

Endüstri 4.0 Altında IoT Özellikli Akıllı Uygulamalar

Mehmet Yasin ÖZSAĞLAM* 

*Necmettin Erbakan Üniversitesi, Uygulamalı Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü,
Konya, Türkiye,
myozsaglam@erbakan.edu.tr (Corresponding Author/Sorumlu Yazar)

Makale Bilgileri	ÖZ
Makale Geçmişi Geliş: 07.11.2021 Kabul: 08.12.2021 Yayın: 29.12.2021 Anahtar Kelimeler: Nesnelerin İnterneti, IoT, Endüstri 4.0, Akıllı Uygulamalar	<p>Tüm dünyada dijital dönüşüm yaşanmaktadır, insanlar iş ve günlük yaşantılarında interneti ve diğer dijital araçları yaygın olarak kullanmaktadır. Endüstri 4.0 kavramı altında artık internete bağlanıp veri alış verişi yapabilen akıllı cihazlar da yaygınlaşmaktadır, bu iletişim ağı Nesnelerin İnterneti (Internet of Things, kısaca IoT) olarak adlandırılmaktadır. IoT çevremizdeki tüm nesnelerin çevrimiçi olarak kontrolünün yanında onlardan gelecek olan verileri işlememize ve daha akıllı sistemler oluşturmamıza imkân sağlamaktadır. IoT, geleceğin teknolojilerinin en önemli alanlarından biri olarak kabul edilmektedir, birçok endüstri alanında büyük ilgi görmekte ve kullanılmaktadır. Üretim alanında çalışan makinelerden anlık veri alınması, bu verilerin işlenmesi ve yapay zekâ desteği ile kararların optimize edilmesi, cihazların kendi aralarında veri aktarması, her cihazın kendi verisini üretmesi ve personele iletmesi bu teknolojinin endüstriyel üretim alanındaki temel faydaları arasında bulunmaktadır. Bu araştırma makalesi, IoT teknolojisinin tanımları, oluşumları, temel gereksinimleri, özellikleri hakkında bilgi vermekte ayrıca IoT tabanlı ürün ve hizmetlerin dağıtımında gerekli olan teknolojileri ve müşteri değerini artırmak için kullanılan kurumsal uygulamalar için IoT kategorileri üzerine literatür taraması içermektedir.</p>

IoT-Enabled Smart Applications Under Industry 4.0

Article Info	ABSTRACT
Article History Received: 07.11.2021 Accepted: 08.12.2021 Published: 31.12.2021 Keywords: Internet of Things, IoT, Industry 4.0, Smart Applications	<p>Digital transformation is taking place all over the world, people widely use the internet and other digital tools in their business and daily lives. Under the concept of Industry 4.0, smart devices that can connect to the internet and exchange data are also becoming widespread, this communication network is called the Internet of Things (IoT for short). IoT enables us to control all the objects in our environment online, as well as to process the data coming from them and to create smarter systems. IoT is considered as one of the most important areas of future technologies, it attracts great attention and is used in many industries. Taking instant data from the machines working in the production area, processing this data and optimizing the decisions with the support of artificial intelligence, transferring data between the devices, producing its own data for each device and transmitting it to the personnel are among the main benefits of this technology in the field of industrial production. This research article provides information about the definitions, formations, basic requirements, features of IoT technology, and also includes a literature review on technologies required in the delivery of IoT-based products and services, and IoT categories for enterprise applications used to increase customer value.</p>

Atf/Citation: Özsağlam M. Y. (2021). Endüstri 4.0 altında IoT özellikli akıllı uygulamalar, *Five Zero*, 1(1), 34-45.



"This article is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/). (CC BY-NC 4.0)"

GİRİŞ

Nesnelerin İnterneti (IoT), birbiriyle etkileşime girebilen küresel bir cihaz, sensör ve makine ağı olarak tasarlanan yeni bir teknoloji paradigması olarak kabul edilmektedir. IoT, geleceğin teknolojisi olarak görülüyor ve birçok endüstri alanı tarafından ilgiyle takip ediliyor. İşletmeler, üretim bandında cihazların birbiri ile haberleşmesi, pazarlama alanındaki envanter yönetimi, müşteri destek sistemleri, iş yönetimi ve analitiği gibi bir çok konuda hızlı ve kesin çözümler sunacak olan bu teknolojiye yatırım yapmaktadırlar. IoT teknolojisi kullanan cihaz sayısı 2009'da 900milyon iken 2021 yılı itibarı ile bu rakam 21 milyarı geçmiştir(Gardner, 2014)(Jianxin et. al., 2021). Bu hızlı dönüşüm, üretim hattı ve depolamadan tedarik zincirinde perakende teslimat ve mağaza raflarına kadar, malzeme ve ürün akışına daha doğru ve gerçek zamanlı görünürlük sağlamaktadır. Firmalar, fabrika iş akışlarını yeniden tasarlamak, kaynak yönetimi, malzeme takibini iyileştirmek ve dağıtım maliyetlerini optimize etmek için IoT'ye yatırım yapmaktadır (Butler, 2006).

Üreticilerin IoT'yi benimsemesine ek olarak, çeşitli hizmet sektörlerinde de pazar payının artırılmasına yönelik çalışmalar yapılmaktadır, bu çalışmalar genellikle, ziyaretçilerle ilgili veri deposuna bağlanan radyo frekansı ile tanımlama yapan (RFID) çipli cihazlar, video analitiği yapan cihazlar, kablosuz cihazlar, POS cihazları, el tipi sensörler, IP kameralar ve video yönetim yazılımlarını içeren platformlardan oluşmaktadır. Teknolojik, toplumsal ve rekabetçi baskılar firmaları yenilik yapmaya ve kendilerini dönüştürmeye ittiğinden, bu teknolojinin benimsenmesi hızla ivme kazanmaktadır. IoT teknolojisi ilerledikçe ve artan sayıda firma teknolojiyi benimsedikçe, IoT maliyet-fayda analizi büyük ilgi görecektir (Feng ve ark., 2018). IoT'nin potansiyel ancak belirsiz faydaları ve yüksek yatırım maliyetleri nedeniyle, firmaların kaynaklarının en iyi şekilde harcandığından emin olmak için IoT teknolojisine geçişten kaynaklanan her fırsatı ve zorluğu dikkatlice değerlendirmeleri gerekmektedir. Bu makale, bu teknolojinin altyapısını, dönüşümünü ve son olarak teknik ve yönetsel zorluklarını ele almaktadır.

IoT TEKNOLOJİSİNİN BİLEŞENLERİ

IoT teknolojisi radyo sinyalleri ile yakın alan iletişim kurabilen RFID ağlarından esinlenerek geliştirilmiştir. İletişimi sağlayan radyo sinyalleri ve diğer kablosuz iletişim yöntemlerinin yanı sıra, sensör teknolojisi, nano teknoloji ve gömülü entegre sistemlerde bu teknolojinin temelini oluşturmaktadır. Nesnelerin internete bağlanması ile fiziksel nesnelere siber dünya alanına girmesi ve veri aktarımını sağlamaktadır. IoT teknolojisi ile internete bağlanan her cihazın tanımlanması için tekil IP adresine ihtiyaç duyulmaktadır. Bağlı cihaz sayısının hızla artacağı önümüzdeki dönemler için yeni adresleme yöntemleri de geliştirilmektedir. Sensör ağları ve tanımlama için kullanılan barkod teknolojileri de IoT ile paralel olarak gelişmektedir. Bu bölümde IoT teknolojisini işler hale getiren teknolojilerden bahsedilecektir.

İnternet Protokolü (IP)

İnternet Protokolü (IP), 1970'lerde geliştirilen internette kullanılan birincil ağ protokolüdür. İnternet ağına bağlanan her bilgisayarın tekil adreslenmesi ve veri iletişiminin ana protokollerinden biridir. Günümüzde İnternet Protokolünün (IP) IPv4 ve IPv6 olmak üzere iki sürümü kullanılmaktadır. Her sürüm farklı bir IP adresi tanımlamaktadır. Yaygınlığı nedeniyle, genel IP adresi terimi tipik olarak hala IPv4 tarafından tanımlanan adresleri ifade etmektedir. IPv4'te beş kullanılabilir IP aralığı sınıfı vardır: A Sınıfı, B Sınıfı, C Sınıfı, D Sınıfı ve E Sınıfı, yalnızca A, B ve C yaygın olarak kullanılmaktadır. Gerçek bağlantı sayısı olarak protokol 4,3 milyar IPv4 adresi sağlarken, IPv6 kullanılabilirliği 85.000 trilyon cihazı adresleyebilecektir.

Radyo Frekansı Tanımlama (RFID)

Radyo Frekansı Tanımlama (RFID), bir nesne veya kişinin kimliğini radyo dalgalarını kullanarak kablosuz olarak seri numarası şeklinde ileten bir sistemdir. RFID cihazının ilk kullanımı 2. dünya savaşında dost ve düşman uçaklarının tanımlanmasında kullanılmıştır. Bu teknoloji zamanla uygun maliyetli tanımlama ve iletişim için kullanılmaya başlamıştır (Abuelkhail ve ark., 2020). RFID'nin ana bileşenleri etiket, okuyucu, anten, erişim denetleyicisi, yazılım ve sunucudur. Daha güvenilir, verimli, güvenli, ucuz ve doğrudur. RFID, dağıtım, izleme, hasta izleme, askeri uygulamalar vb. gibi geniş bir kablosuz uygulama yelpazesine sahiptir.

Barkod

Barkod, farklı genişlikteki çubuklar ve boşlukların kombinasyonu kullanarak sayıları ve harfleri kodlamanın farklı bir yoludur. Günümüzde özelleştirilmiştir bir çok barkod çeşidi mevcuttur. Üretim, tedarik ve pazarlama bandında hızlı, güvenli ve uygun maliyetli bir çözüm sunmaktadır. Genellikle kare matris şeklinde tasarlanan (QR) kodlar daha fazla bilgi saklayabildiği için son yıllarda yaygınlaşmıştır. Genellikle lazer tarayıcılar tarafından okunurlar, kameralar kullanılarak da okunabilmektedirler.

Kablosuz İletişim Yöntemleri

Kablosuz Bağlantı Alanı (Wireless Fidelity, kısaca Wi-Fi), bilgisayarların ve diğer cihazların kablosuz sinyal üzerinden iletişim kurmasını sağlayan bir ağ teknolojisidir. Bugün, milyonlarca ofis, ev ve oteller, kafeler ve havaalanları gibi halka açık yerlere yüksek hızlı Kablosuz Yerel Alan Ağı (WLAN) bağlantısı sağlayan milyonlarca Wi-Fi ağı bulunmaktadır. Wi-Fi kişisel bilgisayarlar, dizüstü bilgisayarlar, cep telefonları, tüketici elektroniği gibi birçok son kullanıcı cihazının internete bağlanmasını sağlamaktadır. Bu teknoloji IoT kullanan cihazların internet ağına bağlanması içinde yaygın bir teknolojidir.

Bluetooth kablosuz teknolojisi, dizüstü bilgisayarlar, el bilgisayarları, kameralar ve yazıcılar gibi cihazlar arasında kablolama ihtiyacını ortadan kaldıran ve 10 - 100 metrelik etkili menzili olan ucuz, kısa menzilli bir radyo teknolojisidir. Bluetooth versiyonları genellikle 1-5 mbs hıza ulaşabilmektedir ve Kişisel Alan Ağları (PAN) oluşturmak için kullanılır. İletişim için ortak bir kanalı paylaşan bir dizi Bluetooth aygıtına Piconet adı verilir. Bu Piconet, veri paylaşımı için aynı anda 2 - 8 cihaz kapasitesine sahiptir ve bu veriler metin, resim, video ve ses olabilir. Özellikle üretim alanında kullanılan cihazların birbirine bağlanmasında uygun fiyatlı bir çözüm sunmaktadır.

Yakın Alan İletişimi (NFC), 13,56 MHz'de tipik olarak 4 cm mesafe gerektiren bir dizi kısa menzilli kablosuz iletişim teknolojisidir. NFC teknolojisi, işlem yapmayı, dijital içerik alışverişini ve elektronik cihazları bir dokunuşla bağlamayı kolaylaştırmaktadır. Akıllı telefonlar ile son kullanıcıya da ulaşan bir teknolojidir. Kablosuz iletişimin otomatik olarak başlamasına izin vermektedir, yaklaşık menzili 10 santimetredir. Görüş olanı gerektirmez, iletişimi engelleyen gürültüden etkilenmez. Son derece güvenli, basit ve düşük maliyetli bir iletişim yöntemidir. Veri değişim oranı günümüzde yaklaşık 424 kbps'dir. NFC'de veri okuma sırasında güç tüketimi 15mA'nın altındadır. Bu durum güç kaynağına ulaşma da sıkıntı çekilen bir çok yerde küçük bataryalar ile uzun süre iletişimin sağlanmasına yardımcı olmaktadır (Zhang ve ark., 2014).

ZigBee, kablosuz sensör ağlarının özelliklerini tanımlamak için geliştirilmiş protokollerden biridir. ZigBee'nin özellikleri düşük maliyetli, düşük veri hızı, nispeten kısa iletim aralığı, ölçeklenebilirlik, güvenilirlik, esnek protokol tasarımıdır. ZigBee yaklaşık 100 metre menzile ve 250 kbps bant genişliğine sahiptir ve çalıştığı topolojiler yıldız, küme ağacı ve ağdır. Ev otomasyonu, dijital tarım, endüstriyel kontroller, tıbbi izleme ve güç sistemlerinde yaygın olarak kullanılmaktadır (Chanak

& Banerjee, 2020).

Kablosuz Sensör Ağları (WSN)

Kablosuz Sensör Ağları (Wireless Sensor Network, kısaca WSN), sıcaklık, ses, titreşim, basınç, hareket veya kirleticiler gibi fiziksel veya çevresel koşulları farklı konumlarda işbirliği içinde izlemek için sensörler kullanan, mekansal olarak dağıtılmış özerk cihazlardan oluşan bir kablosuz ağıdır. Birbiriyle iletişim kuran ve birinden diğerine veri aktaran yüzlerce veya binlerce cihazdan oluşur. Bir kablosuz sensör ağı, IoT teknolojisinin temel unsurlarından biridir. Sensör düğümleri, büyük miktarda ek yük ve çok sayıda sensör nedeniyle global ID'ye sahip olmayabilir. IoT'ye dayalı WSN, askeri, iç güvenlik, sağlık, hassas tarım izleme, üretim, habitat izleme, orman yangını ve sel tespiti gibi birçok alanda dikkat çekmektedir. Sağlık alanında hastanın vücuduna yerleştirilen sensörler ilaca verilen tepkileri izliyor, böylece doktorlar ilaçların etkilerini daha ayrıntılı ölçebiliyorlar.

Sürücü Yazılımları, Motorlar ve Diğer Mekanik Cihazlar

Elektrik motorları, enerjiyi harekete dönüştüren ve üretim bandında sıklıkla kullanılan cihazlardır. Elektrik motorlarının yanı sıra hidrolik, pnömatik sistemlerde sıklıkla kullanılan araçlardır. Elektrik motorları ac ve dc motorlar, kademeli motorlar, solenoidlerden oluşmaktadır. Hidrolik sistemler hareketi sağlamak için hidrolik sıvı kullanırlar. Pnömatik sistemler hareketi sağlamak için basınçlı hava kullanır. Bunlar arasında elektrikli motorlar en yaygın kullanılan tiptir. Hidrolik ve pnömatik sistemler, daha küçük motordan daha fazla kuvvet ve tork elde edilmesini sağlar. Üretimin aksamaması için bu motorların ve sistemlerinde senkronize çalışması gerekmektedir. IoT bu tür hareket sağlayan sistemleri kontrol etmek içinde ideal bir teknolojidir. Genellikle 10-50 metreye kadar, 1 mbps hızla iletişimi gerçekleştirecek kapasitede kablosuz ağlar ile veri akışı sağlanmaktadır.

Sürücü yazılımları, sistem ile cihazlar arasında iletişim ve giriş/çıkış gerçekleştirmesini sağlayan ara yazılımlardır. Bu yazılımlar farklı sistemleri kapsayacak şekilde mimari özelliklere sahiptir. Bu şekilde yazılım geliştiriciler program arayüzlerini geliştirip dağıtmaktadırlar.

Bulut Bilişim

Bulut bilişim son yıllarda hızla yaygınlaşan bir teknolojidir. Bu teknolojinin temel amacı yetkili kullanıcıların, veri depolaması, uygulamaları çalıştırması, sunucu hizmetlerinden yararlanması ve veri ağının kurulmasıdır. Birçok IoT uygulaması, büyük veri depolamasının yanında gerçek zamanlı karar vermeyi sağlamak için büyük işlem hızı, ses veya video akışı için yüksek hızlı geniş bant ağları gerektirir(Bazzaz ve ark., 2020). Bulut bilişim, devasa veri akışlarını yönetmek ve bunları benzeri görülmemiş sayıda IoT cihazı kontrol etmek için ideal bir arka uç çözümü sağlar.

IoT Platformları

Üretim ve hizmet alanında kurumların IoT cihazlarını kurmaları ve yönetmeleri oldukça maliyetli olabilmektedir. Mimarinin kurulması ve yönetilmesi ek sunucu bilgisayar ve personel giderlerine yol açmaktadır. Bu maliyetlerin düşürülmesi için birçok büyük bilişim firması uygun maliyetli, açık kaynak kodlara sahip ve genişletilebilir hizmetler sunmaktadır. Tablo 1, çeşitli firmaların 2021 yılı itibari ile sunduğu servisler ve ücretler hakkında bilgi içermektedir.

Tablo 1. *IoT Platformları servis ve ücret bilgileri (2021)*

IoT Platformu	Servisler	Cihaz Yönetimi	Ücret
Google IoT	Belgeleri düzenleme, yönetme ve paylaşma. Akıllı şehirler ve binalar için çözümler ve gerçek zamanlı takibi.	Evet	1758\$ (aylık başlangıç ücreti)
OpenRemote	Tamamen açık kaynak kodlu uygulamalar, akıllı enerji ve akıllı bina kontrolü	Evet	Ücretsiz
IRI Voracity	Uçtan uca çalışma, veri toplama ve analiz hizmetler	Hayır	Yıllık veya kalıcı değişken fiyatlar Wi-Fi: \$25 cihaz başına
Particle	Donanım, Bağlantı, Cihaz Bulutu ve Uygulamalar.	Evet	hücresel: \$49 cihaz başına Ağ: \$15 cihaz başına
ThingVortex	Uçtan uca endüstriyel IoT Platformu	Evet	Yıllık veya kalıcı değişken fiyatlar
IBM Watson IoT	Bağlantı Hizmeti, Analitik Hizmeti, Blockchain Hizmeti.	Evet	500\$ uygulama başına aylık fiyat

Yapay Zekâ

Yapay Zekâ, bir üretim alanında binlerce cihazın oluşturacağı ağdan gelecek verinin işlenmesi, kararların alınması ve uygulanması açısından önemli bir teknolojidir. İnsan faktörünün oluşturabileceği negatif etkileri en aza indirmekte, zamandan ve maliyetten kazanç sağlamaktadır (Rathore & Park, 2018). IoT teknolojileri ile yapay zekâ yan yana kullanılan iki terimdir.

ENDÜSTRİYEL ÜRETİMDE IoT

IoT teknolojileri endüstriyel üretimde üç ana başlık altında sınıflandırılabilir: izleme ve kontrol, büyük veri ve iş analitiği ve bilgi paylaşımı ve işbirliği. Bir kuruluşun ürettiği değerlerin kalitesini artırmak ve müşteri memnuniyetini sağlamak için bu üç IoT kategorisini benimsemesi gerekmektedir

İzleme ve Kontrol

Son kullanıcı için akıllı ev teknolojileri IoT teknolojisinin izleme ve kontrol amacının güzel bir örneğidir. İzleme ve kontrol, evin uzaktan akıllı sistemler ile korunması, bilgi amacı ile evin sıcaklık, nem gibi verilerinin kullanıcıya anlık gönderilmesi, ev içindeki cihazların uzaktan kontrolü olarak kabul edilebilir. Endüstriyel üretimde ise donanım performansı, enerji kullanımı ve çevre koşulları hakkında verilerin toplanması ve gerçek zamanlı izlenmesi IoT tarafından sağlanmaktadır (Gigli & Koo, 2011). Akıllı şebeke ve akıllı ölçüm gibi gelişmiş izleme ve kontrol teknolojileri, operasyonel modelleri ortaya çıkarır, potansiyel iyileştirme alanlarını tespit eder veya gelecekteki sonuçları

Büyük Veri ve Analizler

Gömülü sensörlere ve motorlara sahip IoT cihazları ve makineleri, muazzam miktarda veri üretir. Bu veriler karar destek sistemleri için büyük öneme sahiptir, analiz edilen veriler yöneticilerin karar almasında büyük öneme sahiptir. Ayrıca bu veriler, müşteri memnuniyetini artırmak ve müşterilere katma değerli hizmetler sunmak için müşteri davranışlarındaki ve pazar koşullarındaki değişiklikler gibi iş sorunlarını keşfetmek ve çözmek için kullanılmaktadır (Zawoad & Hasan, 2015).

IoT ve iş analitiğindeki ilerlemeler artık çok büyük miktarlarda bireysel sağlık verilerinin

yakalanmasını mümkün kılmaktadır. IoT, sağlık hizmeti veren kurumların, hasta bakımını kişiselleştirmesini sağlamaktadır. Bir hastanın günlük davranışları ve sağlığı hakkında veri sağlayarak, bakım hizmetinde çalışanların, hastaları çok daha sık ve etkili bir şekilde kontrol etmesi için fırsatlar yaratmaktadır. Sağlık sektöründe veri aktarımı sağlayacak olan sensörler giyilebilir donanımla hastalardan veri toplayabilir. Bu verilerde yeni tedavi yöntemlerinin gelişmesine, dolayısı ile yaşam kalitesinin artmasına olanak sağlayacaktır.

Bilgi Paylaşımı ve İşbirliği

IoT'de bilgi paylaşımı ve işbirliği, insanlar arasında, insanlar ve nesnelere arasında ve nesnelere arasında gerçekleşebilir. Önceden tanımlanmış bir olayı algılamak genellikle bilgi paylaşımı ve işbirliği için ilk adımdır. Tedarik zinciri alanında, bilgi paylaşımı ve işbirliği durumsal farkındalığı artırır ve bilgi gecikmesi ve çarpıklığını önler (Stallings, 2015). Örneğin, soğutmanın gerekli olduğu bir perakende mağazasına sensörler yerleştirilirse, buzdolapları arızalandığında mağaza yöneticisinin mobil cihazına uyarılar gönderilebilir. Yönetici daha sonra kimin müsait olduğunu görmek için çalışan durum raporunu kontrol edebilir ve IoT özellikli mobil cihazı aracılığıyla bu çalışana görev atamaları gönderebilir.

IoT MİMARİSİ

Temel olarak IoT cihazların internete bağlanarak veri paylaşımını, bu verilerin depolanmasını, analiz edilmesini ve kontrol edilmesini hedeflemektedir. Bu bağlamda IoT teknolojisi oluşturulurken dört temel katmana sahiptir, bunlar; Fiziksel Katman, Ağ Katmanı, Bulut Katmanı ve son olarak Uygulama Katmanıdır (Kosmatos ve ark., 2011).

Fiziksel Katman

Mimarinin en altında bulunan fiziksel katman cihazları, sensörleri, elektrik motorlarını, hidrolik ve pnömatik tüm hareket üreten sistemleri kapsamaktadır. Bu cihazların kendi sürücü yazılımları, ara kontrol yazılımlar ve hatta küçük işletim sistemleri bulunabilir, bu cihazların otomasyonu için kullanılan tüm yazılımlarda fiziksel katmanda kabul edilmektedir (Joshi and Pilli, 2016). Aynı şekilde cihazların barındırdığı entegre devreler ve gömülü yazılımlarda bu katmanda yer almaktadır.

Ağ Katmanı

Bu katmanın amacı fiziksel katmanda bulunan cihazların çevrimiçi ağa ya da internete bağlanmasını sağlamaktır. Switch, gateway gibi tüm ağ geçidi cihazları bu katmanda yer almaktadır. Aynı şekilde Http ve IP protokolleri de bu katmanda yer almaktadır (Lianos & Douglas, 2000). Bu katmanda ağ hızı ve kararlılığı önem kazanmaktadır.

Bulut Katmanı

Fiziksel katmanda bulunan her cihaz çok büyük veri üretmektedir. Bu verilerin işletmelerin kendi çabaları ile sunucu bilgisayarlarda depolanması ve yönetilmesi maliyeti artırmaktadır (Stoyanov, 2014). Verilerin güvenli ve uygun maliyet ile depolanması ve yönetilmesi bulut sistemler ile gerçekleştirilmektedir.

Uygulama Katmanı

Mimarinin en üstünde bulunan katman uygulama katmanıdır. Bu katmanda sistem yöneticilerinin veya son kullanıcıların kullandığı bilgisayarlar, tabletler veya benzer cihazlar ile yazılımlar bulunmaktadır. Sistemin izlenmesi ve yönetilmesi için yapılan tüm hazırlıklar bu katmanda işlenmektedir, aynı şekilde karar alma süreçleri bu katmanda gerçekleştirilmektedir (Narasimha & Solomon, 2020).

IOT TEKNOLOJİSİNİN KULLANIMINDA KARŞILAŞILAN ZORLUKLAR

Her dönüşüm beraberinde yeni problemlerin doğmasına yol açmaktadır. IoT teknolojisi de beraberinde işletmeler için çeşitli zorluklar getirmektedir. Üretilen verinin güvenliği, işletme ve tüketici gizliliği, verilerin depolanması ve yönetimi, sunucu teknolojileri ve veri merkezi ağ iletişimi konularında zorluklarla çeşitli zorluklarla karşılaşacaktır. Bu bölümde işletmelerin karşılayacağı temel sorunlar ele alınacaktır.

Veri Yönetimi Zorluğu

IoT sensörleri ve cihazları, işlenmesi ve depolanması gereken çok büyük miktarda veri üretiyor. Veri merkezinin mevcut mimarisi, kişisel ve kurumsal verilerin heterojen doğası ve büyük hacmi ile başa çıkmaya hazır değildir (Gartner, 2014). Çok az kuruluş, ağlarından toplanan tüm IoT verilerini barındırmak için yeterli veri depolamaya yatırım yapabilir. Sonuç olarak, ihtiyaçlara ve değere göre operasyonlar veya yedekleme için verilere öncelik vereceklerdir. IoT cihazları daha yaygın olarak kullanıldıkça ve daha fazla bant genişliği tükettikçe, veri merkezleri işleme verimliliğini ve yanıt süresini iyileştirmek için daha fazla kaynak ayırmak zorunda kalacaktır. Bilişim sektöründeki gelişmeler, bulut depolama ve bulut bilişim maliyetlerini azaltmaktadır (Haghi ve ark., 2020). Veri yönetiminin zorluğu bulut sistemlerin yaygınlaşması ile aşılabilecektir fakat buradaki en büyük handikap ise IoT kullanan cihaz sayısının katlanarak artması olacaktır.

Veri Madenciliği Zorluğu

IoT altyapısı ile üretilen büyük verinin işlenmesi için ayrık analiz yöntemleri yetersiz kalacaktır bu sebeple veri madenciliği araçlarının kullanımı bir zorunluluk haline gelmektedir. Verilen analiz edilmesinde yapay zeka ve makine öğrenmesinden yararlanılması gerekmektedir. Depolanan veriler birçok kanaldan gelmektedir ve ilişkisel olarak çok farklı veri türlerini ihtiva etmektedir. Veriler endüstriyel ekipmanlar, otomobiller, elektrik sayaçları ve nakliye kasalarındaki dijital sensörlerden vb. çok farklı veri türünü içermektedir. Ayrıca anlık elde edilen akış verileri de mevcuttur bunlar konum, hareket, titreşim, sıcaklık, nem ve hatta havadaki kimyasal değişikliklerle ilgili çok farklı türlerde olabilmektedir (He & Zeadally, 2015). Veri madenciliği akış içindeki verilerin hızla işlenip işletmelerin gerekli kararları zamanında alabilmeleri için olanak sağlamaktadır.

Verilerin bilgisayar ve matematiksel modeller kullanılarak anlaşılabilir hale getirilmesi gerekmektedir. Dijitalleştirilmiş veriler sadece sayısal verilerden ibaret olmayabilir. Görüntü ve video kaydı alan cihazlardan gelen verilerin işlenmesi için ise görüntü işleme, makine öğrenmesi ve yapay zeka yöntemlerinin kullanılması gerekmektedir. Oluşan verilerin işlenmesi için gerekli insan gücünü oluşturmak için veri analistliği ve veri mühendisliği gibi çeşitli iş kolları oluşmuş bulunmaktadır. McKinsey Global Institute, Amerika Birleşik Devletleri'nin büyük veri analizine dayalı iş kararları vermek için analitik becerilere sahip 140.000 ila 190.000 daha fazla işçiye ve analitik becerilere sahip 1.5 milyon yönetici ve analist ihtiyacı olduğunu tahmin ediyor (Manyika ve ark., 2011).

Güvenlik ve Gizlilik Sorunu

IoT, şirketlerin üretkenliğini ve insanların yaşam kalitesini artırsa da, bilgisayar korsanları ve diğer siber suçlular için potansiyel saldırılarını da artıracaktır. İnternete bağlanan cihaz sayısı arttıkça bu cihazların saldırılara maruz kalma ihtimali de artacaktır. Bu saldırılar sistemlerin işlevsiz kalmasına yol açabileceği gibi verilerin çalınmasına ve sızdırılmasına sebep olabilecektir (Cutillo & Manulis., 2010). Bu işletmeler endüstri alanında işletmelerin büyük zarar etmelerine sebep olabilir, son kullanıcı tarafında ise kişisel verilerin çalınmasına sebep

olabilmektedir.

Güvenlik, askeri amaçlı uygulamalar ve sağlık sektöründe kullanılan IoT sistemlerinin saldırılar sonucu işlevsiz kalması çok daha büyük tehlikelerin doğmasına sebep olacaktır (Ammar ve ark., 2018). İşletmelerin bu tür saldırılara karşı önlem alması, firewall benzeri ekstra güvenlik yazılımlarının kullanımı veya sunucu bilgisayarların korunması sağlayacak ek uygulamalar maliyetleri artıracaktır (Elmisery ve ark., 2010). Cihaz sayısındaki hızlı artış, güvenlik testlerin yanlış yapılması, üçüncü parti üreticilerin maliyeti düşük cihazları bu güvenlik riskini artıran en büyük özelliklerdendir.

Kaos Sorunu

İot gelecekte birbirine bağlanmış milyonlarca cihazdan oluşan büyük bir ağ oluşturacak. Üretimden, savunmaya, sağlıktan, son kullanıcıya kadar bir çok alanda insanlığın işlerini kolaylaştıracak. Bağlantısız bir dünyada küçük bir hata veya yanlışlık bir sistemi çökertmez fakat bir çok sistemin birbirine bağlandığı bir sistemde bir parçadaki hata, baştan sona düzensizliğe neden olabilir. Akıllı ev uygulamaları, tıbbi izleme ve kontrol sistemleri, güvenlik kontrol sistemleri gibi kritik öneme sahip sistemlerde birbirine bağlı sensörler, iletişim cihazları ve kontrolörlerde gelebilecek arıza ve hatalar can kayıplarına yol açabilir (Adjei ve ark., 2018). Aynı şekilde gerek üretim bandında, gerekse son kullanıcıya hitap eden sistemlerdeki, termostatlar ve ev tipi elektrik sayaçları gibi akıllı ev kitlerinin bozulduğunu veya bilgisayar korsanları tarafından saldırıya uğrayabilir veya beklenmedik güvenlik sorunlarına sebep olabilir. Gelecekte IoT cihazlarının internet bant genişliğinin büyük bir kısmını kullanacağı kesin, internet bağlantısında yaşanacak olası kesintiler zincirleme olarak sistemin çökmesine sebep olabilir. Bu durum tek bir cihaz için önemsiz bir sorundur, ancak bir bütün olarak sistem için felakete yol açabilir. IoT dünyasında kaosu önlemek için işletmelerin bağlı sistemlerin karmaşıklığını azaltmak, uygulamaların güvenliğini ve standardizasyonunu geliştirmek ve her zaman, her yerde, herhangi bir cihazda kullanıcıların güvenliğini ve gizliliğini garanti etmek için her türlü çabayı göstermeleri gerekmektedir.

SONUÇ

IoT hayatımızı daha kolay ve konforlu hale getirecek olan geleceğin teknolojisidir. IoT uygulamalarının tıbbi, imalat, endüstriyel, ulaşım, eğitim, yönetim, madencilik, habitat vb. tüm alanlarda sayısız faydası bulunmaktadır. Bu teknolojinin son on yılda hızla gelişmesinin temel sebebi de budur. Bu çalışmada IoT teknolojisinin bileşenleri olan çeşitli protokoller, cihazlar ve iletişim yöntemleri ile ilgili bilgi verilmiştir. Endüstriyel üretimde benimsenmesi gereken üç temel unsur olan izleme ve kontrol, büyük veri ve analiz, bilgi paylaşımı ve işbirliğinden bahsedilmiştir. IoT mimarisinin katmanları olan fiziksel katman, ağ katmanı, bulut katmanı ve uygulama katmanlarından bahsedilmiştir. Son olarak işletmelerin IoT sistemi kurarken karşılaşılabilecek temel sorunlar olan veri yönetimi, güvenlik, gizlilik, kaos sorunlarından bahsedilmiştir. IoT teknolojisi önümüzdeki yıllarda tüm sektörlerde etkin kullanılacak ve son kullanıcıların yaşamına etkisi çok daha fazla olacaktır.

KAYNAKÇA

- Abuelkhail, A., Baroudi, U., Raad, M., & Sheltami, T. (2021). Internet of things for healthcare monitoring applications based on RFID clustering scheme. *Wireless Networks*, 27, pp. 747–763 <https://doi.org/10.1007/s11276-020-02482-1>
- Adjei O., Babu, N. & Yakubu O. (2018). A review of digital forensic challenges in the Internet of Things (IoT). *Int. J. Mech. Eng. Technol.*, 9(1), pp. 915-923

- Ammar M., Russello G. & Crispo B. (2018). Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Security Appl.*, vol. 38, pp. 8-27
- Bazzaz Abkenar, S., Kashani, M. H., Mahdipour, E. & Jameii, S.M. (2020). Big data analytics meets social media: a systematic review of techniques, open issues, and future directions. *Telematics and Informatics*. 57 , pp. 101517-110555. <https://doi.org/10.1016/j.tele.2020.101517>
- Butler, D. (2006). Everything, everywhere. *Nature*, 440, 402-405. <http://dx.doi.org/10.1038/440402a>
- Chanak, P., & Banerjee, I. (2020). Congestion free routing mechanism for IoT-enabled wireless sensor networks for smart healthcare applications. *IEEE Transactions on Consumer Electronics*, 66(3), pp. 223-232. <https://doi.org/10.1109/TCE.2020.2987433>
- Cuttillo L.A., & Manulis M., T. (2010). StrufeSecurity and privacy in online social networks. B. Furht (Ed.), *Handbook of Social Network Technologies and Applications*, Springer US, Boston, MA , pp. 497-522.
- Elmisery, A. M., Rho, S., & Aborizka, M. (2010). A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. *Cluster Computing*, 22(1), pp. 1611-1638. <https://doi.org/10.1007/s10586-017-1298-1>
- Feng X., Dawam E. & Amin S., (2018). A new digital forensics model of smart city automated vehicles, *Proc. IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber Phys. Soc. Comput. IEEE Smart Data iThings-GreenCom-CPSCoM-SmartData*, pp. 274-279
- Gartner (2014). Gartner says the internet of things will transform the data center. Retrieved from <http://www.gartner.com/newsroom/id/2684616>
- Gigli, M. & Koo, S. (2011). Internet of things, services and applications categorization. *Advances in Internet of Things*, 1, 27-31. <http://dx.doi.org/10.4236/ait.2011.12004>
- Haghi Kashani, M., Rahmani, A. M., & Jafari Navimipour, N. (2020). Quality of service-aware approaches in fog computing. *International Journal of Communication Systems*, 33(8), Article e4340. <https://doi.org/10.1002/dac.4340>
- He D., & Zeadally S. (2015). An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE Internet Of Things Journal*, 2(1) , pp. 72-83. <https://doi.org/10.1109/JIOT.2014.2360121>
- Wang, J., Lim, M. K., Wang, C., & Tseng, M. L. (2021). The evolution of the internet of things (IoT) over the past 20 years, *Computers & Industrial Engineering*, (155), pp. 207-211. <https://doi.org/10.1016/j.cie.2021.107174>
- Joshi R. & Pilli E. S. (2016). *Computer Communications and networks fundamentals of network forensics a research perspective*, London, U.K.:Springer-Verlag,
- Kosmatos, E. A., Tselikas, N. D. & Boucouvalas, A. C. (2011) Integrating RFIDs and smart ob-jects into a unified internet of things architecture. *Advances in Internet of Things: Scientific Research*, 1, 5-12. <http://dx.doi.org/10.4236/ait.2011.11002>
- Lianos, M. & Douglas, M. (2000) Dangerization and the end of deviance: the institutional environment. *British Journal of Criminology*, 40, 261-278. <http://dx.doi.org/10.1093/bjc/40.2.261>
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). Big data: The next frontierfor innovation, competition, and productivity. *International Transaction of Electrical and Computer Engineers System*. (4)1, 14-25.
- Swamy, S. N., & Kota, S. R. (2020). An empirical study on system level aspects of internet of things (IoT). *Access IEEE*, (8), pp. 1 88082-188134, <https://doi.org/10.1109/ACCESS.2020.3029847>

- Rathore S. & Park J. H. (2018). Semi-supervised learning based distributed attack detection framework for IoT. *Applied Soft Computing*, (72), pp. 79-89.
- Stallings, W. (2015). The internet of things: network and security architecture. *Internet Protocol J*, 18(4), 2-24.
- Stoyanov, Y. R. (2014) An approach to use the Web services and open source software to store and share user applications and data. *Proc. Annu. Univ. Sci. Conf. NVU*, vol. 9, pp. 92-96.
- Zawoad, S. & Hasan, R. (2015). Digital forensics in the age of big data: Challenges approaches and opportunities. *Proc. IEEE 17th Int. Conf. High Perform. Comput. Commun. IEEE 7th Int. Symp. Cyberspace Safty Security IEEE 12th Int. Conf. Embedded Softw. Syst.*, pp. 1320-1325. <https://doi.org/10.1109/HPCC-CSS-ICISS.2015.305>
- Zhang, T., Antunes, H. & Aggarwal, S. (2014). Defending connected vehicles against malware: Challenges and a solution framework. *IEEE Internet of Things journal*, 1(1), 10-21. <http://dx.doi.org/10.1109/JIOT.2014.2302386>

EXTENDED ABSTRACT

Introduction

The Internet of Things (IoT) is recognized as a new technology paradigm designed as a global network of machines and devices that can interact with each other. IoT is seen as the technology of the future and is followed with interest by many industry areas. In addition to the adoption of IoT by manufacturers, efforts are being made to increase market share in various service sectors, these studies generally include radio frequency identification (RFID) chip devices, video analytics devices, wireless devices, POS devices, It consists of platforms that include handheld sensors, IP cameras and video management software. Adoption of this technology is gaining momentum as technological, societal and competitive pressures push firms to innovate and transform themselves. As IoT technology advances and an increasing number of companies adopt the technology, IoT cost-benefit analysis will be of great interest. Due to the potential but uncertain benefits and high investment costs of IoT, firms need to carefully consider every opportunity and challenge from IoT to ensure their resources are spent judiciously. This article discusses the infrastructure, transformation, and finally the technical and managerial challenges of this technology.

Materials and Methods

IoT technology was developed by being inspired by RFID networks that can communicate with radio signals in near field. In addition to radio signals and other wireless communication methods that provide communication, sensor technology, nano technology and embedded integrated systems form the basis of this technology. By connecting objects to the internet, physical objects enter the cyber world and transfer data. A unique IP address is needed to identify each device connected to the Internet with IoT technology. New addressing methods are also being developed for the upcoming periods when the number of connected devices will increase rapidly. Sensor networks and barcode technologies used for identification are also developing in parallel with the IoT. Basically, it aims to share data, store, analyze and control this data by connecting IoT devices to the internet. In this context, when creating IoT technology, it has four basic layers, these are; The Physical Layer is the Network Layer, the Cloud Layer, and finally the Application Layer. The physical layer at the bottom of the architecture includes devices, sensors, electric motors, hydraulic and pneumatic motion generating systems. These devices may have their own driver software, intermediate control software and even small operating systems, all software used for automation of these devices is accepted at the physical layer. Likewise, the integrated circuits and embedded software of the devices are located in this layer. The purpose of this layer is to connect the devices in the physical layer to the online network or the Internet. All gateway devices such as switch, gateway are located in this layer. Likewise, HTTP and IP protocols are also included in this layer. Network speed and stability are important in this layer. Every device in the physical layer produces huge data. Storing and managing this data on server computers with the efforts of the enterprises increases the cost. Safe and cost-effective storage and management of data is carried out with cloud systems. The top layer of the architecture is the application layer. In this layer, there are computers, tablets or similar devices and software used by system administrators or end users. All preparations for the monitoring and management of the system are processed in this layer, likewise, decision-making processes take place in this layer.

Findings

Every transformation leads to the emergence of new problems. IoT technology also brings with it various challenges for businesses. The security of generated data will face a variety of challenges, with challenges in business and consumer privacy, data storage and management, server technologies, and data center networking. IoT sensors and devices generate huge amounts of data that must be processed and stored. The current architecture of the data center is not prepared to cope with the heterogeneous nature and large volume of personal and corporate data. Few organizations can invest in enough data storage to house all the IoT data collected from their networks. As a result, they will prioritize data for operations or backup based on needs and value. As IoT devices become more widely used and consume more bandwidth, data centers will have to dedicate more resources to improve processing efficiency and response time. The data should be made understandable using computers and mathematical models. Digitized data may not be just numeric data. Image processing, machine learning and artificial intelligence methods should be used to process data

from devices that receive images and video recordings. Various business lines such as data analytics and data engineering have been formed in order to create the necessary manpower for processing the generated data.

Discussion

IoT is the technology of the future that will make our life easier and more comfortable. IoT applications can be found in medical, manufacturing, industrial, transportation, education, governance, mining, habitat, etc. It has numerous benefits in all areas. This is the main reason why this technology has developed rapidly in the last ten years. In this study, information about various protocols, devices and communication methods, which are components of IoT technology, is given. Monitoring and control, big data and analysis, information sharing and cooperation, which are the three basic elements that should be adopted in industrial production, are mentioned. The physical layer, network layer, cloud layer and application layers, which are the layers of the IoT architecture, are mentioned. Finally, data management, security, privacy and chaos problems, which are the main problems that businesses will encounter when establishing an IoT system, are mentioned. IoT technology will be used effectively in all sectors in the coming years and its impact on the lives of end users will be much greater.