

NESNELERİN İNTERNETİ VE GÜVENLİĞİ

Yiğit Turak

İstanbul, 2015

İÇİNDEKİLER

GİRİŞ	2
I. NESNELERİN İNTERNETİ	3
1. “NESNELERİN İNTERNETİ” NEDİR?	3
2. TARİHSEL GELİŞİMİ	4
3. GEÇMİŞTEN GELECEĞE DURUMU	5
II. “NESNELERİN İNTERNETİ”NDE BİLGİ GÜVENLİĞİ	8
1. BİLGİ GÜVENLİĞİ PROBLEMLERİ VE ÖNEMİ	8
2. GÜVENLİK ÖNEMLERİ	9
III. SONUÇ	12
IV. KAYNAKÇA	13

GİRİŞ

Günümüzde teknolojik gelişmelerin en hızlı uygulandığı alanlardan biri de nesnelerdir. Gerek teknolojik yeniliklerin getirdiği yaşamsal kolaylık ve faydalar, gerekse insanların teknolojiye çok hızlı adapte olup kullanımlarının hızla artması, nesnelerle iletişim en güncel konu olmuştur.

Birinci bölüm, son yıllarda akademik ve profesyonel çevrelerce çokça kullanılan “Nesnelerin İnterneti” kavramını incelemeye ve geçmişten geleceğe durumunu göstermeye yöneliktir. Öncelikle “Nesnelerin İnterneti” kavramının anlamının ne olduğu açıklanacaktır. İkinci başlıkta tarihsel gelişimi ve öngörülen geleceğe dönük tahminler özetlenmeye çalışılacaktır.

İkinci bölüm, bilgi güvenliğinin önemi ve “Nesnelerin İnterneti” teknolojisi üzerinde kullanımını incelemeye yöneliktir. İlk başlık Nesnelerin İnterneti kavramında bilgi güvenliğinin önemine ve bu alanda yaşanan örnek olaylara ayrılmıştır. İkinci başlık ise “Nesnelerin İnterneti” kavramında bilgi güvenliği uygulamalarına yöneliktir.

I. NESNELERİN İNTERNETİ

Bu bölümde nesnelerin interneti kavramı teorik açıdan ele alınmayı çalışılacaktır. Öncelikle bu kavramın çıkış noktası ve anlamı açıklanmaya çalışılacaktır. Daha sonra nesnelerin interneti kavramının geçmişten geleceğe incelemesi yapılacaktır.

1. “Nesnelerin İnterneti” Nedir?

Orijinal ismi Internet of Things (IoT) olan “Nesnelerin İnterneti” kavramı teknoloji öncülerinden Kevin Ashton tarafından ilk kez 1999 yılında Procter&Gamble şirketi için hazırlanan bir sunumda kullanıldı. Bu sunumda şirketin tedarik zincirinde RFID teknolojisi uygulamasının firmaya faydaları sıralanmakta ve kullanımı önerilmekteydi.

Daha sonraki yıllarda gelişen teknolojiler sayesinde milyarlarca insanın bilgisayarlar ya da taşınabilir mobil araçlarla internete bağlanmaları sağlanmıştır. Bu aşamadan sonra beklenen büyük adım birbirlerine bağlı bilgisayarların, birbirlerine bağlı nesneler ile bilgi alışverişi yapmasıdır. Arabalardan kitaplara, elektrikli aletlerden yiyeceklere, buzdolaplarından su ısıtıcılarına, akıllı binalardan ayakkabılara kadar aklınıza gelebilecek tüm şeylerin/nesnelerin birbirleriyle bağlanmaları gelecekte bizleri bekleyen bir gelişme olacaktır. İşte bu da Nesnelerin İnterneti (Internet of Things) olarak tanımlayabileceğimiz aşamadır. Her geçen gün gelişmekte olan bir uygulama ve kavram olduğu için şimdiye kadar birbirinden farklı tanımlar yapılmıştır.

Örneğin: Avrupa Birliği tarafından yayınlanan Dijital Ajanda da “Nesnelerin ve uygulamaların kendileri arasında iletişim kurmalarını, veri üretmelerini, bu verilerin paylaşımını sağlayan gelişmekte olan bir teknoloji ve pazardır. Bu yapı, “insanların hayatlarını kolaylaştıran ve yaşam standartlarını yükselten akıllı uygulama ve hizmetlerin ekosistemidir” şeklinde tanımlanmaktadır.

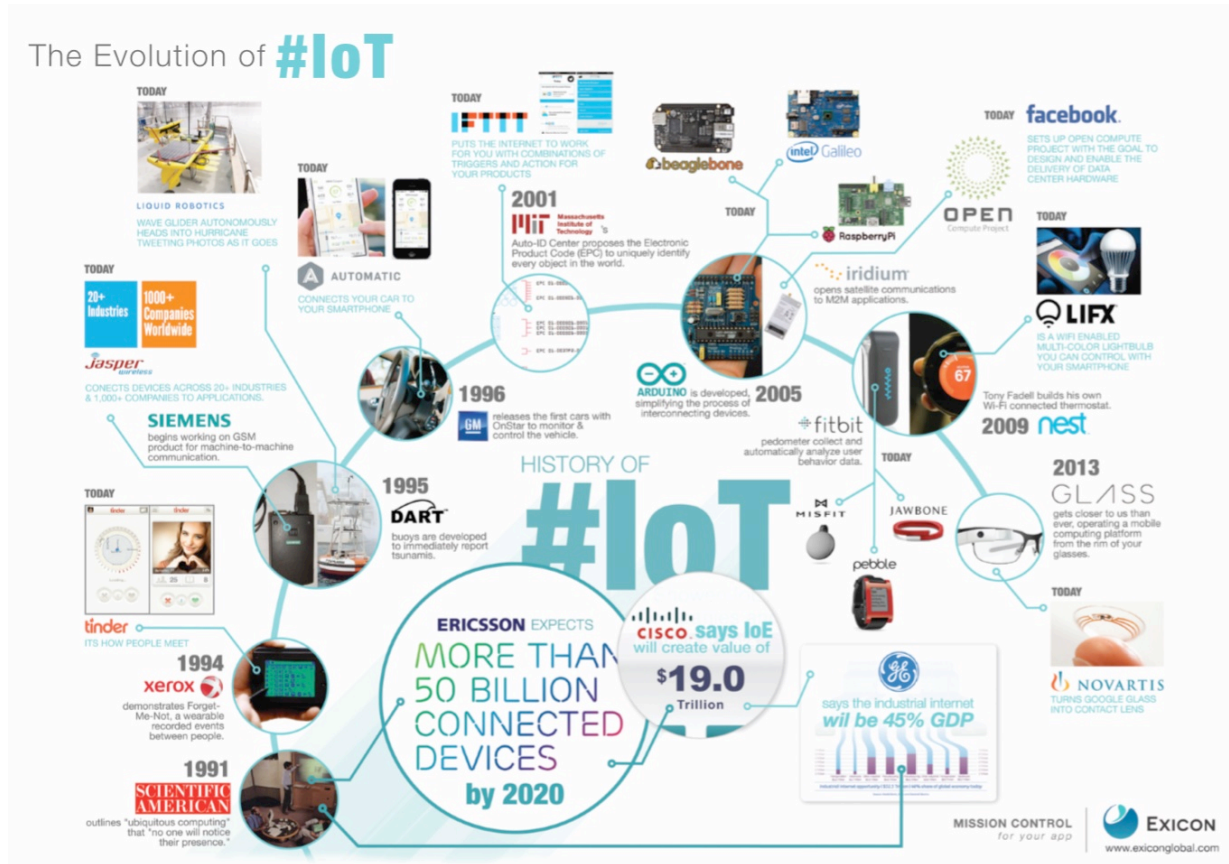
Avrupa Teknoloji Platformu ise “Fiziksel ve sanal özellikli olabilen, aynı zamanda önceden tanımlı işlevlere sahip, akıllı ortamlarda çalışan şeylerin/nesnelerin aralarında kurdukları ortak bir ağ ve bu ağın diğer ağlar ve kullanıcılar ile bilgi alış-verişine girmesi” şeklinde tanımlanmaktadır.

Genel anlamda ise “Nesnelerin İnterneti, çeşitli haberleşme protokolleri sayesinde birbirleri ile haberleşen ve birbirine bağlanarak, bilgi paylaşarak akıllı bir ağ oluşturmuş cihazlar sistemi” olarak tanımlamak mümkündür.

2. Tarihsel Gelişimi

1991 yılında Cambridge Üniversitesi'ndeki yaklaşık 15 akademisyenin kahve makinesini görebilmek için kurduğu kameralı sistem o günün koşullarında değerlendirildiğinde ufuk açıcı bir uygulamaydı. 2001 yılına kadar kullanılan sistem, kahve makinesinin görüntüsünü dakikada üç kez bilgisayar ekranlarına gönderiyordu. Çevrimiçi ve gerçek zamanlı olması sebebiyle "nesnelerin interneti" kavramının ilk örneği olarak tarihte yerini aldı.

Şekil 1: Nesnelerin İnterneti kavramını gelişimi



1994 yılında giyilebilir teknolojilere ait ilk örnekler ortaya konulmuştur. Xerox firması tarafından geliştirilen “Forget-Me-Not” isimli giyilebilir demo ürünü, insanların aktivitelerini kaydetmeyi amaçlamış olup; Steve Mann tarafından geliştirilen giyilebilir kablosuz ağ kullanan web kamera ile hayatın her anı kaydedilmeye başlanmıştır.

1995 yılında GSM isimli iletişim protokolünün kullanımı ile başlayan ve çok hızlı bir şekilde yayılan mobil cihazların kullanımı ile makineden makineye iletişim başlamıştır.

1996 yılında General Motors tarafından üretilen OnStar ürünü ile uzaktan arabaların kontrol edilebilmesine olanak sağlanmıştır.

Daha sonraki yıllarda gerek internetin gerek bilgisayar ve mobil teknolojilerin gerekse de yarı iletken teknolojisinin çok hızlı bir şekilde yaygınlaşması ve ucuzlamasıyla birlikte arabalardan kitaplara, elektrikli aletlerden yiyeceklere, buzdolaplarından su ısıtıcılarına, akıllı binalardan ayakkabılara kadar aklınıza gelebilecek her nesne teknolojiler aracılığıyla birbirleri arasında iletişime geçmektedir.

Günümüzden “nesnelerin interneti”nin hayatımızda yer aldığı belirli örnekler:

- **Doorbot:** Evlerin kapılarının akıllı telefonlar aracılığıyla evde olmadan da açılacak bir üründür. Akıllı telefonla ev diyafonu kablosuz internet üzerinden iletişime geçmektedir.
- **iKettle:** Mutfaka gitmeden su ısıtıcısının düğmesine basmadan akıllı telefonlar aracılığıyla kontrol edilebilen bir su ısıtıcısıdır. iKettle ile suyun sıcaklığı uzaktan ayarlanabilmektedir.
- **Nest:** Dünyada “nesnelerin interneti” denilince akla gelen ilk girişimlerden olan Nest akıllı ev sistemleri üzerine çalışmaktadır. 2013 başında 80 milyon \$ yatırım alan girişim daha öncesinde de akıllı termostadı duyurmuştu. İkinci olarak da duman detektörünü duyurdu. Akıllı telefon ile iletişim halinde çalışan duman detektörü telefon üzerinden acil durumlarda uyarı veriyor.
- **Revolv:** Revolv akıllı ev sistemleri üzerine geliştirilmiş nesnelerin interneti örneklerinden birisi olup, evlerdeki müzik sistemi, akıllı ampuller, elektrik prizleri gibi akıllı cihazlar Revolv ile yönetilebilmektedir.

3. Geçmişten Geleceğe Durumu

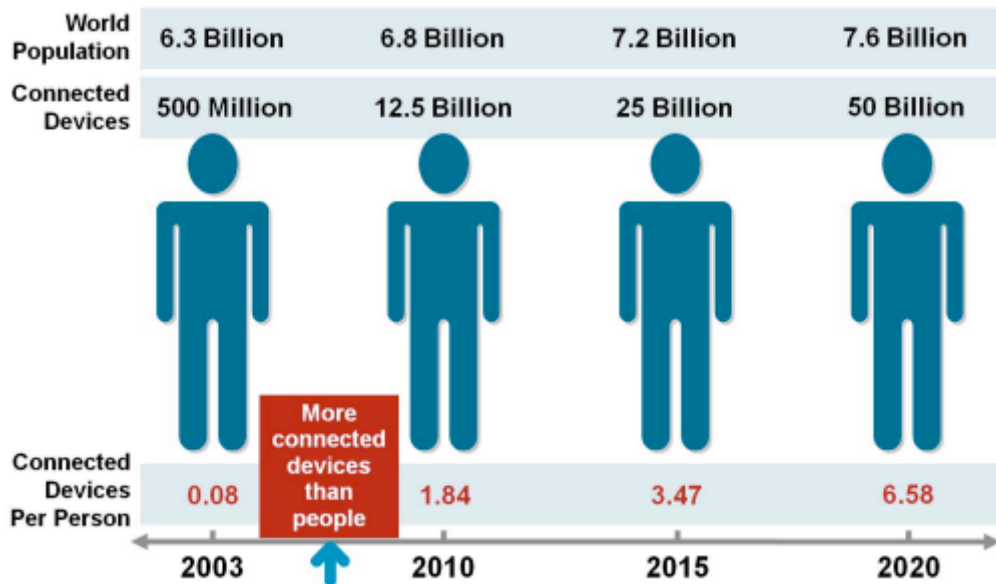
İnsanlık tarihinde yaşam tarzları, ekonominin gelişimi gibi kriterler göz önüne alındığı zaman toplumlar belirli kategorilere bölünebilmektedir. Başlıca toplum kategorileri:

- Avcı – Toplayıcı toplum tipi
- Tarım toplumu
- Sanayi toplumu
- Bilgi toplumu

İnternetin ve özellikle mobil teknolojilerin hızla yayılmasıyla birlikte, son 10 senede Sanayi toplumdan Bilgi toplumuna hızlı bir geçiş olmuştur. Günümüzde insanların geçim kaynakları, ülkelerin ekonomileri tamamen bilgi olmuştur. Bilgiyi toplamak ve onu işleyebilmek en önemli noktadır. Bilgi toplumuyla değişen bilgi anlayışıyla birlikte insanlar bilgiye en hızlı ve pratik şekilde ulaşmak istemektedir. Bilgi üretiminde ve işlenmesinde kullanılan yeni teknolojiler ile bu isteklere cevap verilmeye çalışılmaktadır.

Cisco tarafından 2011 yılında yayınlanmış raporda, 2003 yılında 500 milyon cihaz ağ yapısına bağlı ve kişi başına düşen cihaz sayısı 0.08 iken, 2010 yılında bu rakamlar 12,5 milyar cihaza ve kişi başı yaklaşık 2 cihaza çıkmıştır. Yapılan araştırmalara göre her 5 yılda bir rakamların ikişer kat artacağını göstermektedir.

Şekil 2: Akıllı cihazlar ve İnsan sayısı



Source: Cisco IBSG, April 2011

2020 yılına ait öngörüler arasında; herkesin Google Glass vb bir ürün ile her hareketi kaydedip, gözlük üzerinden internete bağlanması, arabaların insansız gidebilmesi, akıllı evler ile buzdolabından internete girmek veya işten robotlar aracılığıyla yemek yapılması, araba arızalandığında servisin bilgisayar ile araca bağlanarak sorunu çözmesi, giyilebilir teknoloji ile sağlık durumu anlık olarak takip edilen bir kişinin kalp krizi geçirmeden kıyafeti sayesinde hastaneye haber verilerek ambulansın gelmesi vardır.

2013 yılında 613 milyar dolar ekonomik katkısı olan IoT teknolojisinin 2020 yılında değeri 19 trilyon dolar olması öngörülmektedir. Aynı şekilde 2008 yılında üretilmiş olan toplam veri boyutunu, 2020 yılında bir evde var olan 20 adet akıllı cihaz üretebilecektir. Buradan da

görüldüğü gibi gerek teknolojinin ekonomik boyutu, gerekse üretilen veri boyutu sınırları zorlamaktadır.

Birbirleriyle ve insanlarla bağlantı kuracak cihaz sayısının astronomik boyutta artmasıyla birlikte cihazların bağlantı için kullanmış olduğu IP adres sayısının yetmeyeceği 2000li yılların başında ön görülmüş ve IPv6 geçişi planlanmaya başlanmıştır.

II. “NESNELERİN İNTERNETİ”NDE BİLGİ GÜVENLİĞİ

İlk bölümde değindiğimiz IoT kavramı ve teknolojisinin gelişimi; hayatı kolaylaştırması, yaşam standartlarını yükseltmesi, verimliliği artırması ve ekonomilere katkısı toplumsal yapıyı değiştirmektedir. Her güzel şey gibi dikkat edilmediği zaman bunun da kötü noktaları ciddi boyutlardadır. En kilit noktası bilgi güvenliğidir. Bu bölümde akıllı nesnelerle ilgili yaşanabilecek bilgi güvenliği problemleri, neden güvenlik konusunun gerçekten çok önemli olduğu ve alınabilecek önlemler görülecektir.

1. Bilgi Güvenliği Problemleri ve Önemi

Günümüzde üreticiler bütün elektronik cihazları akıllı kelimesiyle pazarlamaktadır. Oysa akıllı telefonlar, akıllı televizyonlar, akıllı beyaz eşyalar, akıllı arabalar, ısıtma, soğutma, iklimlendirme ve havalandırma sistemleri, ışıklandırma ve priz çözümleri, yangın ve hırsız alarmları, bilgisayarlı kapı ve kasa kilitleri, modemler ve bilgisayarlar aslında hiç de akıllı cihazlar değildir. Çünkü gerçekten üzerinde çok fazla derecede güvenlik açığı barındırmaktadır.

2013 yılında Rusya’nın devlet kanalı Rossiya 24, Çin’de üretilen ve ülkeye ithal edilen hacker ütülerin özel bir kablosuz internet kontrol çipi barındırdığını, böylece kullanıcıların evindeki kişisel bilgisayarlarına siber saldırı düzenleyerek casusluk yapıldığını öne sürmüştür. Bu haber önce abartı bir haber veya yalan haber gibi gelse de yapılan incelemelerde doğruluğu tespit edilmiştir.

Bir başka açıdan bakılırsa; bir evdeki bütün eşyalar konut otomasyon sistemi ile tek bir merkezden yönetilirse, o sistemi siber saldırı ile ele geçirmek, fırın ayarları ile oynayarak yangın çıkarmak, alarm sistemini kapatarak ve kapıyı açarak hırsızlık yapmak, bilgisayardaki tüm kişisel verileri kopyalamak veya kamera sisteminden evi izleyerek özel hayatın gizliliğini ihlal etmek mümkün hale gelmektedir.

AV-Test sitesinin 2014 Mayıs ayında yapmış olduğu araştırmaya göre akıllı ev kurulum cihazlarında çok sayıda güvenlik açığı bulunmaktadır. Bu testlerde eSaver firmasının iConnect çözümü, tapHome’dan EuroiSytle, Gigaset’in Elements serisi, REV Ritter iComfort, RWE SmartHome, Deutsche Telekom Qivicon ve Hama’nın Xavax Max ürünleri incelenmiştir. Test sonuçlarında Gigaset, RWE ve Qivicon ürünlerinin siber saldırılarla izinsiz erişime karşı korumalı olduğu ortaya çıktı. Ancak iComfort ve tapHome kitlerinin inceleme yapıldığı tarihte

güvenlik açıklarına sahip olduğu tespit edilmiştir. Yani eve giren siber hırsızlar akıllı evlerin merkezi kontrol birimine eriştikten sonra odaları kullanıcıları gözetlemek üzere yeniden yapılandırabilir ardından internet üzerinden izleyebilirler. Hatta tüm dünyaya da yayın yapabilirler. Ayrıca iComfort ve Xavax Max ürünlerindeki güvenlik açıklarından faydalanarak cihazların kontrolü internet üzerinden de ele geçirilebilmektedir.

Akıllı cihazların insanların yaşam standartlarını yükseltmesi ve hayatı kolaylaştırması, kişinin ihtiyaç ve alışkanlıklarına göre özelleştirilmesinin tek yolu, özel hayatın günde 24 saat gözlemlenmesidir. İnsanların bu tür çözümlerle ne kadar veri paylaşmak istediği ve günlük yaşantısını BBG (Biri Bizi Gözetliyor) yarışmacıları gibi yaşamaya razı olup olmaması önemlidir. Bu kişilerin özel ve kişisel bilgilerine sahip sistemlere sızmayı başaran siber saldırganların, politik muhaliflerden rakip şirket çalışanlarına ve gazetecilere kadar çok sayıda kişiyi gözetleyebilecek olması önümüzdeki yıllar için çok ciddi tehditler yaratmaktadır. Akıllı cihazlar yaşam kalitesini artırsa da bu akıllı nesneleri izinsiz gözetleyenler olması durumunda özel hayatın gizliliği ve güvenliği riske girmektedir.

2. Güvenlik Önemleri

Akıllı cihazlarla yaşanabilecek bilgi güvenliği ihlallerinin, gerek üretici firmanın gerekse kullanıcının yapacağı belirli kontrollerle engellenme şansı bulunmaktadır. OWASP isimli bir topluluk tarafından yayınlanmış akıllı cihazlarda en çok karşılaşılan 10 güvenlik zafiyetine bakıldığı zaman aşağıdaki kontrol noktalarının yapılması gerektiği belirlenebilir.

- 1. Web Arayüzü Yapılandırması:** Kullanıcıların akıllı cihazları yönetebilmesi için Web teknolojisi kullanılarak yapılan arayüzlerin güvenlik yapılanlandırmaları ciddi öneme sahiptir. Varsayılan şifrelerin kurulum sırasında değiştirilmesi, karmaşık şifre kullanılması, web arayüzlerine özel geliştirilmiş ataklara (XSS, SQL injection, CSRF vb) karşı kontrollerin yapılmış olması ve kullanıcı hesap bilgilerinin ağ yapıları üzerinde açık olarak taşınmaması gerekmektedir.
- 2. Kimlik Kontrolü/Yetkilendirme:** Akıllı cihazlara sadece sahibi olduğu kullanıcı tarafından bağlanabilmesi ve bağlanan kişiler için yetki kontrolünün yapılabilmesi önemlidir. “Şifremi unuttum” mekanizmalarının çok ciddi derecede güçlü ve güvenli olması, atak yapan kişilerce bu mekanizma kullanılarak şifrelerin elde edilememesi, kullanıcıların karmaşık şifre kullanmaya zorlanması, granüler erişim kontrollerinin yeterli seviyede olması, yeterli sayıda rol profillerinin var olması ve izinsiz yetki yükseltmelerine karşı kontrollerin yapılmış olması gerekmektedir.
- 3. Ağ Servisleri:** Gerek kullanıcıların erişebilmesi gerekse kendi aralarında iletişime geçebilmeleri için akıllı cihazlarda belirli ağ servisleri açık olmak zorunda olup, gerekli

kontrollerin yapılamadığı durumlarda ciddi zafiyetler ortaya çıkmaktadır. Sadece gerekli olan servislerin açık olması ve diğerlerinin kapatılması, bu servislere erişimlerin kontrol edilmesi, açık olan servislerde olabilecek zafiyetlere karşı güvenlik önlemlerinin alınmış olması, servis durdurma saldırılarına karşı korumalı olması gerekmektedir.

4. **Şifreli Taşıma:** Kullanıcı ile akıllı cihazlar veya sadece akıllı cihazlar arasındaki veri transferlerinin standart hale gelmiş ve güvenli olduğu bilinen şifreleme algoritmaları ile şifrelenerek yapılması son derece önemlidir. Bir şekilde ağ trafiğine sızmış kötü niyetli kişi trafiği izlediği zaman şifrelenmiş verileri görmelidir. Bunun için SSL ve TLS şifreleme protokollerinin kullanılması, protokollerin içerisinde pratikte kırılamayacağı ön görülen anahtar uzunluklarının ve algoritmaların kullanılması gerekmektedir.
5. **Gizlilik:** Akıllı cihazlar insanların yaşamlarını kolaylaştırmak ve yaşam standartlarını yükseltmek için kişisel ve özel birçok veriyi kaydetmekte ve işlemektedir. Burada önemli nokta her akıllı cihaz sadece ihtiyacı dâhilindeki verileri toplamalıdır. Örneğin iklimlendirme sisteminin facebook üzerinde yaptığınız paylaşımlarınızı kaydetmesi anlamlı değildir. Cihazların sadece ihtiyacı dâhilindeki minimum veriyi kaydetmesi ve işlemesi, kaydedilecek veri türlerini kullanıcının seçimine bırakması ve verilerin gizliliğini korumak için şifreli olarak saklaması gerekmektedir.
6. **Bulut Arayüzü:** Akıllı cihazlar kendi üzerinde çok fazla veri tutmamaktadır ve o verileri işleyecek güçte işlemcilerle sahip değildir. Üretici firmalar bulut hizmetleri aracılığıyla bu verileri bulut ortamında toplamakta ve işlemektedir. Bulut sistemlerinin güvenliği bu yüzden ciddi önem taşımaktadır. Şifre sıfırlama mekanizmasının güçlü olması, yanlış şifre denemelerine karşı hesabın kilitlenerek güvenliğin sağlanması ve cihazlar ile bulut hizmeti arasındaki bağlantıda kimlik kontrollerinin yapılarak trafiğin şifreli olması gerekmektedir.
7. **Mobil Uygulamalar:** Akıllı cihazlar web arayüzleri haricinde mobil uygulamalar aracılığıyla da yönetilebilmektedir. Şifre sıfırlama mekanizmasının güçlü olması, yanlış şifre denemelerine karşı hesabın kilitlenerek güvenlik sağlanması ve cihazlar ile mobil uygulamalar arasındaki bağlantıda kimlik kontrollerinin yapılarak trafiğin şifreli olması gerekmektedir.
8. **Güvenlik Yapılandırmaları:** Akıllı cihazların güvenlik yapılandırmaları kötü niyetli kişilerin saldırılarına karşı korunabilmek için ciddi önem taşımaktadır. Yönetici yetkilerine sahip özel kullanıcı hesapları ile normal kullanıcı hesaplarının birbirinden ayrılması, verinin taşınması ve saklanması şifreli bir şekilde yapılması ve güçlü şifre politikalarının belirlenmesi gerekmektedir.
9. **Yazılım:** Akıllı cihazlar üzerinde çalışan yazılımlar aracılığıyla kullanıcı-cihaz iletişimleri yapılabilmektedir. Yazılım üzerinde yer alan güvenlik zafiyetlerinin üretici firma tarafından sürekli yayınlanan güncellemeler ile kapatılması, güncelleme

paketlerinin üretici firma tarafından imzalanmış olması ve güncelleme paketlerinin şifreli olarak taşınması gerekmektedir.

- 10. Fiziki Güvenlik:** Akıllı cihazlara yapılabilecek saldırıların başında fiziki müdahaleler gelmektedir. Cihazların fiziksel olarak korunması da ciddi önem taşımaktadır. Cihazlar üzerindeki veri depolama disklerinin kolaylıkla sökülememesi, verilerin şifrelenmiş olarak saklanması, USB gibi bağlantı portlarının kapatılmış olması gerekmektedir.

III. SONUÇ

Akıllı cihazların yaygınlaşması ile birlikte toplum yapıları değişmiş, “Bilgi Toplumu” olgusu tam anlamıyla oluşmuştur. Eskiden bilgi sadece kişilerin kendi istekleriyle verdiği bilgilere dayanmakta olup alınan verilerin doğrulukları sıklıkla tartışılmaktaydı. Ancak gelinen noktada artık veriler akıllı cihazlar ile kişilerin beyanından bağımsız olarak toplanmakta ve doğruluk dereceleri yükselmektedir. Bu şekilde güvenilir bilgi birikimi de akıllı nesneler ile artacaktır.

İnternetin ve akıllı nesnelerin; iletişim, eğitim, iş yaşantısı, bilim, hükümetler, sağlık, bankacılık gibi sayabileceğimiz onlarca başlıktaki konuları nasıl etkilediği, işleyişlerini nasıl değiştirdiği ve hatta yeni baştan yapılandırabildiği görülmektedir. Bunun yanı sıra; IoT, bir teknoloji devrimi olarak, bu gelişmeyi hızlandıracak ve daha üstün boyutlara taşıyarak, çok açık bir şekilde her şeyi değiştirecek gibi görünmektedir.

Diğer yandan bakacak olursak insanların 7/24 izleniyor ve her hareketinin kaydediliyor, sağlık verilerinin, günlük aktivitelerinin saklanıyor olması; bilgi güvenliği konularını, kişisel verilerin ve özel hayatın gizliliğini gündemin en üst maddelerinden birisi haline getirmektedir.

Kullandığımız arabanın saldırganların hedefi olup kaza yapmasına sebep olması, akıllı alarm ve kilit sistemlerinin kırılıp siber hırsızlıkların olması, giyilebilir nesnelere sızarak, vücut aktivitelerinden rahatsızlıkların tespit edilerek siber cinayetlerin ortaya çıkması artık bilim kurgu filmlerinden gerçek hayatta görülmeye başlanacaktır.

Çalışmada nesnelerin interneti teknolojisi ve bilgi güvenliğinin önemi konu edilmiştir. Ancak bilgi güvenliğinin yanı sıra kişisel verilerin ve özel hayatın gizliliği konularıyla “nesnelerin interneti” kavramının incelenmesi geleceğe dönük faydalı bir çalışma olacaktır.

IV. KAYNAKÇA

- Rolf H. Weber, Internet of Things – New security and privacy challenges, Computer Law & Security Review, Volume 26, Issue 1, January 2010, Pages 23–30
- Cisco, Joseph Bradley, Jeff Loucks, James Macaulay, Andy Noronha, Internet of Everything (IoE) Value Index, http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe-value-index_Whitepaper.pdf, 2013
- OWASP, The OWASP Internet of Things Top 10, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014, 2014
- PC Magazine, FAHMIDA Y. RASHID, How to Secure Your Internet of Things, NOVEMBER 5, 2014
- KAREL, Emrah Yetimler, Internet of Things (Nesnelerin İnterneti) Nedir? Cihazların Etkileşim Trendleri, <http://www.karel.com.tr/blog/internet-things-nesnelerin-interneti-nedir-cihazlarin-etkilesim-trendleri>
- Cisco, Dave Evans, How the Next Evolution of the Internet Is Changing Everything, April 2011
- Exiconglobal, The Internet of Things: A History of Computer Networks Between Everyday Objects, <http://www.exiconglobal.com/report-download/iot-timeline>
- The Hacker News Bulletin, Praveen Kashyap, Russia: Chinese Irons have hidden chips which serve malware in systems, November 2, 2013
- AV-TEST-Studie, Michael Schiefer, 7 Smart-Home-Starter-Kits im Sicherheits-Test, April 28, 2014