



Turkish Studies

Information Technologies & Applied Sciences

Volume 13/13, Spring 2018, p. 53-66

DOI Number: <http://dx.doi.org/10.7827/TurkishStudies.13872>

ISSN: 1308-2140, ANKARA-TURKEY

Research Article / Araştırma Makalesi

Article Info/Makale Bilgisi

✍ **Received/Geliş:** Haziran 2018

✓ **Accepted/Kabul:** Haziran 2018

✍ **Referees/Hakemler:** Prof. Dr. Metin GÜMÜŞ

Dr. Öğr. Üyesi Abdullah DEMİR – Dr. Öğr. Üyesi Dursun AKASLAN

This article was checked by iThenticate.

NESNELERİN İNTERNETİNİN GETİRDİĞİ YENİLİKLER VE SORUNLARI

Aytürk KELEŞ - Ali KELEŞ***

ÖZET

Sabah işe gitmek için uyandınız. Sizin kalktığınızı kahve makinası algıladı. Sevdiğiniz şekilde kahvenizi hazırladı. Kahvenizi içerken günlük gazetelere göz attığınızı bilgisayarınız biliyor. İlgili sitelerdeki haberleri derleyip size otomatik olarak sundu. Hatta bir yapay zekâ yazılımı aracılığıyla hangi haberler daha çok ilginizi çekiyorsa bu haberleri öncelikli listesine dâhil etti. İşe gitmek için evden hareket ettiğiniz anda garajdaki arabanız bunu algıladı. Garajın kapısını açıp kendisini çalışır hale getirdi. Arabanıza bindiğinizde, gitmek istediğiniz yol doğrultusunda trafiğinin yoğun olduğunu tespit edip size alternatif yolları sundu. Nesnelerin İnterneti'nin değiştirdiği yeni hayata hoş geldiniz! Bunlar hayal değil, birçoğu bugün kullanımda ve bir kısmı da çok yakın gelecekte kullanabileceğimiz duruma gelecektir. Tüm bunlar “Nesnelerin İnterneti” (IoT - Internet of Things) adı verilen teknolojiler sayesinde mümkün olmaktadır.

Bu çalışma hayatımızı çepeçevre kuşatmaya başlayan ve gelecekte de onlarsız yapamayacağımız pek çok uygulamanın kaynağı haline gelen Nesnelerin İnterneti konusuna odaklanmıştır. Bu çalışmada nesnelerin internetinin mevcut durumu, hayatımızdaki önemi, kullanım alanları, üstünlükleri ortaya koyulurken diğer taraftan hızla yayılan ve gelişen IoT sistemlerinin zayıf yönleriyle beraberinde getirdiği ciddi tehlikeler üzerine durulmaktadır. Bu tehlikelerin kaynaklarının iyi tespit edilerek ortaya koyulması çözüm çalışmalarına hız kazandıracaktır. Bu anlamda çalışma, nesnelerin internetinin özellikle güvenlik sorunlarını analiz etmeye ağırlık vermiştir. Uluslararası alanda ayrıntılı bir araştırma sonucunu sunan bu çalışmanın alana önemli bir katkı sağlayacağı düşünülmektedir.

*  Doç. Dr., Ağrı İbrahim Çeçen Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, El-mek: aykeles@agri.edu.tr

**  Dr. Öğr. Üyesi, Ağrı İbrahim Çeçen Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, El-mek: akeles@agri.edu.tr

Yakın gelecekte güvenli IoT çözümleri, en çok maliyetlerini düşürmek ve yeni pazarlara açılmak isteyen işletmeler tarafından uygulamaya koyulacaktır. Gelişen hücresel ağ teknolojileri ile IoT aygıtları, bireyler ve kurumlar ile iletişimde olabilecekler ve biz de bu sayede onları her yerden, her zaman gözlemlene ve kontrol edebilme imkânına sahip olacağız. Böylece insanoğlu uzun zamandır hayalini kurduğu “Akıllı ve Güvenli Dünya”ya kavuşmuş olacaktır.

Anahtar Kelimeler: nesnelerin interneti, bağlanabilir nesneler, IoT uygulamaları, IoT güvenliği ve gizliliği

INNOVATIONS AND PROBLEMS COMING WITH INTERNET OF THINGS

ABSTRACT

You woke up in the morning to go to work. The coffee machine sensed you woke up. It prepared the coffee as you like. Your computer knows that you glance the daily newspaper while drinking the cafe. So it compiled the related news and offered them to you automatically. Even it added the news which most attracted your attention into its preferred list through artificial intelligence software. Our car in the garage sensed that you were ready to go work. It opened the garage door and got ready itself for your trip. When you got in your car, it determined the traffic intensity that your route had and it offered different route options to you. You are welcome to new life which has been changed by Internet of Things (IoT). All this is not a dream. Although most of these are in use, some haven't been in use yet but they will be in use soon after.

This study focused on IoT which is the resource of many applications which have begun to surround our life and we can't do without. The current situation of IoT, its importance for our life, its benefits and usage areas were revealed in this study. The study emphasizes the threats that come with the weaknesses of the IoT systems which have developed and spread very quickly. Identifying well the resources of these threats will accelerate solutions works greatly. In this mean, the study concentrates on analyzing the especially security troubles of IoT. It is thought that this study which presents the results of a detailed study in the international area will contribute to the field a lot.

In the near future, secure IoT solutions mostly will be put into practice by businesses who want to reduce their production costs and get into new markets. With developing cellular network technologies, IoT devices will be able to be in contact with individuals and organizations and we will always have the opportunity to observe and control them from anywhere thanks to this. Thus, we will have had a "Smart and Secure World" that human beings have dreamed for a long time.

STRUCTURED ABSTRACT

The Internet of Things (IoT) is the whole system that monitors physical objects, controls the data, thinks, decides, data sharing, and communicates with each other. IoTs include devices with low power

consumption, electronic sensors, and wireless networking. IoTs have the ability to detect, communicate, address, and manipulate data. IoTs have the ability to detect, communicate, address and process data. The number of system applications which are used these devices is increasing.

Smart Home systems are at the beginning of these applications. Many electronic devices in the home are now able to connect directly to the wireless network. Thanks to IoTs, before you come home, the house is brought to the desired temperature, baking oven, washing your clothes, setting the house lighting. These are just a few examples. Many applications that will make our lives easier still continue to be developed thanks to IoTs. The Internet of Things (IoT) consists of three main components:

Objects: Objects we use in everyday life such as coffee machines, oven and lamps. These physical objects are equipped with the ability to receive data and respond to instructions using sensors / necessary equipment.

Communication Infrastructure: Most important of all is the communication infrastructure which consists of protocols and technologies which enable two physical objects to exchange data.

Computer Systems: Computer systems containing software and hardware that process and use data received or transmitted by objects.

Most resources assume that the History of the Internet of Objects is parallel to the development of the Internet. According to this, the foundation of the internet of the objects started with the discovery of ARPANET in 1969 and continued to develop with different studies. The first IoT device in this area was a toast machine controlled from the internet (Romkey, 1990). The next device was a coffee machine that could be watched in real time by Stafford-Fraser and Jardetzky in 1993. Later, many studies began to come. Today we can now talk about wearable technologies and smart systems that can be developed for many purposes. Today, IoTs are used in three different ways. These are person-to-person, person-to-object and object-to-object communication.

The communication from person to person: In this use form, a person can communicate with another person by using an object. Nowadays, it is most used form. Classic internet users are an example of this type of usage.

The communication from person to object: A person is on one side of this communication and an object is also on the other side. It means that people communicate with a device with the aim to use information. It involves also that people access to objects and using them remotely. Gaining access to a website and taking the data from the website is an example of this usage.

The communication object to object: In this usage, an object is on the both sides of the communication. An object needs to communicate

with another object to receive or send information. Just as objects are physical devices and products, they can contain logical contents and sources as well as. That while a person drive to home, his or her car report the arrival time to smart home system, thereby the system trigger

some other systems that regulate the house heat and do various actions is an example of this type usage.

Internet of things has influenced our daily life greatly from small wearable devices to huge industrial systems in many fields. IoT devices extend the cyber world to the physical world, which creates new types of and more complex security issues and concerns. Scientists think that such a world with many networks connected to each other might turn into a paradise for attackers.

Protecting the sensitive data and critical physical infrastructures is a must for IoT systems. Without sufficient security measure, it can't be expected for users to adopt many IoT systems and applications. Without a sufficient security protection, it can't be expected for users to adopt many IoT systems and applications. While even in conventional network based systems, providing the security requires great effort, providing the security of IoT systems bring more many challenges because of several special characteristics of IoT systems. A thorough understanding of these challenges is essential to develop novel security solutions. These challenges are; integration with the physical world, heterogeneous devices and communications, resource constraints, privacy, large scale, trust management.

If those security concerns cannot be adequately addressed, wider adoption of IoT applications will be greatly hindered (Sha ve diğ., 2018). Before IoT becomes more prevalent, many serious problems must be solved. Unless these are resolved in cooperation with, it is a matter of time when the opportunities turns into major threats. These problems are not only the problem of the companies that produce devices, but also of governments, of individuals and of all the people who are responsible to protect the world we live in.

Keywords: internet of things, connettable objects, IoT applications, IoT security and privacy

1. GİRİŞ

IoT fiziksel nesnelerin görmesini, verileri algılamasını, düşünmesini, karar vermesini, veri paylaşımını, birbirleri ile iletişim içinde olmasını denetleyen veya düzenleyen sistemler bütünüdür. Nesnelerin İnterneti kavramı ilk olarak 1999 yılında Massachusetts Institute of Technology (MIT) Auto-ID Center kurucularından olan Kevin Ashton tarafından bir sunumun başlığı olarak kullanılmıştı (Ashton, 2009). Ancak 2005 yılında International Telecommunication Union (ITU) tarafından yayınlanan “The internet of things. ITU Internet Reports” raporu ile birlikte “Nesnelerin İnterneti” kavramı tüm dünyaya duyurulmuştur (ITU, 2005).

IoT'lar genelde düşük güç tüketimli işlemcilere sahip elektronik duyarga ve kablosuz ağ bağlantısına sahip elektrikli aygıtları kapsar (Sha, 2018). Bu duyargalar, sıcaklıktan neme, basınçtan sese, yer çekiminden harekete kadar her şeyi algılayabilir ve aygıt üzerindeki yazılım yoluyla ölçümleri internet üzerinden aktarabilir.

Aygıtların birbirine bağlanmasıyla elde ettiğimiz veriler, bizlere iş dünyasında müşterilerimizin davranışlarını ve alışkanlıklarını anlamamızı, bu verilerle nasıl bir ürün geliştireceğimizi ve nasıl bir servis sağlayacağımızı görmemizi sağlamaktadır. Verilerin anlamlı hale getirilmesi bu açıdan çok önemlidir. Nesnelerin İnterneti sistemi; algılama haberleşme,

adresleyebilme ve verileri işleyebilme yeteneklerine sahiptir. Bu yeteneklere sahip aygıt veya nesnelerin oluşturduğu küresel bir ağ olan Nesnelerin İnterneti (IoT)'nin kullanım alanları her geçen gün artmaktadır.

IoT'lar aklınıza gelebilecek her nesnenin bir şekilde internete erişip, diğer aygıtlarla iletişim halinde olmasıdır. Bugün her elektronik aygıt nesnelerin internetini mümkün kılan teknolojiler sayesinde birbirleriyle iletişim kurabilir duruma getirilebilir. Günümüzde IoT konusunda birçok yeni fikir ve teknoloji geliştirilmeye devam etmektedir.

Bunların en başında ise “Akıllı Ev” ve “Akıllı Şehir” gelmektedir. Ev içerisinde çalışan pek çok elektronik aygıt artık doğrudan kablosuz ağa bağlanabilir duruma gelmiştir. Bu sayede siz eve varmadan eviniz istediğiniz sıcaklığa getirilir, fırındaki yemeğiniz pişirilir, çamaşırlarınız yıkanır, evin ışıklandırması ayarlanır. Bunlar sayılı birkaç örnektir. Daha hayatımızı kolaylaştıracak pek çok uygulama IoT'lar sayesinde geliştirilmeye devam etmektedir. Nesnelerin İnterneti (IoT) üç ana bileşenden oluşur:

1. Nesnelerin kendileri: Günlük hayatta kullandığımız nesnelerin kendileri. Evimizde kullandığımız kahve makinesi, buzdolabı veya fırın gibi nesnelere veri yakalama veya üretme kabiliyetine sahip aygıtların ve duyargaların eklenmiş hali.
2. Nesneleri birbirine bağlayan sistem: Veri yakalama veya üretme kabiliyetine sahip nesneleri birbirine bağlayan iletişim ağı.
3. Bilgisayar sistemleri: Nesneler tarafından alınan ve/veya gönderilen verileri işleyen ve kullanan yazılım ve donanım içeren bilgisayar sistemleridir.

2. NESNELERİNİN İNTERNETİNİN TARİHSEL GELİŞİMİ

1990 yılında, internet konusunda çalışan bilim insanları bilgisayar aygıtı, elektronik ve internet ile ilgili ürünlerin birlikte çalışabilirlik testi için bir ticaret fuarı olan Interop'ta bir araya gelmekteydi. John Romkey ve arkadaşları Basit Ağ Yönetimi Protokolü olan SNMP üzerine çalışıyorlardı. John Romkey bu protokolün aygıtların fiziksel kontrolü için kullanılabileceğini göstermek istedi. Tost makinesi herkesin kullandığı basit bir aygıttı. John tost makinasını TCP/IP protokolünü kullanarak bilgisayara tanıttı ve SNMP protokolünü kullanarak aygıtı internet üzerinden açıp kapatılabileceğini gösterdi. Böylece tost makinasını internete taşımayı başardı. İnternetin ilk nesnesi bu tost makinasıdır (Romkey, 2017).

İnsanoğlunun birçok buluşu ihtiyaçtan doğmuştur. 1993 yılında, Cambridge Üniversitesi'nde onlarca akademisyenin bulunduğu bir yerleşkede, herkesin kullanımına sunulmuş sadece bir tane kahve makinesi mevcuttur. Kahve makinesinin bulunduğu kattaki çalışanlar için olmasa da, diğer katlarda çalışan akademisyenler için, onlarca basamak merdiven çıkıp, kahve makinesinin içinin boş olduğunu görmek, çalışanlar için olumsuz bir durum ve zaman kaybı demektir. Yani kahve makinasının yanına gitmeden kahvenin olup olmadığını bilmek önemli hale gelmiştir. Bunun üzerine, Quentin Stafford-Fraser ve Paul Jardetzky kahve makinesinin dakikada 3 görüntüsünü yakalayarak server üzerinden bu görüntüleri bilgisayarlara aktarmayı sağlayan bir program yazdılar. Bu sayede Stafford-Fraser ve Jardetzky “Trojan Room Coffee Pot” çalışmaları ile bir kahve makinasının web üzerinden gerçek zamanlı kontrolünü gerçekleştirdiler¹.

Çoğu kaynak Nesnelerin İnternetinin tarihini internetin gelişimiyle paralel olduğunu varsaymaktadır. Buna göre nesnelerin internetin temeli 1969 yılında ARPANET'in keşfi ile başlayıp günümüze kadar farklı çalışmalar ile gelişmeye devam etmiştir. Bu gelişimin daha da devam edeceği öngörülmektedir. Aşağıda IoT'ların ortaya çıkışını ve gelişmesini belirleyen temel olayların tarihsel bir kronolojisi verilmiştir.

¹ <https://www.postscapes.com/internet-of-things-history/>

1969: Arpanet

1974: TCP/IP

1984: Alan adı sistemi

1989: World Wide Web (Tim Berners-Lee)

1991: İlk web sayfası (Tim Berners-Lee)

1997: “Sensors: The Next Wave of Infotech Innovation” çalışması (Paul Saffo)

1998: MIT’de yapılan “in Touch” projesi MIT (Scott Brave, Andrew Dahley, Prof. Hiroshi Ishii)

1999: Barkodların yerini alacak EPC (Electronic Product Code), a global RFID tabanlı nesne tanımlama sistemi (Auto-ID Labs -MIT Auto-ID Center)

2003-2004: The Guardian, Scientific American ve Boston Globe yayınlarında Cooltown, Internet ve Disappearing Computer gibi projeler ile IoT alanında bazı fikirlerin hayata geçirilmesi üzerine çalışıldı. IoT terim olarak ilk defa kitap başlıklarında görünmeye başladı. RFID, ABD Savunma Bakanlığı’nın “Savi” programında ve Walmart ticari dünyasında devasa bir ölçekte uygulamaya koyuldu.

2005: Violet (Nabaztag) şirketi tarafından Küçük WiFi erişimi olan tavşan üretildi. Bu tavşan borsa raporları, haber başlıkları, alarm saati, RSS-Feeds, vb. konularda sizi uyarıp konuşabiliyordu.

2006-2008: İlk kez Avrupa’da Nesnelerin İnterneti resmen tanınmış oldu ve “European IoT Conference” düzenlendi.

2008: Bir grup şirketi olan IPSO “Akıllı Nesneler” ağında Internet Protokolü (IP) kullanımını teşvik etti.

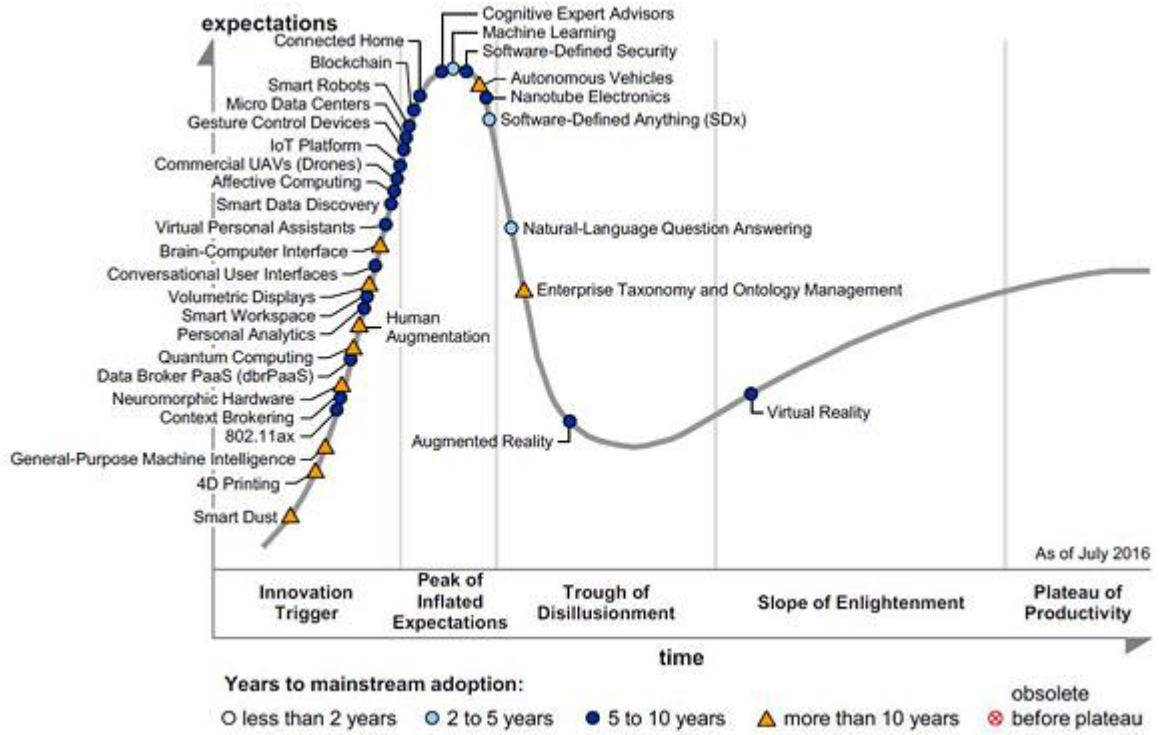
2010: İnternet’e bağlı aygıtların (akıllı telefon tablet ve PC’ler) sayısı 2010 yılında 12,5 milyara ulaştı. Dünya insan nüfusu ise 6,8 milyardı. Kişi başına 1,84 aygıt düşmekteydi. Tarihte ilk kez kişi başına 1’den fazla aygıt (tam olarak 1,84) düşüyordu.

2011: IPV4 ile 2^{32} , yeni IPV6 protokolü 2^{128} (approximately 340 undecillion adresleme) Steven Leibson “IPV6 ile Dünya yüzeyindeki her atomu adresleyebilirdik ve hala yeterli adresimiz kaldı. Hatta 100’den fazla dünyayı daha adresleyebiliriz”.

2012: 1966’da Ivan Sutherland tarafından geliştirilen “Head Mounted Display” ile başlayan sanal gerçeklik çalışmaları Palmer Luckey tarafından geliştirilen ilk bağımsız başlık Oculus Rift ile sanal gerçeklik sektöründe hızlı gelişmeler yaşanmıştır.

2015: IoT’ların en iyi uygulamalarından biri olan giyilebilir teknolojiler 3 kat artarak 2019 yılı itibari ile 249 milyon aygıtı ulaşması beklenmektedir² (forbes.com, 2015).

² <https://www.forbes.com/sites/paullamkin/2015/10/29/wearable-tech-market-to-treble-in-next-five-years/#e528d7d2c77f>



Şekil 1. Gelişen Teknolojiler için Tırmanma Döngüsü (Gartner, 2016)

2017: Gartner'a göre Gelişen Teknolojilerin Tırmanma Döngüsü grafiğinde Nesnelerin İnterneti, "Yenilik Tetikleyici" zaman sınıfından çıkarak, "Beklentilerin Zirvesi (Peak of Inflated Expectations)" zaman sınıfına geçiş yapmıştır (Gartner, 2017).

2018: Greenstein'a göre yapay zekâ, IoT sistemlerini çalıştıran beyin rolünü üstlenecektir. Her geçen gün daha fazla sayıda aygıt birbirine bağlı ve birbirleriyle konuşma yeteneğine sahip olmaktadır. Bununla birlikte yapay zekâ biliminin derin öğrenme, doğal dil işleme, görüntü tanıma ve nöral ağa dayalı karar alma teknolojileri IoT'ların bizi anlamalarını mümkün kılacaktır³ (forbes.com, 2018).

3. NESNELERİN İNTERNETİNİN KULLANIM ALANLARI

Günümüzde IoT'lar üç farklı şekilde kullanılmaktadır. Bunlar insandan-insana, insandan-nesneye ve nesneden-nesneye iletişim sağlamak şeklindedir.

İnsandan-insana iletişim: Bu kullanım şeklinde bir insan bir nesneyi kullanarak başka bir insanla iletişim sağlamaktadır. Günümüzde en çok kullanılan yapıdır. Klasik internet kullanıcıları bu tür kullanıma örnekler.

İnsandan-nesneye iletişim: Bu kullanım şeklinde bir tarafta insan diğer tarafta nesne vardır. İnsanların bir bilgiyi kullanmak maksadıyla bir aygıtla iletişim kurmasını ifade eder. İnsanların nesnelere uzaktan erişip onları kullanmasını da içerir. Bir sistemde bulunan verilere bir kullanıcının ulaşım alması bu tür kullanım şekline girer.

³ <https://www.forbes.com/sites/bernardmarr/2018/01/04/the-internet-of-things-iot-will-be-massive-in-2018-here-are-the-4-predictions-from-ibm/#2b7f5260edd3>

Nesneden-nesneye iletişim: Bu kullanım şeklinde her iki tarafta da nesne vardır. Bir nesnenin bir bilgiyi alması veya göndermesi için diğer bir nesne ile iletişime geçmesidir. Nesneler fiziksel aygıtlar ve ürünler olabileceği gibi mantıksal içerik ve kaynakları da içerebilir. Yolda olan bir kişinin kullandığı otomobilin eve varış zamanını evdeki sistemlere bildirmesi ve bu bilgileri alan nesnelerin, evin ısısını ayarlayıp fırındaki yemeği pişiren sistemleri harekete geçirmesi bu tür kullanım şekline örnektir.

Nesnelerin interneti çok geniş bir programlama platformu haline dönüşmüştür (Atzori & Morabito, 2010). Akıllı taşıma (Greengard, 2015), Akıllı Şehir (Pan ve diğ., 2015, Akaslan ve diğ., 2017), Akıllı Ev (GhaffarianHoseini, 2013) ve Akıllı Şebeke (Amin & Bruce, 2005) gibi yeni geliştirilen uygulamalar ile IoT teknolojileri yaşam tarzımızı önemli ölçüde değiştirmektedir (Gubbi ve diğ., 2013; Liu, Choo & Zhao, 2017).

Günümüzde IoT'ların kullanımı savunma, sağlık, endüstri, üretim, lojistik, tarım, pazarlama, eğitim gibi pek çok alana yayılmıştır. Bu alanlarda daha kaliteli hizmet vermek, verimliliği ve üretkenliği arttırmak için duyarğaların aracılığıyla veriler toplanır. Bu veriler "Veri Tabanı" oluşturarak Bulut Bilişim sistemlerinde depolanır. Makine öğrenimi yöntemleriyle analiz edilirler ve ilgili iyileştirmelerin yapılmasına katkı sağlarlar (Bozuklu, 2016). Günümüzde IoT'ların en göze çarpan uygulama alanları, akıllı üretim sistemleri ve bağlı üretim alanlarının geliştirilmesidir. Akıllı enerji uygulamaları akıllı elektrik, gaz ve su sayaçlarına odaklanırken; akıllı ev veya bina alanında akıllı termostatlar ve güvenlik sistemleri IoT uygulamaları açısından çok ilgi görmektedir (Wortmann ve Flücher, 2015).

Günlük hayatta kullandığımız araba, televizyon, su ısıtıcısı, fırın, buzdolabı, ütü, kitap, kamera, klima, modem gibi akla gelebilecek birçok aygıtın kablosuz ağ ya da Radyo Frekanslı Tanımlama (RFID: Radio Frequency Identification) teknolojisi sayesinde birbirleri ile iletişim kurup internete bağlanarak yaşamımızı kolaylaştıracağı ve bazı alanlarda işleri daha verimli hale getireceği görülmektedir. Nesneler birbirleri ile veya insanlarla direk olarak iletişim kurarak veri alışverişinde bulunabilir. Örneğin kalbe takılan bir kalp pili tükenmekte olduğu bilgisini sahibine ve sağlık kurumuna göndererek önceden tedbir alınmasını sağlayabilir. Sulanması veya ilaçlanması gereken bitkiler akıllı sistemler aracılığı ile tespit edilerek gereği yapılabilir. Akıllı ev sistemleri güvenliği ihlal eden teşebbüsleri ve hırsız güvenlik birimlerine haber verebilmektedir. Evcil hayvanlarımızı takip nesneleri vasıtasıyla nerede olduklarını kontrol edebilir güvenli bölgeyi aştıklarında gelen uyarı ile bulundukları yeri harita üzerinde görebiliriz. Sokakta oynayan çocuğumuzu veya bakıma muhtaç, yaşlı, sakat kişileri bulunduğu ortamlarda, uzaklık tehlike gibi parametreleri kullanarak koruyup gerekli tedbirleri alabiliriz. Akıllı çevre uygulamaları hava kirliliği, yağış durumu, baraj doluluğu, orman yangını gibi çevresel faktörlerin gözlenmesini ve gereken durumlarda acil tedbirlerin alınması maksadıyla kullanılabilir.

4. NESNELERİN İNTERNETİNİN ÇÖZÜM BEKLEYEN SORUNLARI

Buraya kadar IoT'ların faydaları ve hayatımızı olumlu yönde ne kadar değiştirebileceğine değindik. Ancak yaşamımıza sunduğu lütufların cezaya dönüşmemesi için acilen çözülmesi gereken ciddi sorunları ve eksikleri vardır. Bunlardan biri evrensel standartların eksikliğidir. Standartların belirlenmesi için birtakım çalışmalar yürütülmektedir (Fuaha, ve diğ., 2015) ancak bu konuda fikir birliği sağlanmadan geliştirilecek standartlar da çok işe yaramayacaktır.

Bir diğer sorun enerjidir. Geleneksel altyapılardan bağımsız olarak geniş bir alana dağılmış aygıtları birbirine bağlayan IoT'ların tam potansiyelini ortaya çıkarabilmek için IoT donanımlarını şu an kullandıkları enerji kaynaklarından bağımsız bir hale getirmek gerekir. Ancak bunu yapmak için gereken teknoloji günümüzde henüz mevcut değildir. Ancak IoT aygıtlarında kullanılan pillerin çok daha uzun ömürlü olarak tasarlanabilmeleri ya da güneş pillerinin bir aygıtı sürekli besleyebilmesi zaman alacaktır.

Şuanda en çok üzerinde durulması gereken en önemli problem güvenlik ve gizlilik. Bu aygıtlar, kullanıcıların sadece isim ve telefon numarası gibi kişisel bilgilerini toplamakla kalmıyor, işten saat kaçta ayrıldınız, evinize ne zaman geldiğiniz ve hatta öğle yemeğinizi kiminle ne yediğinizi de izleyebiliyor. Paylaşımlı ya da özel buluttan sürekli ortaya çıkan güvenlik ihlallerinin sonucu kullanıcılar haklı olarak gereğinden fazla kişisel veri yüklemekten çekiniyorlar.

Nesnelerin internetinin yukarıda da ifade edildiği gibi çözüm bekleyen önemli sorunları vardır. Ancak IoT aygıtlarının tam kapasiteye erişebilmesi için tedarikçilerinin öncelikli olarak bu güvenlik ve gizlilik açıklarına eğilmeleri gerekmektedir (Channel Futures, 2018). Bu yüzden çalışmada özellikle güvenlik sorunlarına odaklanılmıştır.

5. NESNELERİN İNTERNETİNİN GÜVENLİĞİ

Fiziksel olarak dağılmış akıllı IoT aygıtlarının birbirleri ile olan kolay iletişimleri sayesinde bilgi ve iletişim farklı özellikleri olan nesnelere yayılabilmektedir. Algılama yeteneğine sahip IoT'lar, fiziksel dünyadan verileri doğrudan veya uzaktan toplamaya yardımcı olur. Toplanan verilerin analizi ise bize akıllı bir dünya inşa etme, onu daha iyi yönetebilme yeteneği sağlar.

İnternet nesneleri giderek yaygınlaşmaktadır ve bunlar siber dünyayı fiziksel dünyaya yaymaktadır. Bu da çok daha fazla kompleks ve yeni türde güvenlik sorunlarını ve kaygılarını beraberinde getirmektedir. Eğer güvenlik kaygıları konusunda gereken önlemler alınmazsa IoT uygulamalarının daha geniş bir şekilde adaptasyonu büyük ölçüde engellenmiş olacak. Örneğin İnternet nesnelerinin en yaygın uygulamaları olan akıllı ev ve akıllı sağlık hizmetleri göz önüne alındığında sistemde dolaşan hassas bilgiyi ve kritik varlıkları korumak esastır (Holdsworth ve diğ., 2017; Anjum, 2018). Bunun için İnternet nesnelerinin nitelikleri onları öncekinden daha güvenli bir tasarıma sahip olmaya zorlamaktadır.

Bu nitelikler çok geniş ölçek, düşük tasarım maliyeti, kaynak kısıtlamaları, aygıt çeşitliliği, güvenlik üzerindeki fonksiyonların tercihi, daha yüksek gizlilik gereksinimleri ve daha sıkı güven yönetimini içerir. Örneğin kaynak kısıtlamaları göz önüne alındığında bu kısıtlar sınırlı hesaplama gücü, enerji kaynağı ve bellek kapasitesi şeklindedir. Bu özellikler, yaygın şekilde kullanılan “genel anahtar şifreleme” ve IP temelli güvenliği içeren birçok geleneksel güvenlik çözümünün IoT'lara uygulanmasını zorlaştırmaktadır. Yetersiz güvenlik tasarımına sahip IoT aygıtları bilgisayarlara göre daha fazla tehlikeye açıktır. Örneğin Forbes.com'un raporuna göre ABD'de Houston bölgesindeki bir bebek monitöründe başarılı bir hackleme gerçekleşmiştir⁴ (forbes.com, 2014).

Yine ABD'de 2015 yılında hackerlar seyir halindeki bir jeepin kontrolünü nasıl ele geçirilebileceğini göstermek için aracı uzaktan kontrol ederek durdurdular⁵. CCNN Money tarafından hackerların akıllı fişler (Ling et al., 2017), akıllı kameralar^{6,7} ve DVRs⁸ içeren çoğu akıllı ev⁹ aygıtlardaki açıkları bulduklarını bildirilmiştir. Buna ilaveten başka zayıf noktalar da araştırmacılar tarafından ortaya çıkarılmıştır (D'Orazio ve diğ., 2017; Do ve diğ., 2017).

Nesnelerin internetinde hassas verileri ve kritik fiziksel alt yapıyı korumak bir zorunluluktur (Sha ve diğ., 2016). Yeterli güvenlik önlemi olmadan kullanıcıların birçok IoT sistemine ve uygulamalarına adapte olması beklenemez. Geleneksel ağ tabanlı sistemlerde bile güvenliği

⁴<http://www.forbes.com/sites/kashmirhill/2014/04/29/baby-monitor-hacker-still-terrorizing-babies-and-their-parents/#5b91ff7717e2>

⁵ <https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained>

⁶ <http://www.ibtimes.co.uk/hackers-turning-millions-smart-cctv-cameras-into-botnets-ddos-attacks-1525736>

⁷ <https://www.forbes.com/sites/thomasbrewster/2016/09/25/brian-krebs-overwatch-ovh-smashed-by-largest-ddos-attacks-ever/#705007235899>

⁸ <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>

⁹ <https://edition.cnn.com/2013/08/02/tech/innovation/hackable-homes/index.html>

sağlamak önemli bir çaba gerektirirken internet nesnelerini güvenli hale getirmek sahip oldukları belirli nitelikler nedeniyle çok daha zordur. Bu zorlukların derinlemesine anlaşılması yeni güvenlik çözümleri geliştirmek için gereklidir. Bu zorluklar aşağıdaki başlıklar altında toplanabilir.

5.1. IoT'ların Fiziksel Dünya ile Entegrasyonu

Tipik bir IoT uygulamasında cyber dünya ile fiziksel dünya sıkı bir şekilde bağlıdır. Fiziksel dünya şuanda son derece önemli zarara neden olabilecek sonuçları doğurabilen siber dünya vasıtasıyla kontrol edilebilir veya tehlikeye atılabilir bu yüzden bu bağıllık ekstra kaygılara yol açmaktadır.

Pek çok IoT sistemi, petrol ve gaz endüstrisinde kullanılan SCADA sistemleri gibi kritik öneme sahip ve kesintisiz çalışmak zorundadır. Geleneksel güvenlik kurtarma düzenekleri bu tür senaryolarda genellikle uygulanabilir değildir. Örneğin üretim işlemleri durdurulamadığı için kapatma, resetleme ve daha sonra yeniden başlatma sıralaması basit bir şekilde çalıştırılmaz. Ayrıca bir IoT sistemi siber ve fiziksel parçalardan oluşur. Sistemin düzgün bir şekilde çalışabilmesi için bu iki parça uyumlu olmalıdır. Ancak bu da sorun olabilir. Şöyle ki satıcı firma tarafından artık desteklenmeyen ve güncellenmeyen eski bir işletim sistemiyle yalnızca çalışan bir sürücü yazılımını kullanan pek çok fiziksel aygıt vardır. Bu durumda eski işletim sistemine bağımlı kalan bu fiziksel aygıtlar ciddi saldırılar için açık kapı oluşturur. Bu zayıf halka tüm sistemi tehlikeye atabilir.

Fiziksel sistem ve cyber dünya arasındaki sıkı bağ ile bir sistem bir diğer sistemi tehlikeye sokabilir ve olumsuz etki her iki tarafa da yayılabilir. Örneğin sistemin siber kısmını tehlikeye atmak saldırganların fiziksel sistemi kontrol etmesine olanak sağlar böylece sadece tehlikede olan fiziksel aygıt değil daha fazlası yani hassas ve özel verilerden oluşan bilgilerdir. Akıllı şebeke veya akıllı sağlık gibi IoT uygulamaları göz önünde bulundurulduğunda hem finansal hem de insan hayatı kayıpları söz konusu olabilir. Diğer taraftan ele geçirilmiş IoT aygıtları saldırganların ona bağlı siber bölümlere erişmesine imkân sağlar. Çünkü bu aygıtlar sofistike geleneksel hesaplama araçları gibi değildir ve birçok IoT aygıtı yeteri kadar korumalı değildir. Bir kez bu korumasız ve zayıf aygıtlara erişim elde edildiğinde saldırganlar siber sistemleri istila edebilir ve tehlikeye atabilir (Boyer, 2009; Lin & Wu, 2013).

İnternet nesnelerinin temel amacı sistem üzerinden toplanılan verilerin analiz sonuçlarının baz alınmasıyla zeki bir dünya inşa etmektir. Tipik olarak fiziksel dünyayı kontrol etmek için kontrol mesajları genellikle buluttan veya kenar katmandan çalıştırıcılara veya aygıtlara gönderilir. Bu yol boyunca, siber sistem tüm katmanları ve iletişim ağını içeren pek çok noktadan saldırıya uğrayabilir. Bu yüzden IoT güvenlik tasarımında güvenliği ihlal edilmiş sistemleri ayırmalıyız böylece negatif etkiler yayılmayacaktır. Bunu başarabilmek için güvenlik ihlallerinin çoğalmasını kısıtlayan kontrol modelleri ve mekanizmaları üzerinde çalışılmalıdır (Alramadhan & Sha, 2017).

5.2 IoT Aygıtlarında Çok Çeşitlilik ve İletişim

IoT teknolojisinin değeri büyük ölçüde çok yönlülüğünde ve uygulanabilirliğinde yatmaktadır. Farklı uygulama alanları için kullanıldığı zaman IoT sistemleri, genellikle farklı donanım ve yazılım özelliklerine sahip aygıtlara adapte olurlar. Örnek olarak akıllı evi ele alalım, sistem güç kullanımı; basit hesaplamalar yapabilen ve arasıra okuma yapan basit duyargalar tarafından gözlenir. Bunun aksine ev güvenliği gözetleme sistemi ise gerçek zamanlı ev alanının izlenmesini sağlar. Anormal aktiviteleri belirlemek için özel tespit algoritmaları çalıştırması gerekir. Ayrıca akıllı evlerde çok akıllı televizyon ve karmaşık hesaplama görevleri yapması gereken oyun konsolları gibi çok güçlü aygıtlar görebiliriz. Kısaca çeşitli iletişim kanalları kullanan işletim sistemlerinin geniş yelpazesinde çalışan birçok IoT aygıtı görebiliriz. Bu çok çeşitlilik geleneksel güvenlik çözümlerini IoT sistemlerinde uygulanamaz kılmaktadır.

Geleneksel güvenlik çözümleri belirli tür yazılım ve iletişim metotlarını kullanır. Bu yüzden Windows sisteminde çalışan güvenlik çözümleri Android, iOS, TinyOS, Contiki ve mbed gibi diğer işletim sistemleri için çalışmayabilir. Ayrıca IP tabanlı güvenlik çözümleri IPSec, SSL, HTTPS ve SSH gibi, IP tabanlı protokolleri (iletişim kurallarını) düşük yetenekli basit aygıtlarda çalışmaz. Örneğin IP tabanlı protokolleri doğrudan desteklemeyen akıllı metre ve duyargalar. Sonuç itibarıyla tek bir IoT sisteminin farklı kısımlar için farklı güvenlik seviyeleri görebiliriz. En az güvenli aygıt en zayıf giriş noktası olur ve IoT sistemlerinin genel güvenlik derecesini belirler. Bir kez bu zayıf giriş ele geçirildiğinde diğer araçlarda çıkar amacıyla sömürülebilir.

Sonuç olarak IoT güvenlik sistemi çözümleri tasarlarken güvenlik algoritmalarını ve protokollerini (iletişim kurallarını) aygıtların yazılım ve donanımın özelliklerine (spesifikasyon) adapte etmemiz gerekmektedir. Düşük yetenekli aygıtların güvenliği, daha yetenekli aygıtlardan yararlanılarak artırılmalıdır.

5.3. IoT'larda Kaynak Sınırlılığı

IoT satıcıları geliştirme ve üretim maliyetini düşürmek için, genellikle aygıtları sınırlı yeteneklerle donatırlar. Bu da küçük bellek alanı, düşük hesaplama kapasitesi, düşük iletişim bant genişliği ve sınırlı güç kaynağı gibi çeşitli kaynak kısıtlamalarına sahip düşük yetenekli aygıtlar demektir.

Örneğin RFID etiketleri (Wang, 2004) için durum çok daha kötüdür çünkü bu etiketler AES, DES ve 3DES gibi simetrik anahtar tabanlı kriptografik algoritmaları bile destekleyemezler. Kimlik doğrulama durumunda ise sadece simetrik anahtar tabanlı kimlik doğrulama veya diğer daha hafif yaklaşımlar IoT sistemleri tarafından kullanılabilir. Ancak dijital imza tabanlı kimlik doğrulamalarında durum farklıdır. Bu uygulamada public-private anahtar şemasının kullanılması gerekir. IoT sistemleri için etkili bir güvenlik tasarımı yapabilmek için kaynak kısıtlamalarına dikkat etmeli ve hafif ve uygulanabilir olmaya odaklanılmalıdır.

5.4. Gizlilik

Büyük ölçekli IoT sistemleri genellikle istihbarat elde etmek için büyük miktarda veri üretir, toplar ve analiz eder. Bu da gizlilik açısından büyük bir endişe kaynağı demektir. Örneğin sağlık alanında kullanılan güvensiz IoT aygıtları insanların tıbbi bilgilerinin mahremiyetini tehdit edebilir hatta çok daha ciddi hayati sonuçlar bile doğurabilir. Gizlilik ve güvenlik arasında da bir uyumsuzluk vardır. Daha yüksek gizlilik talebi, daha zayıf bir kimlik gerektirme eğilimindedir. k-anonymity gibi algoritmalar (Sweeney, 2002) bu amaç için tasarlanmıştır. Diğer taraftan güçlü güvenlik, güçlü kimlik ister. İzinsiz giriş tespiti ve güvenlik duvarları göz önüne alındığında güvenlik de gizlilik de izlenebilirliğe ve çalışacak bağlantıya ihtiyaç duyar. Ancak bunlar gizlilik için kaçınılmazı gereken şeylerdir. IoT güvenlik çözümlerinin tasarımında, gizlilik önemlidir. Ancak gizlilik ve güvenlik arasında en uygun denge bulunması zordur.

5.5. Geniş Ölçeklilik

IoT sistemlerinin giderek daha büyük ölçekte kullanılması güvenlik çözümleri tasarım çalışmalarını güçleştirmektedir. Bunu sebepleri şöyle sıralanabilir; öncelikle tüm aygıtlar arasındaki büyük etkileşim, güvenlik dağıtım maliyetini önemli ölçüde artırmaktadır İkincisi, ölçeklenebilirlik sorunlarıyla uğraşan anahtar yönetim şemalarını büyük ölçekli IoT sistemlerine uygulamak zordur (Qi, 2014). Üçüncü olarak, dağıtım sonrası sistem yönetimi de ayrı bir sorun olacaktır. Örneğin, insanlar televizyon, buzdolabı gibi aygıtları güvenlik ihtiyacı olan araçlar olarak görmezler. Öte yandan tüm IoT aygıtlarını bilgisayarlarımız gibi yönetmeye çalışmak hem finansal açıdan hem de teknik açıdan pratik değildir.

Ayrıca gerekli güvenlik güncellemeleri zamanında yapılmamaktadır (Yu ve diğ., 2015). Birbirine bağlanmış IoT aygıtlarının sayısı saldırı alanını da büyük ölçüde arttıracaktır. Saldırı

durumunda her bir aygıt bir sonraki hedef olabilir. Bu yüzden IoT'lar için ideal güvenlik çözümleri ölçeklenebilir, dağıtılmış ve otomatik olarak yapılandırılabilir olması önerilmektedir (Sha ve diğ., 2018). Bununla birlikte çözüm ayrıca hiyerarşik ve yalıtılabilir olmalıdır.

5.6. Güven Yönetimi

Güvenlik tasarımında temel bir bileşen güvendir (Yan ve diğ., 2015). IoT sistemleri büyük oranda eşler arası (peer to peer) veya Ad-Hoc ağlar kullanılarak organize edilmektedir oysa bu tür ağlarda güven yönetimi hala önemli bir sorun olmaya devam etmektedir (Han, 2016).

Ayrıca, yüksek mobilite, global kimliksizlik ve IoT aygıtları arasında geçici ilişki güven yönetimi için çözümü daha da karmaşık hale getirmektedir. Ayrıca IoT sistemleri genel olarak merkezi bir yönetime sahip değildir ve sistem içindeki aygıtların davranışlarını kaydetmek için de iyi bir alt yapıları yoktur. Bu nedenle, aygıtlar için itibar derecelendirmeleri yapabilmek de güçtür. Bununla birlikte IoT aygıtlarının itibarını değerlendirecek yeni güven modelleri üzerinde çalışılması gerekir.

6. SONUÇ

İnsanoğlunun ihtiyaçları yüz yıllar boyunca yeni buluşlara sebep olmuştur ve her çağda hayatı kolaylaştırmanın yollarının bıkmadan usanmadan aramıştır. Her buluş başka yeni buluşların kapılarını aralamıştır. İnternetin keşfi de insanlık tarihinin en önemli buluşlarından biridir. Başlarda bu ne işe yarar diye çekimser kalınan bu muazzam teknoloji şimdilerde neredeyse vazgeçilmezdir. İnternet ise “Nesnelerin İnterneti” (IoT) teknolojisini ortaya çıkarmıştır. Bugün hayatımızı kolaylaştıran Akıllı Ev, Akıllı Şehir, Akıllı Sağlık gibi uygulamaları şimdiden görmekteyiz. ve bunların sayısı hızla artmaktadır.

Nesnelerin İnternet'i (IoT), küçük giyilebilir aygıtlardan büyük endüstriyel sistemlere kadar birçok alanda günlük yaşantılarımızı büyük ölçüde etkiliyor. Farklı IoT çerçeveleri kullanılarak çok çeşitli IoT uygulamaları geliştirildi ve geliştirilmeye devam etmektedir. Nesnelerin birbirine internet gibi güçlü bir iletişim ağıyla bağlanmasının getireceği fayda ve üstünlüklerin yanında sahip olduğu bazı sınırlılıklar nedeniyle ciddi risk ve güvenlik problemlerini de beraberinde getirmektedir. Öyle ki bu kadar çok birbirine ve ağa bağlı IoT aygıtının olduğu bir dünya hacker cenneti haline dönüşebilir mi endişesi bilim insanları tarafından paylaşılmaktadır.

Kalp pilleri, insülin pompaları ve kardiyak defibrilatörler siber güvenlik konusunda en çok endişe duyulan tıbbi aygıtlar arasındadır. Bu tür IoT aygıtlar doktorlar tarafından takip edilerek kontrol edilebiliyor. Ancak diğer taraftan savunmasız olan bu kablosuz vericiler, hackerlar tarafından siber saldırılar ile kontrol altına da alınabiliyor.

Gün geçtikçe akıllı aygıtların sayısı yüksek bir ivme ile artmaktadır. Buna karşın pek çok firma enerjisinin büyük kısmını piyasaya çıkaracakları yeni nesil ürünlere harcamakta ve mevcut eski ürünlerinin güncellemesini yapmamaktadır. Bu da başta güvenli olan bilgilerimizin artık saldırıya açık hale gelebildiği anlamına gelir. Bazı firmalar ise kişisel bilgilere erişip bunları reklam şirketlerine satma teşebbüsünde dahi bulunabilmektedir.

Nesnelerin interneti daha da yaygınlaşmadan ciddi çözüm bekleyen sorunları vardır. Bunlar işbirliği ile çözülmedikçe fırsatların büyük tehlikelere dönüşmesi an meselesi olacaktır. Bu sorunlar sadece aygıt üreten şirketlerin sorunu değildir aynı zamanda bireylerin, devletlerin ve hatta yaşadığımız dünyayı koruması gereken tüm insanlığın sorunudur.

KAYNAKÇA

Akaslan, D., Taşkın, S. & Oğuz, Y., The Extensible Analogy for Supporting the Aspects of Smart Cities: Demander and Supplier, the 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG), 20-21 April 2017, Istanbul, Turkey

- Alramadhan M. & Sha K. (2017). An overview of access control mechanisms for in-ternet of things, in: *Proceedings of the 26th International Conference on Computer Communications and Networks (ICCCN 2017)*.
- Amin, M. & Bruce, W. (2005). Toward a smart grid: power delivery for the 21st century, *IEEE Power Energ. Mag.*, 3 (5), 34–41.
- Ashton, K. (2009). That ‘internet of things’ thing. *RFiD Journal*, 22(7), 97-114.
- Atzori A.L.L. & Morabito, G. (2010). The internet of things: A survey, *Comput. Netw.*, 54 (15) , 2787–2805.
- Boyer, S. (2009). SCADA: Supervisory Control and Data Acquisition, *International Society of Automation*.
- Bozuklu, M. (2016). Çevresel veriler ile gerçek zamanlı nesnelerin interneti uygulaması. Yayınlanmamış Yüksek Lisans Tezi. Gaziosmanpaşa Üniversitesi.
- D’Orazio, C. & Choo, K.-K.R. A. (2017). technique to circumvent ssl/tls validations on ios devices, *Future Gener. Comput. Syst.*, 74, 366–374.
- Do, Q., Martini, B. & Choo, K.-K.R. (2017). Is the data on your wearable device secure? An Android Wear smartwatch case study, *Softw. Pract. Exper.*, 47 (3), 391–403.
- Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols and applications. *IEEE Communications Surveys Tutorials*, 99.
- GhaffarianHoseini, A. et al. (2013). The essence of future smart houses: From em-bedding ict to adapting to sustainability principles, *Renewable Sustainable Energy Rev.*, 24 (1), 593–607.
- Greengard, S. (2015). Smart transportation networks drive gains, *Commun. ACM*, 58 (1), 25–27.
- Gubbi, J., et al. (2013). Internet of Things (iot): A vision, architectural elements, and future directions, *Future Gener. Comput. Syst.*, 29 (7) , 1645–1660.
- Han, Q., Wen, H., Feng, G., Wu, B. & Ren, M. (2016). Self-nominating trust model based on hierarchical fuzzy systems for peer-to-peer networks, *Peer-to-Peer Netw. Appl.*, 9 (6), 1020-1030.
- Lin, C. & Wu, G. (2013) Enhancing the attacking efficiency of the node capture attack in wsn: a matrix approach, *J. Supercomput.*, 66 (2), 989–1007.
- Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., Fu, X. (2017). Security vulnerabilities of internet of things: A case study of the smart plug system, *IEEE Int.-of-Things (IoT) J.*, 99, 1–1.
- Liu, Z., Choo, K.-K.R. & Zhao, M. (2017). Practical-oriented protocols for privacy-preserving outsourced big data analysis: Challenges and future re-search directions, *Comput. Secur.*, 69, 97–113.
- Pan, G. et al. (2015). Trace analysis and mining for smart cities: issues, methods, and applications, *IEEE Commun. Mag.*, 121 (6), 120–126.
- Romkey, J. (2017). “Toast of the IoT: The 1990 Interop Internet Toaster”, *IEEE Consumer Electronics Magazine*, 6(1), 116-119
- Sha, K., Wei, W., Yang, A. & Shi, W. (2016). Security in internet of things: Opportunities and challenges, in: *Proceedings of International Conference on Identification, Information & Knowledge in the Internet of Things (IIKI 2016)*.
- Sha, K., Wei, W., Yang T.A., Wang, Z. & Shi, W. (2018). On security challenges and open issues in Internet of Things, *Future Generation Computer Systems*, 83, 326–337.
- Sweeney, L. (2002). k-anonymity: a model for protecting privacy, *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10 (5), 557–570.

- Qi, J. et al. (2014). Security of the internet of things: Perspectives and challenges, *Wirel. Netw.*, 20 (8), 2481–2501.
- Wang, R. (2004). The magic of RFID, *ACM Queue*, 2 (7), 41-48.
- Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering*, 57(3), 221-224.
- Yan, Z., Zhang, P., Vasilakos, A.V. (2015). A survey on trust management for internet of things, *J. Netw. Comput. Appl.*, 42 (4), 120–134.
- Yu, T., Sekar, V., Seshan, S., Agarwal, Y., Xu, C. (2015) Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things, in: *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*.

İnternet Kaynakları

- Russon, M.-A Hackers turning millions of smart cctv cameras into botnets for ddos attacks, <http://www.ibtimes.co.uk/hackers-turning-millions-smart-cctv-cameras-into-botnets-ddos-attacks-1525736>, online; (Erişim Tarihi: 12.04.2018).
- T. Fox-Brewster, How hacked cameras are helping launch the biggest attacks the internet has ever seen, <https://www.forbes.com/sites/thomasbrewster/2016/09/25/brian-krebs-overwatch-ovh-smashed-by-largest-ddos-attacks-ever/#705007235899>, online; (Erişim Tarihi: 24.06.2018).
- KrebsOnSecurity.com, Hacked cameras, dvrs powered today's massive internet outage, <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>, online; (Erişim Tarihi: 24.06.2018).
- Baby monitor hacker still terrorizing babies and their parents. URL <http://www.forbes.com/sites/kashmirhill/2014/04/29/baby-monitor-hacker-still-terrorizing-babies-and-their-parents/#5b91ff7717e2>. (Erişim Tarihi: 24.06.2018).
- Previous next black hat usa 2015: The full story of how that Jeep was hacked. <https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained> (Erişim Tarihi: 02.03.2018).
- How hackable are your smart home gadgets? <https://edition.cnn.com/2013/08/02/tech/innovation/hackable-homes/index.html> (Erişim Tarihi: 25.03.2018)
- Channel Futures (2018). IoT Past and Present: The History of IoT, and Where It's Headed Today <http://www.channelfutures.com/msp-501/iot-past-and-present-history-iot-and-where-its-headed-today?page=1> (Erişim Tarihi: 20.06.2018)
- Cisco (2014). The cisco connected learning experience strategies for higher education. *White Paper*. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/learning-experience-whitepaper.pdf (Erişim Tarihi: 01.06.2018).
- Gartner (2016). Gartner's 2016 hype cycle for emerging technologies identifies three key trends that organizations must track to gain competitive advantage. <http://www.gartner.com/newsroom/id/3412017> (Erişim Tarihi: 15.07.2018).
- Gartner (2017). Top trends in the gartner hype cycle for emerging technologies, 2017. <https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/> (Erişim Tarihi: 15.07.2018).
- ITU (2005). The internet of things. *ITU Internet Reports*. <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf> (Erişim Tarihi: 12.07.2018).