Nesnelerin İnternetinin Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Açısından İncelenmesi

Examination of Internet of Things in Terms of Personal, Enterprise and National Information Security

Mehtap Ülker, Yavuz Canbay, Şeref Sağıroğlu
Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, ANKARA
mehtapulker@gazi.edu.tr, yavuzcanbay@gazi.edu.tr, ss@gazi.edu.tr

Öz

Kişisel, kurumsal ve ulusal değer varlıklarından olan bilginin korunması, kişisel güvenlik, kurum işleyişi ve ulusal güvenlik açısından önemlidir. Bilgi güvenliğinin sağlanmasında birçok önlem alınmasına rağmen, yine de istenilen düzeyde bir koruma sağlanmamaktadır. Son yıllarda, Nesnelerin İnterneti (IoT) hayatımızın birçok alanına girmiş ve bundan dolayı her alanda bu teknoloji için gerekli bilgi güvenliği tedbirlerin alınması ihtiyacı ortaya çıkmıştır. Bu çalışmanın amacı, nesnelerin internetini kişisel, kurumsal ve ulusal bilgi güvenliği açısından irdelemek, bu sistemlere karşı yapılabilecek saldırıları araştırmak, incelemek ve alınabilecek önlemler konusunda önerilerde bulunmaktır. Çalışma kapsamında nesnelerin interneti kişisel, kurumsal ve ulusal bilgi güvenliği çerçevesinde ele alınmış, nesnelerin internetinin bileşenleri, güvenlik mimarisi, bu sistemlere karşı yapılabilecek güvenlik tehditleri ve alınabilecek önlemlere yer verilmiştir. Sonuç olarak, bu araştırmada sunulan önerilerin IoT güvenliğine ve dolayısıyla sistem güvenliğine katkı sağlayacağı değerlendirilmektedir.

***Anahtar Sözcükler*:** Nesnelerin interneti, bilgi güvenliği, güvenlik tehditleri, kurumsal bilgi güvenliği, kişisel bilgi güvenliği, ulusal bilgi güvenliği, öneriler

Abstract

The protection of personal, enterprise and national information is very important in terms of the operation and sustainability of the institution, the personal security and national security. Despite taking a lot of measures in order to provide information security, it is not provided at the desired level. Recently, when it is considered that Internet of Things (IoT) fall within every field of our lives, the requirements of taking the necessary information security measurements is emerged for this technology. The aim of this paper is examining IoT in terms of personal, enterprise and national information security, researching the attacks target these systems and making some suggestions about measurements. In the scope of this study, IoT was came up at the personal, enterprise and national sense in the frame of information and it has been mentioned that the component of internet of thing, security architecture, security threats that could be made against these systems and precautions that could be taken. As a result, it is necessary to examine, investigate and configure the IoT in the context of personal, institutional and national information security and also process the collected data from IoT devices to increase the security and reliability of the security systems . In addition, new solutions need to be developed rapidly by examining new and different vulnerabilities that may appear on the IoT systems.

***Keywords*:** Internet of things, information security, enterprise information security, personal information security, national
information security, recommendation

Gönderme ve kabul tarihi: 21.08.2017-13.12.2017

1. Giriş

Nesnelerin interneti olarak bilinen IoT, cihazların kendi aralarında haberleşmesidir. IoT yapısı, kablosuz algılayıcı ağlara dayanan bir teknolojidir [1]. Kablosuz algılayıcı ağlar askeri alan, kent yönetimi gibi birçok alanda kullanılmaktadır. Kablosuz algılayıcı ağların temel mantığı gerçekleşen olayı algılama ve son kullanıcıya bildirmektir [2]. Fakat nesnelerin internetinde bu durum algılama ve işlemi gerçekleştirmekten ibarettir. Sıcaklık sensörlerinden alınan verinin son kullanıcıya bildirilmesi kablosuz algılayıcının bir uygulaması, kullanıcının sıcaklık arttığını görüp olaya müdahale etmesi nesnelerin interneti uygulaması olarak örneklendirilebilir. Nesnelerin internetinin temel amacı insan yardımı olmaksızın nesnelerin kendi aralarında bilgi verme/alma imkânını sürdürmektir. Nesnelerin internetinin yaygın bir şekilde kullanılması, birçok endüstri alanı için çok miktarda veri elde edilmesini ve öngörüde bulunulmasını kolaylaştırmaktadır. Araştırmalar, internete bağlı cihazların sayısının insan sayısından fazla olduğunu ve 2020 yılına kadar bu sayının 50 milyara yaklaşacağını göstermektedir [3].

IoT teknolojisinin gelişmesiyle birlikte insanların hayatı kolaylaşmaktadır. İnsanlar herhangi bir zamanda herhangi bir yerde sahip olduğu verisini gözlemleyebilir ve gerekli gördüğü takdirde olaya müdahale edebilmektedir. Bu faydalarının yanında cihazların ağ ortamında olması, pek çok güvenlik tehditlerini beraberinde getirmesine yol açmaktadır.

Nesnelerin interneti, kullanıcıya hizmet verme amacıyla cihazların ağ ortamına bağlanılması ve birbirleriyle uzaktan haberleşerek gerekli görülen işlemleri yerine getirmesini sağlayan bir yapıdır [4]. Bir başka ifadeyle, kişilerin herhangi bir zamanda herhangi bir yerde herhangi bir cihazı kullanmasına izin veren bir teknolojidir [3]. Nesnelerin internetinin temel özelliği, sensörler ya da RFID sistemler yardımıyla dış dünyadan alınan verileri kontrol, analiz ve bilgilendirme için ağ üzerinden son kullanıcıya iletmektir.

Bu çalışma 5 bölümden oluşmaktadır. İkinci bölümde nesnelerin internetinin kurumsal bilgi güvenliği açısından incelenmesi, üçüncü bölümde kişisel bilgi güvenliği açısından incelenmesi, dördüncü bölümde ulusal bilgi güvenliği açısından incelenmesi yer alırken, beşinci bölümde sonuçlar ve değerlendirmeler bulunmaktadır.

2. Nesnelerin İnternetinin Kurumsal Bilgi Güvenliği Açısından İncelenmesi

Bu bölümde nesnelerin interneti kurumsal bilgi güvenliği açısından değerlendirilmiş, nesnelerin interneti mimarisi ve bu mimarinin alt katmanları, bu mimariye ait her bir bileşene yönelik saldırı türleri ve alınabilecek önlemler açıklanmıştır.

A. Nesnelerin İnterneti Mimarisi

Nesnelerin interneti mimarisi, algılama katmanı, ağ katmanı, destek katmanı ve uygulama katmanı olmak üzere dört katmandan oluşmaktadır bu yapı Şekil 1'de gösterilmiş ve kısaca aşağıda açıklanmıştır.

Şekil 1. IoT Katmanları [5]

Algılama Katmanı: IoT yapısının en alt katmanı olup, fiziksel dünyadaki bilgilerin RFID okuyucu veya sensörler yardımıyla toplanıldığı katmandır [1].

Ağ Katmanı: Algılama katmanından alınan verilerin güvenli bir şekilde iletilmesinden sorumludur. Bu katmanda bilgi iletimi internet, mobil iletişim ağı, uydu ağları, kablosuz ağ, ağ altyapısı ve cihazlar arası iletişimde gerekli olan protokoller tarafından gerçekleştirilir [5]. Ağ katmanı yardımıyla cihazlar diğer cihazlarla verilerini paylaşabilir. Ağ katmanı için önemli olan unsur ağdaki diğer nesnelerin rotasını bilmektir [1,6].

Destek Katmanı: Uygulama katmanı için güvenilir bir platform sağlar. Bu platform üzerinde nesneler bulut bilişim ile organize edilir [5]. Aynı zamanda kullanıcı ve uygulamalar için gerekli olan hizmet yönetimini sağlar [1].

Uygulama Katmanı: Kişinin ihtiyaçlarına göre hizmetler sunan en üst katmandır. Kullanıcılar, uygulama katmanı ara yüzü yardımıyla nesnelerin interneti sistemine erişebilir [5].

B. Nesnelerin İnternetinde Güvenlik, Saldırı Türleri ve Alınabilecek Önlemler

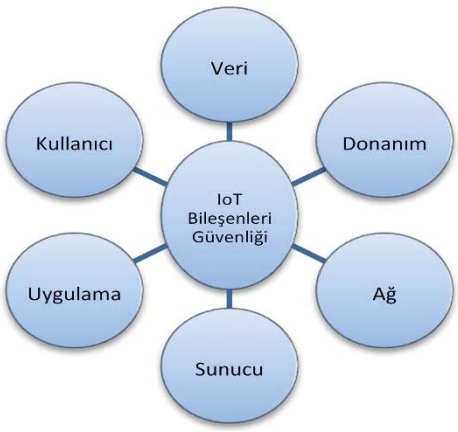
Bilgi güvenliği, bilginin göndericiden alıcıya kadar gizlilik içerisinde, bozulmadan, değiştirilmeden ve yetkisiz kişilerce ele geçirilmeden bir bütün içerisinde güvenli bir şekilde iletilme süreci olarak tanımlanabilir [7,8]. Bilgi güvenliliğinin tam olarak sağlanabilmesi için bilgi güvenliğinin temel ilkeleri olan gizlilik, bütünlük, erişilebilirlik kavramlarının sağlanması gerekmektedir [1]. Bu bileşenlerin yanında kimlik doğrulama, erişim denetimi, inkâr edememe gibi unsurlar da dikkate alınmalıdır. Kurumsal bilgi güvenliği ise kurumlar için önem arz eden bilgilerin tehdit ve tehlikelerden korunması için gerekli tedbirlerin alınması olarak düşünülebilir. Kullanıcılar bilgi sistemlerini kullanarak doğrudan ya da dolaylı olarak kurumlar için önem arz eden bilgi varlıklarına erişebilmektedir. Saldırganlar, gerekli tedbirler alınmadığı takdirde kurumun bilgisayarına, sunucularına, veri tabanlarına, kuruma özgü geliştirilen teknoloji iş yapma biçimleri/yöntemleri, diğer kurumlarla ilişkileri, ürün ve hizmetlerinin yapılanması, fiyat politikaları, geçmişe ait çalışan bilgileri, geleceğe ait planları gibi bilgi varlıklarına rahatlıkla erişebilmektedir. Kurumsal bilgi güvenliği birçok faktörün bir arada düşünülerek yönetilmesi gereken bir süreçtir. Bu süreç, bilgi sistemlerinin güvenlik politikaları ve standartlarına göre yapılandırılmasıyla birlikte insan faktörünün de ele alınıp yönetilmesi gibi durumları içerir [8].

Günümüzde, nesnelerin internetinin sağladığı faydaların yanında, ağ ortamına ihtiyaç duymaları nedeniyle güvenlik açıklıklarının sayısı veya çeşidi de artmaktadır. IoT uygulamalarında nesnelerin mobil ağ, sensör ağ ve yerel ağlarla internete bağlı olmaları siber tehdide maruz kalmalarına yol açabilmektedir. Bu kapsamda nesnelerin interneti mimarisi gereğince nesnelerin interneti bileşenlere yönelik güvenlik tehdidi hedefleri bu çalışma çerçevesinde kullanıcı, sunucu, ağ, veri, donanım ve uygulama olarak belirlenmiştir. Saldırı türleri ve güvenlik tehditleri bu kapsamda değerlendirilerek ele anılmıştır.

Tüm bilişim sistemlerinde olduğu gibi IoT'de de her geçen gün teknolojinin gelişmesi yeni saldırılara maruz kalınabileceği gerçeğini ortaya çıkarmaktadır. Bu duruma bakıldığında, bir IoT sisteminin sürekli olarak güvenlik açısından yüksek öncelikli olduğu, kurumun bünyesinde gerçekleştirilen böylesi bir sisteminin gerekli güvenlik standartlarını sağlaması gerektiği, sistem yöneticilerinin güvenlik prosedürlerine uyması ve bunu en iyi şekilde uygulaması gerektiği kaçınılmaz bir gerçektir. Yapılan araştırma çerçevesinde IoT sistemine yapılabilecek saldırılar ve bu saldırılara karşı alınabilecek önlemler mümkün olduğu ölçüde irdelenmeye çalışılmıştır. IoT sistemlerine yönelik gerçekleştirilebileceği düşünülen saldırı türleri, açıklamaları ve alınması gereken önlemler Tablo 1'de listelenmiştir. Bu sistemlerde, belirtilen saldırıların dikkate alınarak, karşı önlem olarak alınabilecek tedbirlerin de iyi bir şekilde anlaşılması ve uygulanması gerekmektedir. Literatürde nesnelerin internetinin güvenlik tehditlerine ve saldırılara karşı güvenli bir şekilde yapılandırılması için aşağıda verilen gereksinimlerin karşılanması gerektiği ifade edilmektedir [9].

- Saldırılara karşı dayanıklılık
- Sunucu gizliliği
- Şifreleme algoritmaları
- Erişim denetimi ve
- Kimlik doğrulamadır.

Şekil 2'de, nesnelerin interneti mimarisinin sahip olduğu temel bileşenler belirtilmiştir. Bu çerçevede nesnelerin interneti genel olarak veri başta olmak üzere, uygulama, kullanıcı, sunucu, ağ ve donanım olarak altı bileşene ayrılmış olup, her biri için güvenlik mekanizmalarının tam bir şekilde sağlanması gerektiği değerlendirilmektedir.



Şekil 2. Nesnelerin İnterneti Bileşenleri

Veriye Yönelik Güvenlik Tehditleri ve Alınabilecek Önlemler

Nesnelerin internetinde en temel unsur veridir. Veri her katmanda saldırıya maruz kalabilir. Verinin ilk kullanıcıdan son kullanıcıya kadar içeriğinin değiştirilmeden gizlik ve bütünlük içerisinde iletilmesi gerekmektedir. Saldırgan, veriye yönelik tehditlerini gerçekleştirebilmek adına sensörlere zarar verme, gizli dinleme ile elde edilen verinin içeriğini değiştirme, yok etme, veriyi tekrar üretme, sunuculara ve uygulamaya yönelik saldırılarda bulunabilir. Bu süreç için en temel unsur şifreleme algoritmasının kullanımıdır. Şifreleme algoritması kullanarak verinin gizliliği ve bütünlüğü sağlanmaktadır.

Veriye yönelik gerçekleştirilebilecek saldırılar ve alınabilecek önlemler Tablo 2'de gösterilmekte olup, bu saldırıların açıklamaları Tablo 1'de belirtilmiştir.

Donanıma Yönelik Güvenlik Tehditleri ve Alınabilecek

Önlemler

Nesnelerin interneti mimarisinin en alt katmanı olan algılama katmanı donanım cihazlarını barındırmaktadır. Nesnelerin internetinde en kritik unsur donanım cihazlarının düşük işlemcili, düşük kapasiteli ve düşük maliyetli cihazlar olmasıdır [25]. Bu durum bilgi güvenliği ihlali ortaya çıkarabilmektedir. Cihazların verimli kullanılmasına yönelik yönlendirme tabloları, güvenlik ve benzeri konular sensör düğümündeki düşük belleğe sığacak şekilde yapılandırılmıştır [5,18].

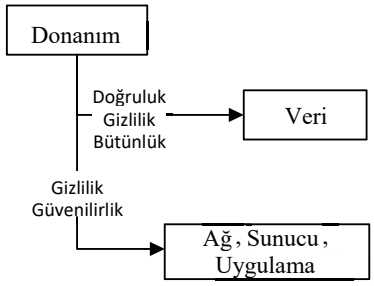
Açık anahtar alt yapısı ile bilgi güvenliği ilkelerinden olan kimlik doğrulama, inkâr edeme unsurları sağlanmaktadır [26,27]. Güç tüketimi fazla olan açık anahtar algoritması kullanımı bakımından bu cihazlar elverişli değildir. Böylesi cihazlar kullanımı ile kimlik doğrulama ve inkâr edememe ilkesini sağlamak oldukça güçtür. Cihazların düşük kapasiteli olması hizmet aksatma saldırılarına maruz kalmasına sebebiyet vermektedir [5, 28, 29].

Şekil 3'te donanım bileşeni ile IoT'un diğer bileşenleri arasındaki ilişki ve güvenlik gereksinimleri gösterilmiştir. Bu yaklaşımla, donanım ile veri arasındaki her türlü ilişkide doğrulama, gizlilik ve bütünlük unsurlarının dikkate alınması, donanım ile de ağ, sunucu ve uygulama arasındaki her türlü ilişkide gizlilik ve güvenilirlik ilkelerinin göz önünde bulundurulması ve bu yapı dikkate alınarak bir sistemin tasarlanması gerekliliği ortaya konulmuştur. Literatür incelendiğinde, IoT konusu içerisinde donanıma yapılabilecek saldırıların genel olarak hizmet aksattırma saldırısı olduğu tespit edilmiş olup buna ek olarak fiziksel olarak gerçekleştirilebilecek olan yetkisiz fiziksel erişim ve zarar verme gibi durumların da söz konusu olduğu belirlenmiştir. Donanıma yönelik gerçekleştirilebilecek saldırılar ve alınabilecek önlemler Tablo 2'de gösterilmiş, bu saldırıların açıklamaları Tablo 1'de belirtilmiştir.

Tablo 1. Saldırı türleri ve güvenlik tehditleri

No	Saldırıtürü	Saldırı türü açıklaması	Alınabilecek önlemler
S1	SYN saldırısı	Saldırgan hedef sisteme ardışık olarak SYN bayraklı TCP paketi göndererek hizmet veremez hale getirir [10]	SYN cookies, SYN cache, SYN Proxy Güvenlik duvarı, ISP ve Saldırı tespit sistemi kullanılmalı Yönlendirme seviyesinde koruma sağlanmalı [11,12]
S2	Smurf saldırısı	Saldırgan ağdaki bilgisayarlara hedef sistemin ip adresinden ICMP paketi yollayarak alıcı bilgisayarın sürekli ACK mesajı yollamasına neden olan saldırı türüdür [10].	Saldırı tespit sistemi, güvenlik duvarı ve anti-virüs programı kullanılmalı, Yönlendirme seviyesinde koruma sağlanmalı [13]
S3	Ölümcül ping	Saldırgan büyük boyutlu paketleri hedef sisteme göndererek hizmet dışı kalmasına neden olan saldırı türüdür [10].	Saldırı tespit sistemi ve Güvenlik duvarı kullanılmalı Yönlendirme seviyesinde koruma sağlanmalı[14]
S4	ACK saldırısı	Saldırgan kaynak ip adresini hedef ip adresi olarak gösterip syn paketi yollar ve alıcının hedef ip syn paketi yollamadığı halde ack yollamasıyla gerçekleşen saldırı türüdür [14].	Saldırı tespit sistemi ve Güvenlik duvarı kullanılmalı Yönlendirme seviyesinde koruma sağlanmalı, Timeout değerini düşürmeli[12]
S5	UDP saldırısı	Saldırının temel prensibi farklı bir ip adresini kullanarak hedef sistemin portlarına büyük boyutlu UDP paketleri yollamaktır [14].	Saldırı tespit sistemi ve Güvenlik duvarı kullanılmalı Yönlendirme seviyesinde koruma sağlanmalı, Timeout değerini düşürmeli [12]

S6	IP sahteciliği	Saldırgan gizli dinleme sonucu elde edindiği paketin şifreli olmaması durumunda kaynak ip adresini değiştirerek hedef sistemi yanıltmasıdır [10].	Timeout değerini düşürmeli, Kaynak IP adresini doğrulama mekanizması ve Hop sayısını filtreleme (HCF) kullanılmalı[13]
S7	E-posta sahteciliği	Sahte e-posta adresini güvenilir olarak gösterilerek gerçekleştirilen saldırı türüdür [15].	E-posta doğrulama mekanizması, Alan adı anahtarı kimlik doğrulama mekanizması (Domain keys), Tek kullanımlık şifre, şifreleme algoritmasının kullanılmalı [15,16]
S8	Web sahteciliği	Güvenilen bir web sitesinin sahtesini kullanarak gerçekleştirilen saldırı türüdür [16].	Tek kullanımlık şifre ve şifreleme algoritmasının kullanılmalı [16]
S9	Oturum Çalma	İstemci ile sunucu arasına girerek kullanıcını oturumunu ele geçirme yönelik gerçekleştirilen saldırı türüdür [14].	Güvenli protokol kullanımı, Koruma mekanizması ve şifreleme algoritması kullanılmalı[14] ,
S1	Ortadaki adam saldırıları	Haberleşen iki uç arasına girerek veriyi dinlemeye yakalamaya yönelik gerçekleştirilen saldırı türüdür [17].	Şifreleme algoritması, güvenlik duvarı ve IPS kullanılması [5,18-20]
S1	Tekrarlama saldırıları	Haberleşen iki uç arasındaki paketin saldırgan tarafından ele geçirilerek tekrar tekrar alıcıya iletilmesiyle gerçekleşen saldırıdır.	Şifreleme algoritması, Güvenlik duvarı kullanılmalı [5,18-20] ,
S1	DNS Zehirlenmesi	Önbellek veri tabanına veri ekleme, silme, değiştirme ile hedefi şaşırtmaya yönelik saldırı türüdür [21]	Saldırı tespit sistemi kullanılmalı
S1	SQL Enjeksiyonu	SQL sorgularına müdahale ederek hedef sistemin bilgilerini edinmeyi amaçlar [17].	Güvenli veri tabanı konfigürasyonu, saldırı tespit sistemi kullanılmalı [22]
S1	Virüsler	Zararlı bilgisayar yazılımı olup bilgisayarın işleyişini değiştirmektedir [23].	Anti-virüs ve güvenlik duvarı kullanılmalı [23]
S1	Solucanlar	Ağ bağlantısı üzerinden bulaşarak sistemdeki dosyalara zarar verme, bilgisayarın işleyişini bozmayı hedeflemektedir [23].	Anti-virüs ve güvenlik duvarı kullanılmalı [23]
S1	Truva Atları	Bilgisayar yazılımı olup bulaştığı bilgisayardaki bilgileri dışarı sızdırmaktadır ve saldırgan ağ bağlantısı üzerinden kurbanın bilgisayarını kontrol etmektedir [17].	Anti-virüs ve güvenlik duvarı kullanılmalı[23]
S1	Oltalama	E-mail yardımıyla kişisel bilgileri ele geçirmeye yönelik gerçekleştirilen saldırı türüdür [23].	Oltalama saldırıları saptama mekanizması kullanılmalı [24]
S1	Reklam yazılımı	Reklam görüntülemek ve kişilerin ilgi odağına göre verileri toplanılmasına yönelik yazılımdır [17].	Anti-virüs ve güvenlik duvarı kullanılmalı [23]
S1	Spam	Herhangi bir amaç doğrultusunda hedef sistemin e-postalarına gelen iletilerdir [17].	Anti-virüs ve güvenlik duvarı kullanılmalı [23]
S2	Arka Kapılar	İşletim sistemi ya da uygulamalarda açıklık oluşturmaya yönelik gerçekleştirilen saldırı türüdür [17].	Anti-virüs ve güvenlik duvarı kullanılmalı [23]
S2	Sosyal Mühendislik	Hedef sistemdeki kişi hakkında bilgi edinebilmek için kişilerin kandırılması yöntemiyle gerçekleştirilen saldırı türüdür [23].	Anti-virüs ve güvenlik duvarı kullanılmalı [23]
S2	KeyLogger	Klavyeye basılan tuşları kaydetmeyi amaçlayan yazılımdır [17].	Anti-casus yazılım, güvenlik duvarı kullanımı [23]



Şekil 3. Donanım bileşeni ile IoT bileşenleri arasındaki ilişki

Ağa Yönelik Güvenlik Tehditleri ve Alınabilecek Önlemler

Nesnelerin internetinde cihazların birbirleriyle iletişime geçebilmeleri için ağ katmanı önemli katmandır. Ağ katmanı birden fazla teknolojik yapının buluştuğu ve verinin bir üst katmana iletilmesinden sorumludur. Farklı yapıda cihazların oluşturduğu ağ ile farklı teknolojiler bir arada kullanılabilmektedir. Böylesi büyük öneme sahip bir yapının da gerek içeriden gerekse de dışarıdan çeşitli saldırılara maruz kalabileceği düşünüldüğünde, bu saldırılara karşı alınabilecek önlemlerin de önemi anlaşılmaktadır. Bu doğrultuda ihtiyaç duyulan en önemli unsur güvenilirlik mekanizmalarıdır. Kimlik doğrulama mekanizması, güvenilirlik mekanizmalarından biri olup herhangi bir yerden erişimine izin verilmeyen durumlardan sistemi korumayı hedefler [30]. Aynı zamanda şifreleme algoritması kullanımı ile gizlilik ve bütünlük mekanizması sağlanmalıdır.

Nesnelerin internetini oluşturan cihazlar düşük güç işlemciye sahip, düşük bellekli ve düşük maliyetli cihazlar olduğu düşünülürse hataya yatkınlığı fazladır [25]. Bu bakımdan kullanımda olan cihaz her an devre dışı kalabilir. Bu durum ağ topolojinin değişken olmasına neden olmaktadır. Nesnelerin internetinde bir diğer önemli husus verinin iletilmesi sürecinde kullanılan protokolün belirlenmesidir. Veri iletilirken TCP ve UDP protokolleri kullanılmaktadır. TCP, verinin alıcısına güvenilir bir şekilde iletilmesini sağlarken UDP'de böyle bir durum söz konusu değildir. TCP güvenilirliği sağlamak adına, başlığında birçok bilgiyi barındırarak alıcıya iletir. Verinin iletilme süreci, gönderici-alıcı ve alıcı-gönderici şeklindedir. Gönderici bu durumda sensör olan düşük kapasiteli cihazdır. Göndericiden alıcıya yani sensörlerden son kullanıcıya TCP protokolü kullanılarak veri aktarılması, yüksek band genişliği ve ek yük gerektirdiği için bu adımda veri UDP protokolü kullanarak alıcısına iletilmelidir. Alıcı kısımdaki cihazlar IoT cihazlarına göre daha kaliteli cihazlar olduğu düşünüldüğünde, TCP protokolü kullanımının herhangi bir sakıncası yoktur [31].

Tablo 2'de ağa yönelik gerçekleştirilebilecek saldırılar ve alınabilecek önlemler gösterilmekte olup, bu saldırıların açıklamaları Tablo 1'de belirtilmiştir.

Sunucuya Yönelik Güvenlik Tehditleri ve Alınabilecek Önlemler

Nesnelerin internetinde kaynaklar bulut bilişime göre organize edilir [5]. Bulut bilişim, ortak kullanılan kaynaklar üzerinde, ihtiyaca göre hizmet veren, kaynak ataması ve yönetimi kolay yapılabilen model olarak düşünülebilir. Bir başka deyişle, bulut bilişim genel olarak yazılımın, altyapının ve platformun hizmet olarak sunulması ve kaynaklara internet üzerinden her yerden bağımsız erişilmesine imkân verebilen teknolojidir [32]. Bulut bilişim yüksek depolama alanı, hızlı veri transferi, maliyet ve iş gücü tasarrufunun yanında, veri güvenliği ve gizliliği, veri bütünlüğü, yönetim riski, bant genişliği ve veri transferi gibi birçok riski de beraberinde getirir [33]. Nesnelerin interneti mimarisi gereğince hizmet veren sunucuların bulut bilişimle organize edilmesi saldırganlar için önemli bir güvenlik açığı oluşturabilmektedir. Hizmet sağlayıcılarında yazılımsal, donanımsal ve mimari hataları, güvenlik politikası zafiyetleri, yetkilendirme zafiyetleri, yanlış yapılandırmalar gibi olumsuzluklar ortaya çıkabilmektedir. Literatürde, bu saldırıların önüne geçebilmek adına şifreleme protokolleri, anti-virüs ve şifreleme algoritması kullanımı üzerinde durulmuştur.

Tablo 2'de, sunucuya yönelik gerçekleştirilebilecek saldırılar ve alınabilecek önlemler irdelenmiş olup, bu saldırıların açıklamaları Tablo 1'de belirtilmiştir.

Uygulamaya Yönelik Güvenlik Tehditleri ve Alınabilecek Önlemler

Uygulama katmanı en son katman olup kişinin ihtiyaçlarına göre hizmet veren katmandır. Bu katmanda sistemin yönetilmesi ve işletilmesi adına gerekli yazılımlar mevcuttur. Dolayısıyla bu yazılımları hedef alan saldırılar aynı zamanda sistemin işleyişini veya yönetimini de bir anlamda ele geçirme niyetinde olabilir. Bu sayede kaynakların kötücül niyetlerle yönetilmesi, bu kaynaklardan

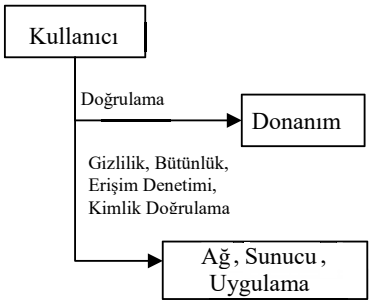
kurumsal verilerin ele geçirilmesi gibi durumlarla karşı karşıya kalınabilmektedir. Literatürde, bu alandaki güvenlik problemleri irdelendiğinde, heterojen ağdalarda anahtar yönetimi, doğrulama ve kullanıcı gizliliğinin korunması gibi önlemlerin alınması gerektiği anlaşılmaktadır [5]. Aynı zamanda kullanıcıların bilinçlendirilmesi bu alandaki güvenlik sorunlarının çözümünde oldukça önemlidir. Tablo 2'de, uygulamaya yönelik gerçekleştirilebilecek saldırılar ve alınabilecek önlemler irdelenmiş ve bu saldırıların açıklamaları Tablo 1'de belirtilmiştir.

Kullanıcı Güvenlik Tehditleri ve Alınabilecek Önlemler

Nesnelerin internetinde en önemli güvenlik tehditlerinden birisi de kullanıcı faktörüdür. Kullanıcı, sistemden hizmet almak isteyen ve sonuçları analiz eden olmak üzere iki farklı biçimde tanımlanabilir. Sisteme giriş yapacak olan kullanıcı verileri, son kullanıcı tarafından doğru bir şekilde değerlendirmesi için ilk aşamada doğrulamanın yapılması gerekmektedir. Bununla birlikte iletişimin gizlilik ve veri bütünlüğü sağlanarak yapılması da önemlidir [30].

İnsanlar çalıştıkları kuruma bilinçli veya bilinçsiz bir şekilde zarar verme amacıyla verileri değiştirebilir ya da silebilir. Yalnızca kurum içinde çalışanlar değil aynı zamanda geçici olarak çalışanlar, danışmanlar, iş ortakları, tedarikçiler, taşeronlar ve bilişim korsanları da kuruma zarar verme amaçlı verilere erişip yetkisiz işlemler yapabilir. Bu gibi durumlar göz önünde bulundurularak güvenlik kuralları oluşturulmalı, kurumlar kurallar çerçevesinde yönetilmeli ve bu kurallar kurum bünyesinde uygulanmalıdır [34]. IoT'nin karmaşık yapısı göz önüne alındığında, kullanıcı unsuru güvenlik yönetiminde ve uygulanmasında en önemli bileşendir. Bu çalışmada kullanıcı bileşeni ile IoT'nin diğer bileşenleri arasındaki ilişki ve güvenlik gereksinimleri Şekil 4'deki gibi gösterilmiştir [30]. Aynı zamanda kullanıcıya yönelik gerçekleştirilebilecek saldırılar ve alınabilecek önlemler Tablo 2'de gösterilmekte olup, bu saldırıların açıklamaları Tablo 1'de belirtilmiştir.

Şekil 4 'te, kullanıcının doğrudan erişebildiği IoT bileşenleri donanım ve uygulamadır. IoT güvenilirliğini sağlanması adına, kullanıcı ve donanım arasında doğrulama, kullanıcı ile ağ, sunucu ve uygulama arasında gizlilik, bütünlük, kimlik doğrulama ve erişim denetimin sağlanması gerekmektedir.



Şekil 4. Kullanıcı bileşeni ile Iot bileşenleri arasındaki ilişki

- *Doğrulama:* Kullanıcı verisi ile donanım (nesne) arasında sağlanması gereken önemli unsur doğrulamadır. Literatürde, bu alanda birçok çalışma vardır. Bu çalışmada, önemli olanlardan birkaçı irdelenmiştir. İlk olarak SENSEI (Integrating the Physical with the Digital World of the Network of the Future) projesinde, kablosuz sensör ağları ile farklı ağ yapıları arasında etkileşimin sağlanması için bir mimari önerilmiştir. Bu projede, doğrulama ile birlikte güvenilirlik ve gizlilik sağlanmaktadır [35]. Bu alanda diğer bir proje olan BRIDGE(Building Radio Frequency IDentification for the Global Environment) irdelenmiştir. Bu projede ise doğrulma mekanizmasına odaklanmaktadır [37]. Aynı zamanda doğrulamanın gerçekleşebilmesi için kullanılan diğer projeler, SmartProduct, SWITFT (SecureWidespread Identities for Federated Telecommunicatiın), kare koddur [37].

Gizlilik: Kullanıcı ile teknolojik ekosistem (ağ, sunucu ve uygulama) arasında olması gereken bilgi güvenliği unsurudur. Bu çalışma kapsamında gizlilik üç başlık altında sınıflandırılmıştır [30]. Bunlardan ilki, veri alınması sırasında gizlilik olup çözüm önerisi olarak şifreleme algoritması üzerinde durulmuştur [38]. İkincisi ise veri paylaşılırken ve yönetilirken gizlilik; veri paylaşımında ve yönetiminde şifreleme algoritması gizliliği sağlamakla birlikte P3P ve semantik web gizliliği sağlamada çözüm önerisi oluşturmaktadır [30,39,40]. Bir diğeri ise son kullanıcıda gizlilik olup gizliliği sağlamadaki en önemli unsurlar kimlik doğrulma, erişim denetimi, anti-virüs programı, şifreleme algoritması kullanılmasıdır [5,30].

Literatür incelendiğinde, donanım, ağ, sunucu, veri ve uygulamaya yönelik olarak pek çok saldırı gerçekleşebileceği ve siber tehditler haline gelebileceği anlaşılmaktadır. Tablo 2'de IoT bileşenlerine yönelik gerçekleşen saldırı türleri, ihlal edilen güvenlik unsuru ve IoT bileşenleri arasında ağırlık derecesi gösterilmiştir. Literatür incelendiğinde, donanım, kullanıcı, ağ, sunucu, veri ve uygulamaya yönelik olarak çeşitli saldırıların gerçekleşebileceği ve siber hedef haline gelebilecekleri anlaşılmaktadır. Tablo 2'de IoT bileşenlerine yönelik gerçekleştirilebilecek saldırı türleri, ihlal edilen güvenlik unsuru ve IoT bileşenleri arasında ağırlık derecesi gösterilmiştir.

Tablo 2. Nesnelerin internetini bileşenlerine yönelik saldırı türleri, güvenlik tehditleri, ihlal edilen güvenlik unsuru ve ağırlık derecesi

Hedef alınılan IoT bileşeni	**IoT güvenlik unsurlarına yönelik saldırılar (Sno)**	**İhlal edilen güvenlik unsuru**	**IoT bileşeninin güvenlik ağırlık derecesi**
Veri	#6, #7, #8, #9, #10, #11, #14, #15, #16, #17, #18, #19, #20, #21, #22	Gizlilik, Bütünlük, Erişim denetimi	3
Donanım	#1, #2,#3	Erişilebilirlik	1
Ağ	#1, #2, #3, #4, #5,#6, #10, #11, #12, #13, #14	Erişilebilirlik, Gizlilik, Bütünlük	3
Sunucu	#1, #2, #3, #4, #5, #6, #14, #15	Erişilebilirlik, Gizlilik, Bütünlük, Erişim denetimi	4
Uygulama	#14, #15, #16, #20, #22	Erişilebilirlik, Gizlilik, Bütünlük, Kimlik doğrulama, Erişim denetimi	5
Kullanıcı	#7, #8, #9, #17, #18, #19, #21	Erişilebilirlik, Kimlik doğrulama, Erişim denetimi	3

Bu çalışmada ağırlık derecesi, en çok ihlale maruz kalınan güvenlik unsurlarına göre belirlenmiştir. İhlale daha açık olanın skoru daha yüksek verilmiştir. Saldırılar irdelendiğinde, IoT bileşenlerinden en çok saldırıya maruz kalan bileşen veri olup ağa yönelik saldırılarda oldukça fazla olduğu anlaşılmaktadır. Ağırlık derecelendirmesine göre, IoT bileşenlerinden kullanıcı ve uygulama, ihlale maruz kalma olasılığı en yüksek olan bileşenlerdir.

Literatürde, nesnelerin interneti için bilgi güvenliğinin temel ilkelerini sağlamak adına birçok çözüm önerisinde bulunulmuştur. Bu çalışmaların sağladığı üstünlüklerin; ortadaki adam saldırısı, tekrarlama saldırıları, yetkisiz erişim, oturum çalma, gizli dinleme, veri değişikliği ve çalınmasını engelleme, anahtar paylaşımı ve doğrulamayı sağlama, kablosuz sensör ağ yönetimi ve kontrolü, protokol dönüşümü sağlama, doğrulama ve bütünlüğü sağlama, CoAP kaynaklarına erişim, düz metin saldırılarını engelleme, zararlı yazılımları çalıştırmayı engelleme, kullanıcı erişimi ve kontrolü, doğrulama ve erişim denetimi, saldırıları ve karmaşıklığı engelleme olduğu gözlemlenmiştir [41-48]. Bu çalışmalardan elde edilen sonuçlardan yola çıkılarak güvenilir bir IoT mekanizması oluşturmak için aşağıdaki unsurların sağlanması gerekliliği anlaşılmıştır.

- Saldırı tespit sistemi
- Kablosuz sensör ağ yönetimi ve kontrolü
- Şifreleme algoritması
- Erişim denetimi
- Kimlik doğrulama mekanizması
- Anahtar paylaşımı
- Anti-virüs programı
- Güvenlik kurallarının belirlenmesi ve uygulanması
- Kişilerin bilinçlendirilmesi

3. Kişisel Bilgi Güvenliği Açısından IoT'un İncelenmesi

Kişisel bilgi, kişiyi ifade eden ve kişi ile ilişkilendirilen her türlü bilgidir [50]. Bu bilgiler, kişinin yaşı, adresi, mesleği, banka ve kredi kartı numarası, vergi numarası gibi bilgileri kapsamaktadır. Günümüzde kişisel bilgiler bazen kişinin istediği doğrultuda, çoğu zaman ise istem dışı her türlü platformda paylaşılmaktadır. Bu durum özel yaşamda gizlilik kavramını büyük oranda ortadan kaldırmaktadır. Günümüz teknolojileriyle kişisel verilerin çeşitli platformlarda paylaşılıyor olması kişinin her türlü tehdide maruz kalmasına neden

olmaktadır. Güvenilir olmayan bir e-ticaret sitesinden alışveriş yaparken banka ve kredi kartı bilgilerinin saklanıyor olması maddi zarara yol açabilmektedir. Nesnelerin interneti kavramı da düşünüldüğünde kişisel verinin korunması oldukça güç hale gelmektedir. Kişisel verilerin etkin olarak kullanıldığı birçok IoT uygulaması bulunmaktadır. Saldırgan bu verilere yönelik birçok saldırı ve güvenlik tehdidinde bulunabilmektedir [40].

Günümüz teknolojisi, cihazların kendi aralarında haberleşmesi ve öngörülen işlemi yapmasından ibarettir. Kişinin kontrolüne gerek kalmadan gerçekleşen bu durum, kişisel bilgi güvenliğini tehdit etmektedir. Akıllı kilit ile evine anahtarsız bir şekilde giren kullanıcı, evde olmasa dahi uzaktan misafirine evinin kapısını açmaktadır. Böylesi bir durumda eve giriş için kullanılan şifre, kişisel veri olup ağ üzerinde paylaşılması kişisel bilgi güvenliğini tehdit etmektedir. Gerekli tedbirler alınmadığı takdirde saldırgan, evini bu yöntemle açan kişinin verisine erişip eve rahatlıkla giriş yapabilmektedir.

Kullanıcıların kişisel verilerini farklı platformlarda paylaşıyor olması bazı şifreleme algoritmalarının güvenliğini de azaltmaktadır. IoT teknolojisinde şifreleme algoritması olarak basit yapıda şifreleme algoritmalarının kullanılması birçok çalışmada önerilmiştir [40,41]. Bu şifreleme algoritmaları kimlik tabanlı şifreleme temeline dayanıp kimlik doğrulama ve inkâr edememeyi sağlamak amacıyla kullanılmaktadır. Bu algoritma, açık anahtar algoritmaları mantığı gibi açık ve gizli anahtardan oluşmaktadır. Bu algoritmada, her iki tarafın da anladığı kişisel veriler olan gizli anahtar, kullanıcının yaşı, TC kimlik numarası, telefonu gibi bilgileri içermekte olup kişisel verilerin her türlü platformda paylaşılıyor olması ile algoritmanın güvenilirliğini büyük oranda ortadan kaldırmaktadır [40].

Nesnelerin internetinde kişisel önem arz eden bilgilerin gizlilik ve bütünlük içerisinde alıcısına ulaşması gerekmektedir. Böylesi bir durumda öne çıkan unsur verilerin şifrelenerek alıcısına iletilmesidir. Şifreleme algoritması, bilgi güvenliğinin temel unsurları olan erişilebilirlik, bütünlük ve gizliliği sağlamaktadır. Bu süreçte verinin depolandığı bulut bilişim güvenliği de ön plana çıkmaktadır. Kişisel verilerin korunmasında bulut hizmet modeli olan yazılım hizmetinin (SaS) kullanılması ile etkili bir çözüm sunulmaktadır [52].

Türkiye'de, Kişisel Verilerin Korunması Kanununa göre, "Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir." hükmü yer almaktadır. İlgili kanunun 4. maddesinde belirtildiği gibi kişisel verilerin, bu kanunda ve diğer kanunda öngörülen usul ve esaslara göre işletilebileceği açıklanmıştır. Bu kanunda, IoT teknolojilerinden dolayı oluşabilecek ihlaller neticesinde kişisel verilerin mahremiyetine saygı gösterme zorunluğu vardır.

4. Ulusal Bilgi Güvenliği Açısından IoT'un İncelenmesi

Ulusal güvenlik, kamu bilişim sistemleri ile gerçek ve tüzel kişilerce işletilen veya kullanılan bilişim sistemlerinden oluşan ortamdaki her türlü hizmet, işlem, bilgi/veri ve bunların sunumunda yer alan donanım ve yazılım sistemlerinin ulusal ölçekte güvenliğin sağlanması olarak ifade edilir [53]. Ülkemizde bilgi sistemleri; kamu kurumları, özel sektör, sağlık, ulaşım, haberleşme gibi sektörlerde faaliyet gösteren kurum ve kuruluşlarda hızla yaygınlaşmaktadır. Kamu kurumlarının bilgi sistemlerini yaygın olarak kullanması ve bilgi sistemlerinde gerekli güvenlik tedbirlerinin alınmaması nihayetinde, ulusal güvenliğimizin tehlike altında olması kaçınılmazdır. Bilgi sistemleri güvenlik tedbirleri alınmadan yönetildiğinde can, mal ve itibar kaybına, ekonomik zarara, kamu düzeninin bozulmasına ve dolayısıyla ulusal güvenliğin ihlaline sebebiyet vermektedir. Böylesi bir süreçte ulusal güvenliğin sağlanması adına bütün kurum ve kuruluşların siber güvenlik kurulu tarafından belirlenen politika, strateji ve eylem planları çerçevesinde belirtilen görevleri yerine getirmesi gerekmektedir.

Bilgi sistemleri doğru yapılandırılarak ulusal güvenliğin, toplum refahının ve güvenliğinin, ülke ekonomisine katkı sağlaması amacıyla bilgi sistemlerinin etkin şekilde kullanılmasına yönelik gerekli tedbirler alınmalıdır. Bu kapsamda hazırlanmış 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının amaçlarından biri, ulusal güvenliğin ancak ve ancak siber güvenlikle sağlanabileceği bilincinin yerleşmesini sağlamaktır. Bu doğrultuda bilişim sistemlerinin siber saldırılara karşı korunması gerekliliği ön plana çıkmaktadır. Siber güvenlik sağlanmadığı takdirde karşılaşılabilecek durumlar aşağıdaki gibidir [53].

- Bilişim sistemlerine yapılacak hizmet aksatma saldırıları ile birçok hizmetlerin kesintiye uğraması,
- Kişisel bilgilerin etkin kullanıldığı hizmetlere yönelik saldırılar sonucu bilgilerin ele geçirilmesi ve yok edilmesi,
- Ticari verilerin saldırgan tarafından ele geçirilmesi ve maddi zararlara sebebiyet vermesi,
- Kurum ve kuruluşlara oltama saldırıları ve kötücül yazılım gibi saldırılar uygulanarak gizli verilerin ele geçilmesi,
- E-ticaret kuruluşlarının yaygın olarak kullanılmasından dolayı saldırganların bu sistemleri hedef alarak gerçekleştirdiği saldırılarla kişisel verileri ele geçirmesi ve maddi kayıplara neden olması olarak belirtilmiştir.

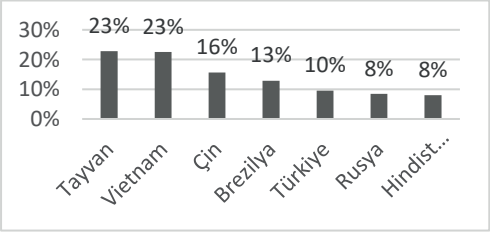
Sensörlerden alınan verinin analiz edilmesi ve işlenip kullanılması amacını taşıyan nesnelerin interneti birçok kurum ve kuruluşlarca kullanılmaktadır. Askeri sistemler ve ulaşım gibi kritik alanda kullanılan uygulamalara yönelik siber saldırılar ile ulusal bilgi güvenliği tehdit edilmektedir. Bu sistemlere yönelik siber saldırılar ulusal bilgi güvenliğini riske atmakta, can, mal ve itibar kaybına, kamu düzeninin bozulmasına neden olmaktadır. Böylesi sistemlerin belli politika çerçevesinde yapılandırılması gerekliği ön plana çıkmaktadır.

2016-2017 Ulusal Siber Güvenlik Eylem Planına göre gerçekleştirilmesi planlanan stratejik eylemler, siber savunmanın güçlendirilmesi ve kritik alt yapının korunması, siber suçlarla mücadele, farkındalık ve insan kaynağı geliştirme, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin milli güvenliğe entegrasyonu olarak belirlenmiştir. Nesnelerin interneti de temel alınarak oluşturulan stratejik planlara göre bilgi sistemleri yapılandırılırken aşağıdaki hususların dikkate alınması gerekmektedir [53].

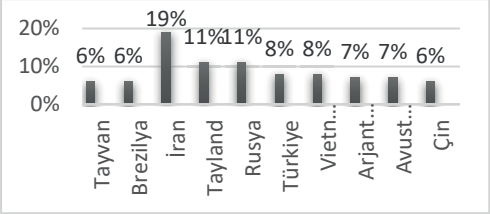
- ISO 27001 bilgi güvenliği yönetim sistemi standardının kamu kurumları ve özel sektörde zorunlu hale getirilmesi,
- Sızma testlerinin zorunlu hale getirilmesi,
- Bilgi/veri paylaşımı esnasında, iletişim güvenliğinin sağlanmasına yönelik güvenlik esaslarının oluşturulması,
- Güvenli IPv6 kullanımının yaygınlaştırılması,
- Milli adli analiz kapasitesinin genişletilmesi,
- Siber suçları tespiti için büyük veri analiz altyapısının kurulması,
- Siber güvenlik teknoloji yol haritasının ve araştırma gruplarının oluşturulması,
- Yerli ve teknolojik ürün kullanımı,
- Pardus'un yaygınlaştırılması,
- Kritik ürünleri denetleyecek ve sertifikalandırılacak mekanizmaların çalıştırılması,
- Kurumların sahip oldukları kritik verileri iyi bir şekilde tespit edip, bu verilerin mahremiyetinin ve güvenliğinin sağlanması.

Nesnelerin interneti ulusal bilgi sistemlerinde çok dikkat edilmesi gereken önemli bir kavramdır. Cihazların etkin kullanılması, verinin güvenilir iletilmesi, bilgi güvenliği ilkelerinin sağlanması düşünülerek yönetilmesi gereklidir. Ulusal anlamda, bilgi sistemlerini veri gizliliğini sağlamak adına oluşturulan eylem planındaki stratejilerin, nesnelerin interneti kavramı da düşünülerek yapılandırılması gerekliliği ön plana çıkmaktadır.

2016 yılının sonlarına doğru ABD'ye yönelik gerçekleştirilen "Mirai" adlı dağıtık hizmet aksatma saldırısı ülkemiz dâhil birçok ülkede erişim sorunlarına yol açmıştır. IoT cihazlarını hedef alan bu saldırı ile ülkemizdeki cihazların %10'nun kontrolü ele geçirilmiştir [54]. IoT'ye yönelik gerçekleştirilen bir diğer saldırı ise Hajime botnettir. 2016 Ekim ayının sonlarına doğru keşfedilen bu saldırı, açık portlar yardımıyla ya da varsayılan şifre ve kullanıcı adıyla IoT cihazların kontrolünü ele geçirmeyi hedefler. Bu saldırılar ile ülkemizde cihazların %8'nin kontrolü ele geçirilmiştir [55]. Nesnelerin internetine yönelik bir başka saldırı ise BrickerBot saldırısıdır. Cihazların güvenlik açıklıklarından faydalanarak yazılımı değiştirmeyi amaçlayan saldırıdır. Mirai saldırı ile benzer bir saldırı olup hedeflediği cihazı kalıcı olarak çalışamaz hale getirmektedir. Hindistan, Tayvan, İsrail gibi birçok ülkede olduğu gibi ülkemizde de cihazların büyük bir kısmı bu saldırıdan etkilenmiştir [56].



Grafik 1. Ülkelerdeki cihaz sayılarının Mirai saldırısından etkilenme oranları [54]



Grafik2. Ülkelerdeki cihaz sayılarının Hajime saldırısından etkilenme oranları [55]

5 - Sonuçlar ve Değerlendirmeler

Bu çalışmada, nesnelerin interneti konusu kişisel, kurumsal ve ulusal bilgi güvenliği çerçevesinde değerlendirilmiş, güvenlik açıklıkları ve saldırılar konusu araştırılarak bunlara karşı alınabilecek önlemler açıklanmıştır. Nesnelerin internetinin kullanımı arttıkça güvenlik ve gizlilik unsurlarını hedef alan saldırıların çeşitliliğinin de artma eğiliminde olduğu görülmüştür. Her ne kadar bu saldırıların sayısı ve çeşitliliği artsa da, gerek sistemsel zafiyetler gerekse de bu saldırıları engellemeye yönelik alınabilecek önlemlerin de iyi bir şekilde irdelenmesi gerektiği anlaşılmıştır. Saldırganların, nesnelerin internetinden faydalanarak bilgi güvenliğinin temel unsurlarını hedef alıp kişisel, kurumsal ve ulusal bilgi güvenliğini ihlal edebileceği unutulmamalıdır. Bu hususlara tasarımlarda dikkat edildiği kadar uygulamalarda da dikkat edilmelidir.

Bu makale kapsamında incelenen ve elde edilen bulgular değerlendirildiğinde, aşağıdaki hususlara dikkat edilerek, bu konuda karşılaşılabilecek zafiyetler ve olumsuzlukların azalmasına ve daha yüksek seviyede bilgi güvenliği sağlanmasına katkılar sağlanacaktır.

- IoT teknolojilerinin ve sistemlerinin bilgi güvenliği unsurlarını kapsayacak bir biçimde geliştirilerek, güvenlik bazlı uygulanmalıdır.
- Sistemler güvenlik politikaları ve standartlarına göre yapılandırılmalıdır.
- Donanımların veya cihazlarının konfigürasyonları doğru bir şekilde yapılandırılmalıdır.
- Bu sistemlerin de siber saldırılar başta olmak üzere pek çok saldırı türüne maruz kalabileceği ve bu tür saldırılardan korunma amacıyla saldırı tespit sistemi, basit yapıda şifreleme algoritması kullanımı, yönlendirme seviyesinde korunması gerekmektedir.
- Kablosuz sensör ağ yönetiminin, kontrolünün veya güvenliğinin sağlanması gereklidir.
- Sunuculara yönelik çözümlerin ve güvenliğin çok iyi seviyede olduğu günümüzde, saldırıların sunucuları etkileyebileceği ve bu saldırılardan korunması gerektiğini ve bu tarz saldırılardan korunma amacıyla saldırı tespit sistemleri, zararlı yazılım çalışmasını engelleme, güvenlik duvarları, güvenilir veri tabanı oluşturulması gereklidir.
- IoT sistemlerinde dış dünyadan alınan verinin en son kullanıcıda analiz edilerek kullanıldığı düşünülürse, saldırganın hedef unsuru son kullanıcı ve uygulama olabilmektedir. Saldırganın kullanıcıya ve uygulamalara yönelik saldırı gerçekleştirebileceği, bu amaç doğrultusundaki saldırılardan korunabilmesi için kullanıcıların bilinçlendirilmesi gerektiği, anti-virüs programları, güvenlik duvarı kullanımı, zararlı yazılım çalışmasını engelleme, kullanıcı yetkilerine göre erişim ve kontrolün sağlanması, kimlik doğrulamanın sağlanması, asimetrik şifreleme algoritması kullanımı gibi çözümler kullanılmaya başlanılmalı veyahut kullanımı yaygınlaştırılmalıdır.
- İçeriden ve dışarıdan gelebilecek saldırılara karşı sistemlerin nasıl daha üstün bir şekilde tasarlanabileceği konusuna daha çok önem verilmeli ve yeni çalışmalar yapılmalıdır.
- Ağ alt yapısı başta olmak üzere donanım, yazılım, kullanıcı ve sunucu bileşenleri özelden genele doğru bir mantık çerçevesinde güvenli hale getirilmelidir.
- IoT yeni gelişen bir alan olsa da yeni tehditleri ve beraberinde de fırsatları getirebileceği

unutulmamalıdır. Bu konuda da yeni çalışmalar mutlaka yapılmalıdır.

- Tablo 2'de verilen hususlara ve özetlere dikkat edilmeli ve bu özetten faydalanılarak yeni tasarımlar yapılmalı ve çözümler geliştirilmelidir.
- IoT'den elde edilen bilgiler mutlaka toplanmalı ve büyük veri analitiği yaklaşımlarıyla analiz edilmeli, meydana gelebilecek olası tehditler belirlenmeli ve giderilmelidir. Bu sayede mahremiyet ihlallerinin giderilmesine yönelik çalışmalar da yapılabilecektir.
- Nesnelerin interneti, birçok kurum ve kuruluşlarda kullanıldığı için bu sistemlere yapılan saldırılar ulusal bilgi güvenliğini tehdit etmektedir. Böylesi sistemler belli bir güvenlik politikasına göre yapılandırılmalıdır.

Kaynakça

[1] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers,* vol. 17, no. 2, pp. 243-259, 2015.

[2] H. Karl, F. Mattern, and K. Rmer, *Wireless Sensor Networks*. Springer, 2006.

[3] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by internet of things," *Transactions on Emerging Telecommunications Technologies,* vol. 25, no. 1, pp. 81-93, 2014.

[4] I. Gudymenko and M. Hutter, "Security in the Internet of Things," *Proceedings of Intensive Program on Information Communication Security (IPICS 2011),* pp. 22-31, 2011.

[5] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, 2012, vol. 3, pp. 648-651: IEEE.

[6] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics,* vol. 10, no. 4, pp. 2233-2243, 2014.

[7] V. Pachghare, *Cryptography and information security*. PHI Learning Pvt. Ltd., 2015.

[8] Y. Vural and Ş. SAĞIROĞLU, "Kurumsal Bilgi Güvenliği ve Standartlari Üzerine Bir Inceleme," *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi,* vol. 23, no. 2, 2008.

[9] J. Du and S. Chao, "A study of information security for M2M of IOT," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, 2010, vol. 3, pp. V3-576-V3-579: IEEE.

[10] M. Darwish, A. Ouda, and L. F. Capretz, "Cloud-based DDoS attacks and defenses," in *Information Society (i-Society), 2013 International Conference on*, 2013, pp. 67-71: IEEE.

[11] A. Zuquete, "Improving the functionality of SYN cookies," in *Advanced Communications and Multimedia Security*: Springer, 2002, pp. 57-77.

[12] A. Piskozub, "Denial of service and distributed denial of service attacks," in *Modern Problems of Radio Engineering, Telecommunications and Computer Science, 2002. Proceedings of the International Conference*, 2002, pp. 303-304: IEEE.

[13] I. Mopari, S. Pukale, and M. Dhore, "Detection and defense against DDoS attack with IP spoofing," in *Computing, Communication and Networking, 2008. ICCCn 2008. International Conference on*, 2008, pp. 1-5: IEEE.

[14] Y. Wang and J. Chen, "Hijacking spoofing attack and defense strategy based on Internet TCP sessions," in *Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013 2nd International Symposium on*, 2013, pp. 507-509: IEEE.

[15] S. Zadgaonkar, V. C. Pandey, and P. S. Pradhan, "Developing a Model to Enhance E-Mail Authentication against E-Mail Address Spoofing Using Application," *International Journal of Science and Modern Engineering (IJISME),* vol. 1, pp. 13-17, 2013.

[16] A. A. Khan, "Preventing phishing attacks using one time password and user machine identification," *arXiv preprint arXiv:1305.2704,* 2013.

[17] A. Prakash and D. P. Agarwal, "Data Security in Wired and Wireless Systems," in *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*: IGI Global, 2016, pp. 1-27.

[18] L. Yang, P. Yu, W. Bailing, B. Xuefeng, Y. Xinling, and L. Geng, "IOT secure transmission based on integration of IBE and PKI/CA," *International Journal of Control & Automation,* vol. 6, no. 2, pp. 50-61, 2013.

[19] H. Ning and H. Liu, "Cyber-physical-social based security architecture for future internet of things," *Advances in Internet of Things,* vol. 2, no. 01, p. 1, 2012.

[20] A. Sivabalan, M. Rajan, and P. Balamuralidhar, "Towards a Light Weight Internet of Things Platform Architecture," *Journal of ICT Standardization,* vol. 1, no. 2, pp. 241-252, 2013.

[21] B. Yan, B. Fang, B. Li, and Y. Wang, "Detection and defence of DNS spoofing attack," *Jisuanji Gongcheng/ Computer Engineering,* vol. 32, no. 21, pp. 130-132, 2006.

[22] W. G. Halfond, J. Viegas, and A. Orso, "A classification of SQL-injection attacks and countermeasures," in *Proceedings of the IEEE International Symposium on Secure Software Engineering*, 2006, vol. 1, pp. 13-15: IEEE.

[23] K. Dunham, *Mobile malware attacks and defense*. Syngress, 2008.

[24] K. Nirmal, B. Janet, and R. Kumar, "Phishing-the threat that still exists," in *Computing and Communications Technologies (ICCCT), 2015 International Conference on*, 2015, pp. 139-143: IEEE.

[25] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems,* vol. 29, no. 7, pp. 1645-1660, 2013.

[26] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 1996, pp. 33-48: Springer.

[27] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2004, pp. 357-370: Springer.

[28] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2M: From mobile to embedded internet," *IEEE Communications Magazine,* vol. 49, no. 4, pp. 36-43, 2011.

[29] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," *Wireless Networks,* vol. 20, no. 8, pp. 2481-2501, 2014.

[30] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A systemic approach for IoT security," in *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on*, 2013, pp. 351-355: IEEE.

[31] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials,* vol. 17, no. 4, pp. 2347-2376, 2015.

[32] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future Generation Computer Systems,* vol. 56, pp. 684-700, 2016.

[33] D. C. Chou, "Cloud computing risk and audit issues," *Computer Standards & Interfaces,* vol. 42, pp. 137-142, 2015.

[34] Y. Song, "Security in Internet of Things," 2013.

[35] M. Presser, P. M. Barnaghi, M. Eurich, and C. Villalonga, "The SENSEI project: integrating the physical world with the digital world of the network of the future," *IEEE Communications Magazine,* vol. 47, no. 4, pp. 1-4, 2009.

[36] Y. Song, "Security in Internet of Things," ed, 2013.

[37] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks,* vol. 54, no. 15, pp. 2787-2805, 2010.

[38] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," in *Proceedings of the 11th ACM conference on Computer and communications security*, 2004, pp. 210-219: ACM.

[39] F. L. Gandon and N. M. Sadeh, "Semantic web technologies to reconcile privacy and context awareness," *Web Semantics: Science, Services and Agents on the World Wide Web,* vol. 1, no. 3, pp. 241-260, 2004.

[40] L. Yang, P. Yu, W. Bailing, B. Xuefeng, Y. Xinling, and L. Geng, "IOT secure transmission based on integration of IBE and PKI/CA," *International Journal of Control and Automation,* vol. 6, no. 2, pp. 245-254, 2013.

[41] C. Liu and J. Qiu, "Study on a Secure Wireless Data Communication in Internet of Things Applications," *International Journal of Computer Science and Network Security (IJCSNS),* vol. 15, no. 2, p. 18, 2015.

[42] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," *Journal of Cyber Security and Mobility,* vol. 1, no. 4, pp. 309-348, 2013.

[43] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "Iot gateway: Bridgingwireless sensor networks into internet of things," in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, 2010, pp. 347-352: IEEE.

[44] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. Moreno, "A decentralized approach for security and privacy challenges in the internet of things," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, 2014, pp. 67-72: IEEE.

[45] M. B. Shemaili, C. Y. Yeun, K. Mubarak, and M. J. Zemerly, "A new lightweight hybrid cryptographic algorithm for the internet of things," in *Internet Technology And Secured Transactions, 2012 International Conference for*, 2012, pp. 87-92: IEEE.

[46] H. Shafagh and A. Hithnawi, "Security Comes First, A Public-key Cryptography Framework for the Internet of Things," in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*, 2014, pp. 135-136: IEEE.

[47] Z. Bohan, W. Xu, Z. Kaili, and Z. Xueyuan, "Encryption Node Design in Internet of Things Based on Fingerprint Features and CC2530," in *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International*

Conference on and IEEE Cyber, Physical and Social Computing, 2013, pp. 1454-1457: IEEE.

[48] R. Prasad, *My personal adaptive global NET (MAGNET)*. Springer, 2010.

[49] W. Zhang and B. Qu, "Security Architecture of the Internet of Things Oriented to Perceptual Layer," *International Journal on Computer, Consumer and Control (IJ3C),* vol. 2, no. 2, pp. 37-45, 2013.

[50] W. Jones, *Keeping found things found: The study and practice of personal information management*. Morgan Kaufmann, 2010.

[51] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, "On the design of lightweight link-layer security mechanisms in IoT systems," *Networks (Elsevier),* vol. 76, pp. 146-164, 2015.

[52] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation computer systems,* vol. 28, no. 3, pp. 583-592, 2012.

[53] (27.01.2017). *2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı*. Available: http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf

[54] (24-07-2017). *The Future is Here – Assaulting the Internet with Mirai*Available: https://umbrella.cisco.com/blog/blog/2017/01/05/future-assaulting-internet-mirai/

[55] (24-07-2017). *Hajime worm battles Mirai for control of the Internet of Things* Available: https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things

[56] (24-07-2017). *IoT Malware that Wipes Data from Infected Devices* Available: https://antivirus.comodo.com/blog/computer-safety/iot-malware-wipes-data-infected-devices/