Nesnelerin İnterneti I

HAFTA IV

ENDÜSTRİ 4.0

İnternet kavramı

- İnternet büyümekte ve gelişmektedir. İnternetin ortaya çıktığı ilk zamanlarda bu ilerleme yavaş gerçekleşmekteydi. Günümüzde ise ağların ağı olarak ifade edilen internetin iletişim kapasitesi ve hızı ilk zamanlarına göre olağanüstü seviyelere ulaşmıştır. 1969 yılında ortaya çıkan, çok az sayıda cihazın haberleşmesini sağlayan ve internetin temelini oluşturan ARPANET (Advanced Research Projects Agency Network) ile başlayan devasa ağ sistemi olan internete 2020 yılına kadar yaklaşık olarak 50 milyar nesnenin bağlı olacağı öngörülmektedir. İnternetin gelişen teknolojileri her türlü cihazın/nesnenin kendisine bağlantı kurmasına olanak sağlamaktadır.

Nesnelerin İnterneti (Internet of Things-IoT) kavramı

- Nesnelerin İnterneti (Internet of Things-IoT) kavramı modern kablosuz iletişim teknolojilerinin gelişimi sayesinde popülaritesi artan yeni sayılabilecek bir kavramdır. Bu kavramın temel oluşumu dünyada bulunan nesnelerin birbirleriyle haberleşmesini sağlayarak insan hayatını kolaylaştırmaya yönelik uygulamaların geliştirilmesidir. IoT standart iletişim protokolleri üzerine kurulu ve adreslenebilme özelliğine sahip nesnelerin, internet aracılığı ile haberleşebilmesidir. 2025 yılına kadar mobilya, kağıt dokümanlar, besin maddeleri, elektronik cihazlar gibi bir çok nesnenin internete bağlı olacağı öngörülmektedir.

İnternetin Gelişim Evreleri

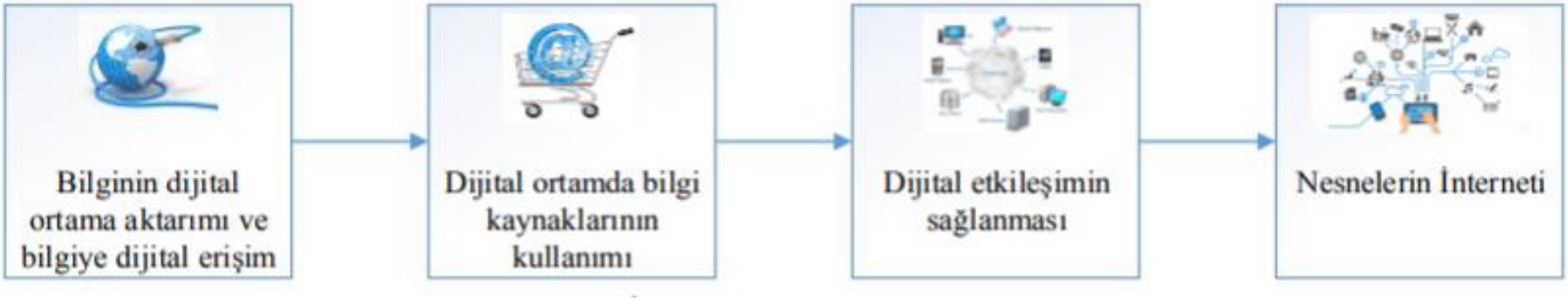
1. Evre: Bilginin dijital ortama aktarılması ve bilgiye dijital erişim sağlanması (1990-1995),

2. Evre: Dijital ortama aktarılmış bilgi kaynaklarının işbirliği ile kullanımının sağlanması ve e-ticaret faaliyetlerinin başlaması (1990 yıllarının sonları),

3. Evre: Sosyal medya, mobil medyaların kullanımı, bulut bilişim, videoların sanal ortama aktarılması gibi etkileşimlerin dijitalleştirilmesi (2000 yıllarının başları)

4. Evre: Nesnelerin dijital olarak internete bağlanması (Günümüz).

İnternetin Gelişim Süreci Evreleri



Nesnelerin interneti (Internet of Things-IoT)

Kısa bir zaman içerisinde internet insanoğlunun çalışma, yaşam, öğrenme gibi yetilerine farklı bir boyut kazandırmıştır. IoT ise bunu akıllı ev, akıllı şehir, akıllı stadyum gibi daha farklı bir boyuta taşımaktadır. İnternete bağlı olan geleneksel cihazlar dışındaki nesnelerin internet ortamından kontrolünün sağlanabilmesi ve analizlerinin yapılabilmesi ile IoT evresi başlamıştır. Nesnelerin İnterneti; insan müdahalesine ve herhangi bir verinin elle girişine gerek olmadan cihazların veya makinelerin kendi aralarında veri iletişimi yaptığı, bilgi topladığı ve toplanan bilgiler ile karar verdiği bir ağ yapısı olarak tanımlanmaktadır.

Tanımlar

IoT için şu tanımları yapmak da mümkündür:

1. Nesnelerin interneti, benzersiz bir şekilde adreslenebilen nesnelerin kendi aralarında oluşturduğu, dünya çapında yaygın bir ağ ve bu ağdaki nesnelerin belirli bir protokol ile birbirleriyle iletişim içinde olmalarıdır,

2. Nesnelerin İnterneti, günlük hayatta kullanılan nesnelerin internet aracılığıyla diğer nesnelerle veri alışverişi yapabilmesi ve bu nesnelerin birbirleriyle tamamen senkronizasyon halinde olma durumudur,

3. IoT insanların hayatlarını kolaylaştıran ve yaşam standartlarını yükselten akıllı uygulama ve hizmetlerin ekosistemidir.

Örnekler

- Buzdolabında sütün bittiğini haber verip, arabanın GPS'sini en yakın markete yönlendirilmesi ve bu noktada telefonla ödeme yapılabilmesi,
- Arabaları takip eden sistemler ile herhangi bir kaza anında bunu algılayıp yardım çağrılabilmesi,
- Kapıları kilitleyen, alarmı kuran ve bu aygıtları açıp kapatabilen ev araçları uygulamaları,
- Televizyonlar, ev sunucu ve depoları, panjur sistemleri, bebek monitörleri vb. cihazların çevrimiçi kontrolü,
- Sağlık uygulamaları ile hastaya ve doktoruna ihtiyacı olan bilgilerin aktarılması ve hastanın sağlığı ile ilgili olumsuz durumların önceden belirlenmesi, IoT'ye birer örnektir.

Nesnelerin Internetinin Uygulamaları

Tam bir IoT uygulaması geliştirmek için bu uygulamaların birlikte çalışabilirliğini sağlamak hayatidir. Bu birlikteliğin sağlanması ile birçok alanda IoT uygulamaları uygulanabilmektedir. Bu uygulamalar ile insan hayatına kolaylıklar sağlanabilmektedir. Buna göre;

1. Enerji tüketiminde opsiyonel kullanımının sağlanması,

2.Askeri alandaki uygulamalarda kolaylık sağlanması,

3. Yapılacak işin tek bir yerden değil de istenilen yerden istenildiği şekilde ve istenildiği zamanda yapılabilmesi kolaylığının sağlanması gibi IoT'nin sağladığı bazı kolaylıklar görülebilir.

Nesnelerin Internetinin Uygulamaları

Akıllı ev uygulamaları, akıllı şehir uygulamaları, bilimsel çalışma uygulamaları, bilişim sektörü uygulamaları, enerji uygulamaları, günlük kullanım uygulamaları, güvenlik uygulamaları, imalat/üretim uygulamaları, inşaat uygulamaları, kamu sektörü uygulamaları, sağlık uygulamaları, servis sağlayıcı uygulamaları, tarımsal üretim uygulamaları, taşımacılık uygulamaları, ticaret uygulamaları.

Uygulama Örnekleri

Akıllı evde güvenlik sistemi, ışık, klima kontrol gibi birçok eleman mobil bir cihaz ile izlenebilir ve uzaktan kontrol edilebilir. Buzdolabı, fırın ve ısıtma sistemi gibi ev donanımları internete bağlanabilir. Bu durum ev sahibine cihazların açılıp-kapanması, aletlerin durumunun gözlenmesi ve farklı durumların bildirimi gibi durumlarda yetkilendirme ve bilgilendirme sağlar. Ayrıca yaşlı ve engelli insanların hayatlarının kolaylaştırılmasına yönelik IoT uygulamaları da vardır.

Akıllı şehir uygulamalarında gerçekleştirilebilecek su kalitesi kontrolü, köprü sağlamlık kontrolleri, yangın söndürme sistemleri, hava kirliliği kontrolü, çöp konteynerlarının doluluk kontrolleri, araç park etmek için otoparkların kontrolü, radyasyon oranı kontrolü, gürültü seviyesi kontrolü, şehir trafik yoğunluğu kontrolü, su sistemlerinin sağlamlık kontrolleri, insan yoğunluğu tespiti gibi bazı IoT uygulamalarıdır.

miCoach Smart Ball

Nest

Babolat

Edyn

Dropcam

August Smart Lock

Belkin WeMo Smart Slow Cooker

Amazon Echo

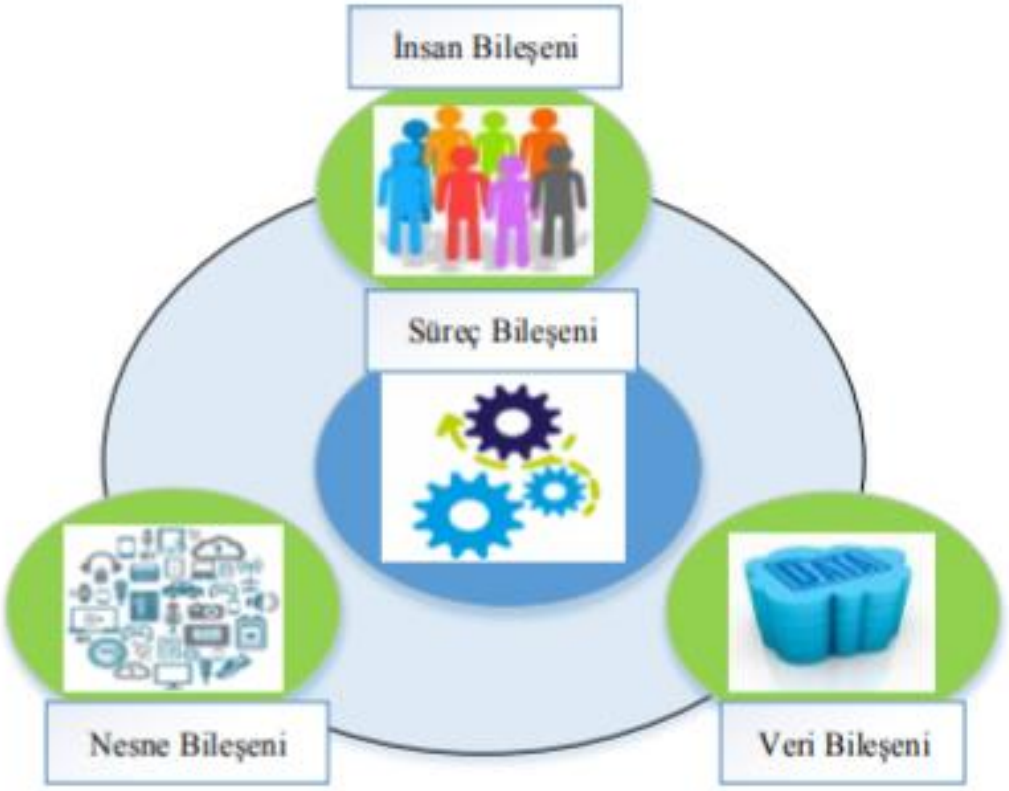
Bluesmart

Amazon Dash

Jindo Bridge

Akıllı Durak

Nesnelerin İnterneti Bileşenleri



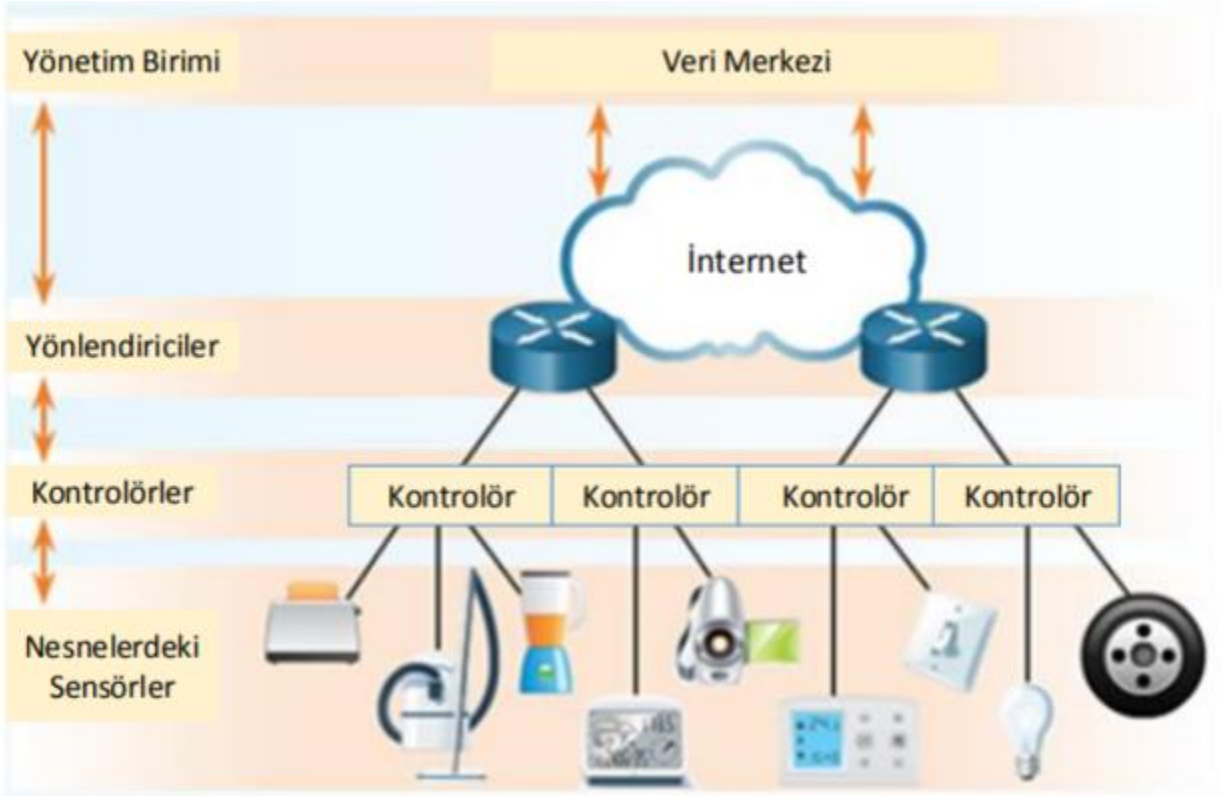
Nesne Bileşeni

IoT’nin amacı internet aracılığıyla nesneleri birbirleriyle haberleştirmektir. IoT her tür nesneyi içerir. İstenen nesnelerin hemen hemen tamamının IoT ile bağlanabileceği öngörülmektedir. Bu nesneler dâhili sunucu ve harici çevre ile haberleşmek için gömülü sistemler kullanırlar. Gelecekte birçok nesne internete bağlanacak ve uzaktan gözlemlenip konfigüre edilebilecektir. Nesne bileşeni kararlar verebilmek için internete ve birbirine bağlanan cihazları ifade eden kavramdır. Nesnelerin önemli olanlarından bazıları şu şekildedir:

Nesne Bileşeni

Sensörler: Sensörler çevredeki fiziksel özellikleri, bilgisayarlar tarafından işlenebilmesi için elektriksel sinyallerine dönüştüren cihazlardır.

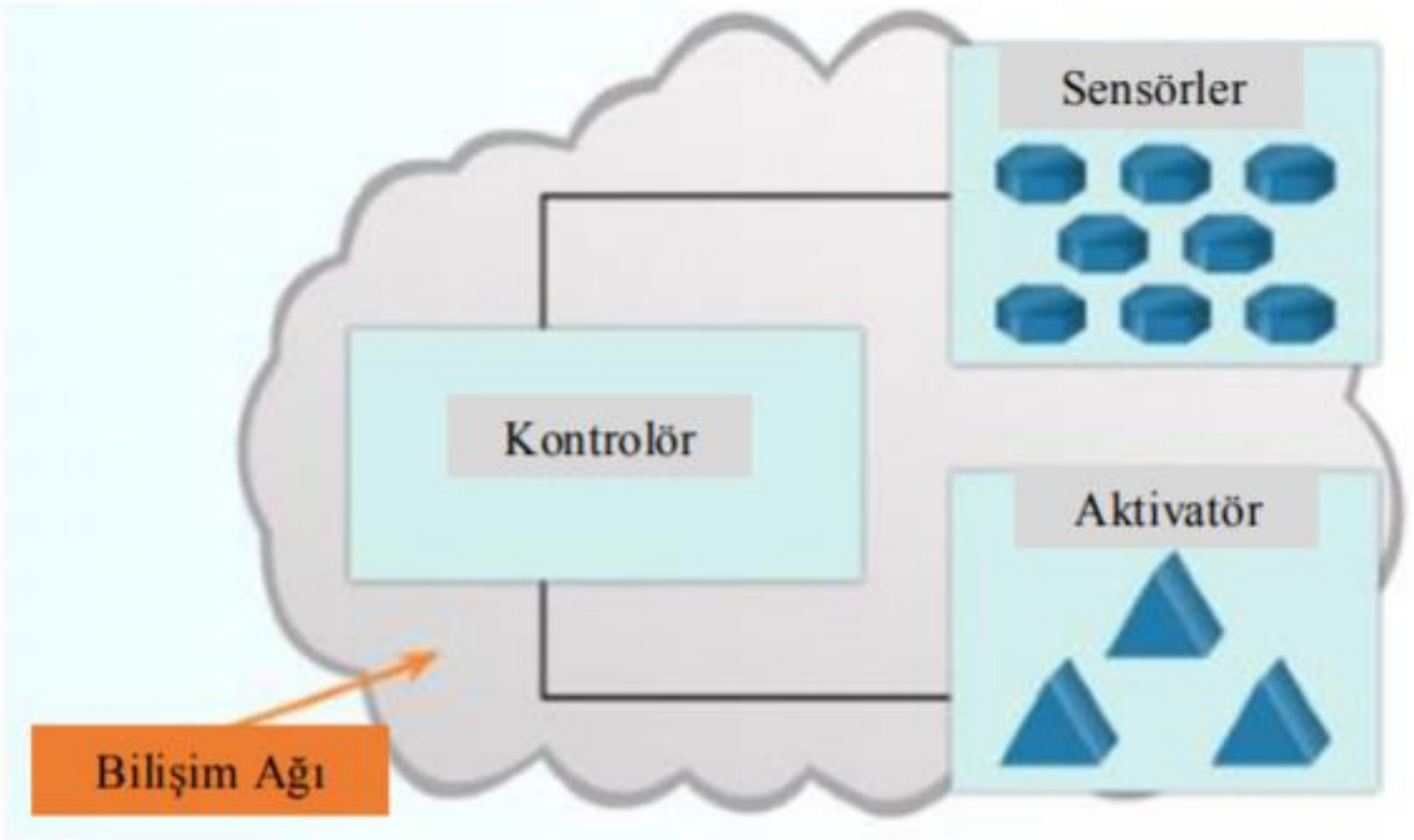
Kontrolörler: Sensörler ortamdan aldıkları ölçüm verilerini sinyallere dönüştürür ve daha sonra bu verileri kontrolör olarak adlandırılan ana cihazlara yollarlar. Kontrolörler ise bu veriyi buluttaki herhangi bir cihaza/aktivatöre yollayabilirler. Bu M2M (Machine To Machine) iletişime bir örnektir. Kontrolörlerin görevi sensörlerden veri toplamak ve bir internet bağlantısı sağlamaktır. Kontrolörler anlık kararlar alma veya verilerin analiz edilmesi için verilerin daha güçlü bilgisayarlara gönderilmesi yeteneğine de sahiptirler. Bu güçlü bilgisayarlar kontrolörlerle aynı ağda olabilecekleri gibi internet bağlantısı aracılığıyla erişilebilecek uzak konumlarda da olabilirler. İnternette ve veri merkezlerinde bulunan daha güçlü bilgisayarlara erişmek için kontrolör öncelikle veriyi yönlendiriciye yollar. Yönlendiriciler ise bu veriyi internet üzerinden veri merkezlerine yollarlar


Yönetim Birimi
Veri Merkezi
İnternet
Yönlendiriciler
Kontrolörler
Kontrolör
Kontrolör
Kontrolör
Kontrolör
Nesnelerdeki
Sensörler

Nesne Bileşeni

Aktivatörler: IoT de kullanılan diğer bir cihaz aktivatörlerdir. Aktivatör belli komutları yerine getirebilen bir sistemi ya da mekanizmayı kontrol veya hareket ettirmek için kullanılabilen basit bir motordur. Aktivatörler fiziksel bir fonksiyonu yerine getirebilirler. Yani IoT de nesnelere hareket kazandırabilirler.

Aktivatörlerin hareketi nasıl sağladığına bakılmaksızın, bir aktivatörün temel görevi bir sinyali almak ve bu sinyale göre belirlenen eylemleri yerine getirmektir. Aktivatörler veri üzerinde işlem yapamazlar.


Sensörler
Kontrolör
Aktivatör
Bilişim Ağı

Veri Bileşeni

Veri ortamdaki herhangi bir şeye atanmış değerdir. Fakat veri bazen kendi başına bir anlam ifade etmeyebilir. Veri yorumlandığında, ilişkilendirildiğinde, bir işleme tabi tutulduğunda veya karşılaştırıldığında daha anlamlı bir hale gelir. Anlamlandırılan veri, bilgi (information) haline dönüşür. Bilgi uygulandığında veya anlaşıldığında ise özbilgi (knowledge) haline gelir.

Veri Bileşeni

Yapılandırılmış Veri (Structured Data): Yapılandırılmış veri bir dosya veya kayıt alanına girilmiş veriyi ifade eder. Yapılandırılmış veri bir bilgisayar tarafından kolayca sınıflandırılabilir, sorgulanabilir ve analiz edilebilir. Örneğin bir kullanıcı bir web sitesine adı, adresi, iletişim bilgileri gibi verilerini girdiğinde aslında yapılandırılmış veri oluşturmaktadır. Yapılandırma bir bilgisayarın veriyi yorumlaması ve hataları en aza indirgemesi için güçlü bir yöntemdir. Örneğin 11 haneli TC kimlik numarasının girilmesi için 11 hane zorunluluğu bir yapılandırmadır.

Yapılandırılmamış Veri (Unstructured Data): Yapılandırılmamış veri ham veriyi ifade eder. Büyük verinin büyük kısmı yapılandırılmamış yani veri tabanlarında belirtilen klasik formatlara sokulmamış veri halinde bulunur.

Veri Bileşeni

Veri Depolamanın üç çeşidi vardır:

1. Local Data: Lokal cihazlar üzerinde bulunup doğrudan erişilebilen veriyi gösterir. HDD, USB bellek, CD, DVD vb. üzerindeki veriler örnek olarak gösterilebilir,

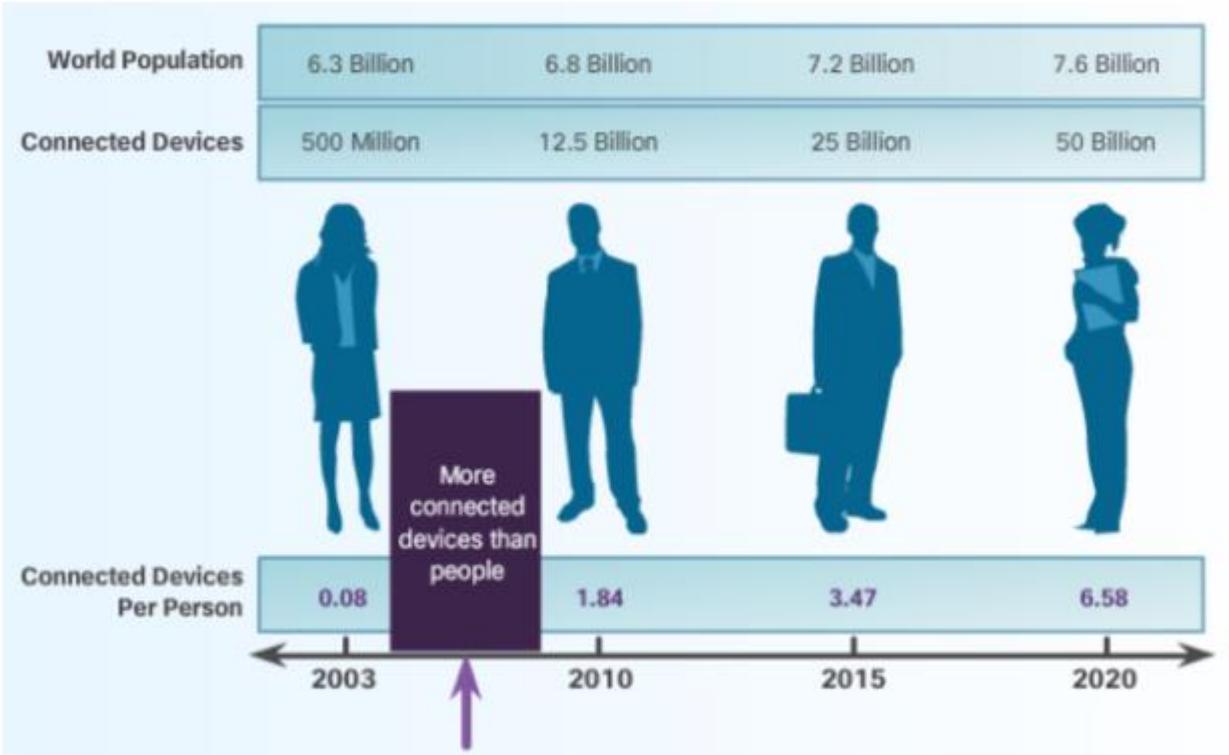
2. Centralized Data: Verinin tek bir merkezde depolanıp paylaşıldığı depolama şeklidir. Bu veriye internet veya ağ üzerinden bir çok cihaz tarafından erişilebilir. Merkezi veri depolama sunucularının kullanımı veriye erişimde darboğaza, tıkanıklığa, verimsiz çalışmaya ve tek bir merkezden kaynaklı hataların erişimi engellemesi gibi sorunların ortaya çıkmasına sebep olabilir,

3. Distributed Data: Veri merkezi bir DBMS (Database Management System) tarafından yönetilir. Ama veri tek bir merkezde değil de birçok farklı konumda depolanır ve kopyalanır. Bu durum verinin paylaşımının daha etkili ve kolay olmasına olanak sağlar. Dağıtık verilere lokal ve global düzeyde erişim sağlanabilir. Dağıtık sistemde tek bir merkez olmadığı için bir merkez çalışmasa bile sisteme erişim verilerin farklı konumlarda kopyaları bulunacağından devam eder. Bu yapı veriye erişimin en kesintisiz olduğu yapıdır. Bulut bilişim distributed dataya örnektir.

Veri Bileşeni

Büyük Veri

Son on senede bir yılda üretilen verinin hacmi, günümüzde bir hafta içinde üretilmektedir. Bu bir haftada yaklaşık olarak 20 exabytes veri demektir. İnternete bağlı olmayan cihazların IoT sayesinde internete bağlanması ile bu veri miktarı daha da artacaktır. Veri miktarının bu denli fazlalaştığı dijital evrendeki tüm veriler ve bu verilerin analizine Büyük Veri (Big Data) denmektedir.



Belli yıllara göre insan ve internete bağlı cihaz sayısı

Veri Bileşeni

Büyük Veri

IoT ile 2020 yılına kadar elli milyar nesnenin internete bağlanması öngörüsü ile internet ortamında var olacak veri miktarının trilyonlarca gigabyte olacağını söylemek kaçınılmazdır. Bu kadar fazla miktardaki veri Big Data kavramını ortaya çıkarmaktadır. Bu kadar büyük verilerin analizi ise önemli bir çalışma sahası olarak ortaya çıkmaktadır. Bu veriler çevrimiçi işlemlerden, e-postalardan, videolardan, ses dosyalarından, log kayıtlarından, arama sorgularından, sağlık kayıtlarından, sosyal ağ etkileşimlerinden, bilimsel verilerden, sensörlerden, mobil cihazlardan ve uygulamalarından elde edilir.

Veri Bileşeni

Büyük veri için göz önüne alınması gereken üç temel özellik vardır.

1. Hacim (Volume): Taşınan ve depolanan verinin miktarını gösterir. Günümüzde veri miktarı tahmin edilemeyecek kadar çok miktarda olup sürekli artış göstermektedir. Örneğin sadece Facebook'ta günde 10 milyar mesaj gönderilmektedir. Sensörler, makineler, kameralar vb. her an kayıtta bulunan mobese kameraları sürekli veri üretmekte ve veri hacmini genişletmektedirler,

2. Çeşitlilik (Variety): Verinin tipini gösterir. Çeşitlilik özelliği büyük verinin bünyesinde fotoğraflardan, tıklama sayılarına, maillerden, ses kayıtlarına, videolardan ekg verilerine kadar farklı veri türlerini barındırmaktadır,

3. Hız (Velocity): Bu kavram verinin üretilmesindeki ve üretilen verinin yayılımındaki hızı ifade etmektedir. Hız, üretilen verinin saklanmadan, anında analiz edilip değerlenmesini de kapsar. Günümüzde veri çok hızlı üretilir, çok hızlı yayılır, çok hızlı analiz edilir olmalıdır

Veri Bileşeni

Büyük Veri

Büyük veri yönetimindeki amaç büyük veride gizli olan veri değerini (value) keşfetmektir. Değere ulaşmak için büyük verinin yukarıda belirtilen özelliklerinden yararlanılır. Value veri içindeki desenleri, iç görüleri, ilişkileri görmek, veriden bilgiyi keşfetmek ve geleceği tahmin etmektir. Bunların sağlanabilmesi için veri analizinin etkin yapılması gerekmektedir. Büyük veriler analiz edilirken şu sorulara cevap aranır:

1. Ne kadar veri üretildiği,

2. Verinin kullanılabilir bilgi haline nasıl dönüştürüldüğü,

3. Karar alınabilmesinde bu verilerin nasıl kullanıldığı,

4. Verinin nasıl tanımlandığı ve yönetildiği.

Veri Bileşeni

Büyük Veri

Büyük veri modelinde maliyet ve karmaşıklık artmaktadır. Büyük veri için öne çıkan etkenler erişim, depolama ve analizdir. Bu bağlamda büyük verinin amacı veriyi toplayıp önemli bilgi haline getirmektir. Günümüzde kurum ve kuruluşlar büyük veri ihtiyaçlarını karşılamak için veri modellerini düzenlemektedir. Büyük veri ile alakalı ihtiyaçlarının karşılanması için bulut bilişim teknolojileri kullanılmaktadır.

Veri Bileşeni

Bulut Bilişim

Sahip olunan tüm uygulama, program ve verilerin sanal bir sunucuda yani bulutta depolanması ve internete bağlı olunan herhangi bir ortamda cihazlar aracılığıyla bu bilgilere, verilere, programlara kolayca ulaşımın sağlanabildiği hizmetler bütününe Bulut Bilişim denir. Hard disklerde depolanan verilerin internet ortamında sanal sunucularda saklanması işlemi bulut bilişimdir. Bulut bilişim daha fazla depolama alanı, hızlı veri transferi, maliyet tasarrufu yapabilme gibi bir takım olanaklar sağlamaktadır. Bu durum büyük veri ihtiyaçlarının karşılanması ve IoT'den yararlanılması açısından organizasyonlara avantajlar sunmaktadır.

Bulut bilişim veriye erişim, yönetme ve depolamanın farklı bir yöntemidir. Bulut bilişim bir ağda bulunan çok fazla sayıda bilgisayarı içerir. Bulut bilişim sağlayıcıları servislerini çalıştırmak için sanallaştırma yöntemini kullanırlar. Bu durum kaynakların daha verimli kullanılarak maliyetlerin azalmasını sağlar. Bulut bilişim sayesinde kullanıcılar verilerine istedikleri zamanda ve yerde erişim sağlayabilirler. Bulut bilişim kullanımına olanak sağlayan kuruluşlar dört servis çeşidi sunarlar.

Veri Bileşeni

Bulut Bilişim

Bulut bilişim servisleri şunlardır:

1. SaaS (Software as a Service): Uygulamalar web üzerinden son kullanıcılara sunulur,

2. PaaS (Platform as a Service): Uygulamaların çalıştırılması için araç ve servis hizmetleri sunulur,

3. IaaS (Infrastructure as a Service): İşletim sistemi, ağlar, depolama birimleri ve sunucuları güçlendirmek için donanımsal ve yazılımsal altyapının tamamı sunulur,

4. ITaaS (IT as a Service): Uygulamalar, platformlar ve alt yapıların kontrolünde teknik destek sağlanır.

Bulut Bilişim; maliyetleri düşürür, altyapı karmaşasını ortadan kaldırır, çalışma alanını genişletir ve çok daha ucuza, kurulum gerektirmeden, her yerden çalışmayı destekler.

İnsan Bileşeni

Kimsenin erişemediği çok miktardaki veri kendi başına pek bir anlam ifade etmez. En uygun kararların alınıp uygun eylemin gerçekleştirilmesi için bu verinin insanlarca kullanılabilecek faydalı bilgiler haline dönüştürülmesi gerekir. İnsanın kullanımı için verinin ortaya çıkarılması M2M (Machine to Machine), M2P (Machine to People), P2P (People to People) olmak üzere üç şekil etkileşim ile olmaktadır.

IoT'nin hareket noktası, internetten elde edilen verilerden çıkarılan bilgilerden faydalanarak bir eylemi gerçekleştirmektir. IoT insanların faydaları için insan davranışlarını değiştirebilecek doğru ve zamanlı bilgiyi insanlara ulaştırma yeteneğine sahiptir. İstenen çıktı ile gerçek çıktı farklılıkları arasında köprü kuran kararları vermek için insanlara geri besleme sağlayan IoT, bu işi kolaylaştırmaktadır. Bu durum geri besleme döngüsü olarak adlandırılmaktadır

İnsan Bileşeni

Bir geri besleme döngüsü o anki davranışlar üzerinde gerçek zamanlı bilgi ve daha sonra o davranışı değiştirmek için uygulanabilir bilgi sağlayabilir. Bir geri besleme döngüsü sürekli değişen iş çıktılarının planlanması ve yeni hamlelerin belirlenmesi için işletmelere ve kişilere önemli bir kazanç sağlar. Örneğin; IoT'nin, insanları etkilemek için reklam endüstrisinde yoğun şekilde kullanıldığı görülmektedir. E-ticaret siteleri kullanıcıların ilgilerini tespit ederek ihtiyaç duyabilecekleri alakalı ürünleri karşılarına çıkartmaktadır.

Süreç Bileşeni

Süreç bileşeni IoT deki diğer üç bileşenin uyumlu çalışmasını ifade eder. Süreçler insan-nesne-veri arasındaki etkileşimi kolaylaştırır. Süreç bilginin doğru kişiye doğru zamanda ve uygun şekilde ulaştırılmasını sağlar. IoT bileşenleri, süreç bileşeni sayesinde üç şekilde bir araya getirilir.

Süreç Bileşeni

1. M2M Bağlantı: M2M kavramı makinelerin birbirleri ile haberleşmesine dayalı teknolojileri ifade etmektedir. Bir ağ sisteminde verinin bir makineden veya nesneden diğer bir makine veya nesneye aktarıldığında gerçekleşen bağlantı şeklidir.

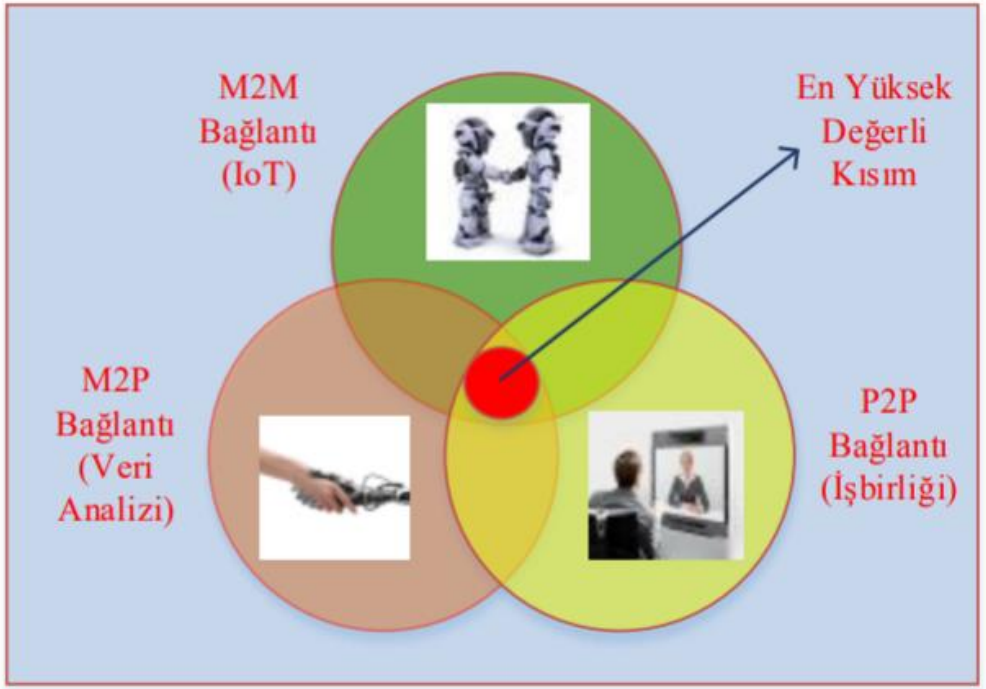
M2M bağlantı genellikle IoT olarak da adlandırılmaktadır. Eve varmak üzere olan bir otomobilin, ev ağına sinyal göndererek ev sıcaklığını ve ışık düzenini ayarlaması için komut yollaması M2M bağlantıya örnektir.

M2M bağlantının en önemli elemanları, sensörler, aktivatörler ve kontrolörlerdir. M2M'nin en önemli ayırt edici özelliği, yaygın ve açık altyapısı olan IP'nin üzerine kurulu olmasıdır.

2. . M2P Bağlantı: Bilginin bir makine ile insan arasında aktarımını ifade eden bağlantı şeklidir. Bu etkileşimde her iki taraf veri alışverişinde bulunabilir. M2P bağlantı, insanlara hüküm çıkarmada yardım etmek için, makineler tarafından bilginin taşınması ya da bildirilmesine olanak sağlar. Bu durum M2P bağlantının veri analizi ile de isimlendirilmesine sebep olmaktadır. İnsanların veri analizi sonucu çıkardıkları hükümlerden gerçekleştirdikleri eylemler IoT'nin geri besleme döngüsünü tamamlar. M2P bağlantıya, ev güvenlik sistemleri, akıllı park sistemleri örnek olarak verilebilir.

Süreç Bileşeni

3. P2P Bağlantı: Bir kişiden bir kişiye veri aktarımı ile gerçekleşen bağlantı şeklidir. P2P bağlantı ortamı video, mobil cihaz ve sosyal ağlar aracılığı ile olmaktadır. P2P bağlantılar genellikle birlikte çalışma anlamına gelmektedir. Örnek olarak uzaktan eğitim, sosyal medya, TV verilebilir.



Nesneleri Interneti ve Güvenlik

IoT kavramı ve teknolojisinin gelişimi; hayatı kolaylaştırması, yaşam standartlarını yükseltmesi, verimliliği artırması ve ekonomilere katkısı ile 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 üzerinde durulmaktadır.

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 bilgisayarlara 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 evdeki bütün nesneler 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.

Nesneleri Interneti ve Güvenlik

Genel Güvenlik Önlemleri

Bir IoT uygulamasında güvenlik yaklaşımı şu niteliklerde olmalıdır:

1. Tutarlı, otomatik çalışan bir sistem,
2. Dinamik, güvenlik zafiyetlerini gerçek zamanlı analiz edebilme yeteneği,
3. Zeki sistem, ağdaki tüm bağlantıları ve alt yapı elemanlarını görüntüleyebilen,
4. Ölçeklenebilir, büyüyen ağın ihtiyaçlarını karşılayabilme özelliği,
5. Gerçek zamanlı tepki verebilme yeteneği,
6. Kapsamlı, tüm ağı gözetleme/denetleyebilme yeteneği,
7. Şifreleme, sadece izinli/yetkili kullanıcıların okuyabilmesi için bilgiyi kodlama/şifreleme.

Nesneleri Interneti ve Güvenlik

Genel Güvenlik Önlemleri

Niteliklere sahip bir güvenlik yaklaşımı/politikası karmaşıklığı artıran, yönetilmesi zor olan, teknik bilgi desteği ve personel ihtiyacı gerektiren tutarsız güvenlik uygulamalarını engeller. Ayrıca güvenlik sistemleri gerçek zamanlı tepki verebilmelidir. Bu yüzden yüksek performanslı olmalıdır. Güvenlik sistemi insan müdahalesi olmadan veya az bir müdahale ile ağdaki güvenlik tehditlerini algılayıp anlık çözümler sunmalıdır.

İnsanlar bir ağ sistemindeki en zayıf halkayı teşkil ederler. Bazı insanlar kötü niyetli olabilirken, bazıları da hata yapabilir ya da güvensiz uygulamalar çalıştırabilirler. Bu durum ekipmanları ve verileri riske atabilir. Varlıkları/nesneleri korumak için kurallar ve yönetmelikler/düzenlemeler ile kullanıcıların nasıl hareket edecekleri ve hangi eylemlerin doğru ya da yanlış olduğu, nelerin yapılıp yapılmayacağına izin verildiği ve sisteme ve veriye nasıl erişileceği belirlenmelidir.

Nesneleri Interneti ve Güvenlik

Genel Güvenlik Önlemleri

Akıllı cihazlarda en çok karşılaşılan güvenlik zafiyetlerine bakıldığı zaman aşağıdaki kontrol noktalarının yapılması gerektiği belirlenebilir:

1. Web Ara Yüzü Yapılandırması: Kullanıcıların akıllı cihazları yönetebilmesi için Web teknolojisi kullanılarak yapılan arayüzlerin güvenlik yapılandırılmaları ciddi öneme sahiptir. Varsayılan şifrelerin kurulum sırasında değiştirilmesi, karmaşık şifre kullanılması, web ara yüzlerine özel geliştirilmiş ataklara 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 bağlanılabilmesi 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, yeterli sayıda rol profillerinin var olması ve izinsiz yetki yükseltmelerine karşı kontrollerin yapılmış olması gerekmektedir,

Nesneleri Interneti ve Güvenlik

Genel Güvenlik Önlemleri

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 şifreleme protokollerinin kullanılması, protokollerin içerisinde pratikte kırılamayacağı ön görülen anahtar uzunluklarının ve algoritmaların kullanılması gerekmektedir,

Nesneleri Interneti ve Güvenlik

Genel Güvenlik Önlemleri

5. Gizlilik: Akıllı cihazlar insanların yaşamlarını kolaylaştırmak ve yaşam standartlarını yükseltmek için kişisel ve özel birçok veriyi kaydetmekte ve işlemektedir. Her akıllı cihaz sadece ihtiyacı dâhilindeki verileri toplamalıdır. Örneğin iklimlendirme sisteminin facebook üzerinde yapılan paylaşımları 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 üzerlerinde çok fazla veri tutmamaktadır ve o verileri işleyecek güçte işlemcilere sahip değildir. Bu veriler bulut ortamında toplamakta ve işlenmektedir. 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,

Nesneleri Interneti ve Güvenlik

Genel Güvenlik Önlemleri

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 saklanmasının şifreli bir şekilde yapılması ve güçlü şifre politikalarının belirlenmesi gerekmektedir,

Nesneleri Interneti ve Güvenlik

Genel Güvenlik Önlemleri

9. Yazılım: Akıllı cihazlar üzerinde çalışan yazılımlar aracılığıyla kullanıcı-cihaz iletişimleri yapılabilmektedir. Yazılım üzerinde yer alan güvenlik zafiyetlerinin üretici tarafından sürekli yayınlanan güncellemeler ile kapatılması, güncelleme paketlerinin üretici 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 ciddi önem taşımaktadır. Cihazlar üzerindeki veri depolama disklerinin kolaylıkla sökülememesi, verilerin şifrelenmiş olarak saklanması, USB gibi bağlantı portlarının kapatılmış olması gerekmektedir.

Nesneleri Interneti ve Güvenlik

Güvenlik Politikaları

Güvenlik politikası sistem güvenliğinin sağlanması için takip edilmesi gereken tüm kuralları, yönetmelikleri ve prosedürleri tanımlar. Bir güvenlik politikası özel risk tiplerini çözmek için birçok farklı alana uygulanabilir. Bu risk tipleri şunlardır:

1. Remote Access Policy (Uzaktan Erişim Politikası): Sisteme kimin, ne zaman, nasıl bağlanabileceği ve bu sisteme uzaktan ne tür cihazlarla bağlanılabileceğinin standardize edilmesidir,

2. Information Privacy Policy (Bilgi Gizliliği Politikası): Hassasiyet seviyesine bağlı olarak bilgiyi korumak için hangi metotların kullanılacağının tanımlanmasıdır. Genellikle daha hassas bilgiler daha fazla güvenlik seviyesine sahip olmaktadır,

Nesneleri Interneti ve Güvenlik

Güvenlik Politikaları

3. Computer Security Policy (Bilgisayar Güvenliği Politikası): Kullanıcıların hangi bilgisayarları kullanacaklarını tanımlar. Bu politika belli bilgisayarları kimin kullanacağını ve bir bilgisayarın korunması için hangi programların kullanılacağını ya da belli bir depolama cihazının kullanılıpkullanılmayacağını tanımlar,

4. Physical Security Policy (Fiziksel Güvenlik Politikası): Fiziksel varlıkların nasıl güvenlik altına alınacağını tanımlar,

5. Password Policy (Parola Politikası): Bir parolanın ne kadar süreyle değiştirilmesi gerektiğini, ne tür şifrelerin kullanılacağını ve parola güvenlik seviyelerinin tanımlanması kriterlerini belirler.

Nesneleri Interneti ve Güvenlik

Güvenlik Politikaları

Bir güvenlik politikasının en önemli kısmı kullanıcıların eğitilmesidir. İnsanlar güvenlik politikalarının sadece varlığından haberdar olmak yerine insanların, verilerin ve nesnelerin güvenliklerini garanti altına almak için bu kuralları aynen uygulamalıdırlar.

Nesnelerin interneti konusunda güvenliğin ve gizliliğin günümüz şartlarında garanti edilmesi zor görünmektedir. Bu alandaki güvenlik çalışmaları hızla gelişmekte, akademik ve ticari anlamda birçok çalışma yapılmaktadır. Bununla beraber son kullanıcıların dikkat etmesi gereken bir takım tedbirler bulunmaktadır. Akıllı cihazlardaki güvenliği ve gizliliği sağlamak için genel ve temel güvenlik önlemlerine dikkat edilmelidir.

Diğer yandan 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. Kullanılan arabanın saldırganların hedefi olup kaza yapmasına sebep olunması, akıllı alarm ve kilit sistemlerinin kırılıp siber hırsızlıkların olması, giyilebilir nesnelere sızılarak, vücut aktivitelerinden, rahatsızlıkların tespit edilerek siber cinayetlerin ortaya çıkması gibi örnekler IoT'nin güvenlik eksiklikleri olarak değerlendirilebilir.

Özetlersek

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 IoT nesneleri ile artacaktır.

IoT’nin etkin kullanımının sağlanması için birçok çalışma yapılmaktadır. Özellikle IoT’nin etkin kullanımının sağlanması için yeni nesil kablosuz ağ teknolojileri ve protokol tasarımı çalışmaları yapılmaktadır. IoT’de TCP protokolü uçtan uca iletişimde doğası gereği verimli kullanılamamaktadır. Ayrıca IoT de akıllı nesneler tarafından değiştirilen trafik karakteristiğinin gelecekte nasıl olacağı tam olarak bilinmemektedir. IoT’nin etkin kullanımının sağlanması için protokollerin ve standartların geliştirilmesi açısından akademik ve ticari çalışmalar yapılmaktadır.

Kaynakça

- Gündüz, M. Z., & Daş, R. (2018). Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları. *Pamukkale University Journal of Engineering Sciences*, *24*(2).