Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 34, S. 226-233, Mart 2022

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 34, pp. 226-233, March 2022

Research Article

Akıllı Evlerde IoT Teknolojileri ve Siber Güvenlik

İsa Avcı[1*]

[1*] Karabuk Üniversitesi, Mühendislik Fakültesi, Bilgisayar Bölümü, İstanbul, Türkiye, (ORCID: 0000-0001-7032-8018), isaavci@karabuk.edu.tr

(2nd International Conference on Applied Engineering and Natural Sciences ICAENS 2022, March 10-13, 2022)

(**DOI:** 10.31590/ejosat.1080228)

ATIF/REFERENCE: Avcı, İ. (2022). Akıllı Evlerde IoT Teknolojileri ve Siber Güvenlik. *Avrupa Bilim ve Teknoloji Dergisi*, (34), 226-233.

Öz

Teknolojinin hızlı gelişmesiyle insanların kullanımına birçok akıllı cihazlar sunulmuştur. Akıllı cihazlar Nesnelerin İnterneti (IoT) birlikte akıllı evlerdeki cihazların akıllı hale gelmesi ile akıllı ev konsepti oluşmuştur. Akıllı evlerdeki cihazları kullanan kullanıcıların bu konudaki eksikliklerinden dolayı hırsızların, bilgisayar korsanlarının ya da kötü niyetli diğer kullanıcıların saldırıları giderek artmaktadır. IoT teknolojileri çevremizde bulunan fiziksel olayları kontrol etmemizi, onları takip, analiz etmemizi sağlayan cihaz, yazılım ve erişim hizmetlerini kapsayan bir iletişim ağıdır. Teknolojinin hızla geliştiği, internet kullanımının yaygınlaştığı, ayrıca yaşam şartlarının ortaya çıkardığı ihtiyaçlar dolayısı ile IoT' ye olan ilgi her geçen gün artmaktadır. IoT artık hayatımızın her alanında yaygın bir şekilde kullanılan ve duyduğumuz bir kavram olmuştur. Akıllı sistemler olarak da bilinen IoT uygulamaları akıllı şebeke, akıllı şehir, akıllı ev, akıllı sağlık, akıllı çevre ve buna benzer birçok alanda kullanılmaktadır. Bu çalışmada, akıllı ev ve özellikleri, akıllı evlerde kullanılan IoT teknolojileri ve IoT güvenlik katmanları incelenmiştir. Akıllı evlerde kullanılan IoT cihazlarının ve uygulamalarının siber güvenlik açısından yaşanan sorunlar, siber saldırılar, güvenlik açıklıkları ve güvenlik açısından korunabilmek için alınması gereken önlemler incelenmiştir. Ayrıca yaşanan güvenlik sorunları siber güvenlik açısından değerlendirilerek çözüm yolları önerilmiştir.

Anahtar Kelimeler: Akıllı Ev, Nesnelerin İnterneti, Siber Güvenlik.

IoT Technologies and Cyber Security in Smart Homes

Abstract

With the rapid development of technology, many smart devices have been offered to people's use. Smart devices the concept of smart home has emerged with the Internet of Things (IoT) making smart devices in smart homes. The attacks of thieves, hackers, or other malicious users are increasing due to the shortcomings of users using devices in smart homes. IoT technologies are a communication network that includes devices, software, and access services that enable us to control, monitor, and analyze physical events in our environment. The interest in IoT is increasing day by day due to the rapid development of technology, the widespread use of the internet, and the needs of living conditions. IoT has now become a concept that is widely used and heard in every aspect of our lives. IoT applications, also known as smart systems, are used in smart grids, smart cities, smart homes, smart health, smart environment, and many similar areas. In this study, the smart home and its features, IoT technologies used in smart homes, and IoT security layers are examined. The precautions to be taken to protect the IoT devices and applications used in smart homes in terms of cyber security, cyber attacks, security vulnerabilities, and security are examined. In addition, security problems were evaluated in terms of cyber security, and solutions were suggested.

Keywords: Smart Home, Internet of Things, Cyber Security.

[*] Sorumlu Yazar: isaavci@karabuk.edu.tr

1. Giriş

Bu ünümüzde hayatımızı daha kolay yaşanabilir hale getirebilmek için teknoloji her geçen gün gelişmektedir. Gelişen teknolojiyle beraber Nesnelerin interneti (IoT) her birey tarafından bilinen bir kavram haline gelmiş, hayatımızın bir alanında yer verilmiştir. Akıllı telefonlar, Akıllı cihazlar ve akıllı bir dünya IoT' un akıllı vizyonudur. Amaç, günlük yaşantımızın ana hususu olup, kullanıcının davranış ve istekleri doğrultusunda gelişmesidir. Nesnelerin interneti 1999 yılında IoT bir radyo frekansı ile tanımlama teknolojisinde Kevin Ashton tarafından ilk kez kullanılmıştır (Asthon, 2009). 1991 yılında ilk IoT uygulaması, Cambridge Üniversitesi'ndeki bir grup akademisyen tarafından kameralı bir sistem ile bir kahve makinasının görüntülerinin internet üzerinden paylaşılarak uzaktan izlenmesi ile kullanılmaya başlamıştır (López-de-Armentia et al., 2012). Akıllı ev kavramı ise günümüzde kullanımı artırmakta olup her geçen gün hayatımıza daha çok girmeye başlamıştır. Akıllı ev sistemleri ise insan hayatının günlük yaşantısına çeşitli hizmetler sunarak, yaşamımıza kolaylıklar sağlayan, hayat kalitemizi artıran ve uzaktan kontrol gibi konularda evlerimizde bize çeşitli faydalar sunan bir teknolojidir. Tomaş yapmış olduğu çalışmada, akıllı ev çeşitlerinden hangileri günümüzde uygulanmakta ve bunlara örnek olan birkaç ev örneği incelemesi ele alınmış, akıllı ev üreticileri, tasarımcıları, teknik yetkililer ile görüşmeler yapılmış ve bu sonuçlar doğrultusunda akıllı evlerin zayıf güçlü fırsat tehdit yönleri SWOT analizi yöntemi ile ele alınması gerektiğini belirtmiştir (Tomaş, 2019). Akıllı ev otomasyonu sisteminde kullanılan tüm cihazlar birbirleriyle kablosuz ağlar veya kablosuz sensör ağlar yardımıyla haberleşmektedir. Bu haberleşmenin gerçekleşmesi için Makine-To-Makine (M2M) uygulama tabanlı bir akıllı ev ve güvenlik sistemi kurulmaktadır (Jiang et al., 2021).

Kullanıcı uygulama ile uzaktan kablosuz bir şekilde ev sistemine giriş yapmakta, evdeki elektrik, su, sıcaklık, hareket algılama vs. gibi birçok alanda uzaktan kontrollerini sağlayıp güncellemeler yapabilmektedir (Ozkaya vd, 2018). IoT sayesinde ev ortamında kullanılan cihazların durumları bildirilmekte ve kullanılmayan cihazlar otomatik olarak kapatılabilmesi durumu kurulan sistemler sayesinde elektrik, su tasarrufunda verimliliği de artırılmaktadır (Gökrem ve Bozuklu, 2016). Ayrıca Blynk sisteminin sunduğu bulut hizmeti sistem ile ilgili verileri depolama imkânı sunar ve veriler ile cihaz ile haberleşme sağlayarak cihazın çalışması durması işlemi gerçekleşir (Taştan, 2019). Akıllı ev sistemleri; ışık kaynakları, aydınlatma kontrolü, soğutma sistemlerin, havalandırma, ısıtma, panjur, sensör ve detektörler, alarmlar, kamera, gaz kontrolü vs. gibi araçlar üzerindeki sistemler ve kullanılan teknolojileri kapsamaktadır (Şahinoğlu, 2006). Bir başka çalışmada ise akıllı mutfak çalışmaları, günümüz teknolojisi ve insan gereksinimleri doğrultusunda, mutfağın ve mutfakta bulunan materyallerin uzaktan erişilerek kontrol edilebilmesini sağlamak ve akıllı sistemlere ek çeşitli sistemler ile konforu artırmak gibi birçok amaçlarla yapılmıştır (Küçük ve Ekren, 2020). Özdemir ve arkadaşlarının yapmış olduğu başka bir çalışmada ise, akıllı ev sistemleri teknolojisinin henüz yeni bir teknoloji olduğu, kullanım oranının hızla arttığı ve yaygınlaştığı belirtilmektedir. IoT cihaz sayısının 2030 yılında 50 milyara ulaşacağı göz önünde bulundurulduğunda gelecekte güvenlik zafiyetlerinin çok ciddi problemlere yol açacağı kaçınılmaz bir gerçektedir. Bununla ilgili olarak üretici, kullanıcı ve devletlerin tedbir almaları ve çözüm üretmeleri gerekmektedir (Özdemir, 2019). Ayrıca günümüzde siber saldırılar her geçen gün arttıkça IoT cihazları için güvenlik ve önlemlerinin alınması gerekmektedir. Böylece, internet ağı üzerinden gelebilecek olası saldırılardan korunmak üzere özellikle VPN kullanımı tercih edilmektedir. OpenVPN noktadan noktaya bağlantı kurduğu ve gönderilen veriler şifrelendiği için kullanılmaktadır (Kalyoncu ve Turan, 2020).

Simülasyon yardımı ile ise bir akıllı evde planlanan ve yapılması gereken işlemlerin simülasyon ile test edilmesi ve olağan durumlara karşı önceden önlemler alınabilmesi hakkına yapılan araştırmalarda ise Orta ve arkadaşları tarafından yapılan çalışmada; Simülasyon ile gerçekleştirilen çalışmada, gelecekte akıllı evlere eklenecek yeniliklerin testleri gerçekleştirilmeden simülasyon üzerinde test edilebilir, doğruları yanlışları ölçülür ve hayata geçirilebilir (Tomaş ve Dostoğlu, 2020). Ayrıca buna ek olarak Özdoğan ve arkadaşlarının yapmış olduğu çalışmada ise; IoT' u geliştirirken simülasyon yazılımı ile çalışılması gereksiz zaman kaybında önleyeceği sonuçlarına varılmıştır (Özdoğan ve Daş, 2021). Özçekiç' in yapmış olduğu çalışmada ise "Akıllı Evlerde Kullanılan Teknolojiler" incelenmiş, teknolojiler arası karşılaştırmalar yapılmış, Ev içindeki cihazların haberleşmesi için HomeRF, noktadan noktaya haberleşme için Bluetooth, az masraf yaparak UPnP yöntemiyle ise X-10 sistemlerini ya da daha az masraf ile SMS yöntemini kullanmak gerekmektedir (Özçekiç, 2005). Bu çalışmada akıllı ev ve IoT, akıllı evlerin özellikleri, akıllı evler alınacak güvenlik sorunları ve önlemleri konuları detaylı olarak incelenecektir.

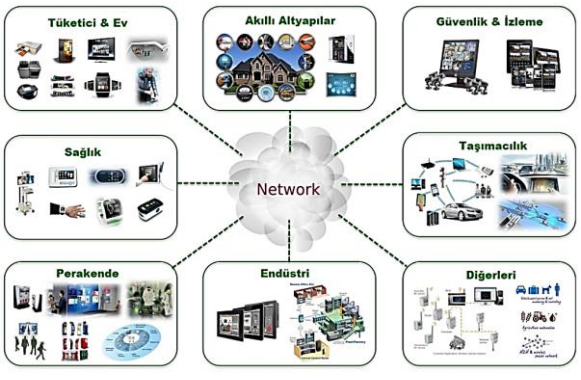
2. Akıllı Ev ve IoT

2.1. Nesnelerin İnterneti (IoT)

Nesnelerin İnterneti (IoT) ifadesi fiziksel cihazların internet üzerinden dünyayla bağlantısını temsil etmektedir (Gokhale et al., 2019). Nesnelerin interneti kavramının içerisine sadece telefonlar, televizyonlar, buzdolapları değil internet üzerinden veri paylaşımı yapabilecek kabiliyete sahip, en az 1 sensör bulunan ve tekil bir isme sahip bütün fiziksel yapılar dahil edilebilir. Bu özelliklere sahip fiziksel cihazlar kendi aralarında veya internet üzerinden bir ekosistem oluşturarak veri alışverişinde bulunabilir.

2.2. Nesnelerin İnterneti Uygulama Alanları

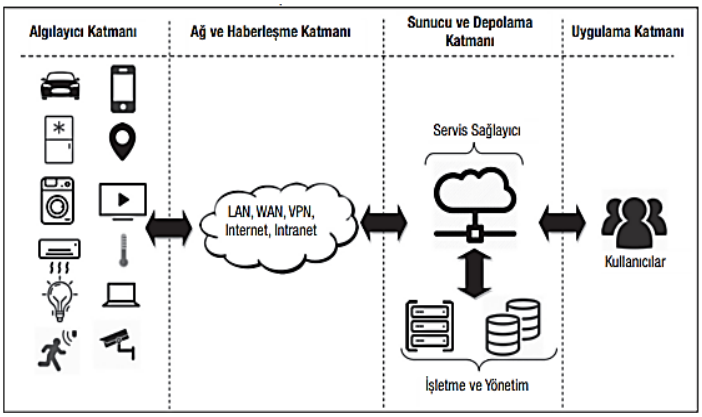
İnternet ve mobil cihaz teknolojisinin hızla gelişmesi ve her yere uygum sağlayabilme kabiliyeti sayesinde nesnelerin interneti de hayatımız içerisinde çok fazla uygulama alanına sahip olmuştur. Bu şekilde hızlı bir uygulama kabiliyetine sahip olan nesnelerin interneti akıllı ev, akıllı şehir, akıllı park, akıllı sokak, akıllı tarım, akıllı hayvancılık, akıllı tedarik uygulamaları, akıllı sağlık hizmetleri, akıllı mağazalar, akıllı askeri kullanımı gibi birçok alanda yaygın bir kullanıma sahiptir (Innova, 2022).



Şekil 1. IoT Kullanım Alanları (Innova, 2022).

2.3. IoT Katmanları

IoT katmanları algılayıcılar, ağ ve haberleşme, sunucu ve depolama ve uygulama katmanı olmak üzere genel olarak dört katmandan oluşmaktadır. Ağ ve haberleşme sayesinde tüm kullanıcılar ve sistemler arasında iletişim sağlanmaktadır.



Şekil 2. IoT Katmanları (Zeybek ve Yılmaz, 2019).

2.4. Akıllı Ev

"Akıl Ev" fikri ilk 1980'lerin başlarında ABD'de ortaya çıkmış olup, ilk defa ise şu ifadeler ile tanımlanmıştır. "Akıllı bina, kullanıcıların performansını, ilk yatırım, işletme maliyetlerinde tasarrufu arttırmak, esnekliği maksimuma çıkarmak ve kaynakları koordinasyonlu bir şekilde verimli olarak yönetmek için çeşitli sistemlere entegre eden binalara verilen isimdir." Türkiye'deki ilk uygulama örneği ise 1984 yılında yapılmıştır (Soumyalatha, 2016).

Akıllı evlerde de çokça adından söz ettiren IoT birçok cihazın internet aracılığı ile birbiri ile haberleşmesidir. Akıllı evler ise IoT teknolojisinin en önde gelen örneklerindendir. Akıllı ev, IoT teknolojileri vasıtası ile ev sahiplerinin ihtiyaçlarına yardımcı olan, onların hayatlarını kolaylıklar sağlayan ve daha konforlu, rahat, güvenli ve daha tasarruflu bir yaşam imkânı sunan evlere verilen isimdir. Akıllı evler, sistemleri ve otomatik işlevselliği ile kullanıcılar tarafından kontrol edilebilen, yönetilebilen cihazları kapsar.

Şekil 3. Akıllı Ev Konsepti (Soumyalatha, 2016).

2.5. Akıllı Ev Çeşitleri

Akıllı evler geçmişten günümüze her geçen gün gelişmekte olup teknolojinin ilerlemesi ile sürekli yenilenebilmektedir. Geçmişten günümüze akıllı evleri inceleyecek olursak;

2.5.1. Uzaktan kumanda ile Kontrol Edilebilen Evler

Uzaktan kumanda ile kontrol edilebilir evler, herhangi bir Ana kontrol ünitesi olmayan, sistemi kumanda ile yönetilen evlerden oluşmaktadır.

2.5.2. Programlanabilir Evler

Programlanabilir evlerin gelişimi ile sistemi uzaktan kumanda ile kontrol edilebilen evlerin yanına bir zamana bağlı programlanabilme özelliği de eklenmiştir.

2.5.3. Senaryolandırılmış Evler

Sistem uzaktan kumanda ile kontrol edilebilen ve bir zamana bağlı programlanabilir evlerin özelliklerini içermektedir. Bunların yanında ana kontrol ünitesi, yani akıllı ev sisteminin modüller ve sensörler bulunmaktadır. Bu sisteme senaryolar girilerek sistemin çalışması beklenmektedir.

2.5.4. Yapay Zekaya Sahip Evler

Yapay zekaya sahip akıllı evlerin çıkması ile senaryolaştırılmış akıllı evlerde geri planda kalmıştır. Çünkü bu akıllı evlerde, senaryolar insanlar tarafından belirlenirken, yapay zekaya sahip evlerin, öğrenme yetenekleri vardır. Kullanıcılarını bir süre izleyip, tekrar eden hareketlerini analiz edip kullanıcılarının tepkilerine göre gerçekleştirilecek olan komutu ya da komutları devreye sokmaktadır.

2.6. Akıllı Evlerin Özellikleri

Akıllı evler kişinin ihtiyaçları doğrultusunda onların ihtiyaçlarını giderecek ve hayatlarını kolaylaştıracak sistemlerden oluşmaktadır. Bu sistemler tek bir noktadan kontrol edilebilmesiyle birlikte programlama özelliğiyle bu kontrolleri kendisi tarafından da sağlayabilmektedir.

2.6.1. Duman Sensörü

Detektörler sayesinde gaz kaçağı durumunda uyarı veren, evi yangına karşı koruyan ve haberdar eden sistemdir. Siren sistemi, eve habersiz birinin girmesi, hırsızlık durumlarında ve gaz kaçağı olduğunda siren çalarak çevredeki insanları ve ev sahibini haberdar eden sistemdir. Su baskını sensörü evi, su basmalarına karşı koruyan ve uyarı sistemi ile elle ya da otomatik olarak vanaları kapatan sistemdir.

2.6.2. Kapı Giriş Kontrolü

Belirlenen mekanlara girişi şifre kontrolü ile gerçekleştirir ve kart okutarak giriş yapılabilir. Manyetik kapı sensörü, evde bulunan pencereler, kapıların kontrolsüz açılması durumda ev sahibine uyarı gönderen sistemdir. Garaj giriş sensörü, garaja giriş yapan araçları algılayıp kapının açılması kapanması durumlarını kontrol eden sistemdir.

2.6.3. Güvenlik Sensörü

Evde yaşayan kişiler evde yokken evde biri varmış izlenimi vermek için pilot programın çalıştırıldığı sistemdir. Hareket ve hareketsizlik sensörü, kullanıcının eve girişi ile tasarlanan senaryoların devreye girdiği sistemdir. Kamera izleme sistemiyle, evin her yeri ev sahibinin evde olmaması durumunda bile uzaktan izlenebilir.

2.6.4. Enerji Ölçümü

Akıllı evdeki enerji tüketimini ölçebilir, her oda için sıcaklığı ayrı ayrı kontrol edebilir ve tasarruf sağlar. Akıllı priz, sayesinde prizdeki cihazlar uzaktan kontrol edilebilip, cihazlar kapatılabilir.

2.6.5. Panik Butonu

Panik butonu, acil bir durum karşısında ev sahibi yakınları ve ilgili kurumlar ile iletişime geçebilen bir sistemdir.

2.6.6. Sulama Sistemi

Sulama, bahçenin sulama durumunu kullanıcının kontrol edebildiği, otomatik hava koşulları doğrultusunda sulama programı yapabilen sistemdir.

2.6.7. Sarsıntı Sensörü

Sarsıntı sensörü, sarsıntı durumunda veya ihtimalinde erken uyarı ile kullanıcıyı bilgilendiren ve önlemler alınan sistemdir. Perde ve panjur sistemleri, perdelerin, panjurların açma kapama durumunu tek bir tuş ya da tek bir hareket ile kontrol edilmesini sağlayan sistemdir. Havalandırma sisteminde ise kullanıcının klima ve havalandırma sistemlerini açıp kapayabildiği sistemdir.

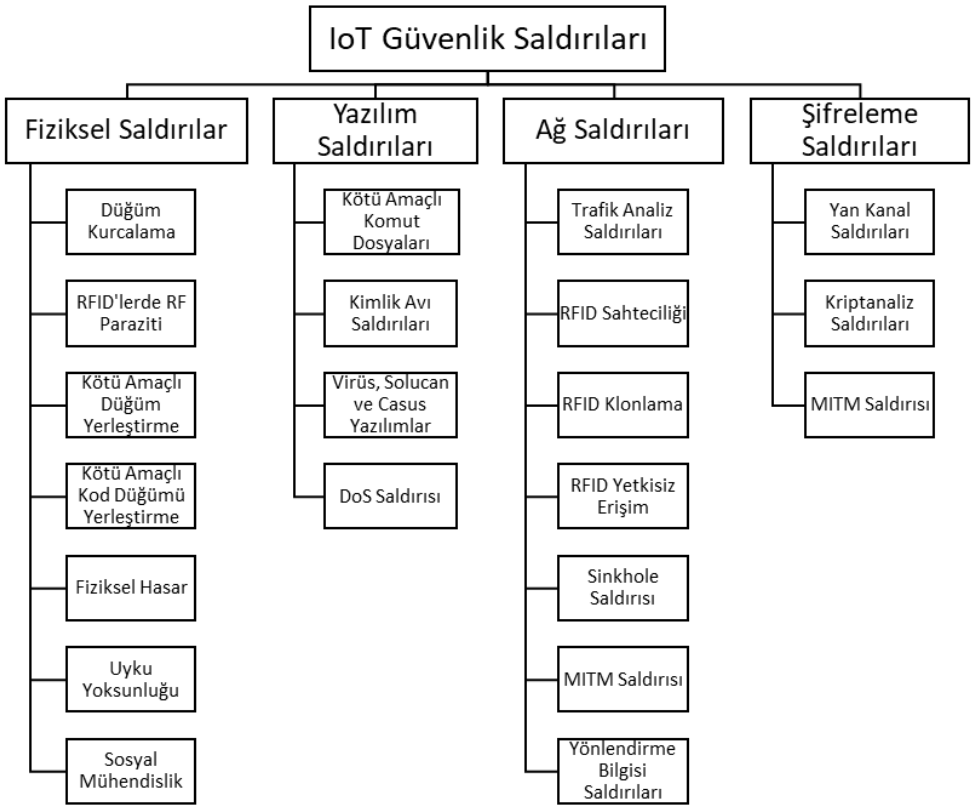
2.6.8. Aydınlatma Sistemi

Aydınlatma sistemi, ışıkların kullanıcının evde olma veya gitmedi durumunda otomatik ve manuel olarak kapandığı bir sistemdir ışıkların kullanıcı işe giderken veya uyurken otomatik olarak. Termometre sistemi, dışarının hava koşulları doğrultusunda içerinin sıcaklığını kontrol eden sistemdir. Multimedya kontrolü, evde bulunan video ve ses sitemlerinin uzaktan kontrol edilebildiği sistemlerdir. Akıllı evlerde kullanılan sistemlere kişinin ihtiyacı doğrultusunda eklemeler yapılabilmekte ve kullanıcının konforlu bir yaşam sürmesi sağlanmaktadır.

3. Akıllı Ev ve IoT Akıllı Evlerde IoT Güvenliği

3.1. Akıllı Evlerde IoT Güvenliği ve Siber Saldırı Yöntemleri

Akıllı evde cihazların sayısı günümüz şartları ve ihtiyaçları doğrultusunda artmaktadır. Bu durum insan hayatında büyük kolaylıklar sağlasa da önlemlerin alınmaması durumunda IoT güvenlik açıklarının oluşmasına ve tehditlere yol açmaktadır. Siber saldırılara karşı evdeki araçlar ile ev içine erişim sağlanabiliyor. ECHO ve Google Home cihazları gibi dijital asistanlar dünya çapında evlere erişim sağlamışlar. Eğer banka bilgileri, parolalar veya hassas, gizli bilgilerimiz paylaşılıyorsa siber saldırılara karşı evimizin içine erişim söz konusu olabiliyor. Aynı durum bebek kameralarımızdan web kameramızı ele geçirebilecek olan bilgisayar korsanlarının evde olup olmadığımızı tespit edebilmesi de söz konusudur. Bu ve benzeri ihtimallerin gerçekleşmesi düşük ihtimalli olsa da imkânsız değildir. Bu durumda evimizde IoT güvenliğine karşı önlemler almamız gerekmektedir. Oluşabilecek tehdit durumlarının en başında gizlilik, veri hırsızlığı gelmektedir. Evimizi de birçok cihaz veri toplamaktadır bu veri bilgileri yanlış ellere düşmesi durumunda kimlik hırsızlığı sahte işler için kullanılabilir.



Şekil 4. IoT Sisteminde Çeşitli Güvenlik Saldırıları (Atlam ve Wills, 2020).

Bu durum karşısında önlem olarak mutlaka kimlik doğrulama işlemi ve şifreleme yapmamız gerekir. Bir diğer tehdit durumu ise cihazlarımızın ele geçirilmesidir. Saldırgan tarafından ele geçirilen cihazımız ilk başlarda işlevselliğini koruduğu için ele geçirildiğini anlamak mümkündür. Ancak normal çalışan bir cihazın tuhaf hareketler sergilemesi durumunda (mesela televizyonun tuhaf davranışlar sergilemesi, bahçe sulama sistemimizin gereğinden fazla çalışması) saldırgan bir cihazı ele geçirse bile bu durum diğer cihazlarımızı da tehlikeye sokmaktadır. DDoS saldırısı dediğimiz bir diğer adı ile kalıcı hizmet reddi olarak da bilinen bu saldırı türünde ise cihazlarımız ağır hasarlar görebilir ve bu hasarlar sonucu donanımlarının bile değişimi gerekmektedir. Düzenli bir şekilde güvenlik izlemesinin yapılması şarttır. Güvenlik tehditlerinden korunmak için özellikle şifreleme, kimlik doğrulama ve erişim kontrolüne dikkat edilmelidir. Saldırılar açısından incelendiğinde fiziksel saldırılar,

yazılımsal saldırılar, ağ saldırıları ve şifreleme saldırıları olarak gruplamak mümkündür. Özellikle siber saldırı yöntemleri incelendiğinde Man-in-the-Middle saldırıları her güvenlik saldırı gruplarında yer almaktadır. Bu saldırılar özellikle IoT cihazların kablosuz olarak birbiri ile haberleşmesinden dolayı araya girerek sistemlere sızmayı hedeflemektedir. Bu saldırılar ağ üzerinde farklı bir ağ adı ile cihazların ve kullanıcıların bağlanmalarını beklemektedirler.

3.2. Akıllı Evlerde IoT Güvenliği Sorunları ve Alınması Gereken Önlemler

Akıllı ev sistemimizin güvenliğinin güçlü olması Wi-Fi ağı ile başlar. Güvenliği artırmak için ağ adını gizemli tutarak, bilgisayar korsanlarının ağ adı üzerinden marka ve modelini belirlemesini engellemiş olup, cihazlara ulaşımını zorlaştırırız. Varsayılan ad ve şifre bilgilerini değiştirerek, saldırganlara karşı önlemler alabiliriz. Şifre belirlemede başka yerde kullanmadığımız şifreleri tercih etmemiz önemlidir. Yazılımı güncel tutarak, IoT güvenliğine güçlü bir iyileştirme getirir. Modemi açıp kapatarak, VPN filtre gibi kötü amaç içeren yazılımların modemlerimize erişimini engelleriz. IoT cihazları için varsayılan ayarlarımızı değiştirmemiz gerekmektedir. Örneğin, uzaktan erişim kullanacaksak faydalı fakat kullanmayacaksak güvenlik riski yaratmaktadır. Kullanmadığımız cihazları devre dışı bırakmak güvenlik tedbiri açısından önemlidir. İki Faktörlü kimlik doğrulamayı etkinleştirerek ise sistemimizi ve cihazlarımızı koruma açısından çok etkili bir faktördür.

Teknolojinin hızlı gelişmesiyle insanların kullanımına birçok elektronik cihaz sunulmuştur. Fakat insanların bu cihazları kullanım kabiliyetleri maalesef aynı hızda gerçekleşmemiştir. Kullanıcıların bu konudaki eksikliklerinden dolayı hırsızların, bilgisayar korsanlarının ya da kötü niyetli diğer kullanıcıların saldırıları giderek artmaktadır. Her gün insanların bilerek ya da bilmeyerek ortaya çıkardıkları güvenlik açıklarından dolayı kişisel veriler, bilgisayar korsanları tarafından çalınmakta, işlenmekte ve değiştirilmektedir. Bilgilerin elde edilmesi için artık fiziksel olarak kullanıcılara veya cihazlara yakın olmaya dahi gerek duyulmamaktadır. İnternete bağlı olan her cihaz tedbir alınmadığı zaman tehlike altındadır. Bu konuda bilişim okuryazarlığın artırılması, kullanıcıların bilgilendirilmesi gerekmektedir. Kişisel olarak alınabilecek önlemler kapsamında; modemlerin, cep telefonlarının vb. cihazların varsayılan yapılandırmaları değiştirilmelidir. Varsayılan olarak gelen ağ adları kişisel olarak adlandırılmalı, güçlü şifreler oluşturulmalıdır. Bu şekilde saldırganların elektronik eşyalara erişimleri zorlaşacaktır. Ayrıca eve gelen misafirler için farklı bir kısıtlı ağ tanımlaması yapılabilir. Böylece hassas veriler tehlikeye atılmadan ağ paylaşımı yapılabilir.

Tablo 1. Olası Güvenlik Sorunları ve Çözümleri (Strecker ve ark., 2021), (Islam ve ark., 2021), (Karunarathne ve ark., 2021).

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

Açılış şifreleri, BIOS şifresi gibi başlangıç güvenlik önlemleri alınmalıdır. Güvenlik duvarı güncellemeleri zamanında yapılmalıdır. Herhangi bir açık bulunduğu takdirde bu güncellemeler güvenlik ihlallerini engelleyecektir. Lisanslı yazılımlar tercih edilmeli, korsan yazılım kullanmaktan kaçınılmalıdır. Lisansız yazılımların içinde kötü niyetli kodların olabileceği unutulmamalıdır. Eğer bir uygulama, program indirilecekse mutlaka orijinal sitesinden edinilmelidir. Kaynağı bilinmeyen sitelerden herhangi bir dosya indirilmemelidir. Bu sitelerin zararları ilerleyen zamanlarda daha kötü sonuçlar ortaya çıkarabilir. Kullanılmadığı durumlarda Wi-Fi ve Bluetooth özelliği kapatılmalıdır. Bu hem cihazın bataryasının daha geç deşarj olmasını sağlayacak, hem de izinsiz erişim sağlamak isteyen kullanıcıları engelleyecektir. Son olarak cihazların fiziksel güvenliği sağlamak için koruyucu donanım kullanmaya dikkat edilmeli, çalınma ihtimaline karşı önlemler alınmalıdır.

3.3. IoT Uygulamalarında Bütüncül Güvenlik Yaklaşımı

Bir IoT sisteminde yer alan tüm bileşenler ve bu bileşenlerin muhtemel güvenlik riskleri üzerinde yaptığım analizler sonucunda sağlık alanındaki IoT uygulamaları için bütüncül bir güvenlik yaklaşımı sergilemek gerektiği kanaatine vardım. Bu sistemde her bir IoT bileşeninin güvenliği tüm sistemi etkilediği için, kuruluş aşamasında muhtemel zafiyetlerin tüm yönleriyle ele alınması gerekmektedir. Önerdiğim bütüncül güvenlik yaklaşımı metodu aşağıda görüldüğü gibi dört ana adım ve iki destekleyici adımdan oluşmaktadır.

Şekil 5. Bütüncül Güvenlik Yaklaşımı

3.4. Yaşanan En Büyük 10 Güvenlik Sorunları ve Çözümü

Mobil cihazlarda ve bilgisayarlarda olduğu gibi nesnelerin interneti alanında da çok fazla güvenlik sorunları bulunmaktadır. Aşağıda bu alanda karşılaşılan en büyük 10 güvenlik sorununu incelenip, bu sorunlara ait çözümler paylaşılmıştır.

3.4.1. Eksiz Güvenlik Güncellemeleri

Nesnelerin interneti kolay kullanım için tasarlanmıştır. Bu nedenle ilk alındıklarında güvenilir olsalar dahi zamanla korsanlar tarafından yeni güvenlik açıkları bulunarak bu cihazlar korunmasız hale gelebilirler. Bu sebeple cihaz üreticileri zamanla yeni güvenlik güncellemeleri yayınlayacaktır ve kullanıcılar da cihazlarına bu güncellemeleri yüklemelidirler (Eurofins, 2022).

3.4.2. Brute Force Saldırısı ve Varsayılan Kullanıcı Adı / Şifre

Birçok DDOS saldırılarında korsanlar "admin" kullanıcı adını ve şifresini kullanmaktadır. Bu şifre ve kullanıcı adı birçok cihazda varsayılan olarak tanımlanmakta ve kullanıcılar bu kullanıcı adını ve şifresini değiştirmemektedirler. Bu sebeple birçok cihaz bu saldırılara açık hale gelmektedir. Bu saldırılardan kurtulmak için ise cihaz temin edildikten sonra kullanıcı adı ve şifre değiştirilmelidir (Thalesgroup, 2022).

3.4.3. IoT Cihaz Yönetimi Eksiklikleri

IoT ve IoMT sağlık, perakende, üretim, yaşam bilimleri alanlarındaki bütün cihazları birbirleriyle çalışır bir hale getirdi. Bu şekilde bütün cihazların birbirleriyle iletişim halinde olduğu bir ekosistemde ise cihazların yönetimi ve bir cihazın diğerini güvenlik açısından etkilememesi son derece yönetimi zor bir sorun haline gelmektedir. Özellikle sağlık sektöründe eski cihazlar ile yeni cihazların birlikte kullanılması operasyonel sorunlar, finansal kayıtlar, müşteri veri güvenliği gibi sorunlara sebep olmaktadır (Thalesgroup, 2022). Bu sorunun çözümü için ise IoT cihaz yönetim sistemi kullanılmalı, bu sistem üzerinden gerekli cihaz konfigürasyonları, kontrolleri, yönetimi, sistem güncellemesi ve bakımı yapılmalıdır (Peerbits, 2022).

3.4.4. Yetersiz Veri Koruma

IoT uygulamalarındaki en önemli güvenlik sorunlarından birisi de zayıf veri iletişimi ve veri depolamadan kaynaklanmaktadır. IoT cihazların güvenliği ve gizliliği için en önemli zorluklardan birisi de güvenliği ihmal edilmiş IoT cihazlarının veri sızdırmak için kullanılmasıdır. Bu konuda en önemli çözüm ise şifrelemedir. Verilerim şifrelenmesi, izinsiz kullanımı, yetkisiz erişimi ve verilerin görünürlüğünü engeller (Eurofins, 2022).

3.4.5. Uygulama Güvenlik Açıkları

Her yazılımda olduğu gibi IoT cihazları yazılımlarında da açıklar bulunmaktadır. Bu sebepten dolayı IoT cihazlarının yazılımlarında da ilk baştan itibaren açıkların bulunduğu kabul edilmelidir. Korsanlar ise bu açıkları kullanarak cihazların kendi uygulamalarının normal çalışır halinden önemli verileri elde edebilmektedirler. Bu sorundan tamamen kaçınmak oldukça zordur. Bu soruna en iyi çözüm sisteme girişlerde sağlam bir kullanıcı girişi doğrulaması yapmaktır (Eurofins, 2022).

3.4.6. Tedarikçi Yazılım/Güncelleme Desteği

IoT cihazları için bir diğer önemli unsur da ortaya çıkan bir bug'tan, sistem açığının tespit edilmesinden sonra cihazı üreten firmanın bu açığa ne kadar kısa sürede destek verdiğidir. Bazı sistem açıkları veya bug çok fazla sorun oluşturmasa da bazı açıklar hayati önem taşımaktadır. Bu durumda da IoT cihazlarını üreten firmanın bu konuda en kısa sürede yeni güncellemeler yayınlayıp bu hataları gidermesi gerekmektedir (Peerbits, 2022). Bu sorunun en kısa çözümü IoT cihazlarını üreten firmanın bu tür durumlarda nasıl bir politika izlediğini önceden bilerek o cihazı temin etmek gerekmektedir.

3.4.7. Veri Güvenliği ve Gizlilik Endişeleri

Veri güvenliği ve gizliliği günümüz hayatında en büyük sorunu teşkil etmektedir. Firmalar artık sadece mobil cihazlardan ve web' ten değil IoT sayesinde internete bağlanabilen bütün cihazlardan verileri toplayabilmektedir. Toplanan bu veriler başka firmalara satılabilmekte, veriler üzerinden analizler yapılarak farklı şekillerde anlamlandırılmaktadır. Bütün bunlar ise kullanıcılar için bir güvenlik sorunu soruna haline gelmektedir. Bu sorunlara karşı çözüm olarak, kullanıcılar toplanacak verileri kişisel özel/hassas veri ve depolanabilecek veri şeklinde farklı gizlilik kuralları çerçevesinde toplatmalı, ihtiyaç duyulmayan verilerin hafızadan silinmesi, veri kesin bir şekilde toplanacak ise bunun bir yasal çerçevede toplanabilmesi gibi önlemleri alması gerekmektedir (Thalesgroup, 2022).

3.4.8. Güvenilir Olmayan Arabirim Kullanımı

Kullanılan her IoT cihazı veri alıp veri iletmektedir. Bütün bu veri iletişiminde ise IoT cihazları uygulamalara, iletişim protokollerine ve hizmetlere ihtiyaç duyarlar. Cihazlar arası veri iletişiminde ise yeterli kimlik doğrulamasının olmaması, zayıf şifreleme veya şifrelemenin hiç olmaması büyük güvenlik sorunlarına sebep olabilmektedir. Bu sorunlara karşı çözüm olarak, cihaz kimlik doğrulamasının yapılması, cihazlar arası veri iletişiminde cihazların birbiri ile iletişim protokollerinin yapılması, dijital güvenlik sertifikalarından yardım alınması gerekmektedir (Thalesgroup, 2022), (Peerbits, 2022).

3.4.9. Kötü Amaçlı Yazılımlar

Bilgisayarlar için geliştirilen kötü amaçlı yazılımlar daha sonra mobil cihazlar için şimdi ve gelecekte de IoT cihazları için geliştirilmede devam ediyor. Kısacası internete bağlanabilen bütün cihazlar bu tür yazılımların saldırısı altında kalıyor. Bu yazılımların amaçları daha çok cihazları devre dışı bırakmak, verileri çalmak, hassas bilgilere ulaşmaktır. Bu tür saldırılardan kurtulmak için zamanında güncelleme yapmak, kaynağı bilinmeyen yazılımların kullanılmasının önüne geçmek, cihazlar arasında bir bağlantı var ise bu bağlantıyı belirli protokoller üzerine kurmak gerekmektedir (Strecker ve ark., 2021).

3.4.10. Güvenilir Olmayan İletişim Ağları

Birçok IoT cihazları mesaj gönderimini herhangi bir şifreleme sistemi olamayan ağlar üzerinden gerçekleştirmektedir. Bu güvenlik sorunu IoT cihazları için en büyük güvenlik sorununu oluşturmaktadır. Bu sorunun çözümü için ise, IoT cihazlarının bağlı bulunduğu ağ veri şifreleme ve iletişimi standarttı olan TLS (Transport Layer Security) gibi güvenlik politikalarını uygulamalıdır. Bir diğer çözüm ise IoT cihazlarının bağlı olduğu ağları birbirlerinden ayırmaktır (Sivaganesan, 2021), (Islam ve ark., 2021).

4. Sonuç

Günümüzde birçok alanda kendine yer bulmaya başlayan IoT teknolojisi yakın zamanda içinde hayatımızı birçok yönden değiştirecektir. Yaşadığımız yüzyılın başında akıllı cihazlar ile tanışan insanlık, çeyrek asır geçmeden bu akıllı nesnelerin internet ve bulut sistemleriyle entegre edilmiş hali olan IoT teknolojisine uyum sağlama aşamasındadır. Teknolojinin gelişmesi ile insanların yaşam kalitesi artmaktadır ve bu durum hayatımızı kolaylaştırsa da bazı açılardan hayatımızı zorlaştırabilmektedir. Çalışmadaki araştırma bulguları sonucunda yapılan analizlere göre akıllı evlerin güçlü yanları, enerji, zaman tasarrufu, konfor, güvenlik, fiziksel veya zihinsel eksiği olan insanlar için kolaylıklar sağlamaktadır. Zayıf yönleri ise, insanı tembel bir yaşama itmesi, maliyet yüksekliğidir. Akıllı evlerin fırsatları, insanın hayallerindeki evin ilerleyen teknoloji sayesinde gerçekleştirilmesi,insan bedeninin gerçekleştireceği birçok görevi tek bir tık ile telefondan halledilebiliyor olması, kişinin ihtiyaçları ve istekleri doğrultusunda özellikler ekleyip çıkarabilmesidir. Tehditlerine gelecek olursak, akıllı evlerin yaygınlaşması ile teknoloji daha yaygın hale gelmektedir. Ayrıca bu durumda saldırganların artmasına sertifikasız akıllı ev ürünlerinin satışa sunulması gibi sorunlara sebebiyet vermektedir. IoT cihazlarını akıllı av sistemlerinde kullanan kullanıcılar her şeyden önce temel güvenlik önlemlerini almalıdırlar. Kişisel verilerini kesinlikle bulut sistemlerinde ve lisanssız uygulamalarda bulundurmamalıdırlar. Buna ek olarak dış kaynaklardan temin edilen yazılımlarda akıllı ev ve kişisel verilerin güvenli olduklarına emin olmalıdırlar. Kullanılan uygulamaların gerekli güncellemeleri zamanında yapmalı, satış sonrası desteği zamanında ve eksiksiz veren firmaları tercih etmeli, güvenlik konusunda deneyimli ve bilgili kurum ve kişilerden destek almalıdır.

Kaynakça

Ashton, K. (2009). That 'internet of things' thing, RFID Journal, 22(7), 97-114.

Atlam, H. F. & Wills, G. (2020). IoT security, privacy, safety and ethics. In Digital twin technologies and smart cities, pp. 123-149, Springer, Cham.

Eurofins.(2022), Erişim Adresi: https://www.eurofins-cybersecurity.com/news/security-problems-iot-devices/. (Erişim tarihi:10.02.2022)

Gökrem, L. & Bozuklu, M.(2016). Nesnelerin interneti: Yapılan çalışmalar ve ülkemizdeki durum, Gaziosmanpaşa Bilimsel Araştırma Dergisi, (13), 47-68.

Gokhale, P., Bhat, O. & Bhat, S. (2018). Introduction to IoT. International Advanced Research Journal in Science, Engineering and Technology, 5(1), 41-44.

Innova. (2022), Erişim Adresi: https://www.innova.com.tr/tr/blog/dijital-donusum-blog/nesnelerin-interneti-iot-nedir (Erişim tarihi:15.02.2022).

Islam, N., Farhin, F., Sultana, I., Kaiser, M. S., Rahman, M. S., Mahmud, M. & Cho, G. H. (2021). Towards machine learning based intrusion detection in IoT networks, *Comput Mater Contin*, 69, pp. 1801-1821.

Jiang, T., Yang, M., Zhang, Y. (2012). Research and implementation of M2M smart home and security system. Security Comm. Networks, 8, 16, pp. 2704-2711.

Kalyoncu, A. ve Turan, M. (2020). IoT Teknolojisi Kullanan Pratik ve Güvenilir Akıllı Kapı Kilidi Tasarımı. European Journal of Science and Technology, (August), pp. 43–49. doi:10.31590/ejosat.779045.

Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. IEEE Internet Computing, 25(4), 37-48.

Küçük, Z. K. & Ekren, N. (2020). Akıllı mutfak için tasarlanmış sistemler üzerine bir derleme. International Periodical of Recent Technologies in Applied Engineering, 2(1), ss. 25-34, 2020.

López-de-Armentia, J. Diego Casado-Mansilla, J. and López-de-Ipina D. (2012). "Fighting against vampire appliances through eco-aware things." 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. IEEE.

Ozkaya, U., Öztürk, Ş., Tuna, K., Seyfi, L., & Akdemir, B. (2018). Faults Detection With Image Processing Methods In Textile Sector. In 1st International Symposium on Innovative Approaches in Scientific Studies.

Özçekiç, E. (2005). Akıllı Ev Sistemleri. İstanbul.

Özdoğan, E. & Daş, R. (2021). IoT based a Smart Home Automation System Design: Simulation Case. Balkan Journal of Electrical and Computer Engineering, 9(3), pp. 297-303.

Özdemir, B. (2019). Akıllı Ev Sistemlerinde Güvenlik Zafiyetleri ve Önlemleri, İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü.

Peerbits. (2022). Erişim Adresi: https://www.peerbits.com/blog/biggest-iot-security-challenges.html.

Sivaganesan, D. (2021). A data driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks, Journal of trends in Computer Science and Smart technology (TCSST), 3(01), pp. 59-69.

Soumyalatha, S. G. H. (2016). Study of IoT: understanding IoT architecture, applications, issues and challenges. In 1st International Conference on Innovations in Computing &

Net-working (ICICN16), CSE, RRCE. International Journal of Advanced Networking & Applications (No. 478).

Strecker, S., Haaften, W. V. & Dave, R. (2021). An analysis of IoT cyber security driven by machine learning. *In* Proceedings of International Conference on Communication and Computational Technologies, pp. 725-753, Springer, Singapore.

Şahinoğlu, G. (2006). Akıllı evlerde otomasyon (Doctoral dissertation, Marmara Universitesi (Turkey)).

Taştan, M. (2019). Akıllı Ev Uygulamaları için Yeni Nesil IoT Denetleyici ile Gerçek Zamanlı Uzaktan İzleme ve Kontrol Uygulaması, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23(2), ss. 481-487.

Thalesgroup. (2022), Erişim Adresi: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats. (Erişim tarihi:14.02.2022)

Tomaş, M. (2019). Akıllı Evler Üzerine Bir Değerlendirme. TC. İstanbul Kültür Üniversitesi, İstanbul.

Tomaş, M. ve Dostoğlu, N. (2020). Smart House With Artificial Intelligence, European Journal of Science and Technology, (18), 686–693. doi:10.31590/ejosat.689634.

Zeybek, M. & Yılmaz, E. N. (2019). Nesnelerin İnterneti:Risk Temelli Yaklaşim. Denetişim, 19, ss. 73–88.