NESNELERİN İNTERNETİ: RİSK TEMELLİ YAKLAŞIM

(INTERNET OF THINGS: RISK-BASED APPROACH)

Mine ZEYBEK* / Ercan Nurcan YILMAZ**

ÖZ

Son yıllarda hızla popüler bir teknoloji konsepti haline gelen "nesnelerin interneti" (Internet of Things, IoT), hali hazırda bazı zorluklar ve aşılması gereken problemleri olsa da özellikle 5G teknolojisinin de katkısıyla günlük hayatımızda önemli bir yer tutacaktır. Temel olarak basitten karmaşığa bir takım ana işlevleri olan ürün ya da cihazlar; birçok algılayıcı ve haberleşme arabirimi donanımı eklenerek algoritmalar ile desteklenmesi sonucunda matematiksel ve mantıksal özellikleri olan ve birbirleri ile "konuşabilen" akıllı cihazlar haline dönüşmüştür. Ancak bu yeni teknolojide güvenlik ve mahremiyet kavramları da dikkatle ele alınması gereken en önemli sorunlardandır. Güvenlik konusunda yapılan çok sayıda çalışma ve akademik tartışma bulunmasına rağmen, bahsi geçen akıllı cihazların ortak bir donanım, algoritma ya da arayüze sahip olmaması; hemen hepsi için geçerli bir güvenlik protokolü geliştirilmesinin önündeki en büyük engel olarak görünmektedir. Bu sebeple "nesnelerin interneti" teknolojisine sahip cihazların yaygınlaşıp ev ve işyerlerinde yerlerini almasıyla birlikte, yeterli önlemler alınmazsa, son yıllarda sayısı oldukça artan ve küresel çapta gerçekleştirilmeye başlanan siber saldırılarda, başka bir boyuta geçilmesinin önünü açacağı düşünülmektedir. Makale kapsamında nesnelerin internetinin güvenliği konusunda yapılan çalışmalar incelenmiş, nesnelerin internetinin yapısı ve mimarisinden bahsedilip, nesnelerin internetine yönelik güvenlik tehditleri ile yaşanmış olaylar ele alınmış ve nesnelerin internetinin denetiminde değerlendirilebilecek kontroller belirtilerek, nesnelerin internetinin güvenliğine yönelik alınabilecek önlemler sunulmuştur.

Anahtar Kelimeler: Nesnelerin interneti, siber güvenlik, mahremiyet, bilgi güvenliği, siber saldırı, denetim kontrolleri.

JEL Kodlaması: K42

ABSTRACT

Internet of Things (IoT), which has become a popular technology concept in recent years, will have an important place in our daily lives with the help of 5G technology, even though it already has some difficulties and problems to be overcome. In this new technology, basically, devices including from simple to complex main functions; security and privacy concepts are two of the most important issues to be handled with due to the fact that it is transformed into smart devices that have mathematical and logical features and can be talked to each other through the addition of many sensors and communication interface hardware. Although there are numerous studies and academic discussions about security of IoT, because of the fact that there is no common hardware, algorithm, or interface of these smart devices; developing a commonsecurity protocol for all of them is the biggest obstacle to achieve it. For this reason, devices with IoT technology take their places in the houses and workplaces, and if sufficient measures are not taken, it is thought that the cyber attacks, which have been increasing in recent years and are being carried out on a global scale and organized, will pave the way for another dimension. The previous studies on the security of the IoT were examined within the scope of this article. In addition, the structure, architecture and security threats of the IoT were discussed. The controls that can be evaluated for the audit of the Internet of Things are pointed out and also, the measures to ensure the safety of the IoT were presented.

Keywords: *Internet of Things, cyber security, privacy, data security, cyber attack, audit controls.*

JEL Classification: *K42*

---

*) İç Denetçi, İçişleri Bakanlığı, İç Denetim Birimi Başkanlığı, Ankara, Orcid: 0000-0002-8652-2082, mine.zeybek@icisleri.gov.tr

**) Doç. Dr., Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Bölümü, Ankara, Orcid: 0000-0001-9859-1600, enyilmaz@gazi.edu.tr

Yazı Gönderim Tarihi: 02.04.2019, Yazı Kabul Tarihi: 05.04.2019

1. GİRİŞ

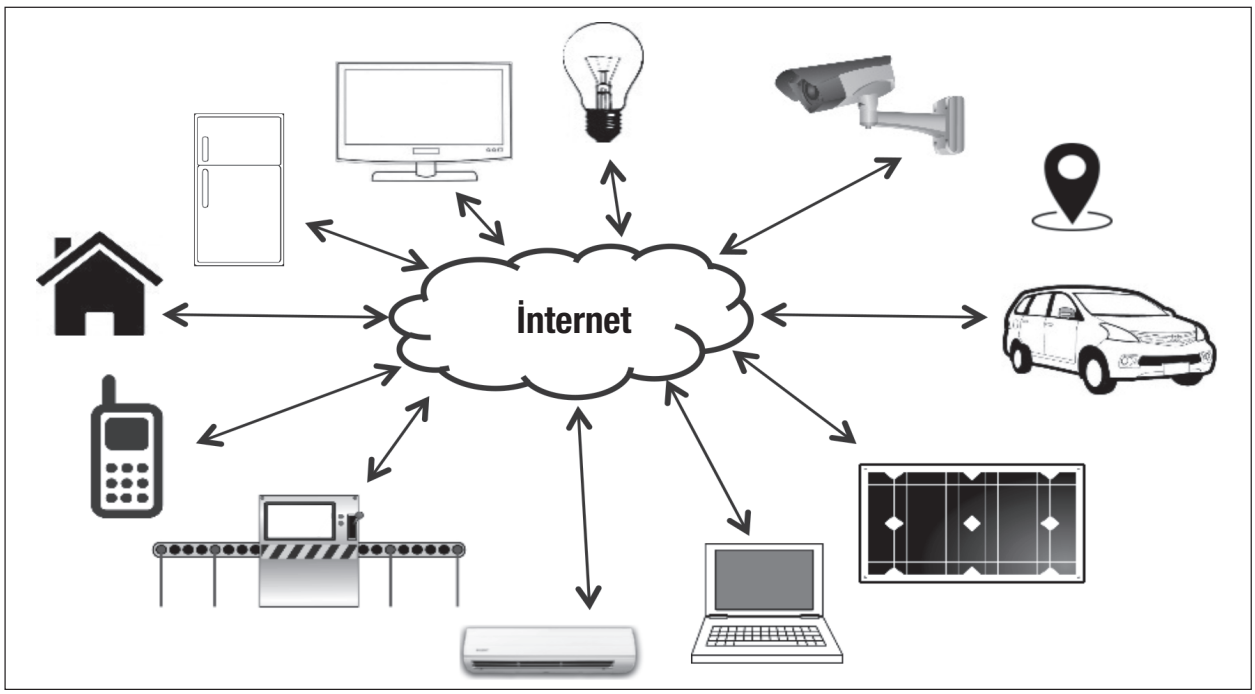
"Nesnelerin interneti" (Internet of Things, IoT) için, birbirlerine oldukça yakın olarak ifade edilen birden fazla tanım yer almaktadır. İlk olarak 1998 yılında Kevin Ashton tarafından yapılan bir sunumda kullanılan bu terim, internet benzeri bir yapıda birbirleri ile haberleşebilen cihazları tanımlamıştır (Weber, 2010) .

Gartner tarafından yayınlanan bir raporda (Gartner, 2017), sadece 2017 yılında internete bağlı olan, dünya çapında 8,4 milyar "nesne" kullanılacağı belirtilmektedir. Bu sayının 2016 yılı verilerinden %16 daha fazla olduğu ifade edilirken 2020'ye kadar 31 milyar cihaza, 2025'te ise 75 milyar cihaza ulaşması beklenmektedir (Brandon, 2016) (Claveria, 2019). Günümüzde ortalama bir akıllı cihaz tüketicisi yaklaşık 4 adet internete bağlı cihaza sahiptir (Buckle, 2016). Teknoloji, gelişmeye ve ilerlemeye devam ederken, nesnelerin interneti bireyin günlük hayatının birçok yönüne nüfuz ettiği için, büyümeyi yönlendiren belirli bir sektör yoktur. 2017 yılında 125.5 milyon olan giyilebilir cihaz sayısının, 2021 yılında 240.1 milyona ulaşması beklenmektedir (Lamkin, 2017). Otomotiv endüstrisinde de, 2020 yılında yeni araçların % 75'inin, internete bağlanabilmek için gerekli donanıma sahip olacağı tahmin edilmektedir (Greenough, 2015).

IoT cihazlarını üreten şirketlerin, cihazların güvenliğini sağlamak için ortalama bütçelerinin sadece % 11'ini harcadıkları ve şirketlerin % 67'sinin veri şifrelemeyi birincil güvenlik yöntemi olarak ele aldıkları rapor edilmektedir (Lohrmann, 2017). Bununla birlikte, 2017 yılında bir anket ile tüketicilerin IoT ile ilgili mevcut güvenlik kaygıları araştırılmıştır. Anket sonucunda tüketicilerin % 65'inin bir korsan tarafından IoT cihazlarının kontrolünün ele geçirebileceğinden, % 60'lık bir kesiminin ise verilerin sızdırılmasından veya çalınmasından endişe ettiği ve ortalama 2 adet akıllı cihaza sahip kullanıcılardan sadece %14'ünün bu cihazların güvenliği konusunda son derece bilgili olduklarına inanıldıkları tespit edilmiştir (Gemalto, 2017).

Bu verilerden de görüleceği üzere, IoT pazarı, akıllı telefonlar ve bilgisayarların benimsenmesiyle başlayarak akıllı saat ve bileklikler, akıllı televizyonlar, akıllı ev aletleri ve hatta akıllı otomobiller de dâhil olmak üzere gittikçe büyümekte ve günlük hayatımızın birçok bölümünde giderek daha yaygın hale gelmektedir (Şekil 1).

Şekil 1. IoT kullanım alanları



(Yazarlar tarafından oluşturulmuştur.)

Bu cihazlar temel olarak hayatlarımızı daha iyi ve daha kolay hale getirmeyi amaçlamakla birlikte, tüketicilerin çoğu zaman fark etmedikleri şey, hızlı büyüyen ağ bağlantılı cihazlarla, göz ardı edilmesi giderek zorlaşan ve giderek artan bir güvenlik riskidir. Son birkaç yılda IoT cihazlarının güvenlik açısından tehlikeye girdiği ve istismar edildiği birçok durum meydana gelmiştir.

Bu çalışmada literatürdeki IoT güvenliği konusundaki mevcut çalışmalar ile IoT'nin genel yapısı ve mimarisi incelenmiş, olası riskler ile son birkaç yılda meydana gelen saldırılar ele alınmış, IoT denetimi için önerilen kontroller belirtilmiş ve son olarak IoT güvenliğinin sağlanmasına yönelik alınması gereken tedbirler ve çözüm önerileri sunulmuştur.

Çalışmanın 2. bölümünde literatür araştırması yapılmış, 3. bölümünde IoT kullanım alanları, mimari yapısı, bileşenleri ve bu bileşenlere yönelik olası saldırılar ve riskler ele alınmıştır. 4. bölümde yaşanmış IoT saldırı vakaları belirtilmiş, 5. bölümde IoT denetimine yönelik kontrol listesi verilmiştir. 6. bölümde ise IoT güvenliğinin sağlanmasına yönelik çözüm önerileri üzerinde durulmuş ve son olarak araştırma sonucu elde edilen sonuçlar 7. bölümde tartışılmıştır.

2. LİTERATÜR ARAŞTIRMASI

IoT güvenliği üzerine bugüne kadar yapılan çalışmalar değerlendirildiğinde IoT ve ilgili sistemlerin güvenlik gereklilikleri, zorlukları ve bu sistemlere yönelik saldırılar ile güvenlik çözümleri üzerinde durduğu görülmektedir. Bu bölümde IoT'de zafiyet olarak görülebilecek unsurlar ile güvenliğin sağlanabilmesi amacıyla yapılan çalışmalar incelenmiştir.

Yapılan bir çalışmada nesnelerin internetinin kullanıldığı akıllı evlerin tasarımı aşamasında farkındalığın olması gerektiği vurgulanmış ve akıllı bina sistemlerinden istenilen verimi elde etmek için, tasarımcıların sistemin gücünün farkında olması ve sistemin deneyimli kişiler tarafından işletilmesi gerektiği ifade edilmiştir. Söz konusu çalışmada akıllı ev uygulamaları için eğitim seti tasarlanmış ve geliştirilen bu sistem sayesinde; kursiyerlerin akıllı bina sistemini öğrenme ve kendi özel sistemlerini geliştirme fırsatı bulacakları belirtilmiştir (Yılmaz, 2011).

Bir başka çalışmada ise IoT için düşünülen güncel protokol parçaları tanıtılarak, oluşabilecek güvenlik zafiyetleri, protokol yığınının her katmanı için irdelenmiştir. Aynı çalışmada, IoT güvenliğinin, yeni nesil internet güvenliğinin ayrılmaz bir parçası olarak düşünülmesi gerektiği ve bu bağlamda düşük karmaşıklığa ve yüksek güvenilirliğe sahip çözümlerin IoT ağları için yapılandırılması gerektiği belirtilmiştir. Ayrıca, interneti oluşturacak 6LoWPAN, 6TiSCH, CoAP ve benzeri protokollerin, güvenliğin ön planda olduğu bir anlayışla tasarlanması gerektiği de vurgulanmıştır (Görmüş vd., 2018).

Rizvi ve arkadaşları tarafından yapılan bir çalışmada da, IoT'nin yoğun olarak kullanıldığı kritik alanlardan bahsedilmiş ve IoT'nin şu anda karşı karşıya olduğu güvenlik gereklilikleri, zorlukları ve mevcut güvenlik çözümlerinden bazılarının tanımlanmasına yardımcı olacak sınıflandırma üzerinde durulmuştur (Rizvi vd., 2018).

Săndescu ve arkadaşları tarafından yapılan çalışmada ise, IoT bağlamında var olan güvenlik açıkları ve saldırıları ele alınmış, dinamik bir IoT Sistemi Güvenlik Testi (DISST) modelinin araştırma ve geliştirme çalışmalarının tamamlanıp hayata geçirileceği belirtilmiştir (Săndescu vd., 2018) .

Hussain ve Abdullah yaptıkları çalışmada IoT'nin büyümesinden dolayı güvenlik ve gizlilik gereksinimlerinin değiştiğinden ve geleneksel şifreleme ve şifre çözme tekniklerinin yetersiz kaldığından söz etmiş ve gelecekteki ihtiyaçları karşılamak için hafif şifreleme teknikleri gerektiğini ifade ederken, güvenlik saldırıları karmaşıklaştıkça bunların da gelecekteki ihtiyaçlara çözüm olamayabileceğini belirtmişlerdir (Hussain ve Abdullah, 2018).

Reyna ve arkadaşlarının yaptığı çalışmada ise, blok zincirin ve IoT'nin başarılı bir şekilde birlikte çalışabilmeleri için ele alınması gereken ana zorlukların bir analizi yapılmış ve blok zincir teknolojisinin nesnelerin interneti uygulamalarını geliştirmeye yardımcı olabileceği önemli noktalar belirlenmiştir. Ek olarak bu konudaki mevcut platformlar ve uygulamalar da incelenerek yasal mevzuatın benimsenmesinin, blok zincir ve IoT'nin, hükümet altyapısının bir parçası olarak dahil edilmesinin anahtarı olduğu ve vatandaş, hükümet ve şirketler arasındaki etkileşimi hızlandıracağı belirtilmiştir. IoT ve blok zincir entegrasyonun,

mevcut kağıt parayla aynı seviyede kripto para birimleri kuracak şekilde, blok zincir kullanımını büyük ölçüde artıracağı da vurgulanmıştır (Reyna vd., 2018).

Banerjee ve arkadaşları, nesnelerin internetinde paylaşılan verinin bütünlüğünü sağlamada blok zincir kullanımının potansiyelini ortaya koydukları çalışmada aynı zamanda, 2016'dan beri yayımlanan IoT ve ilgili sistemler için tasarlanmış güvenlik tekniklerini gözden geçirmişlerdir. Mevcut tehditleri tespit edebilmenin önemli olduğu ancak yakın gelecekte potansiyel tehdit ve saldırıları tahmin etme kabiliyetinin çok daha önemli olduğu vurgulanarak, dokuz potansiyel araştırma sorusuna yer verilmiştir (Banerjee vd., 2018).

Han, Jeon ve Kim yaptıkları çalışmada, akıllı ev sistemini oluşturan bileşenlerin temel güvenlik fonksiyonlarını gizlilik, bütünlük ve kullanılabilirliğe göre sınıflandırmış ve tanımlamışlardır (Han vd., 2015).

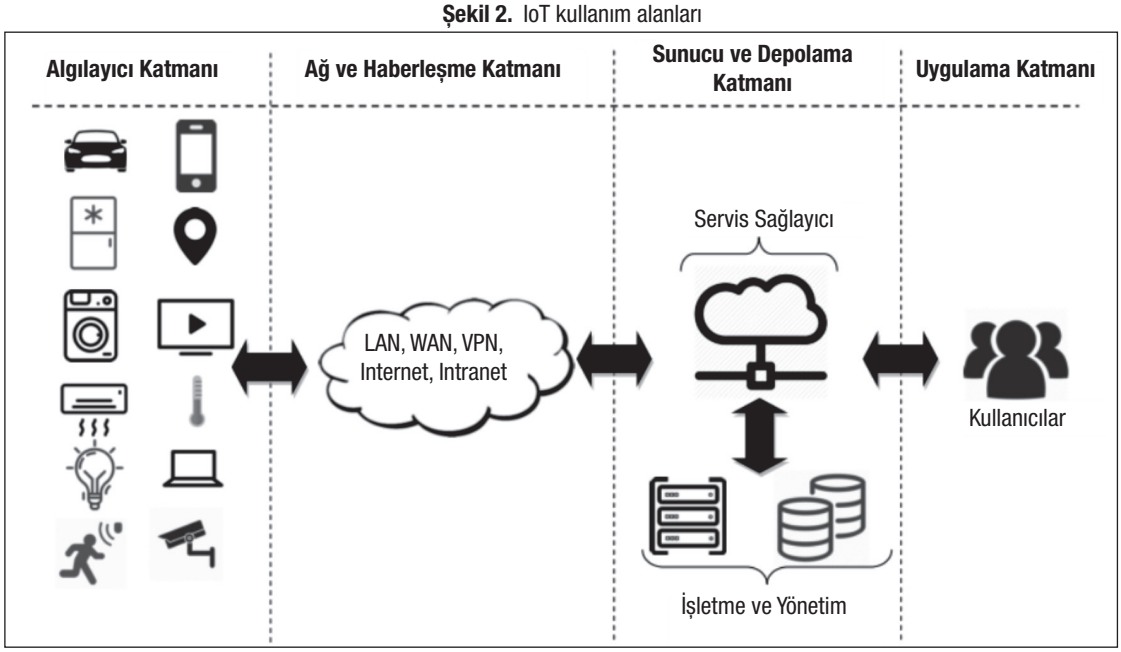
Şenol ve Arslan'ın yaptıkları çalışma ise IoT objelerinin donanımsal olarak çok çeşitli olmasından dolayı ortak bir güvenlik protokolü uygulamasının zor olduğunu, bu yüzden de tüm IoT objelerinin ağ üzerinden TCP/IP protokolü ile haberleşebildiği ve tüm zorlu güvenlik protokollerinin ağ geçidi cihazı üzerinde bulunduğu güvenli bir IoT Güvenli Ağ Geçidi tasarımını önermektedir. Önerilen bu sistemde objeler ve güvenli ağ geçidi arasında, güvenli bir ilişkinin kurulması gerektiği ve bu ilişkinin de iki tarafın da güvendiği bir sertifika otoritesi tarafından sağlandığı belirtilmektedir (Şenol ve Arslan, 2016).

3. NESNELERİN İNTERNETİNİN YAPISI

IoT kavramının terminolojideki tanımı üzerine birçok farklı görüş bulunmaktadır. Bu farklılığın sebebi aslında kavramı oluşturan iki sözcükten gelmektedir. Çeşitli ticari şirketler ve araştırma kurumları kendi altyapılarına, ilgi alanlarına göre ya internet kısmına ya da nesne kısmına ağırlık vererek tanım oluşturmuşlardır (Atzori vd., 2010).

Örneğin, Atzori vd., (2010) yaptıkları çalışmada, standart iletişim protokollerine dayalı, birbirine bağlı ve eşsiz olarak adreslenebilen evrensel nesneler ağı olarak, Madakam vd. (2015) ise çalışmalarında çevre şartlarına göre davranabilme, bilgi, veri ve kaynak paylaşabilme, otomatik organize olabilme yeteneklerine sahip açık ve kapsamlı akıllı nesneler ağı olarak ve Alam vd (2016) ise, bilgi toplama için mevcut ve gelişen bilgi ve iletişim teknolojilerine dayalı, birbirine bağlı nesneler tarafından gelişmiş hizmetler sağlayan küresel bir altyapı olarak tanımlamışlardır.

Şekil 2. IoT kullanım alanları



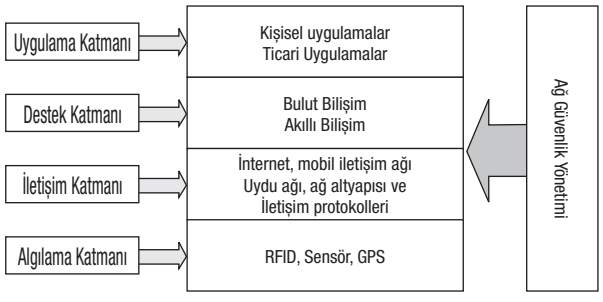
(Yazarlar tarafından oluşturulmuştur.)

E-sağlık, ev otomasyonu, akıllı çevre, akıllı su, akıllı tarım, akıllı hayvancılık, akıllı enerji, akıllı şehirler, akıllı ölçüm, endüstriyel kontrol, güvenlik ve acil durumlar, alışveriş ve lojistik gibi birçok alanda karşımıza çıkan IoT (Gökrem ve Bozuklu, 2016), Şekil 2'de görülebileceği üzere, algılayıcılar ya da harekete geçiriciler gibi fiziksel nesnelerin ağ katmanı üzerinden uygulamalar aracılığıyla son kullanıcılara ulaşması şeklinde özetlenebilecek sistemler bütünüdür (Çavdar ve Öztürk, 2017). Bu bütüne ait iş akışı aşağıdaki şekilde ifade edilebilir.

1) Nesne algılama, nesneye özgü bilgilerin tanımlanması ve iletilmesi. Algılayıcıların türüne bağlı olarak sıcaklık, yönlendirme, hareket, titreşim, hızlanma, nem, havadaki kimyasal değişiklikler gibi veriler algılanmakta ve tanımlanmaktadır. Akıllı hizmetlerin tasarımı için farklı algılayıcıların bir kombinasyonu kullanılabilmektedir.
2) Bir eylemin başlatılması. Alınan nesne bilgisi, çağrılacak otomatik bir işlemi belirleyen bir akıllı cihaz / sistem tarafından işlenmektedir.
3) Akıllı cihaz sistem yöneticisine mevcut sistem durumunu ve gerçekleştirilen eylemlerin sonuçları hakkında geri bildirim sağlayan bir mekanizma içermektedir.

Şekil 3'te de literatürde ortaya konulan IoT güvenlik mimarisi verilmiştir (Suo vd., 2012). Burada; algılama katmanında RFID okuyucu veya algılayıcılar yardımıyla ortamdaki veriler toplanmakta, ağ katmanında nesneler arasında kablolu veya kablosuz bağlantılarla veriler iletilmektedir. Destek Katmanında kullanıcı ve uygulamalar için bir hizmet oluşturulup, hizmet yönetimi sağlanmakta, kullanıcılar da uygulama katmanı yardımıyla IoT sistemine erişebilmektedir.

Şekil 3. IoT güvenlik mimarisi



(Security in the internet of things: a review, Suo vd., 2012)

3.1. Olası IoT Saldırıları

Artan IoT kullanımı ile birlikte savunmasız yapısı da göz önüne alındığında, bu sistemlere yapılan siber saldırılar da giderek artmaktadır. Bu kapsamda IoT güvenliği konusunda yapılan akademik çalışmalarda; potansiyel tehditler ve saldırganlar incelenmiş ve güvenlik ile mahremiyet açısından üç grup saldırgan bulunduğu belirtilmiştir. (Atamli ve Martin, 2014):

- Kötü niyetli kullanıcı: Üreticinin sırlarını öğrenmek ve kısıtlanmış fonksiyonlara erişim sağlamak için saldırı gerçekleştiren kullanıcıdır. Sistemden gizli bilgileri öğrenerek bu sırları farklı firmalara satabilir ya da elde ettiği bir güvenlik açığını aynı özellikteki diğer cihazlarda kullanabilir.
- Kötü niyetli üretici: Ürünlerini sattıkları kullanıcılar ya da onların kullandığı diğer cihazlar hakkında bilgi toplamak için ürün geliştiren üretici firmalardır. Tasarımda cihazlar üzerinde oluşturulan arka kapı ya da zararlı yazılımlar sayesinde topladığı bilgileri casusluk amaçlı kullanabilirler. Ayrıca ortamdaki diğer internete bağlı nesneler ile iletişim kurup zarar vererek onları üreten firmaların güvenilirliğini zedeleyebilirler.
- Dış saldırganlar: Cihaz üzerinde herhangi bir erişimi ve yetkisi olmayan kötü niyetli kişilerdir. Farklı türde saldırılar uygulayarak kullanıcı hakkında bilgi toplamak, maddi zarar vermek gibi amaçları olabilir. Tehdit kaynakları arasında en yüksek orana sahip gruptur.

Literatürde yapılan çalışmalarda; IoT ağlarındaki cihazların kısıtlı bant genişliği, hafıza ve hesaplama yeteneğine sahip olmaları, onları tehditlere karşı savunmasız bıraktığı ifade edilmiştir. Bundan dolayı, bu cihazların geleneksel güvenlik tekniklerini kullanarak internetin ortaya koyduğu güvenlik sorunlarıyla başa çıkmalarının mümkün görülmediği ve IoT mimarisini oluşturan katmanların farklı özellikteki saldırılara karşı savunmasız olduğu belirtilmiştir (Wood ve Stankovic, 2002) (Karlof ve Wagner, 2003) (Görmüş vd., 2018).

Şekil 2'de görüldüğü üzere; IoT sisteminde; alınan ve işlenen veri, cihazlar yani donanım, iletimde kullanılan ağ, verilerin saklandığı bilgisayar/sunucu, kullanıcıların kullandığı uygulamalar ve tabii ki kullanıcı

olmak üzere 6 temel bileşen yer almaktadır. IoT güvenliğinin sağlanabilmesi için, bahsedilen saldırganlar tarafından gerçekleştirilebilecek saldırıların hedef alabileceği tüm bileşenlerin güvenliklerinin sağlanması gerekmektedir. Bu kapsamda IoT sisteminde en önemli bileşen veridir. Verinin temininden kullanıcıya ulaşmasına kadar gizliliğinin ve bütünlüğünün sağlanması gerekmektedir. Algılama katmanında bulunan algılayıcıların, RFID cihazı gibi donanım açısından düşük işlemcili, düşük kapasiteli ve düşük maliyetli olması, bilgi güvenliği ihlali ihtimalini de arttırmaktadır (Gubbi vd., 2013). Ağ ve haberleşme katmanı, farklı ağlardaki verinin aktarımını sağlamakta ve bu sayede değişik yapıdaki cihazlarla çeşitli teknolojiler bir arada kullanılabilmektedir (Ray, 2018). Bu yüzden de; ağ bileşeni gerek içeriden gerekse dışarıdan birçok saldırıya maruz kalabilmektedir. IoT'de sunucular, istenildiği zaman kullanılabilen, her yerden erişim sağlanabilen, ihtiyaca göre hizmet veren ve yönetimi kolay olan bulut bilişim üzerinde organize edilmektedir. Bulut bilişimde de veri bütünlüğüne, gizliliğine, transferine yönelik riskler söz konusu olabilmektedir (Chou, 2015). Uygulama katmanı en üst katman olup, kullanıcıların ihtiyaçlarına istinaden hizmet vermekte ve Sunucu ve Depolama Katmanında bulunan sistem yönetimi ve işletimi ile etkileşim içinde çalışabilmesi için çeşitli yazılımlar bulundurmaktadır. Burada kullanılan yazılımlara karşı gerçekleştirilebilecek saldırılar sistemin yönetiminin yetkisiz kişilerce ele geçirilmesi veya sistemdeki verilerin ele geçirilmesine neden olabilmektedir. Gerek sistemin kurulu bulunduğu kurumda çalışan kişiler, gerekse kurum dışından kişiler tarafından bilinçli ya da bilinçsiz olarak sisteme zarar verilebilmektedir. IoT'nin karmaşık yapısı göz önüne alındığında kullanıcı bileşenine yönelik de saldırı gerçekleştirilmesi söz konusudur.

IoT bileşenlerine yönelik olası saldırılar sınıflandırılmış (Ülker vd., 2017) olup, açıklamaları ve oluşturacağı riskler (İDKK, 2014) ile birlikte Tablo 1'de verilmiştir.

Tablo 1. Olası Saldırılar, Oluşturacağı Riskler ve İlgili Bileşenler

Saldırı Adı	Saldırı Açıklamaları	Saldırı Sonucu Oluşan Risk	Veri	Donanım	Ağ	Sunucu	Uygulama	Kullanıcı
ACK (Acknowledgement) Saldırısı	Saldırgan Kaynak IP adresini hedef IP adresi olarak gösterip SYN paketi yollar ve alıcının hedef SYN paketi yollamadığı halde ACK yoklamasıyla gerçekleşen saldırı türüdür.	Hedef sistemin hizmet veremez hale gelme riski vardır.			X	X		
Arka Kapı	İşletim Sistemi ya da uygulamalarda açıklık oluşturmaya yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, veri bütünlüğünün bozulması, kritik donanımlara yetkisiz erişim, zararlı yazılımların bilgi sistemine iletilmesi riski vardır.	X				X	
DNS (Domain Name Server) Zehirlenmesi	Önbellek veri tabanına veri ekleme silme değiştirme ile hedefi şaşırtmaya yönelik saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, veri bütünlüğünün bozulması, kritik donanımlara yetkisiz erişim, zararlı yazılımların bilgi sistemine iletilmesi, kullanıcının gitmeye çalıştığı siteden farklı bir siteye yönlendirilmesi riski vardır.			X			
E Posta Sahteciliği	Sahte e posta adresini güvenilir olarak gösterilerek gerçekleştirilen saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, kritik donanımlara yetkisiz erişim riski vardır.	X					
Fiziksel Saldırı	Doğrudan ağın çalışmasını sağlayan donanımlara zarar vermeye yönelik saldırılardır.	Sunuculara, cihazlara veya ağa zarar vererek sistemin hizmet veremez hale getirilmesi riski vardır.		X	X	X		

Saldırı Adı	Saldırı Açıklamaları	Saldırı Sonucu Oluşan Risk	Veri	Donanım	Ağ	Sunucu	Uygulama	Kullanıcı
IP Sahteciliği	Saldırganın gizli dinleme sonucu edindiği paketin şifreli olmaması durumunda kaynak IP adresini değiştirerek hedef sistemi yanıltmasıdır.	Sistemin hizmet dışı kalması, DDoS da zombi cihaz olma riski vardır.	X		X	X	X	
Keylogger (Tuş Kaydedicisi)	Klavyeye basılan tuşları kaydetmeyi amaçlayan yazılımdır.	Veri kaybı, veri hırsızlığı riski vardır.	X					
Oltalama	e posta yardımıyla kişisel bilgileri ele geçirmeye yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri hırsızlığı riski vardır.	X					X
Ortadaki Adam Saldırıları	Haberleşen iki uç arasına girerek veriyi dinlemeye, yakalamaya yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri hırsızlığı riski vardır.	X		X			
Oturum Çalma	İstemci ile sunucu arasına girerek kullanıcı oturumunu ele geçirmeye yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri hırsızlığı, kullanıcılar tarafından bilinçli ya da farkında olmadan bilgi sistemleri üzerinde erişim yetkisi arttırma işlemlerinin gerçekleştirilmesi riski vardır.	X					
Ölümcül Ping	Saldırganın büyük boyutlu paketleri hedef sisteme göndererek hizmet dışı kalmasına neden olan saldırı türüdür.	Hedef sistemin hizmet veremez hale gelme riski vardır.		X	X	X		
Reklam Yazılımı	Reklam görüntülemek ve kişilerin ilgi odağına göre veri toplanılmasına yönelik yazılımdır.	Kişiler ve kişilerin ilgi alanları hakkında bilgi toplanması riski vardır.	X					X
Smurf Saldırısı	Saldırganın ağdaki bilgisayarlara hedef sistemin IP adresinden ICMP (Internet Control Message Protocol) paketi yollayarak alıcı bilgisayarların sürekli ACK mesajı yollamasına neden olan saldırı türüdür.	Hedef sistemin hizmet veremez hale gelme riski vardır.		X	X	X		
Solucanlar	Ağ bağlantısı üzerinden bulaşarak sistemdeki dosyalara zarar verme, bilgisayarın işleyişini bozmayı hedeflemektedir.	Veri kaybı, veri sızıntısı, veri hırsızlığı, veri bütünlüğünün bozulması, kritik donanımlara yetkisiz erişim, zararlı yazılımların bilgi sistemine iletilmesi, hedef sistemin zarar görmesi riski vardır.	X			X	X	
Sosyal Mühendislik	Hedef sistemdeki kişi hakkında bilgi edinebilmek için kişilerin kandırılması yöntemiyle gerçekleştirilen saldırı türüdür.	Kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, kritik veri, bilgi ve cihazların bilinçli ya da farkında olmadan değiştirilmesi riski vardır.	X					X
Spam	Herhangi bir amaç doğrultusunda hedef sistemin e postalarına gelen iletilerdir.	Amacına göre değişmekle birlikte; kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, kritik veri, bilgi ve cihazların bilinçli ya da farkında olmadan değiştirilmesi riski vardır.	X					X

Saldırı Adı	Saldırı Açıklamaları	Saldırı Sonucu Oluşan Risk	Veri	Donanım	Ağ	Sunucu	Uygulama	Kullanıcı
SQL (Structured Query Language) Enjeksiyonu	SQL sorgularına müdahale ederek hedef sistemin bilgilerini edinmeyi amaçlar.	Veri kaybı, veri hırsızlığı, veriler üzerinde değişiklik yapılarak bütünlüğün bozulma riski vardır.			X			
SYN (Synchronize) Saldırısı	Saldırgan hedef sisteme ardışık olarak SYN bayraklı TCP (Transmission Control Protocol) paketi göndererek hizmet veremez hale getirir.	Hedef sistemin hizmet veremez hale gelme riski vardır.		X	X	X		
Tekrarlama Saldırıları	Haberleşen iki uç arasındaki paketin saldırgan tarafından ele geçirilerek tekrar tekrar alıcıya iletilmesiyle gerçekleşen saldırıdır.	Verilere yetkisiz erişim riski ile sistemin hizmet veremez hale gelme riski vardır.	X		X			
Truva Atları	Bilgisayar yazılımı olup, bulaştığı bilgisayardaki bilgileri dışarı sızdırmaktadır. Saldırgan ağ bağlantısı üzerinden kurbanın bilgisayarını kontrol etmektedir.	Kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, sistemin zarar görmesi riski vardır.	X				X	
UDP Saldırısı	Saldırının temel prensibi farklı bir IP adresini kullanarak hedef sistemin portlarına büyük boyutlu UDP (User Datagram Protocol) paketleri yollamaktır.	Hedef sistemin hizmet veremez hale gelme riski vardır.			X	X		
Virüsler	Zararlı bilgisayar yazılımı olup bilgisayarın işleyişini değiştirmektedir.	Kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, sistemin zarar görmesi riski vardır.	X		X	X	X	
Web Sahteciliği	Güvenilen bir web sitesinin sahtesini kullanarak gerçekleştirilen saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, kritik donanımlara yetkisiz erişim riski vardır.	X					

(Ülker vd., 2017 ve İDKK, 2014 kaynaklarından faydalanılarak yazarlar tarafından oluşturulmuştur.)

4. YAŞANMIŞ OLAYLAR

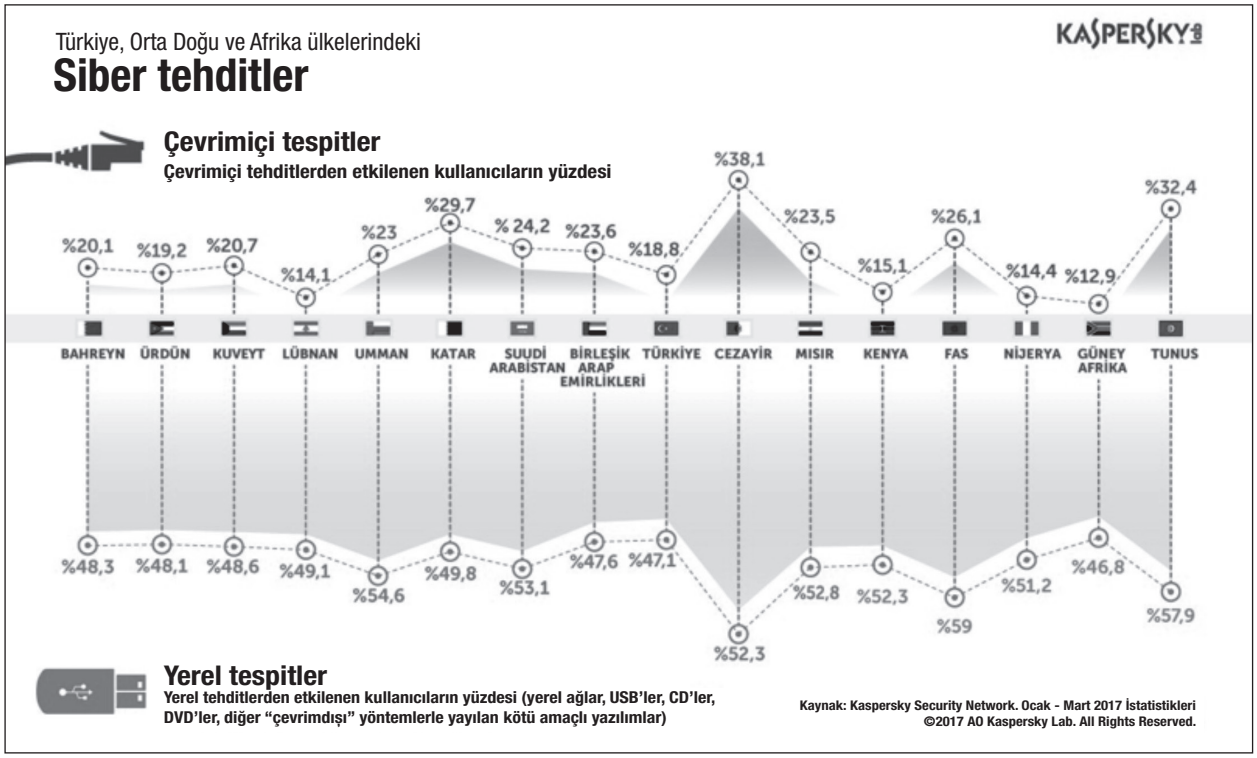
Trend Micro firmasının yayınladığı Akıllı Ev Ağı Güvenlik Özeti (Smart Home Network Security Summary) adlı raporda, IoT güvenlik zafiyetlerinin oluşturduğu tehditlerden en çok etkilenen 10 ülke açıklanmıştır (Trendmicro, 2017). Rapor incelendiğinde ABD, Çin ve İngiltere'nin %28, %7 ve %7 ile ilk üç sırayı aldığı, listede onları Hong Kong, Kanada, Avustralya, İsveç, Hollanda, Tayvan ve Rusya'nın izlediği görülmektedir. Bu ülkelerde yaşanan siber saldırıların, dünya genelinde yaşanan saldırıların %70'ini oluşturduğu ifade edilen raporda, son dönemde özellikle BitCoin üretimi için kullanılan ve birbirleriyle konuşan cihazların da siber suçlular için sömürülecek yeni bir pazar oluşturduğu belirtilmiştir.

Kaspersky firmasının 2017 yılında yayınladığı IoT güvenlik raporu da içerdiği veriler açısından oldukça çarpıcı sonuçlara yer vermektedir (Kaspersky, 2017).

Kaspersky tarafından paylaşılan rapora göre; beyaz eşyadan endüstriyel sistemlere kadar geniş ölçekte kullanılan IoT cihazlarının ülkemizin de içerisinde bulunduğu bölgede %45 oranında siber saldırılara maruz kaldığı görülmektedir. Bunun yanı sıra %47,1 oranında çevrimdışı yerel saldırılara maruz kalındığı tespit edilen ülkemizin %18,8 oranında da çevrimiçi saldırıya maruz kaldığı iletilmiştir.

2016 yılında gerçekleştirilen ve yakın tarihin en büyük siber olaylarından olan DDOS saldırısının hedefi doğrudan dünya çapında internet erişimiydi (Karakullukçu, 2017). Yapılan saldırılar sırasında, o güne

Şekil 4. Siber güvenlik tehditlerine ilişkin tespitler



(Kaspersky Security Network. Ocak – Mart 2017 İstatistikleri)

kadar kullanılan cihazlardan farklı olarak IoT cihazlarının yoğun sayıda kullanıldığı tespit edilmiştir. Mirai isimli bir kötücül yazılım kullanan siber saldırganlar yine bu yazılım sayesinde yaklaşık 620 GB'lık bir veri trafiği oluşturmayı başarmışlardır. Ana hedefi ABD olmasına rağmen ülkemizde de birçok internet servisine erişimde sıkıntılara neden olmuştur.

2017 yılında Amerikan Gıda ve İlaç İdaresi (FDA) tarafından yapılan açıklama ile ülke genelinde yaklaşık 500.000 kalp pilinin, kritik güvenlik açığı nedeniyle geri çağrıldığı duyurulmuştur. Bu geri çağırmaya sebep olan ana neden ise; hayati öneme sahip bu IoT cihazlarının kötü niyetli kişiler tarafından kontrol edilebileceği ya da kullanılmaz hale getirilebileceği endişesi olmuştur (FDA, 2017). Sonrasında cihaz için yayımlanan yazılım güncellemesi ve daha sonraki partilerde üretilen cihazların da güncel yazılım ile kullanıma sunulması bu zafiyetin kapatılmasını sağlamıştır.

2016 yılında gerçekleşen bir başka örnek de, kalp hızı ve egzersiz aktivitesi seviyesi gibi kullanıcı bilgilerini izleyen giyilebilir bir teknoloji olan Fitbit cihazı ile ilgilidir. Bilgisayar korsanları birçok müşterinin hesaplarına sızarak bilgi edinebilmişlerdir. Bu saldırı, cihazın IoT ekosisteminin bir parçası olmasının doğrudan bir sonucu olmasa da, Fitbit'in bu giyilebilir cihazının internete bağlanması nedeniyle faillere sunulan bilgiler büyük oranda artmıştır. Bilgisayar korsanları yalnızca müşteri bilgilerine erişmemişler, aynı zamanda belirli kullanıcıların akşam koşularındaki kullanabileceği popüler rotaları görmelerine izin veren GPS geçmişi gibi bilgilere de ulaşabilmişlerdir. Birçok kişi bu bilginin elde edilebileceğinin farkında olmadığı gibi ve bu türden güvenlik açıklarının farkına varmak, müşterilerin bu ürünleri kullanmak istememesindeki en büyük etkenlerden biridir. Buna ek olarak, bu gibi güvenlik ihlalleri, ele geçirilmiş hesapların çok zayıf şifrelere sahip olmasından dolayı, şirketlerin olduğu kadar tüketicilerin de kusuru olduğu ifade edilmiştir (McGee, 2016).

Bir başka IoT cihazlarındaki açıklardan kaynaklı kötüye kullanım için örnek de (Greenberg, 2017), ses tanıma özelliğini "akıllı asistan" ile birleştiren bir akıllı

hoparlör olan, Amazon Echo cihazıdır. Mark Barnes adında bir İngiliz araştırmacı, kötü niyetli bir kişinin, bu cihazda kötü amaçlı yazılımları kolayca çalıştırabildiğini ve iz bırakmadan "gizlice dinleme mikrofonu" haline getirebileceğinin farkına varmıştır. Bu; kötü niyetli kişilerin, insanların evlerinde yani kendilerini güvenli hissettikleri bir ortamda, izinsiz ve gizlice konuşmalarını dinlemesine olanak sağlayacaktır. Bu tür cihazlar genellikle ofis ve otel odalarında dışarıda gözetim altında olmadan bırakabildiği için oldukça kolay bir şekilde cihaza müdahale edilebilmektedir. Amazon, bu sorunu 2017 model Echo cihazlarında düzeltebilmiştir; ancak, bu önceden satın alınan herhangi bir Echo cihazını güvenli hale getirememiştir. Amazon konu hakkında yorumda bulunduğunda, sadece; Echo cihazının kullanıcılarına güvenliğini "güvenilir perakendecilerden satın aldıkları" ve "yazılımlarının güncel olmasını sağladıkları sürece" iyi olacağını garanti etmekle yetinmiştir.

Otomobillerin internete daha çok bağlanması ve toplumun sürücüsüz araçları benimsemesi sayesinde, bu araçlar da çeşitli saldırıların hedefleri olabilmektedir. Alman Güvenlik Konferansı DIVMA'da, Trend Macro adlı bir güvenlik firması, siber saldırganların, bir aracın dahili ağını kullanmasına ve araç içinde mesaj gönderen bileşenlere müdahale etmesine izin veren, az bilinen bir korsanlık tekniğini vurgulamıştır. Buna göre, bir bilgisayar korsanı bu güvenlik açığından yararlanabilirse, hava yastığını ve kilitlenmeyi önleyici frenleri devre dışı bırakabilecek, aracın kilidini açabilecek ve hatta arabanın çalınmasına izin verebilecektir (Greenberg, 2017). Charlie Miller ve Chris Valasek adında iki araştırmacı ise, yaptıkları çalışmada (Drozhzhin, 2015), standart bir Jeep SUV'un kablosuz internet erişim sistemine girebilmişler ve daha sonra otomobilin kontrol alan ağına erişim sağlayarak ana sistemi ele geçirmişlerdir. Bu aşamadan sonra, otomobili hızlandırabilmek, yavaşlatmak ve hatta yoldan saptırabilmek için aracı kontrol edebildiklerini göstermişlerdir.

Günümüzde evler de, IoT güvenlik açıkları dikkate alındığında güvenli görünmemektedirler. "Akıllı kilitler" veya bluetooth özellikli bir cihazla (cep telefonu gibi) kilitlenebilen ve kilidi açılabilen kilitler kısa bir süre önce DEF CON olarak bilinen bir siber saldırı sözleşmesinde kullanılmıştır (Wollerton, 2016). İki Mercurlite güvenlik çalışanı olan Anthony Rose ve Ben Ramsey, 16 farklı tip akıllı kilitten 12'sini nispeten rahatlıkla kırmayı başarmışlardır. Bu cihazları kilitlemek için kullanılan şifrelerin şifrelenmemiş olduğunu, daha doğrusu düz metinde saklandığını tespit etmişler ve yaklaşık 100 $ için, bu kilitleri ele geçirmeyi, şifreyi keşfetmeyi ve kapıyı açmayı başarmışlardır.

Bir başka örnek olarak, Nest firmasına ait kullanıcıların evlerini bulundukları yerden kolayca izleyebilmelerini sağlayan bluetooth özellikli bir güvenlik kamerası verilebilir (Estes, 2017). Bir güvenlik araştırmacısı olan Jason Doyle, kameranın bluetooth bağlantısını amacı dışında kullanmanın bir yolunu bulmuştur. Söz konusu kameralar internete bağlı olduklarından, bir bilgisayar korsanının basit bir bluetooth komutuyla kamerayı kolayca kapatıp ve işe yaramaz hale getirebileceğini tepsit etmiştir. Bu sayede iz bırakmadan hırsızlık amacıyla bir eve girilebileceği gibi, evdeki internet ağına girilebilmesine bile imkan verecektir. IoT'nin bir parçası olan masaüstü ya da dizüstü bilgisayarlar ile web kameraları da saldırıların hedefi olabilmektedir. Rezitech Inc. isimli bilgisayar firmasında teknisyen olarak çalışan Trevor Harwell, teknik servise tamir için gelen bilgisayarlara kurduğu uzaktan erişim programı (remote acces tool, RAT) ile bilgisayarın dahili algılayıcılarından bir tanesinin arızalandığını bildiren sahte bir mesaj görüntüleyerek kullanıcılardan bilgisayarlarını sıcak buharın yanında birkaç dakika beklettikleri takdirde sorunun düzeleceğini söylemiş ve inanması zor gelse de birçok kullanıcı banyo yaptıkları sırada bilgisayarlarını da yanlarında götürmüş, RAT sayesinde birçok görüntü ve videolarının izinleri dışında kaydedilmesine engel olamamışlardır. CamCapture yazılımı ile görüntüleri adres gösterdiği sunucuya yükleyen saldırgan, eylemleri sonucunda 1 yıl hapis cezası almıştır (Plummer, 2011).

Ayrıca bebek kamerası olarak kullanılan internet üzerinden izlenebilen IP kamera ve monitörlerin de kötü niyetli kişiler tarafından ele geçirildiğini belirten birçok haber bulunmaktadır. Bununla birlikte internete bağlı yazıcılardan buzdolaplarına, termostatlara kadar birçok "akıllı" cihaz siber saldırıların hedefi olabilmektedir (Wang, 2018).

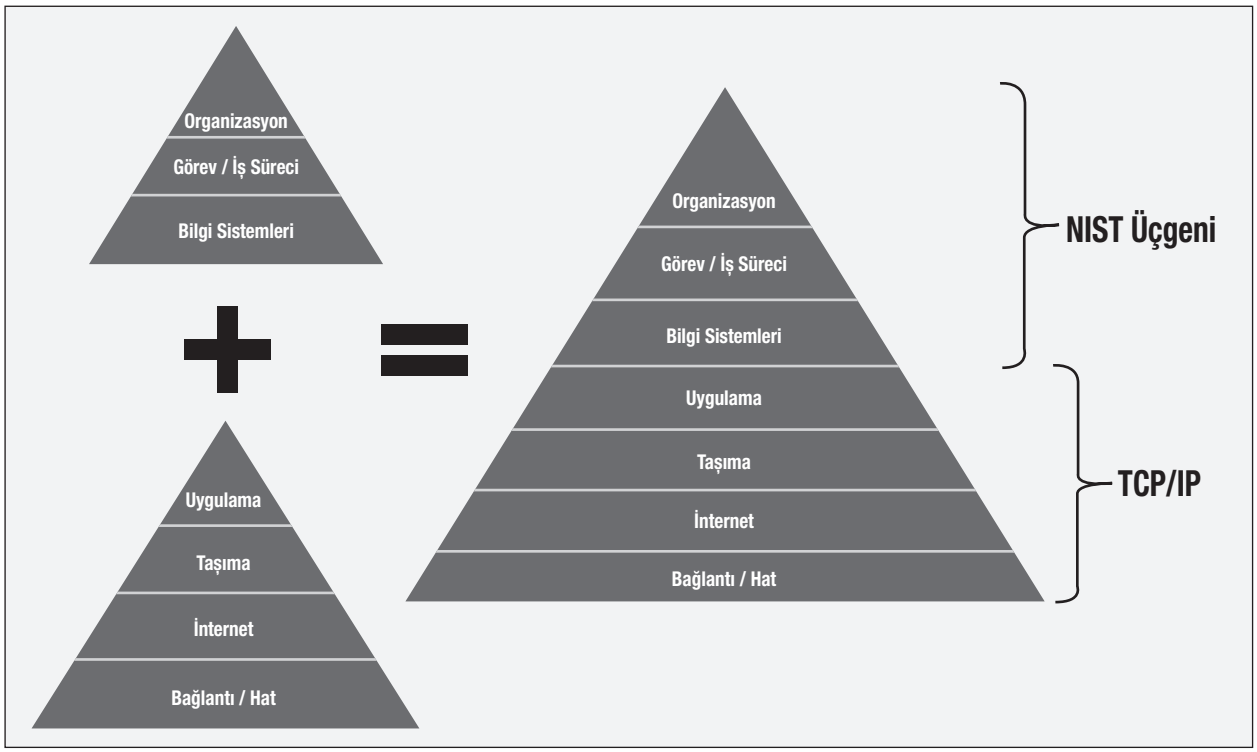
5. IoT DENETİMİNE YÖNELİK KONTROL LİSTESİ

Önceki bölümlerden de görüldüğü üzere IoT giderek artan kullanımıyla artık hayatımızın büyük bölümünde yer almakta olup, birçok saldırının da hedefi olmaktadır. Bu yüzden ilgili sektörlerin, güncel siber güvenlik stratejileri ve operasyonlara yapılacak büyük değişiklikler için hazırlıklı olması gerekmektedir. IoT'nin getirdiği zorluklar sağlam planlama, iyi güvenlik stratejileri ve sıklıkla yapılan IoT denetim değerlendirmeleriyle; ileriye dönük bir şekilde çözülmelidir (Gonzalez, 2015). IoT denetimi için genel bir denetim modelinin benimsenmesi ve mevcut belgelerden uygulanabilir kontrollerin seçilmesi tavsiye edilmektedir (Cooke ve Raghu, 2018). Bu kapsamda Jekot ve Pavlosoglou tarafından yapılan çalışma (Jekot ve Pavlosoglou, 2017) ile bir denetim yöntemi önerilmiştir. Bu yöntemde öncelikle IoT cihazının uçtan uca kullanım durumu, Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (Ulusal Standartlar ve Teknoloji Enstitüsü, NIST) SP 800-53'ün kontrol listesine göre incelenmekte, yüksek öncelikli (P1- Priority 1) atanmış kontroller seçilmektedir. Söz konusu kontrollerde "bilgi sistemi" ifadesi "IoT cihazı", "Organizasyon" ifadesi ise "kullanım ortamları" veya "üretici" olarak değiştirilmiştir. Daha sonra NIST SP 800-53 standardında IoT cihazının kullanım amacı ve kullanım alanı düşünülerek kontroller "uygulanabilir" olarak işaretlenmiştir. Burada IoT'ye özgü kontrollerin listesi elde edilirken ilgili olmayan maddeler ise çıkarılmıştır. Kontroller gruplanırken, IoT cihazlarının ortak TCP/IP yığını ve gerçekleştirilmesi gereken işin amacı özelliklerinin birleştirilmesi düşünülerek oluşturulan ve Şekil 5'te gösterilen TCP/IP yığını ile NIST'in "Organizasyon, Görev ve Bilgi Sistemi Görünümü" katmanlarından seçilerek türetilmiştir.

Bu gruplama ile ortaya çıkan kalıplara dayanarak kullanım durumu için geçerli kontrollerin 12 madde olarak listelenmesi sağlanmıştır.

1. Fiziksel Erişim Kontrolü (NIST 800-53/PE-3):
   - Üretici;
     - IoT cihazına fiziksel erişim yetkilerini zorunlu tutar.
     - IoT cihazına erişim izni vermeden önce bireysel erişim yetkilerini doğrular.
     - Giriş/çıkışı kontrol eder.

Şekil 5. NIST SP 800-39 ile TCP/IP büyütme modeli



(An IoT Control Audit Methodology Jekot ve Pavlosoglou, 2017)

- Fiziksel erişim denetleme kayıtlarını tutar.
- IoT cihazındaki alanlara erişimi kontrol eder.
- Kombinasyonlar tehlikeye girdiğinde IoT cihazındaki kombinasyonları ve anahtarları değiştirir.

2. İletim Gizliliği ve Bütünlüğü (NIST 800-53/SC-8):
   - IoT cihazı, iletilen bilgilerin gizliliğini ve bütünlüğünü korur. Bu kontrol hem iç hem de dış ağlar ve bilginin aktarılabileceği algılayıcı, mobil cihaz, giyilebilir teknolojiler, yazıcı, fotokopi makinesi gibi her türlü IoT bileşeni için geçerlidir.
3. Sınır Koruması (NIST 800-53/SC-7):
   - IoT cihazı:
     - Sistemin dış sınırındaki ve sistem içindeki temel iç sınırlarda iletişimi izler ve kontrol eder.
     - İç kullanım ortamından ayrılmış halka açık sistem bileşenleri için alt ağlar kurar.
     - Harici ağlara veya bilgi sistemlerine, yalnızca üreticinin güvenlik mimarisine uygun olarak düzenlenmiş sınır koruma cihazlarından oluşan yönetilen arayüzler üzerinden bağlanır.
4. Cihaz Tanımlama ve Doğrulama (NIST 800-53/IA-3):
   - IoT cihazı, yerel, uzak veya ağ bağlantısı kurmadan önce diğer cihazları benzersiz bir şekilde tanımlar.
   - Üretici, IoT cihazlarının güvenlik kategorileri tarafından istenen kimlik doğrulama mekanizmalarının gücünü belirler ve ayrıca, doğrulamaya dayalı cihaz tanımlama ve doğrulamanın üretici tanımlı konfigürasyon yönetimi süreçleri tarafından yapılmasını sağlar.
5. Ortak Bilgi İşlem Cihazları (NIST 800-53/SC15):
   - IoT cihazı:
     - Üreticinin açık bir şekilde izin verdiği durumlar haricinde ortak bilgi işlem cihazlarının uzaktan etkinleştirilmesini yasaklar.
     - Cihazlarda fiziksel olarak mevcut olan kullanıcılara açık bir kullanım göstergesi sağlar. (Örneğin, açık kullanım göstergesi, ortak bilgi işlem cihazı etkinleştirildiğinde kullanıcıya sinyal verir.)
6. Kimlik ve Kullanıcı Kimlik Doğrulama (NIST 800-53/IA-2):
   - IoT cihazı, üretici kullanıcılarını (veya üretici kullanıcıları adına hareket eden işlemleri) benzersiz şekilde tanımlar ve doğrular. Üretici, grup hesaplarındaki bireylerin benzersiz tanımlanmasını veya bireysel faaliyetlerin ayrıntılı hesap verebilirliğini talep edebilir. Üretici, kullanıcı kimliklerini doğrulamak için şifreleri, jetonları veya biyometreleri ya da çok faktörlü doğrulama durumunda, bunların bir kombinasyonunu kullanır.
7. Hesap Yönetimi (NIST 800-53/AC-2):
   - Üretici;
     - Görevleri/işletme işlevlerini desteklemek için sistem hesaplarını tanımlar ve seçer.
     - Hesap yöneticileri atar.
     - Grup ve rol üyeliği için koşullar belirler.
     - Her bir hesap için yetkili kullanıcıları, grup ve rol üyeliğini ve erişim yetkilerini belirtir.
   - Üretici veya cihaz sahibi;
     - Üretici tarafından tanımlanan prosedürlere veya koşullara uygun olarak cihaz hesaplarını oluşturur, etkinleştirir, değiştirir, devre dışı bırakır ve kaldırır.
     - Hesap yöneticilerini bilgilendirir, hesap yönetimi gereksinimlerine uyması için hesapları yetkilendirir ve hesapları inceler.
     - Grup kimlik bilgilerini yönetir.
8. En Az İşlevsellik (NIST 800-53/CM-7):
   - Üretici;
   - IoT cihazını sadece temel yetenekleri sağlayacak şekilde yapılandırır.
   - Bir dizi tanımlanmış fonksiyon, port, protokol ve / veya hizmet kullanımını yasaklar veya kısıtlar.
9. Cihaz Beklemedeyken Bilgilerin Korunması (NIST 800-53/SC-28):
   - IoT cihazı, bekleme konumunda iken de hem kullanıcı hem de sistem bilgilerinin gizliliğini ve bütünlüğünü korur.
10. Sistem Güvenlik Planı (NIST 800-53/PL-2):
    - Üretici;
      - Kurumsal mimarisine uygun bir güvenlik planı geliştirir ve izin sınırlarını açıkça tanımlar.

- Cihazın operasyonel bağlamını ve operasyonel ortamını görevler ve iş süreçleri açısından açıklar.
- Sistem için güvenlik gereksinimlerine genel bir bakış sunar.
- Sebepleri de dâhil olmak üzere bu gereklilikleri karşılamak için uygulanan güvenlik kontrollerini açıklar.
- Cihazdaki ve/veya çalışma ortamındaki değişikliklerin veya plan uygulaması veya güvenlik kontrol değerlendirmeleri sırasında tespit edilen sorunların ele alınması için planı günceller.
- Güvenlik planını izinsiz açıklama ve değişiklikten korur.

11. Misyon/ İş Süreci Tanımı (NIST 800-53/PM-11):
    - ➢ Üretici;
        - Bilgi güvenliği ve kullanım ortamı, üretici varlıkları, bireyler, diğer üreticiler ve kullanıcılar için oluşan çevre riskini göz önünde bulundurarak görev/iş süreçlerini tanımlar.
        - Belirlenen görev/iş süreçlerinden kaynaklanan bilgi koruma gereksinimlerini belirler ve ulaşılabilir koruma ihtiyaçları elde edilene kadar gereken süreçleri gözden geçirir.
12. Bilgi Güvenliği Program Planı (NIST 800-53/PM-1):
    - ➢ Üretici;
        - Bir bilgi güvenliği programı planı geliştirir ve yayar.
        - Güvenlik programına ilişkin gereksinimlere genel bir bakış ve bu gereksinimleri karşılamak için yürürlükte olan veya planlanan güvenlik programı yönetim kontrollerinin ve ortak kontrollerin bir tanımını sunar.
        - Bilgi güvenliğinin farklı yönlerinden sorumlu olan örgüt varlıkları arasında koordinasyon sağlar.
        - Planın, riske karşı sorumluluk ve hesap verebilirliği olan üst düzey bir yetkili tarafından onaylanmasını sağlar.

Kullanım durumlarına dayanarak, bu kontrollerin değerlendirilmesi eksiksiz bir denetimin gerçekleştirilmesi için yeterli bir temel teşkil edecektir ancak böyle bir denetimi geçecek bir IoT cihazı henüz geliştirilmemiştir. IoT endüstrisi geliştikçe boşluklar belirlenirse, gerektiğinde söz konusu yönteme daha fazla kontrol eklenebilecektir (Jekot ve Pavlosoglou, 2017).

6. IoT GÜVENLİĞİ İÇİN ÖNERİLER

IoT cihazları; arabalar, oyuncaklar, giyilebilir teknolojiler ve elektrikli ev aletleri gibi çeşitlilik göstermektedir. IoT ekosistemindeki çeşitlilik ve karmaşıklık, güvenlik çalışmalarının farklı seviyelerde ve farklı paydaşlarca yapılmasını gerektirmektedir.

Cihaz güvenliğine, cihazların tasarım ve üretim aşamasından başlanmalıdır. Bu aşamada donanımsal olarak güvenlik önlemi alınabileceği gibi varsayılan parolaların değiştirilmesi ve zor parola seçilmesi gibi bazı kullanıcı ayarları varsayılan olarak zorunlu hale getirilebilir.

Kullanıcıların ve cihazların erişim ayrıcalıklarının sağlanması için kimliklerin doğrulanma, yetkilendirilme ve denetlenme mekanizmaları sağlanmalıdır. Bir ağın güvenli bölümlere ayrılması ile IoT cihazlarının ana bilgi işlem cihazlarından ayrılmasına yardımcı olarak güvenlik artırabilir (BizTech, 2017).

Mümkün olduğunca IoT cihazlarını internetten gizlemek de, internette arama yaparken cihazların keşfedilememesini sağlayacaktır.

Cihaz ve şebeke arasında şifrelenmiş bir sanal özel ağ (VPN) bağlantısı kurmak, cihazdan ağa verilen bilgilerin bütünlüğünü tehlikeye atacak üçüncü kişilerin erişim ihtimalini azaltacaktır.

IoT sistemi, İzinsiz Giriş Tespit Sistemleri (IDS) ile sürekli izlenmelidir.

IoT cihazları kuruluşlara entegre edildiğinden, mevcut bilgi teknolojileri politika ve prosedürleri bu cihazları kapsayacak şekilde genişletilmelidir.

Güvenlik kontrolleri uygulanmalı ve IoT cihazlarının, ağlarının ve altyapısının geçirgenliği değerlendirilmeli ve güncel olmalıdır.

IoT ekosistemi kurumlara entegre edildiğinden, getirdikleri risk de yönetilebilir bir şekilde değerlendirilmelidir.

Bunlarla birlikte, IoT ekosisteminde kullanılan kamera gibi farklı cihazlara özgü güvenlik önlemeleri de alınmalı ve kullanıcı farkındalığı artırılmalıdır.

Ayrıca, Tablo 1'deki bileşenlere yönelik saldırı türlerine karşın alınabilecek önlemler de şu şekildedir (Ülker vd., 2017):

ACK, UDP saldırılarına karşın; zaman aşımı (timeout) değerini düşürmeli, saldırı tespit sistemi ve güvenlik duvarı kullanılmalı, yönlendirme seviyesinde koruma sağlanmalıdır.

Arka Kapı, reklam yazılımı, solucanlar, spam, truva atları ve virüs saldırılarına karşın; anti-virüs ve güvenlik duvarı kullanılmalıdır.

DNS zehirlenmesine karşın; saldırı tespit sistemi kullanılmalıdır.

E-posta sahteciliğine karşın; e-posta doğrulama mekanizması, alan adı anahtarı kimlik doğrulama mekanizması, tek kullanımlık şifre, şifreleme algoritması kullanılmalıdır.

IP sahteciliğine karşın; zaman aşımı değeri düşürülmeli, kaynak IP adresini doğrulama mekanizması ve Hop sayısını filtreleme (HCF) kullanılmalıdır.

Tuş kaydedicisine (keylogger) karşın; anti-casus yazılım ve güvenlik duvarı kullanılmalıdır.

Oltalama (phishing) saldırısına karşın, oltalama saldırıları saptama mekanizması kullanılmalı ve kullanıcılar bilinçlendirilmelidir.

Ortadaki adam (man in the middle) saldırısına karşın; şifreleme algoritması, güvenlik duvarı ve sızma önleme sistemi (IPS) kullanılmalıdır.

Oturum çalma saldırısına karşın; güvenli protokol kullanımı sağlanmalı, koruma mekanizması ve şifreleme algoritması kullanılmalıdır.

Ölümcül ping ve yoğun paket gönderimi (smurf) saldırılarına karşın; saldırı tespit sistemi, güvenlik duvarı ve anti-virüs programı kullanılmalı, yönlendirme seviyesinde koruma sağlanmalıdır.

Sosyal mühendislik saldırısına karşın, kullanıcılarda farkındalık sağlanmalıdır.

Yapılandırılmış Sorgu Dili (Structured Query Language, SQL) Enjeksiyonu saldırısına karşın; güvenli veri tabanı konfigürasyonu ile saldırı tespit sistemi kullanılmalıdır.

Eşzamanlı (SYN) saldırısına karşın; SYN çerezleri (cookies), SYN ön bellek (cache), SYN ağ vekili (proxy) güvenlik duvarı, IPS ve IDS kullanılmalı ve yönlendirme seviyesinde koruma sağlanmalıdır.

Tekrarlama saldırısına karşın, şifreleme algoritması ve güvenlik duvarı kullanılmalıdır.

Web sahteciliği saldırısına karşın; tek kullanımlık şifre ve şifreleme algoritması kullanılmalıdır.

7. SONUÇ

Sensörlerin ve diğer IoT cihazlarının, sağladıkları gerçek zamanlı veriler sayesinde giyilebilir teknolojilerin yanı sıra; güvenlik, otomasyon, tarımsal üretim, meteoroloji, envanter, akıllı ev, hastane, eğitim, aydınlatma, iletişim ve altyapı, kritik altyapılarda kontrol, yapay zeka destekli güvenlik ve takip sistemleri ile başta otomotiv ve ulaşım sektörleri olmak üzere endüstride çokça kullanılmakta olduğu ve hayatımızın her alanında gün geçtikçe daha sık yer aldığı aşikardır.

Kullanımının bu denli yaygınlaştığı IoT cihazlarını içerisinde barındıran söz konusu sistemlere karşı; veri hırsızlığı, veriler üzerinde değişiklik yaparak veri bütünlüğünü bozma; sunuculara, cihazlara, kritik alt yapılara ve bunların iletişiminde kullanılan ağlara zarar vererek bu sistemlerin hizmet veremez hale getirilmesi, kritik donanımlara yetkisiz erişim kritik verilerin ve bilgilerin değiştirilmesi ve/veya silinmesi gibi amaçlarla yapılan saldırılar olmaktadır. Bu saldırıların planlı olabileceği gibi bilinçsiz kullanıcılar tarafından farkında olmadan da doğrudan yapılabildiği ya da yapılan saldırıların parçası olarak gerçekleşebilmektedir. Bu noktada bu tür saldırıların kişisel veya kurumsal olarak maddi ve manevi zarara yol açacağı da çok açık şekilde görülmektedir.

Bu düzeyde kritik öneme sahip olmasına karşın, Internet of Business (2017) tarafından yapılan bir ankette, IoT kullanıcılarının %48'inin, bilgisayarlarının kötü niyetli kişiler tarafından ele geçirilebileceğinin ve geniş çaplı siber saldırıların başlatılmasında kullanılabileceğinin farkında olmadıkları ortaya çıkmıştır. Buna ek olarak, ankete katılan beş kişiden yaklaşık dördünün, IoT saldırılarıyla ilgili bir haber görmedikleri veya okumamış oldukları ve uyarılara rağmen, katılımcıların %78'inin ise IoT güvenliğine olan güvensizlikleri göremedikleri ifade edilmiştir (Fearn, 2017).

Bu çalışmada ortaya konulan önerilerin doğru algılanması IoT sistemlerin güvenliği, bu sistemlerin etkileşim içerisinde olduğu diğer sistemlerin güvenliği ve kurumsal güvenlik konularına katkı sağlayacaktır. Örnekleri verilen gerçekleşmiş olayların bilinmesi-

nin, bireysel ve kurumsal kullanıcıların bu nesneleri satın alırken güvenlik konusunda daha hassas davranmalarına ve hatta kişisel ve kurumsal güvenliklerini kurarken daha doğru önlemler almalarına da olanak sağlayabileceği değerlendirilmektedir.

Bu kapsamda iç denetçiler, IoT cihazlarının üretim aşamasında fabrikalarda olduğu kadar, kullanım aşamasında da kurumlarında gerek risk analizi ve farkındalık konularında danışman, kolaylaştırıcı ya da eğitici gibi roller ile gerekse bu yeni teknolojilerin bilgi teknolojilerine bütünleşik olarak çalıştığını göz önünde bulundurarak yaptıkları denetimlerde, bu konudaki risklerin uygun şekilde kontrol edildiğine dair makul güvence sağlamak suretiyle üst yönetime yardımcı olabilecek, aynı zamanda IoT cihazlarının kullanımı sayesinde ortaya çıkan fırsatların değerlendirilmesine de katkı sağlayabilecektir.

Kaynakça

Alam F., Mehmood R., Katib I., Albeshri A. (2016). Analysis of eight data mining algorthms for smarter internet of things (IoT). *Procedia Computer Science*, 437-447.

Atamli A.W. ve Martin A. (2014). Threat-Based Security Analysis for The Internet of Things. *IEEE*, 35-43.

Atzori L., Iera A., Morabito G. (2010). The Internet Of Things: A survey. *Elsevier B.V.*

Banerjee M., Lee J., Choo K. K. R. (2018). A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, 149-160.

Chou, D. C. (2015). Cloud computing risk and audit issues. *Computer Standards & Interfaces*, 137-142.

Çavdar T., Öztürk E. (2017). Nesnelerin interneti için yeni bir mimari tasarımı. *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 39-48.

Gökrem L., Bozuklu M. (2016). Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum. *Gaziosmanpaşa Bilimsel Araştırma Dergisi*, 47-68.

Görmüş S., Aydın H., Ulutaş G. (2018). Nesnelerin interneti teknolojisi için güvenlik: var olan mekanizmalar, protokoller ve. *Gazi Üniversitesi Mühendislik Mimarlık Fakütesi Dergisi,* 1247-1272.

Gubbi J., Buyya R., Marusic S., Palaniswami M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems*, 1645-1660.

Han J., Jeon Y., Kim J. (2015). Security Considerations for Secure and Trustworthy Smart Home System in the IoT Environment . *IEEE*, 1116-1118.

Hussain R., Abdullah İ. (2018). Review of Different Encryptionand Decryption Techniques Used for Security and Privacy of IoT in Diffirent Applications. *IEEE*, 293-297.

İDKK (İç Denetim Koordinasyon Kurulu). (2014). *Kamu Bilgi Teknolojileri Denetimi Rehberi,* Ankara.

Karlof C. ve Wagner D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *IEEE*, 113-127.

Madakam S., Ramaswamy R., Tripathi S. (2015). Internet Of Things(IoT):A Literature Review. *Journal of Computer and Communication*, 167-173.

Ray, P. P. (2018). A Survey on Internet of Things Architectures. *Journal of King Saud University-Computer and Information Sciences*, 291-319.

Reyna A., Martín C., Chen J., Soler E., Díaz M. (2018). *On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems*, 173-190.

Rizvi S., Pfeffer J., Kurtz A., Rizvi M. (2018). Securing the Internet of Things (IoT): A Security Taxonomy for IoT. *IEEE*, 163-168.

Săndescu C., Grigorescu O., Rughinish R., Deaconescu R., Călin M. (2018). Why IoT security is failing. The Need of a Test Driven Security Approach. *IEEE*.

Suo H., Wan J., Zou C., Liu J. (2012). Security in the internet of things: a review. *IEEE*, 648-651.

Şenol S., Arslan K.S. (2016). Secure Trusted IoT Gateway (STIG). *Information Security Conference 2016.* Ankara: researchgate.

Ülker M., Canbay Y., Sağıroğlu Ş. (2017). Nesnelerin İnternetinin Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Açisindan İncelenmesi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 28-41.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *ScienceDirect*, 23-30.

Wood A.D. ve Stankovic J.A. (2002). Denial of Service in Sensor Networks. *IEEE*, 48-56.

Yılmaz, E. N. (2011). Education set design for smart home applications. *Wiley*, 631-638.

İnternet Kaynakları

BizTech (2017, 09 28). https://biztechmagazine.com/article/2017/09/5-keys-foolproof-iot-security adresinden alındı.

Brandon, J. (2016, 06 01). *CSO*. https://www.csoonline.com/article/3077537/security-concerns-rising-for-internet-of-things-devices.html adresinden alındı.

Buckle, C. (2016, 02 18). *Globalwebindex*. https://blog.globalwebindex.com/chart-of-the-day/digital-consumers-own-3-64-connected-devices/ adresinden alındı.

Claveria, K. (2019, 3 7). *VisionCritical*. https://www.visioncritical.com/blog/internet-of-things-stats adresinden alındı.

Cooke I., Raghu R.V. (2018). ISACA . https://www.isaca.org/JOURNAL/ARCHIVES/2018/VOLUME-5/Pages/auditing-the-iot.aspx?utm_referrer= adresinden alındı.

Drozhzhin, A. (2015, 8 6). Kaspersky. https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/ adresinden alındı.

Estes, A. C. (2017, 03 22). https://gizmodo.com/this-nest-security-flaw-is-remarkably-dumb-1793524264 adresinden alındı.

FDA. (2017, 08 29). https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm adresinden alındı

Fearn, N. (2017, 2 1). internetofbusiness. https://internetofbusiness.com/consumers-security-risks-iot-devices/ adresinden alındı.

Gartner. (2017, 2 7). https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 adresinden alındı.

Gemalto. (2017, 10 31). gemalto. https://www.gemalto.com/press/Pages/Gemalto-survey-confirms-that-Consumers-lack-confidence-in-IoT-device-security-.aspx adresinden alındı.

Gonzalez, M. H., Djurica J. (2015). ISACA. https://www.isaca-istanbul.org/nesnelerin-interneti-buyuk-firsat-saglarken-daha-cok-risk-ortaya-cikarir/ adresinden alındı.

Greenberg, A. (2017, 8 2). https://www.wired.co.uk/article/amazon-echo-alexa-hack adresinden alındı.

Greenberg, A. (2017, 8 16). https://www.wired.com/story/car-hack-shut-down-safety-features/ adresinden alındı.

Greenough, J. (2015, 02 19). Businessinsider. https://www.businessinsider.com/connected-car-statistics-manufacturers-2015-2 adresinden alındı.

Karakullukçu, E. (2017). Webtekno. https://www.webtekno.com/hackerlar-buyuk-hack-saldirisinda-evlerdeki-akilli-cihazlari-kullanmislar-h21383.html adresinden alındı.

Kaspersky. (2017, 05 20). https://www.kaspersky.com.tr/about/press-releases/2017_turkiye-yi-de-kapsayan-bolgenin-siber-tehdit-trenleri-aciklandi adresinden alındı.

Lamkin, P. (2017, 06 22). *Forbes*. https://www.forbes.com/sites/paullamkin/2017/06/22/wearable-tech-market-to-double-by-2021/#6aaf9b03d8f3. adresinden alındı.

Lohrmann, D. (2017, 11 5). *GT*. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/lack-of-trust-in-iot-security-means-more-regulation-is-coming.html adresinden alındı.

Jekot M., Pavlosoglou Y. (2017). *ISACA*. https://www.isaca.org/Journal/archives/2017/Volume-6/Pages/an-iot-control-audit-methodology.aspx adresinden alındı.

McGee, M. K. (2016, 01 11). https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793 adresinden alındı.

NIST 800-53/AC-2. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/AC-2 adresinden alındı.

NIST 800-53/CM-7. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/CM-7 adresinden alındı.

NIST 800-53/IA-2. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/IA-2 adresinden alındı.

NIST 800-53/IA-3. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/IA-3 adresinden alındı.

NIST 800-53/PE-3. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/PE-3 adresinden alındı.

NIST 800-53/PL-2. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/PL-2 adresinden alındı.

NIST 800-53/PM-1. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/PM-1 adresinden alındı.

NIST 800-53/PM-11. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/PM-11 adresinden alındı.

NIST 800-53/SC15. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/SC-15 adresinden alındı.

NIST 800-53/SC-28. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/SC-28 adresinden alındı.

NIST 800-53/SC-7. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/SC-7 adresinden alındı.

NIST 800-53/SC-8. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/SC-8 adresinden alındı.

Plummer, M. (2011, 6 10). *abcnews*. https://abcnews.go.com/US/california-computer-technician-trevor-harwell-suspected-spying-women/story?id=13806697 adresinden alındı.

Trendmicro. (2017, 08 15). https://newsroom.trendmicro.com/press-release/commercial/trend-micro-reveals-top-ten-regions-affected-iot-security-threats adresinden alındı.

Wang A. B. (2018, 12 20). *washingtonpost*. https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/?noredirect=on&utm_term=.4b3cea98a13b adresinden alındı.

Wollerton, M. (2016, 8 9). https://www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/ adresinden alındı.