve Rosidi, I. M. A. (2015). Design and implementation of modular home automation based on wireless network, REST API, and WebSocket. *Proceedings of the 2015 International Symposium on Intelligent Signal Processing and Communication Systems*.

Heartfield, R., Loukas, G. ve Gan, D. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, *78*, 398–428.

Hejazi, H., Rajab, H., Cinkler, T. ve Lengyel, L. (2018). *Survey of platforms for massive IoT.* Proceedings of the 2018 IEEE International Conference on Future IoT Technologies.

Jabbar, W. A., Alsibai, M. H., Amran, N. S. S. ve Mahayadin, S. K. (2018). Automation system for smart home. *Proceedings of the 2018 International Symposium on Networks, Computers and Communications*.

Jacobsson, A., Boldt, M. ve Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733.

Jiang, T., Yang, M. ve Zhang, Y. (2015). Research and implementation of M2M smart home and security system. *Security and Communication Networks*, *8*(16), 2704–2711.

Jiang, Y., Liu, X. ve Lian, S. (2016). Design and implementation of smart-home monitoring system with the Internet of Technology. *Wireless Communications, Networking and Applications*, 473–484.

Jyothi, V., Krishna, M. G., Raveendranadh, B. ve Rupalin, D. (2017). IoT based smart home system technologies. *International Journal of Engineering Research and Development*, *13*(2), 31–37.

Kailas, A., Cecchi, V. ve Mukherjee, A. (2012). A survey of contemporary technologies for smart home energy management. M. S. Obaidat (Ed.), *Handbook of Green Information and Communication Systems* içinde (s. 35–56). Pinguin Yayınevi.

Karampogias, A. (2021). *Internet of Things and smart homes: Cybersecurity and personal data protection in a fragile environment* [Yüksek lisans tezi]. University of Piraeus.

Kim, J. (2021). *Cloud Internet of Things for the smart environment of a smart city* [Yüksek lisans tezi]. California State University.

Kishore, R., Vigneshwari, U. R., Prabagarane, N., Savarimuthu, K. ve Radha, S. (2020). *IoT-based intelligent control system for smart building*. Proceedings of the International Conference on Innovative Intelligence and Informatics Computing Technologies.

Koçyiğit, Y. ve Şine, O. (2020). İnternet üzerinden kontrol edilen tam otomasyonlu akıllı ev sistemleri için örnek bir uygulama. *DUMF Mühendislik Dergisi*, *11*(2), 521–532.

Kopetz, H. (2011). Internet of Things. *Real-Time Systems,* 307–323.

Kramp, T., Van Kranenburg, R. ve Lange, S. (2013). Introduction to the Internet of Things. *Enabling Things to Talk,* 1–10.

Krishna, B. V. S. ve Gnanasekaran, T. (2017). *A systematic study of security issues in the Internet-of-Things (IoT).* Proceedings of the 2017 International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud.

Li, F., et al. (2012). Research on sensor-gateway-terminal security mechanism of smart home based on IoT. *Internet of Things, Communications in Computer and Information Science,* 415–422.

Lin, H. ve Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information*, *7*(3), 44.

Lu, Y. ve Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. *Internet of Things Journal*, *6*(2), 2103–2115.

Madakam, S. (2015). Internet of things: Smart things. *International Journal of Future Computer and Communication*, *4*(4), 250–253.

Malche, T. ve Maheshwary, P. (2017*). Internet of Things (IoT) for building smart home system.* Proceedings of the 2017 International Conference on I-SMAC.

McIlroy, S., Ali, N. ve Hassan, A. E. (2016). Fresh apps: An empirical study of frequently updated mobile apps in the Google Play store. *Empirical Software Engineering*, *21*(3), 1346–1370.

Meng, Y., Zhang, W., Zhu, H. ve Shen, X. S. (2018). Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. *IEEE Wireless Communications*, *25*(6), 53–59.

Mocrii, D., Chen, Y. ve Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, *1–2*, 81–98.

Öztürk, A. ve Sepanta, N. (2017). Akıllı ev sistemlerinde kullanılan yöntemlerin farklılıkarı, avantajları ve dezavantajları. *İstanbul Aydın Üniversitesi Dergisi*, *9*(4), 115–125.

Patru, I. I., Carabaş, M., Bărbulescu, M. ve Gheorghe, L. (2016). *Smart home IoT system.* Proceedings of the RoEduNet International Conference.

Pattanasri, T. (2018). Mandatory data breach notification and hacking the smart home: A legal response to cybersecurity. *QUT Law Review*, *18*, 268–289.

Pranathi, K., Kranthi, S., Srisaila, A. ve Madhavilatha, P. (2018). *Attacks on web applications caused by cross-site scripting.* Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology.

Rodríguez, G. E., Torres, J. G., Flores, P. ve Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. *Computer Networks*, 166. https://doi.org/10.1016/j.comnet.2019.106960

Saeed, F., Paul, A., Rehman, A., Hong, W. H. ve Seo, H. (2018). IoT-based intelligent modeling of smart home environment for fire prevention and safety. *Sensor and Actuator Networks*, *10*(2), 45–59.

Saxena, U., Sodhi, J. ve Singh, Y. (2020). *An analysis of DDoS attacks in smart home networks.* Proceedings of the 10th International Conference on Cloud Computing, Data Science and Engineering.

Sethi, P. ve Sarangi, S. R. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 9(15), 15-16.

Siddhanti, P., Asprion, P. M. ve Schneider, B. (2019). *Cybersecurity by design for smart home environments.* Proceedings of the 21st International Conference on Enterprise Information Systems.

Singh, H., Pallagani, V., Khandelwal, V. ve Venkanna, U. (2018). *IoT based smart home automation system using sensor node.* Proceedings of the 4th IEEE International Conference on Recent Advances in Information Technology.

Singh, S., Ra, I.-H., Meng, W., Kaur, M. ve Cho, G. H. (2019). SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology. *International Journal of Distributed Sensor Networks*, *15*(4), 40-42.

Sivagami, P., Jamunarani, D., Abirami, P., Pushpavalli, M., Geetha, V. ve Harikrishnan, R. (2021). *Smart home automation system methodologies: A review.*

Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks.

Somasundaram, K. ve Selvam, K. (2018). IoT–attacks and challenges. *International Journal of Engineering and Technology Research*, *8*(9), 9–12.

Stojkoska, B. L. R. ve Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, *140*, 1454–1464.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. ve Markakis, E. K. (2020). A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys ve Tutorials*, *22*(2), 1191–1221.

Tuna, G. ve Daş, R. (2015). Wireless sensor network-based health monitoring system for the elderly and disabled. *International Journal of Computer Networks and Applications*, *2*(6), 247–253.

Vlajic, N. ve Zhou, D. (2018). IoT as a land of opportunity for DDoS hackers. *Computer*, *51*(7), 26–34.

Weiser, M. (1993). Some computer science issues in ubiquitous computing. *Communications of the ACM*, *36*(7), 75–84.

Wolf, G. (2010). The data-driven life. *The New York Times Magazine, 38,* 34-36.

Yalcinkaya, F., Aydilek, H., Erteen, M. Y. ve Nihat, I. (2020). IoT-based smart home testbed using MQTT communication protocol. *Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi*, *12*(3), 317–324.

Zeng, E., Mare, S. ve Roesner, F. (2017). End user security and privacy concerns with smart homes. *Proceedings of the 13th Symposium on Usable Privacy and Security*, Paul G. Allen School of Computer Science and Engineering University of Washington, Washington.

Zhang, G., Yan, C., Ji, X., Zhang, T. ve Zhang, T. (2017, 30 Ekim). *DolphinAttack: Inaudible voice commands.* Proceedings of the ACM SIGSAC Conference on Computer and Communications Security.

Zhang, W., Li, G. ve Gao, W. (2015). *The embedded smart home control system based on GPRS and Zigbee*. MATEC Web of Conferences.

İnternet Kaynağı

Ashton, K. (2009, 22 Haziran). *That "Internet of Things" Thing: In the real world, things matter more than ideas.* 02 Aralık 2025 tarihinde https://www.rfidjournal.com/articles/view?4986 adresinden edinilmiştir.

Bassi, A. ve Anderson, S. (2011, 22 Nisan). *We need a killer business model.* 18 Ağustos 2011 tarihinde www.theinternetofthings.eu/content/alessandro-bassi-interviewed-stig-andersen-we-need-killer-business-model adresinden edinilmiştir.

Cisa (2018, 23 Mayıs). *VPNFilter destructive malware – alert.* 23 Mayıs 2018 tarihinde https://www.cisa.gov/news-events/alerts/2018/05/23/vpnfilter-destructive-malware adresinden edinilmiştir.

Ericsson (2024, 19 Ocak). *IoT connections outlook – mobility report.* 15 Haziran 2025 tarihinde https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook adresinden edinilmiştir.

European Commission. (2009, 18 Haziran). Internet of Things — An action plan for Europe. 02 Aralık 2025 tarihinde https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF adresinden edinilmiştir.

Exchange Xforce IBMcloud (2020, 23 Haziran). *Ripple20 vulnerabilities explained.* 20 Temmuz 2020 tarihinde https://exchange.xforce.ibmcloud.com/collection/IoT-Devices-Affected-by-Ripple20-Vulnerabilities-90de8ab55f20a72ccb695270d3b0957c adresinden edinilmiştir.

IoT Analytics (2024, 9 Temmuz). *Global IoT market size grew 22% in 2021 – Factors affecting growth to 2027.* 28 Nisan 2025 tarihinde https://iot-analytics.com/iot-market-size/ adresinden edinilmiştir.

IoT Analytics (2025, 09 Şubat). *Number of connected IoT devices.* 10 Mart 2025 tarihinde https://iot-analytics.com/number-connected-iot-devices/ adresinden edinilmiştir.

Science Direct (2025, 10 Haziran). *Internet of Things Journal article.* 20 Haziran 2025 tarihinde https://www.sciencedirect.com/science/article/pii/S1877050925019209 adresinden edinilmiştir.

Secure List (2020, 29 Nisan). *Remote Spring: Rise of RDP brute-force attacks.* 15 Ağustos 2023 tarihinde https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/ adresinden edinilmiştir.

Sonic Wall (2022, 15 Şubat). *Cyber Threat Report 2022.* 22 Şubat 2022 tarihinde https://www.sonicwall.com/resources/videos/exclusive-2022-sonicwall-cyber-threat-report adresinden edinilmiştir.

Statista (2024, 16 Eylül). *Smart homes – statistics & facts.* 05 Haziran 2025 tarihinde https://www.statista.com/topics/2430/smart-homes/ adresinden edinilmiştir.

UK SagePub (2012, 28 Ocak). *Publishing Journal Articles.* 28 Nisan 2019 tarihinde https://uk.sagepub.com/en-gb/asi/publishing-journal-articles/book236083 adresinden edinilmiştir.

Usenix (2017, 12-14 Temmuz). *SOUPS 2017 technical session presentation.* 12 Temmuz 2017 tarihinde https://www.usenix.org/search/site/SOUPS%25202017%2520technical%2520session%2520presentation adresinden edinilmiştir.

TOPLUMSAL KATKI

Bu çalışma; IoT tabanlı akıllı ev sistemlerinde kullanıcı gizliliği ve siber güvenlik risklerini bütüncül bir çerçevede ele alarak toplumsal düzeyde güvenli, kapsayıcı ve sürdürülebilir bir dijital yaşam kültürüne katkı sunmayı amaçlamaktadır. İnternete bağlı cihazların yaygınlaşması; kişisel verilerin ifşası, hizmet kesintileri ve fiziksel tehlikelere varan sonuçlar doğurabilen saldırı yüzeyini büyütmektedir. Bu bağlamda, araştırma bulgularının odağı, bireylerin mahremiyetini koruyan ve ev içi güvenliği artıran tasarım ve yönetişim ilkelerinin ortaya konmasıdır.

Toplumsal Sorun ve Etkileri: Akıllı evlerdeki güvenlik zafiyetleri; hane güvenliği, ekonomik kayıplar ve psikososyal güven duygusu üzerinde olumsuz etkilere yol açabilmektedir. Özellikle yaşlılar ve özel gereksinimli bireyler için güvenilirlik hayati önemdedir. Çalışma; tehdit tipolojilerini, saldırı vektörlerini ve bunlara karşı uygulanabilecek önlemleri sistematik olarak derleyerek bu sorun alanını görünür kılmaktadır.

Araştırmanın Katkısı: Tez, akıllı evlerin teorik temelleri, tarihsel gelişimi ve teknolojik bileşenleri ile birlikte siber güvenlik ve gizlilik standartlarını, hakları ve en iyi uygulamaları derlemektedir. Bu derleme; geliştiriciler, politika yapıcılar ve son kullanıcılar için uygulanabilir bir referans çerçevesi sağlar; güvenli yazılım güncellemeleri, şifreleme, kimlik doğrulama ve bilinçlendirme gibi önlemlerin toplumsal faydasını somutlaştırır.

Topluma Sağlanacak Somut Faydalar: (i) Kullanıcı farkındalığının artması ve sosyal mühendislik saldırılarına karşı direnç, (ii) üreticilerin güvenlik güncellemelerini ve standart uyumunu öncelemesiyle hanelerde riskin azalması, (iii) acil durumlara (yangın, gaz kaçağı vd.) otonom tepki verebilen güvenli akıllı sistemlerle can ve mal kayıplarının azaltılması, (iv) veri güvenliği sayesinde kamu güveninin güçlenmesi.

Uygulama ve Yaygınlaştırma: Araştırma çıktıları; ulusal/uluslararası güvenlik standartlarının benimsenmesi, cihaz ve ağ seviyesinde uçtan uca şifreleme, otomatik ve süreklilik arz eden yazılım güncellemeleri, ev ağlarında ayrı misafir ağları kurgulanması, kullanıcı eğitim programları ile politika önerilerine dönüştürülebilir. Üniversite-sanayi-kamu iş birliği ile hazırlanacak rehberler ve test protokolleri, yeni ürünlerin piyasaya çıkmadan önce güvenlik doğrulamasını mümkün kılar.

Orta-Uzun Vadeli Etki: Standart uyumunun artması ve iyi uygulamaların yaygınlaşması; ev içi güvenlik göstergelerinde iyileşmeye, kritik olay ve kayıplarda düşüşe, veri ihlali vakalarının azalmasına katkıda bulunacaktır. Böylelikle, akıllı ev teknolojileri toplumsal refahı destekleyen güvenilir bir altyapı olarak konumlanacaktır.

Özetle, bu tez; akıllı ev ekosisteminde güvenlik ve mahremiyet için ölçülebilir, uygulanabilir ve ölçeklenebilir bir yol haritası sunarak bireylerin ve toplumun dijital çağda güven içinde yaşamasına katkıda bulunmaktadır.