NESNELERİN İNTERNETİ (IOTS): KULLANIM ALANLARI VE SİBER GÜVENLİK

Büşra Güler[♣]

Özet

İnternete erişen fiziksel, sanal özellikleri olan, önceden tanımlı işlevlere sahip nesnelerin diğer cihazlarla bilgi alışverişinde olduğu aralarında kurdukları ortak bir ağ olan nesnelerin interneti kavramı 1999 yılında Kevin Ashton tarafından literatüre kazandırılmıştır. IoTs, kullandığımız veya kullanacağımız her nesnenin bir şekilde internet üzerinden diğer cihazlarla iletişim halinde olmasıdır. Nesnelerin İnterneti'nin yaygınlaşmaya başlamasıyla iş ve özel hayatımızın önemli bir parçası haline gelen hemen her alanında birbiriyle iletişimde olan cihazlar var olmaya başlamış ve bunlar hayatımızı kolaylaştırmıştır. Elektronik cihazların birçoğu akıllı olmaya başladığı için artık bu cihazlar da birbirleriyle iletişim halinde olabilmektedir. Gündelik hayatta bilgisayar veya akıllı telefon ile oturduğumuz yerden birçok bilgiye ulaşabilmenin rahatlığı yaşanmaktadır. İnternet üzerinden cihazların birbirine bağlanması, sosyal hayatı kayıt altına almaktadır. Her geçen gün kullanım alanı ve miktarı artan internetin 2020'lerde bugün kullanılan kotanın sadece ev aletleri tarafından kullanılacağı düşünülmektedir. Ayrıca dünya çapında IP trafiğinin zetabaytın üzerine çıkacağı ve yarıdan fazlasını bilgisayar olarak tanımlanmayan cihazların oluşturacağı veriler olacağı tahmin edilmektedir. Veri miktarının inanılmaz derecede artması işlenmesini zor ve karmaşıklaştıracak, verilerin gizliliği ve güvenliği daha da önemli hale gelecektir. Uzaktan kontrol edilebilme, büyük miktarda verilere erişilebilme ile bilişim sistemlerinin saldırılardan korunması, işlenen bilgi/verinin gizliliğinin korunması, bütünlüğünün sağlanması ve güvence altına alınması büyük önem taşımaktadır. Bu çalışmada Nesnelerin İnterneti uygulamasının kullanım alanları, kullanıcıların uygulayabileceği güvenlik önlemleri ve güvenlik farkındalığının artırılma yolları incelenecektir. Çalışmanın amacı, nesnelerin internetinin kullanım alanları, ortaya çıkan fırsat ve risklerin değerlendirilmesi, kişisel verilerin toplanması, saklanması, tehlikelerin minimize edilmesi ve güvenliğin sağlanması için yapılabileceklerin araştırılmasıdır.

Anahtar Kelimeler: Nesnelerin İnterneti (IoTs), Siber Güvenlik, Veri Gizliliği, Akıllı Teknoloji.

Internet of Things (IoTs): Usage Areas and Cyber Security

♣ Endüstri Mühendi, Selçuk Üniversitesi.

Abstract

The concept of the internet of things, which have physical, virtual features, access to the Internet, a common network between objects that have predefined functions and exchange information with other devices, was introduced to the literature by Kevin Ashton in 1999. IoTs is the way in which each object we use or use will communicate with other devices over the Internet in some way. With the spread of the Internet of Things, devices that communicate with each other in almost every area that has become an important part of our business and private lives have started to exist and they have facilitated our lives. As many electronic devices are starting to become smart, these devices can also communicate with each other. In everyday life, it is easy to access a lot of information from where you sit with your smartphone or your phone. Connecting the devices over the Internet records social life. Internet usage area and amount is increasing day by day. The quota used today is thought to be used only by household appliances in the 2020s. In addition, it is estimated that IP traffic across the world will occur in zetabyte and more than half of them will be created as non-computer defined devices. The incredible increase in the amount of data will become difficult and complicated to process, and the privacy and security of the data will become even more important. Remote control, access to large amounts of data, protection of information systems from attacks, protection of confidentiality of information/data, ensuring the integrity and assurance of security are of great importance. In this study, the application areas of the Internet of Things application, the security measures that users can implement and the ways to increase security awareness will be examined. The purpose of the study, the use of the Internet of objects, evaluation of opportunities and risks, collecting and storing personal data, minimizing the dangers and investigating what can be done to ensure security.

Keywords: Internet of Things (IoTs), Cyber Security, Data Privacy, Intelligent Technology.

Giriş

"Fiziksel nesnelerin birbirleriyle ya da daha büyük sistemlerle bağlantılı olduğu iletişim ağı" şeklinde tanımlanan Nesnelerin İnterneti (IoTs) terimi giderek yaygınlaşmasına rağmen bu terimin gerçekte ne içerdiğini ortaya koyan ve fikir birliği sağlanan bir tanımlama bulunmamaktadır. Diğer bir ifade ile Nesnelerin İnterneti, bireyin fiziksel temasına yani dokunmasına, veri girmesine ihtiyaç duymadan nesne, cihaz ya da eşyaların gelişen iletişim teknolojisi sayesinde birbirleriyle bağlanması, iletişim kurabilmesi (Altınpulluk, 2018) ve etkileşim içinde olması anlamına gelmektedir.

Kevin Ashton tarafından 1999 yılında bir sunumda kullanılmasıyla bu kavram literatüre girmiştir. Gelişen teknoloji ile birlikte, çeşitli haberleşme protokolleri sayesinde birbirleri ile haberleşebilen ve birbirine bağlanabilen bir düzeye gelmiştir. Paylaşılan bilgiler neticesinde ise akıllı ağlar oluşturulmuştur (Yetimler). Teknoloji çağında hızla bilimsel gelişmeler ve yenilikler yaşanmaktadır. Halihazırda kullanılan akla gelebilecek her nesne, her elektronik cihaz, internet bağlantısı ile geliştirilebilir ve bu durum ise cihazların akıllı nesneler haline gelmesine olanak sağlamaktadır (Abouzakhar ve diğ., 2017).

Cihaz veya nesnelerin oluşturduğu küresel bir ağ olan IoTs'nin kullanım alanı her geçen gün artmaktadır. Hemen hemen her şeyin internete bağlı olduğu, neredeyse hayatımızın devamı için bağımlı hale geleceğimiz bir döneme doğru ilerliyoruz. Öyle ki eskiden kullanılan takvim, telefon rehberi, termometre, hatta okullarda öğretilen çarpım tablosu, internet üzerinden ulaşılan bilgiler haline gelmiştir. Gelecekte bütün üretim unsurları Wi-Fi ve Bluetooth teknolojisi ile internet üzerinden yönetilebilecektir. Akıllı makinalar yeni bilgiler üretebilecek, dışarıdan aldıkları bilgileri kısa sürede paylaşması gereken birimlere iletecektir. Programların geliştirilebilme imkanına sahip olması kapasitesinin sürekli artırılmasını mümkün kılacaktır. Nesnelerin birbiriyle iletişim halinde olması hayatımıza yeni giren bir kavram değildir. Günümüzde olduğu gibi gelecekte de hareketlerimizi planlayacağımız veriler toplamaya ve bizi bilgilendirmeye devam edecektir. Akıllı telefonlardan, akıllı ev aletlerine, sağlığımızın uzaktan takibi için kullanılan cihazlardan, akıllı gözlükler, akıllı t-shirtler, ev otomasyon sistemleri, akıllı arabalar, akıllı otobüs ve metro duraklarına kadar birçok örnek verilebilmektedir. Kısaca kullandığımız-kullanacağımız her araç-gereç akıllı hale gelecektir. Bu elbette insanın gündelik işlerini daha da kolaylaştırmanın yanında beraberinde ciddi riskleri de getirecektir. Her şey akıllı makinalara havale ettiğimizden arıza halinde ne yapacağımızı bilemeyeceğimiz için hayati risklerle karşı karşıya kalınabilecektir. Her şehirde uygulanmaya başlayan "akıllı durak" uygulaması otobüsün nerede olduğunu veya bulunduğunuz durağa ne zaman geleceğinin bilgisini veren bir sistemdir. Günün birinde buzdolabınızın size neyin eksik olduğunu söylediğini almadığınızda sinirlendiğini veya akıllı bulaşık makinenizin parlatıcısının bittiğini haber vermesi ve farklı bir ürün getirdiğinizde size tavır alması olayları gelecekte mümkün olabilir mi? Bu sorulara henüz net bir cevap verilemese de 21. yüzyılın makineleri artık gerçekten akıllı. Nesnelerin İnterneti ise, kapsama alanını her geçen gün artırmaktadır. Bu teknoloji akımı ile yakın gelecekte nesneler, insan-insan, insan-nesne ve nesne-nesne arasında kendiliğinden iletişim kurulabilir, veri

toplanabilir, iletişim kurup etkileşim halinde olabilir. Daha da önemlisi karar verebilirler ki bu da belki insan için olumsuz sayılabilecek başka durumları ortaya çıkarabilecektir.

Kullanım Alanları

Nesnelerin hala % 99'unun birbirine bağlı olmadığı tespiti ile yolun çok başında olunduğu görülmektedir (Altınpulluk, 2018). Nesnelerin internetinin uygulama alanlarından bazıları, uzaktan algılama, performans izleme ve yürütmedir. Bu açıdan bakıldığında IoTs'nin kısmen belirli alanlarla sınırlı olduğu düşünülmektedir. Ancak yine de getirdiği yenilik ve kolaylıklar azımsanamayacak kadar çoktur. Dikkatli bakıldığında IoTs'nin kullanım alanının oldukça geniş olduğu görülmektedir. Kirlenmemiş su, temiz hava/hava kirliliği, katı atık depolama sahası, ormancılık, çevre, tarım, hayvancılık, akıllı şehirler, akıllı ölçüm, kolay ve güvenilir üretim/yönetim için bu süreçte işletilen endüstriyel kontrol, güvenlik ve acil durumlar, enerji sistemleri, ev otomasyonu, lojistik, sağlık ve hatta alışveriş gibi uygulama alanları bulunmaktadır. Ayrıca bu alanlarda ortaya çıkabilecek muhtemel sorunlar karşısında çözüm üretmek için geniş bir fırsat alanı da sunmaktadır.

Bulut sistemleri yani bilgisayar ve genel cihazlar için kullanılabilen ve kaynak paylaşımı yapmayı mümkün kılan internet merkezli bilişim sistemidir. Bu sistem gelişmiş üretim hedeflerine ulaşmak için yeni fırsatlar sunmaktadır. Algılama yetenekleriyle nesnelerin interneti, sanayi altyapısını birleştirerek farklı endüstriyel işlemleri otomatikleştirmektedir (Gökrem ve Bozuklu, 2016). Uygulama alanlarından dikkat çekenler, akıllı üretim sistemlerinin ve bağlı üretim alanlarının geliştirilmesinin Endüstri 4.0 başlığı içerisinde tartışılmakta olduğu akıllı endüstriyi içermektedir (Altınpulluk, 2018). Endüstrinin önemli yapı taşlarından olan işçi sağlığı konusunda iyileştirici katkısı olmaktadır. Sistem, toplanan bilgiler üzerinden işçi sağlığı ve iş güvenliği risklerini minimuma indirmeyi amaçlar. Üretim süreçleri içerisinde işçilerin fabrikalarda kendilerini güvende ve huzurlu hissedecekleri şartları oluşturan yeni nesil üretim modeli geliştirilmektedir (Gökrem ve Bozuklu, 2016). Böylece işçi sağlığı ve güvenliği yönünde gözle görülür bir ilerleme sağlanabilecektir. Riskler minimum düzeyde tutulabileceğinden istenmeyen olumsuz olaylardan da kaçınılmış olacaktır.

IoTs sensörler, aktüatörler, kontrol sistemleri ve makine ağı ile endüstride üretim ve tedarik zinciri ağlarının gerçek zamanlı optimizasyonu konusu ile de ilgilenmektedir. Proses endüstrilerde gelişmiş verimliliği, güvenli dağıtım sistemini elde etmek için dijital

kontrolörler kullanılarak proses kontrolleri, hizmet bilgi sistemleri ve operatör araçları otomatik hale getirmektedir. Gerçek zamanlı izleme ve süreçlerin kontrolü, özel iletişim ve internet teknolojileri ile akıllı makineleri, akıllı sensörleri, akıllı denetleyicileri görevlendirme, yüksek hassasiyetli otomasyon ve kontrol sayesinde güvenlik, güvenilirlik ve güvenilebilirlik en üst seviyeye çıkmaktadır (Nesnelerin İnterneti ve Endüstriyel Uygulamaları). Özellikle dağıtım süreci izlemesi tüketiciyi de oldukça ilgilendirmektedir. Çünkü tüketici satın aldığı eşya, ürün ya da nesnenin kendine geliş sürecini takip edebilmektedir.

Endüstriyel nesnelerin interneti uygulamalarında, üretimde yer alan işçilerin ve üretilen ürünlerin güvenliği için zararlı gazların seviyesinin ölçülmesi, sıcaklık ve nem ölçümleri, gıdaların kalite ölçümleri gibi örnekler verilebilir. Yakın Alan İletişimi (NFC) teknolojisi radyo frekansıyla cihazlar arasında veri iletişimi sağlamak esasına dayanır. Endüstrinin önemli bir aşaması olan tedarik zinciri alanında da etkili bir uygulamadır. Çünkü stok yenileme sürecinin otomatikleşmesi, raf ve depolarda bulunan ürünlerin rotasyon kontrolünü akıllı ürün yönetimi sistemi ile sağlayabilecektir. Buna ilave olarak ise ürün takibi sağlayan tedarik zinciri ile saklama şartlarının izlenmesi mümkündür. Bu örnekler tedarik zincirinin denetim uygulamalarını oluşturmaktadır (Gökrem ve Bozuklu, 2016). Özetle tedarik zincirinin aşamalarında yer alan akıllı ürün yönetimi sayesinde ürün üretiminden saklanmasına, güvenliğinden sevkiyatına kadar her aşama kontrol altında tutulabilmektedir.

Nesnelerin interneti ve bulut sistemleri lojistikten kaynaklanan maliyet artışlarını ve yaşanan gecikmeleri büyük ölçüde ortadan kaldırmıştır. Araçların güvenli seyahat edebilmesi için geçiş güzergahındaki trafiğin durumu, hava kirliliği, araçta ortaya çıkabilecek arızaların önceden bildirilmesi gibi yararlı bilgileri ilgili birimlere iletip zaman ve gereksiz bakım ücretlerinden kaynaklanan kayıpların önüne geçilebilir (Gökrem ve Bozuklu, 2016). Eğer bu alanda kullanım yaygınlaştırıldığında çevreye duyarlılık konusunda önemli bir ilerleme kaydedilebilecektir.

Nesnelerin interneti lojistik alanında araçların güzergâhlarının takip edilmesi, soğuk zinciri uygulamalarının depolara sağlıklı ulaşıp ulaşmadığının kontrolü, limanlardaki yükleme-boşaltma işlemlerinin sağlıklı yapılabilmesi, malların depolama şartlarının ve alanlarının uygun belirlenmesinde yaygın olarak kullanılmaktadır (Gökrem ve Bozuklu, 2016). Böyle geniş bir uygulama alanının sadece endüstriye değil aynı zamanda genel toplumsal hayata da

etkisi olacaktır. Sistemin hayatı kolaylaştırma etkisinin yanı sıra yasal olarak izin verilmeyen malların taşınabilirliği de daha fazla kontrol altına alınabilecektir.

IoTs teknolojileri kullanan akıllı şehirlerin oluşturulması ve sürdürülebilirliğin gerçekleştirilmesini desteklerken bağlantılı araçların daha fazla bilinçlenme ve potansiyel olarak tehlikeli durumlardan kaçınmalarını sağlamaktadır. Bunun ifade ettiği anlam ise yeni bir güvenlik seviyesidir (Davis, 2017). Yani şehirler daha akıllı olma yolunda ilerlerken tehlikeli durumlar daha erken tespit edilebilecektir. Peki akıllı şehirler ne ifade etmektedir? Akıllı şehir onun kullandığı uygulamaların akıllı olmasıdır. Örnekler şöyle sıralanabilir: akıllı park sistemleri, köprü, bina ve tarihi yapılardaki titreşim ve malzeme koşullarının takip edilmesi, merkezi konumda yer alan yerlerin gürültü seviyelerinin tespiti ve bunun haritasının çıkartılması, mobil ağ sisteminde yayın yapan birimlerin elektromanyetik dalgalarının insan ve çevre sağlığına etkilerinin ölçülmesi. Ayrıca özellikle gelişmiş büyükşehirlerde yaşanan iş ve okul saatlerinde daha da artan trafik sorununa yönelik hava durumu ve sürücü hatalarından kaynaklanan trafikteki yığılmaları önlemek için insanlara yeni güzergâh tavsiyelerinde bulunan akıllı trafik uygulamaları da bulunmaktadır. Zaten hâlihazırda bu uygulamalar yoğun trafiğin yaşandığı yerlerde yaşayan insanların sık kullandığı uygulamalardır. Akıllı sistemlerin diğer kullanım alanı da akıllı sokak ve otoyol aydınlatmalarıdır. Bu aydınlatmalar kendini hava durumuna göre ayarlayabilmektedir ve sağladığı kolaylığın yanında tasarruf da yaptırabilecek bir kullanım alanıdır. Çevreye karşı sorumluluk çerçevesinde yer alabilecek bir uygulama alanı da çöp seviyelerinin belirlenmesini sağlayan atık yönetimi sistemidir (Gökrem ve Bozuklu, 2016). Çevreye karşı sorumluluk çerçevesinde yer alabilecek olan bu uygulama ile kimyasal da dâhil olmak üzere atıklar kontrol edilebilirken çöp seviyesinin belirlenmesi sayesinde sağlığı tehdit eden durumlardan da korunmuş olunacaktır.

IoTs uygulamaları enerji alanında şebekelerin kontrolüne imkan sağlaması yanında sayaçların uzaktan okunarak personel giderlerinin azaltılmasına da yardımcı olur (Keseyak). İşletme maliyetlerinin azalması da özellikle işletmeci açısından önem arz etmektedir. Diğer yandan maliyetin düşmesi tüketiciyi de olumlu yönden etkileyecektir. Bunun yanında hastaneler hastaların uzaktan takip edilmesi, atık yönetimi, binaların enerji verimliliğinin artırılması alanlarında yaygın bir uygulama imkanı bulmaya adaydır (Gökrem ve Bozuklu, 2016).

Nesnelerin interneti güvenlik alanında su toplama havzalarının kontrol edilmesi, su iletim hatlarındaki arızaların ve zararlı sızıntıların tespit edilmesi, nükleer enerji üretim

merkezlerindeki radyasyonun tehlikeli seviyelere ulaşmadan üretimin devamını sağlayacak ölçümlerin yapılması, maden ocaklarındaki gaz seviyesinin zamanında tespit edilerek (Gökrem ve Bozuklu, 2016), patlamalar yaşanmadan önlemlerin alınması konusunda sağladığı veriler kıymeti ölçülemeyecek faydalar sağlamaktadır.

Akıllı evlerde ısıtma ve soğutma sistemlerinin verimli çalışması ve uzaktan kontrol edilebilmesi nesnelerin interneti ile mümkün olabilmektedir. Yaygınlaşmamış olan ancak sıklıkla duyulmaya başlanan akıllı evler, kullanılan ev cihazlarının kontrolünü mümkün kılmaktadır. Ev sahibi evde değilken bile cihazlara erişim imkânı bulunmaktadır. Örneğin evine gitmeden önce ısıtıcı ayarlarını değiştirebilir hava durumuna göre evin daha yüksek sıcaklıkta bulunmasını isteyebilir veya evden çıktıktan sonra ütünün fişini çekip çekmediğini hatırlamıyorsa elektriği devre dışı bırakabilir. Bu ve bunun gibi örnekler nesnelerin interneti uygulamaları ile hayalin ötesine geçmekte ve günlük hayatta kullanım alanı bulmaktadır.

Hastaneler ise, birbirine bağlı sensör cihazlarının çoğalmasından yararlanmış bu da daha iyi sağlık sonuçları ve daha düşük maliyetlerle sonuçlanmıştır. Hastaneler ve genel olarak sağlık hizmetleri hesaplama işlemlerinden büyük ölçüde faydalanmaktadır. Hesaplama, elektronik tıbbi kayıtlar şeklinde daha doğru, daha bilinçli hasta bakımı sağlayabilecektir. Bunun yanında, hastanelerde hesaplamanın sağladığı yararların artmasıyla birlikte, sistem yazılımının kusurları varsa hastaya zarar verme potansiyeli olduğu uzun zamandır bilinmektedir (Fu ve ark., 2017).

Günümüzde havanın sıcaklık, nem, rüzgarın şiddeti ve yönü dikkate alınarak orman yangını riskleri, hava kirliliği nedenleri arasında yer alan zehirli gazlar, toz gibi zararlı unsurların seviyesinin belirlenmesi fay hatlarında ortaya çıkabilecek değişiklikler sonucunda deprem risklerinin analiz edilmesi giderek yaygınlaşan uygulama alanlarıdır (Gökrem ve Bozuklu, 2016). Örneğin Türkiye'de, Boğaziçi Üniversitesi Kandilli Rasathanesi ve Deprem Araştırma Enstitüsü'nün deprem derinlik ve büyüklükleri için herkesin internette ulaşabileceği bir sitesi bulunmaktadır. Ayrıca bu uygulama özellikle Japonya gibi tsunaminin yaşandığı bölgelerde erken önlem alınmasını sağlayabilmektedir. Çünkü depreme bağlı oluşan tsunami ihtimali sistem sayesinde ölçülebilmekte ve bir tehlike hali varsa halk önceden uyarılabilmektedir.

Hayvancılık alanında IoTs kullanım alanı hayvanların takibi ile sür kalitesi ve verimliliğin izlenmesi, yavruların bakım şartlarının sağlanması ya da havalandırmanın kaliteli olarak

sağlanması uygulamaları bulunmaktadır. Tarım alanında da nesnelerin internetinin katkısı olmaktadır (Gökrem ve Bozuklu, 2016). Topraksız tarım uygulamaları, yeni nesil sulama sistemleri, iklimde yağış sisteminde ortaya çıkabilecek ani değişiklikler için uyarıcı önlemler içeren uygulamalar vardır. Bu sistem çiftçilere büyük kolaylık sağlamaktadır. Günlük hava ve çevre kontrolü sayesinde gerekli önlemler alınabilmektedir. Değişen hava sıcaklığına göre çiftçinin telefonuna, tarlayı sulaması gerektiği veya don olayının yaşanabileceği dolayısıyla arazisini koruma altına alması gerektiği yönünde mesaj gelmektedir. Çiftçiler böylece kullandığı bu uygulama ile yaşanabilecek olumsuzlukları en aza indirgeyebilmektedir.

Eğitim alanında akıllı öğrenci kartlarının kullanılmasıyla öğrencinin okulda bulunup bulunmadığı, akıllı tahta uygulamalarıyla tarifi kısmen zor olan ifade ve şekiller tahtaya yansıtılabilmektedir. Öğrencilerin seviyesine uygun kendilerinin seçebileceği eğitim materyalleriyle pekiştirme çalışmalarının yapılabildiği, öğretirken eğlendiren eğitim ortamlarının oluşmasına imkan sağlamaktadır.

Son olarak kişisel egzersizlerin analizinde sporcuların performansları, grup içerisindeki sırlamaları, etkili olduğu konumlar, ne kadar koştukları, hangi hızda koştukları, topa hangi hızda vurdukları, vuruş açıları vb. bilgileri toplanarak performansı artırıcı çalışmalar planlanabilmektedir. Özellikle spor müsabakalarında önemli olan bu istatistikler, hem sporcunun kendi durumunu görmesini sağlarken izleyicilerin de istatistiklere bakarak yorum yapabilmesini sağlamaktadır.

Güvenlik Riskleri Nelerdir?

IoTs kesinlikle esneklik için büyük bir potansiyele sahip ve büyük bir gelecek vaat etmektedir. Ama aynı zamanda bir güvenlik felaketi potansiyeli de bulunmaktadır. Siber güvenlik alanında sorulması gereken zeki, üretici bir rakip ne yapabilir ve böyle bir rakibe karşı nasıl esneklik sağlayabiliriz? Tehditler iki türdür, bunlar dış güvenlik tehditleri ve iç güvenlik tehditleridir. Bir sistemin güvenlik açıkları, yetkisiz erişimden, içeriden yapılan yasadışı faaliyetlerden veya deprem, sel, fırtına, yıldırım gibi doğal afetlerden kaynaklanabilir. Dış güvenlik tehditleri hizmet reddi (DoS) saldırıları, uzaktan kaba kuvvet saldırıları olabilirken, iç güvenlik tehditleri ise şifre alışverişini yakalama, Truva atları, veri kurcalama eylemleri olabilmektedir (Abouzakhar ve diğ., 2017). Yani sistem sadece dışardan gelen tehditlere karşı açık değildir aynı zamanda iç tehditlere de maruz kalabilmektedir.

Birçok IoTs cihazı şu aşamada zayıf ya da hiç var olmayan güvenlik ve gizlilik politikalarına sahiptir. Bazı IoTs cihazları güvenlik yamalarını ve güncellemelerini otomatik olarak indirme konusunda yetersiz olabilmektedir (Harley, 2016). Nesnelerin kolay erişilebilir olmasından dolayı, kötü niyetli bilgisayar korsanları tarafından kolayca sömürülebilir (Farooq ve ark., 2015). Birbirine bağlı akıllı cihazların potansiyel faydaları yani her cihaza algılama ve zekâ yerleştirilmesinin yanı sıra, artan risk ve kötüye kullanım potansiyeli de artmaktadır. Aslında IoTs cihazının temel sorunlarından biri, güvenli ve güvenilir bir şekilde işletmek için gerekli olan karmaşıklığın artmasıdır. Artan karmaşıklık, bireylerin sadece tek bir cihazı güvenceye almasıyla karşılaştıkları zorlukların çok ötesinde yeni emniyet, güvenlik, gizlilik ve kullanılabilirlik zorlukları oluşmaktadır. Birbirine bağlı cihaz ağının yaygınlığı, bazı yeni güvenlik ve gizlilik tehditleri oluşturacak ve tüm cihazları, kişisel avantajları ve cihazların çalışması için güvenlik açıkları durdukça, yüksek bir bilgisayar korsanları riskine maruz bırakacaktır. Örneğin, tüketicilerin varsayılan şifreyi değiştirmemesi nedeniyle, birçok bebek monitörü webdeki yabancıların insanların evlerini görmesine izin vermektedir (Fu ve ark., 2017). Yani çok masumane bir şekilde insanların bebeklerini izlemek amacıyla yerleştirdiği kameralar güvenlik açığı sebebiyle suiistimal edilebilmekte ve kişiler kendi yerleştirdikleri kameralar ile izlenebilmektedir.

Akıllı cihazların çoğalması, yetenekleri ve birbirine bağlılığı, bu sistemleri güvenli, güvenilir, etkili ve kullanılabilir hale getirmek için yeni araştırma ve endüstri yaklaşımları gerektiren çarpıcı yeni fırsat ve zorlukları gündeme getirmektedir (Fu ve diğ., 2017). Avrupa Birliği'nin oluşturduğu ve 2018 başında uygulamaya konan MIFID II gibi yeni standartlar karşı karşıya olduğumuz siber risklerin boyutunu ortaya koymaktadır. Ayrıca Dünya Ekonomik Forumu'nun raporlarına yansıyan 2017'de başlayıp 2020'de hızlanan ve 2025 sonrası olgunlaşan bir yapay zekâ kullanımı öngörüsü dijital dönüşümde önemli bir basamak olma niteliği taşımaktadır (2018'de Artacak Siber Tehlikelere Karşı Hangi Konularda Önlem Alınmalı, 2018).

Açık bir pazar için dağıtılmış bir ortam ve sınırsız sistem etkileşimli zengin bir "büyük veri" kaynağı olarak IoTs, saldırganların savunmasız pek çok hedefi tespit etmelerine ve saldırılarını başlatmasına izin verecektir. Bulut tabanlı yapay zekâ uygulamaları sisteminiz için güvenliği zayıf arka kapılar anlamına gelebilir. IoTs sistemleri ve kullanıcıları bir dizi güvenlik tehdidine ve kötü niyetli etkinliklere karşı savunmasızdır. Asıl sorun, mevcut IoTs

mekanizmalarının ve protokollerinin bu tür zorluklarla başa çıkacak şekilde tasarlanmamış olmasıdır. En önemli risk kaynağı, çoklu IoTs protokolleri ve platformları arasında birlikte çalışabilirliktir. IoTs protokol yığında bulunan protokollerin çoğu, çoklu tehditlere karşı savunmasızdır. Savunmasız bir ağ olarak, GSM 2020'ye kadar kablosuz IoTs ağları için baskın teknoloji olmaya devam edecektir (Abouzakhar ve diğ., 2017).

Toplu olarak hangi bilgilerin toplandığını ve paylaşıldığını açıklamaya yönelik yeni mekanizmalar olmaksızın, uygulama kullanıcıları seçimlerinde gizlilikle ilgili tehditlerin ne olduğunu anlayamayacaklardır. Örneğin, akıllı bir çatal (gerçek bir cihaz) satın almayı düşünün. Tüketici, çatalın hangi bilgileri topladığını nasıl bilir (münferit-tek çatallı kaldırma saymanın ötesinde) ? Tüketici daha sonra akıllı bir tabak alırsa ne olur? Çatal ve tabak bilgi alışverişi yapabilir mi? Ve eğer öyleyse, veri kaynağından belirlenemeyen bilgilerin birleşiminden ne sonuç çıkarılabilir? Daha fazla akıllı cihazın veri topladığını, paylaştığını ve para kazandıracağı bir dünyada gizliliği anlamak ve garanti etmek zordur. Birçok ücretsiz akıllı telefon uygulaması hâlihazırda kullanıcının giderlerinden veri toplar ve bunu tüketiciye açık veya açık olmayan şekillerde satmaktadır. Facebook gibi tek bir uygulamanın gizlilik politikasının anlaşılmasının karmaşıklığı, bireysel kullanıcıları bunaltabilir ve kullanılan her cihaz ve uygulama için bu tür politikaları anlama yükü, çoğu insanın ötesinde dikkat ve karmaşıklık gerektirmektedir (Fu ve ark., 2017). Örneğin internette son zamanlarda yaptığınız aramalara uygun reklamlar gösteren Facebook bireysel kullanıcının lehine bir sonuç mu amaçlamaktadır? Yani internette kıyafet için gezinti yaptığınızda Facebook hesabınızda kıyafet reklamı görmek kişiye faydalı mıdır yoksa onu bunaltır mı? Bu ve bunun gibi konular kötü niyetli olmasa bile kişilerde izlenme hissi uyandırabilmektedir.

Web tabanlı Sağlık Hizmeti uygulamalarının ortaya çıkması, hastaların bilgilerinin güvenliği için bir dizi risk oluşturmuştur. Kötü amaçlı yazılımlar ve yasadışı operasyonlar, özellikle tıbbi kimlik hırsızlığı ve sağlık dolandırıcılığını hedefleyen Elektronik Hasta Sağlığı Bilgilerinin (EPHI) güvenliğine yönelik büyük bir tehdit oluşturmaktadır. Dahası, akıllı telefonlar gibi elde taşınan cihazların çoğalması, hastaların kablosuz iletişim ve sağlık personeli e-postalarının yakalanabileceği bir ortam oluşturmuştur (Abouzakhar ve diğ., 2017). Siber güvenlik araştırmacıları, sağlık sektörünün geniş çaplı siber saldırıların bir sonraki hedefi haline geleceğini tahmin etmektedir. Sağlık hizmeti gibi kritik ortamlarda, daha fazla sistem birbirine bağımlı ve çok yönlü hale gelmektedir. Bilginin yetkisiz kişiler tarafından erişilebileceği riski her zaman vardır. IoTs, bazı cihazların birbirine bağlı hale gelmesiyle bazı

önemli riskler sunmaktadır. Hastanenin güç altyapısına, su kaynağına karşı olan siber saldırılar da hasta bakımını önemli ölçüde etkileyecektir. Hastane sunucularının fidye amaçlı kapatıldığı, böylece sağlık hizmeti sunucularının kâğıt bazlı kayıtlara geri dönmesini gerektiren vakalar olmuştur. Fidye senaryosunda, hastanın elektronik reçetelerini veya dozaj kayıtlarını kasıtlı olarak tehlikeli ilaçlara veya ilaç seviyelerine göre değiştiren kötü amaçlı yazılımlar bulaşabilir (Fu ve diğ., 2017). Böyle durumlara karşı ne kadar tedbir alınabilir ya da yanlış dozda ilaç tedavisinin geri dönüşü mümkün müdür? Ameliyat anında cihazların etkisiz bırakılmasının ölümcül sonuçları hastane hizmetlerini nasıl etkileyecektir? Bu tür siber tehditlerin insan sağlığı ile direkt bağı bulunan hastanelerden uzak olması gerekmektedir. Çünkü sağlık bakım kayıtları açık kaldığında veya değiştirildiğinde yaşamı tehdit edebilir. Bir hasta, belirli bir yerde başka bir cihaza konuşan bir akıllı sensör taşıyorsa, bu iki cihaz arasındaki bağlantı, hastanın hareketinin izlenmesi gibi kabul edilemez amaçlarla da kullanılabilir (Abouzakhar ve diğ., 2017).

Fiziksel tesisler, saldırganların bilgisayar sistemini hem gözlemlemesine hem de manipüle etmesine izin veren yan kanallar sağlamaktadır (Wolf ve Serpanos, 2017). Hasta izleme sistemini barındıran bir sağlık hizmeti ağı bölümüne-segmentine yetkisiz erişim sağlayan kötü amaçlı bir yazılım, uzak bir saldırganın tıbbi cihazları kontrol etmesine izin verecektir. Bir tıbbi sistem ağı için tehlikeye sokulmuş bir IoTs sensörü insan yaşamının kaybına yol açabilir (Abouzakhar ve diğ., 2017). Buna 1980'lerden gelen hastaların almaları gereken radyasyon tedavisinin yaklaşık 100 katını almasına neden olabilecek bir yazılım kusuruna sahip olduğu saptanan bir radyasyon terapisi cihazı olan Therac-25 örnek olarak gösterilebilir (Fu ve diğ., 2017).

Çevrimiçi bulut hizmetlerinin kullanımındaki artış ve çeşitli endüstrilerdeki operasyonlar, güvenlik tehditlerinin ve zararlı faaliyetlerin sayısında artışa neden olmuştur. En önemli sorun, bu saldırıların sadece belirli bir veri tabanından ödün vermekle kalmayıp, aynı zamanda tüm bulut içerik yönetim sistemi içinde ve genelinde farklı dağıtılmış veri tabanı sistemleri üzerinde yıkıcı bir etkiye de yol açabileceğidir (Abouzakhar ve diğ., 2017).

Yazılım hataları-virüs, fiziksel tesisin çalışma hatalarına neden olabilmektedir. Bir tampon taşma problemi, Gezegensel Topluluğun uzay aracı ile teması geçici olarak kaybetmesine neden olmuştur. Bir Airbus A400M'nin yakıt sistemindeki yazılım sorunları, dört kişiyi öldüren bir çarpışmada yer almıştır (Wolf ve Serpanos, 2017). Temmuz 2015'te, iki güvenlik

araştırmacısı hücresel sistem üzerinden aracı yerleşik bilgi-eğlence sistemi aracılığıyla Jeep Chrysler'i 10 mil mesafeden ele geçirmiştir. Ağustos 2015, Amerikan Gıda ve İlaç Dairesi (FDA) bazı infüzyon pompalarının uzaktan korsanlığa karşı savunmasız olduğu konusunda uyarmıştır. Nisan 2015'te güvenlik araştırmacısı Chris Roberts, uçuş sırasında bir ticari uçağın uçuş kontrollerini ele geçirme konusunda tweet attıktan sonra FBI tarafından gözaltına alınmıştır. Roberts daha sonra United Airline tarafından uçaklarında uçmaktan men edilmiştir. 2013 yılı başında ise İranlı hackerlar, New York şehrinin 20 mil kuzeyindeki küçük bir su taşkın kontrolüne uzaktan erişmiştir (Davis, 2017).

Bağlı cihazların amaçlandığı şekilde gizlilikle ilgili etkilerinin anlaşılmasının ötesinde, güvenlik açıkları nedeniyle veri ihlallerinin gizlilik üzerindeki etkileri, yeterli gizlilik garantilerinin sağlanmasında karmaşıklığı ve riski artırmaktadır. Yüksek profilli bireylerin mahremiyetine saldıran kötü niyetli devlet destekli aktörlerin varlığı, bu tür sistemlere genel güven sağlamak için gereken koruma düzeyini büyük ölçüde artırmaktadır (Davis, 2017). Profesyonellerin veya tüketicilerin karmaşık sistemleri anlama ve yönetme kabiliyetlerinin emniyet, güvenlik ve gizlilik açısından önemli savunmasızlık oluşturduğu bilinmektedir. Sonuç olarak, sosyal mühendislik saldırıları ve bu sistemlerin yetersiz insan anlayışına dayanan saldırılar belki de üstesinden gelinmesi gereken en büyük zorluk olmaya devam etmektedir (Fu ve diğ., 2017).

Hangi Önlemler Alınabilir?

IoT'nin başlıca güvenlik hedefleri, kimlik doğrulama mekanizmalarını sağlamak ve veri hakkında gizlilik sağlamaktır. Veri gizliliği, bütünlüğü ve kullanılabilirliği olan üç alandan yararlanarak güvenliği uygulamaktadır. Bu alanlardan herhangi birinin ihlali, sistemde ciddi sorunlara yol açabilir. Veri gizliliği, kullanıcıya harici girişimden özgürlük sağlama ile aynıdır. Kullanıcıya, yetkisiz tarafa ifşa edilmesinin önlenmesi ve sadece izin verilen kullanıcılar tarafından erişilebilmesi için, farklı mekanizmalar kullanılmasıyla, hassas bilgilerin gizliliği konusunda kullanıcıya güven verilebilmesidir (Farooq ve diğ., 2015).

Akıllı cihaz ürünlerinin (hedeflenen Çevre Koruma Ajansı (EPA) emisyon gerekliliklerine benzer) gerekli analiz ve test seviyesinin belirlenmesi için kilometre taşları oluşturulmalıdır. Sistemi yapılandıran kişi yeterli şifreler sağlamazsa veya sistemin yanlış yapılandırıldığını anlarsa, hiçbir yazılım güvenlik düzeyi yeterli değildir. Zor kullanım problemlerinin doğrudan

tüketiciler tarafından ele alınması gerekmektedir. Güvenlik, gizlilik ve kullanılabilirlik sorunları birlikte düşünülmelidir. Cihazlarda varsayılan şifreler kullanılmamalıdır. Ve mümkün olduğunda, bir cihazın siber güvenlik açığı olduğu biliniyorsa o aygıta bir yazılım güncellemesi alınmalıdır (Fu ve ark., 2017). Kritik endüstriyel IoTs sistemleri, sürekli gelişen siber tehditlere karşı operasyonel çevreyi güvenli, güvenilir ve esnek tutmalıdır (Abouzakhar ve diğ., 2017).

Şirketler ürünlerinin ne kadar güvenilir olduğunu düşünseler de, çeşitli saldırılara karşı eğilimli oldukları için (Farooq ve ark., 2015) yazılımın yeni güvenlik açıkları bulunduğunda yamasına izin verecek şekilde dağıtılan aygıtlar için yazılım güncelleştirme gereksinimlerinin iyileştirilmesi, son teknoloji şifreleme kullanarak sömürüye dayanıklı mekanizmaların güncellenmesi, cihazları üreten şirket iflas ettiğinde kullanıcının, zaman içinde güvenli kalmasını sağlayacak şekilde yapılandırmayı anlamasını ve değiştirmesini sağlayan yönetim araçları geliştirilmelidir. Kullanıcıları güvenlik veya gizlilik hataları oluşturan yaygın hatalardan koruyan yapılandırma yönetiminin basitleştirilmesi amacıyla kullanıcıların bireysel cihazları yönetmede zaten aşina oldukları kavramlardan yararlanan bir kullanıcı deneyimi (Fu ve ark., 2017) gerekmektedir.

Birçok siber-fiziksel ve IoTs sistemleri, dış varlıklar tarafından sağlanan karmaşık alt sistemlere dayanan sistemlerdir. Her mühendisin dijital imzalar ve güvenin kökü gibi bilgisayar emniyeti kavramlarına aşina olması gerekmektedir. İnternete özellikli siber-fiziksel sistemlerin sağladığı tehditler, çalışma yöntemlerini önemli hale getirmektedir. Sistemin işlemek üzere tasarlanmadığı internetten yeni tehditler ortaya çıkabilmektedir (Wolf ve Serpanos, 2017). Saldırgan sadece verileri okumakla kalmaz, verileri değiştirilebilir hatta silebilir. Özetle IoTs gelişiminin önündeki en önemli engel güvenlik ve gizlilik sorunlarıdır (Farooq ve diğ., 2015). Bunun için siber güvenlik politikalarına dayalı eğitime ihtiyaç duyulmaktadır. Siber ilkeler, eğitim ekosisteminde daha erken kişi daha anaokulundayken öğretilmelidir (Davis, 2017). IoTs cihazını hangi özelliklerin akıllı hale getirdiğini ve mevcut IoTs'nin akıllı teknoloji olarak nitelendirilip nitelendirilmediğini kesin olarak belirtmek zordur. Güvenlik ve gizlilik, IoTs uygulamaları için temel konulardır ve hala bazı büyük zorluklarla karşı karşıyadır. Bilgi ve ağ güvenliği; kimlik doğrulama, gizlilik, bütünlük ve inkâr edilemezlik gibi özelliklerle donatılmalıdır. Ayrıca ses güvenliği yapısının oluşturulması gereklidir (Suoa ve diğ., 2012). Siber saldırıları önlemede büyük miktarda araştırma ve ticari yatırım yapılırken, cihaz koleksiyonlarının korunması, ele alınmamış yeni zorluklar ortaya

çıkarmaktadır (Fu ve ark., 2017). Tüketiciler **akıllı cihazlara yönelik güvenlik tehditlerini ve gizliliği koruyabilmek bu amaçla üretilen** güvenlik ürünleri kullanmayı tercih edebilirler. Güvenliğin vazgeçilmez olması uzun vadede tüketicinin istekleri doğrultusunda yüksek profilli güvenlik ürünleri geliştirilecektir (Harley, 2016).

Sonuç

Nesnelerin interneti mevcut internet altyapısını, etrafımızdaki tüm fiziksel nesnelerin birbirleriyle benzersiz bir şekilde tanımlanabildiği ve birbirleriyle her yerde bağlantılı olacağı çok daha gelişmiş bir bilgi işlem ağı kavramına dönüştüren büyük bir teknolojik devrimdir (Farooq ve ark. 2015). Son yıllarda hızla gelişmeye başlayan IoTs sistemi hayatımıza çok önemli değişiklikler getirmeye başlamıştır. Gün geçtikçe popülaritesi ve kullanım alanı artmaya başlayan teknolojik gelişmeler dijitalleşen dünyamızda inanılmaz bir hızla hayatımızı etkilemeye başlamıştır. Hayat kalitemizi büyük ölçüde değiştirme potansiyeline sahiptir (Dijitalleşen Dünyamızda, Nesnelerin Interneti (IoTs) ile neler değişecek, 2017).

Nesnelerin interneti faydalarının yanında ağa bağlanmak için kullandığımız cihazlar, cihazlar üzerinde de kontrolü sağlamak amacıyla başka cihazlar ile uygulamalar ve veri paylaşmak için diğer cihazlara bağlanılması bazı sorunlara da yol açacaktır. Saldırı yüzeyinin genişlemesi tehdit riskini artırmaktadır. Maalesef şu aşamada gizlilik, kullanılan cihaza ve kullanıcıya bağlıdır. Nesnelerin interneti, birlikte yaşadığımız bir dünyadır. Siz güvenliğinizi sağlamak için her adımı atmış olsanız bile gizliliğiniz aşılabilir, bu durum gizliliğimizde biraz ödün vermemiz anlamını taşımaktadır (Harley, 2016). Sosyal hayatımızın her aşamasında bilgilerimizi internet üzerinden paylaşıyor olmamız veri tabanının büyük boyutlara ulaşması işlemlerin karmaşık hale gelmesine, güvenliğin saldırılara daha açık hale gelmesine zemin hazırlamaktadır. Her geçen gün akıllı cihazlara bağımlı hale gelmemiz saldırganların motivasyonunu da artırmaktadır.

İnternet kullanıcılarının her geçen artması ve bazı kullanıcıların duyarlı davranmaması sistemde yeni güvenlik açıklarının ortaya çıkmasına yol açabilmektedir. Tanımlar arasındaki farklılıklara rağmen siber güvenlik bireylerin, kurumların ve hükümetlerin bilgi işlem hedeflerine güvenli, özel ve güvenilir bir şekilde ulaşmalarına olanak veren ortak etkinlikleri ve kaynakları ifade etmektedir. Amaç, siber alemdeki hayatın güvenliği ve gizliliğinin korunmasıdır. NATO Güvenlik Danışmanı Rex Hughes'e göre, "yakın gelecekte çıkabilecek

büyük bir savaşta ilk mermi internette atılacaktır" (Siber Güvenlik Nedir?, Haziran 2016). Bazı devletler tarafından finanse edilen terör örgütler, açıktan rakiplerine müdahale edemeyen devletler, değişik amaçlarla faaliyet sürdüren hacker grupları ağ ortamlarının açıklarından yararlanarak hedeflerine ulaştıracak saldırıları gerçekleştirmek için fırsat kollamaktadır. Saldırıların çok uzaklardan ışık hızıyla yapabiliyor olması ve kaynağının bulunmasının zorlukları bazı çevreleri cesaretlendirmektedir (Siber Güvenlik Nedir?, Ağustos 2016).

Mevcut bilişim teknolojileri güvenlik uygulamalarının gelecekteki IoTs güvenlik risklerini ele almak için yeterli olmayabilir. Kötü niyetli bir insan davranışı ile yüksek oranda otomatik bir gerçek zamanlı sistem arasındaki etkileşimin tüm etkilerini tahmin etmek imkânsız gibi görünmektedir (Abouzakhar ve diğ., 2017). Sanal ve gerçek dünya arasındaki sınır kişisel verilerin kötü amaçlarla kullanılmasının artmasına paralel olarak belirsizleşmektedir. Eylül 2015'te ABD'de FBI tarafından hazırlanıp yayınlanan "iot suç olanakları" adlı rapor belirsizliğin boyutlarını açıklamaktadır (Yüksel). Bu nedenle, kritik bulut sistemleri ve hizmetleri, sürekli gelişen bulut siber tehditlerine karşı operasyonel ortamı güvenli ve dayanıklı tutmalıdır (Abouzakhar ve diğ., 2017).

Uzun vadeli düşünüldüğünde sistemdeki belirsizlikler ve karşılaşılacak risklerin önceden görülememesi insan psikolojisi üzerinde ciddi travmalara yol açacaktır. Nesnelerin interneti uygulamasından toplumda hayat kalitesinin yükseltilmesi, zamanın verimli kullanılması, güvenlik risklerinin azaltılması amaçlanmışken tehlikelerden kaynaklanan risklere karşı insanların ruhsal ve bedensel açıdan nasıl karşılık vereceği bilinmemektedir (Yüksel). Yakın zamanda Nesnelerin interneti teknolojileri hayatımızın her evresinin vazgeçilmezi olacaktır (LG, 2017).

Teknolojide ortaya çıkan değişim mahremiyet kavramının dejenere olmasına, ahlaki değerlerimizin değişime uğramasına neden olmaktadır. Bütün değerlerimiz kamuya açık hale gelirken dijital dünyada bireysel etkinlikler ön plana çıkmakta, insanlar hızla yalnızlaşmaktadır. Örnek verilecek olursa aynı ev içerisindeki bireyler birlikte olduklarında bile bireysel dünyaları içerisinde vakit geçirmektedir (Yüksel). Bazen aynı ev içerisinde sohbetler bile telefon üzerinden mesajlaşma ile olabilmektedir.

Kaynakça

Abouzakhar, N.S.,Jones, A., Angelopoulou, O., 2017, Internet of Things Security: A Review of RisksandThreatsto Healthcare Sector, IEEE International Conference on Internet of Things, Exeter, UK.

Altınpulluk, H., 2018, Nesnelerin interneti teknolojisinin eğitim ortamlarında kullanımı, Açıköğretim Uygulamaları ve Araştırmaları Dergisi AUAd, Cilt 4, Sayı 1, 94-111.

Davis, J., 2017, TheLighter Side of Things: TheInevitableConvergence of the Internet of ThingsandCybersecurity, Information Technology ve CIO NASA AmesResearch Center GITEC.

Dijitalleşen Dünyamızda, Nesnelerin Interneti (IoT) ile neler değişecek?, 2017, http://www.pazarlamasyon.com/is-dunyasi/dijitallesen-dunyamizda-nesnelerin-interneti-iot-ile-neler-degisecek/, Erişim Tarihi: 10.04.2018.

Farooq, M.U.,Waseem, M., Khairi, A., Mazhar, S., 2015, International Journal of Computer Applications, Volume 111 - No. 7.

Fu K.,Kohno T., Lopresti D., Mynatt E., Nahrstedt K., Patel S., Richardson D., &Zorn B., (2017). Safety, Security, andPrivacyThreatsPosedbyAcceleratingTrends in the Internet of Things. http://cra.org/ccc/resources/ccc-led-whitepapers/.

Gökrem, L., Bozuklu, M., 2016, Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum, Gaziosmanpaşa Bilimsel Araştırma Dergisi, Sayı: 13, Sayfa:47-68.

Harley, D., 2016, Nesnelerin interneti hakkında her şey, http://www.hurriyet.com.tr/teknoloji/nesnelerin-interneti-hakkinda-her-sey-40053642, Erişim Tarihi: 10.04.2018.

Internet of Things (Nesnelerin İnterneti) Nedir?, 2018, http://www.teknolo.com/internet-things-nesnelerin-interneti-nedir/, Erişim Tarihi: 08.04.2018.

Keseyak, B., Nesnelerin İnterneti ve Endüstriyel Uygulamaları, http://www.endustri40.com/nesnelerin-interneti-ve-endustriyel-uygulamalari/, Erişim Tarihi: 08.04.2018.

LG Electronics Ortadoğu ve Afrika Bölgesi Başkanı KevinCha'dan Nesnelerin İnterneti Teknolojileri Üzerine, 2017, http://www.pazarlamasyon.com/is-dunyasi/lg-electronics-ortadogu-afrika-bolgesi-baskani-kevin-chadan-nesnelerin-interneti-teknolojileri-uzerine/, Erişim Tarihi: 11.04.2018.

Nesnelerin İnterneti ve Endüstriyel Uygulamaları, http://www.endustri40.com/nesnelerin-interneti-ve-endustriyel-uygulamalari/, Erişim Tarihi: 10.04.2018.

Nesnelerin İnterneti ve Kullanım Alanları Nedir?, 2017, https://www.voltimum.com.tr/haberler/nesnelerin-interneti-ve-kullanim, Erişim Tarihi: 10.04.2018.

Suoa, H.,Wana, J., Zoua, C., Liua, J., 2012,Security in the Internet of Things: A Review International Conference on Computer Science and Electronics Engineering, China.

Siber Güvenlik Nedir?, Haziran 2016, http://donencebilisim.com/siber-guvenlik-nedir.html, Erişim Tarihi: 11.04.2018.

Siber Güvenlik Nedir?, Ağustos 2016, http://sibertehdit.com/siber-guvenlik-nedir/, Erişim Tarihi: 11.04.2018.

Yetimler, E., Internet of Things (Nesnelerin İnterneti) Nedir? Cihazların Etkileşim Trendleri, https://www.karel.com.tr/blog/internet-things-nesnelerin-interneti-nedir-cihazlarin-etkilesim-trendleri, Erişim Tarihi: 10.04.2018.

Yüksel, Y.S.S., Nesnelerin İnterneti (İnternet of Things) ve Değerler, http://bs.org.tr/blog/nesnelerin-interneti-internet-of-things-ve-degerler/41, Erişim Tarihi: 10.04.2018.

Wolf, M.,Serpanos, D., 2017, Safetyand Security of Cyber–Physicaland Internet of ThingsSystems, IEEE, Vol. 105, No. 6.

2018'de Artacak Siber Tehlikelere Karşı Hangi Konularda Önlem Alınmalı?, 2018, http://www.pazarlamasyon.com/teknoloji/2018de-artacak-siber-tehlikelere-karsi-hangi-konularda-onlem-alinmali/, Erişim Tarihi: 09.04.2018.