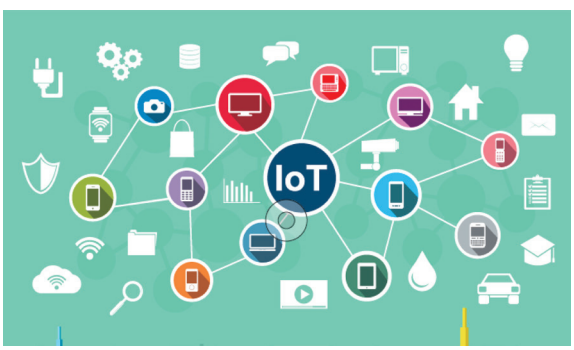
EDİTÖRDEN

Dr. Mehmet Kara
Elektronik ve Haberleşme Mühendisi
mehmet.kara@unwomen.org

NESNELERİN İNTERNETİ

Nesnelerin İnterneti (Internet of Things-IoT) dünya çapında milyarlarca fiziksel cihazın veya sensörün birbirine bağlanması, veri aktarması ve veri paylaşımını ifade eder. Günümüzde bu iletişim ve veri paylaşımı çok ucuzlayan bilgisayar çipleri ve geliştirilen haberleşme protokolleri (TCP/IP, Wi-Fi, GSM, RF-ID, Bluetooth vb.) sayesinde mümkün olmaktadır. Çok farklı cihaz ve sensörlerden toplanan bu veriler, büyük veri analizi (Big Data Analyze), yapay zeka (Artificial Intelligence-AI) yöntemleri ile insan kullanılmadan analiz edilip sistemlerin veya iş süreçlerinin daha verimli, etkin ve güvenli kullanılmalarını sağlamaktadır. Veri toplanan cihazlar hap kadar küçük bir sensörden çok büyük bir uçağa kadar değişiklik gösterebilmektedir.

Temel nesnelere sensör ve zeka ekleme fikri 1980'ler ve 1990'lar boyunca tartışıldı. Muhtemelen bilimkurgu kitaplarında okuduğumuz çok daha eski ataları da vardır. Ancak bazı erken projelerin dışında ilerleme yavaş olmuştur. Çünkü bunun için gerekli olan teknolojiler henüz yeterince olgunlaşmamıştı. Örneğin 1991 yılında Cambridge Üniversitesi'ndeki yaklaşık 15 akademisyenin kahve makinesini görebilmek için kurduğu kameralı sistem o günün koşullarında değerlendirildiğinde ufuk açıcı bir uygulamaydı. Kurulan sistem, kahve makinesinin görüntüsünü dakikada üç kez akademisyenlerin bilgisayar ekranlarına gönderiyordu. Böylelikle akademisyenler kahve olup olmadığını görebiliyorlardı. Çevrimiçi ve gerçek zamanlı olması sebebiyle "Nesnelerin İnterneti" kavramının ilk örneği olarak değerlendirilebilir.



Şekil 1. Nesnelerin İnterneti

Milyarlarca cihazı uygun maliyetle birbirine bağlamak için öncelikle, hepsi tek kullanımlık olacak kadar ucuz ve yeterince güçlü işlemcilere ihtiyaç vardı. RFID etiketlerinin (kablosuz olarak iletişim kurabilen düşük güçlü çipler) benimsenmesi, geniş bant İnternet ve hücresel ve kablosuz ağların artan kullanılabilirliği ile birlikte bu sorunun bir kısmının çözülmesini sağlamıştır. Diğer şeylerin yanı sıra dünyanın (veya aslında bu galaksinin) ihtiyaç duyacağı her cihaz için yeterli IP adresi sağlaması gereken IPv6'nın benimsenmesi de IoT'nin ölçeklenmesi için gerekli bir adımdı. Diğer türlü hali hazırda yaygın olarak kullandığımız ve İnternet'teki cihazlara temel kimlik sağlayan IPv4 adresi 32 bitten oluşuyor. Bu da ancak 2^{32} cihazın (yaklaşık 4.3 milyar) adreslenmesine olanak tanıyordu.

Kevin Ashton 1999'da 'Nesnelerin İnterneti' ifadesini RFID kullanarak tedarik zincirinde ürün izlemenin iyileştirilmesi için kullanılacak yöntemlerin ele alındığı bir sunumda kullandı. Ancak teknolojinin bu vizyonu yakalaması en az 10 yıl aldı. Çünkü o yıllarda çipler çok büyük ve hantaldı, ayrıca yeterince iletişim protokolü yoktu. Bu yüzden nesnelerin etkili bir şekilde iletişim kurmasının bir yolu yoktu.

2008-2009'da, IoT ifadesi küçük bir uzman grubunun kullanımının çok ötesine geçti, tüm nesnelerin birbirleriyle ve insanlarla iletişimini ifade eden bir kavrama dönüştü. Günümüzde akıllı evler, akıllı fabrikalar, akıllı şehirler, akıllı arabalar hepsi veri toplamak ve analiz etmek için IoT yaklaşımını kullanıyorlar.

IoT'nin işletmeler için faydaları, belirli uygulamaya bağlıdır; çeviklik ve verimlilik genellikle en önemli hususlardır. Buradaki fikir, işletmelerin kendi ürünleri ve kendi iç sistemleri hakkında daha fazla veriye erişmesi ve sonuç olarak değişiklik yapma konusunda daha fazla beceriye sahip olması gerektiğidir.

Üreticiler, ürünlerine performansları hakkında geribildirim gönderebilmeleri için sensörler ekliyorlar. Bu sayede takılan bileşenin ne zaman arızalanacağını tespit edilmesi ve hasara neden olmadan önce o bileşenin değiştirilmesine yardımcı olunmaktadır. Şirketler ayrıca sistemlerini ve tedarik zincirlerini daha verimli hale getirmek için bu sensörlerin ürettiği

verileri kullanabiliyorlar, çünkü sensörler sayesinde gerçekte neler olup bittiğine dair çok daha doğru ve güvenilir verilere sahip olmaktadırlar.

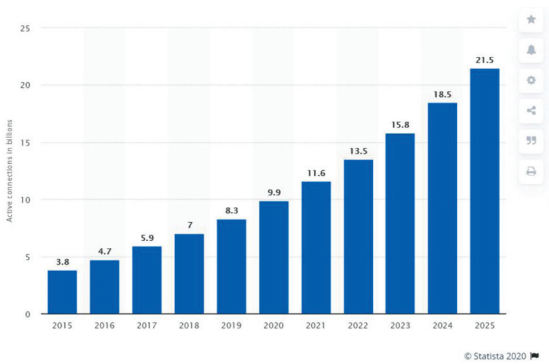
Örneğin İtalya'nın tren işletme operatörü Trenitalia, demiryolu taşımacılık sistemini iyileştirebilmek için 3 yıllık bir plan dahilinde IoT'yi kaldıraç olarak kullanarak, gelişmiş güvenilirlik ve tasarruf alanında önemli iyileştirmeler sağlamıştır. Tren işletmecisinde 1.500'den fazla tren seti çalışıyor ve günde 7.000'den fazla rota var. İş ortağı SAP ile birlikte tren parçalarının kullanımı, bakımı, tedariği konusunda sağlam bir IoT alt yapısı oluşturdu. Dinamik bakım modeli adı verilen bu modelde hem yere döşenen hem de parçalarda bulunan sensörlerden alınan veriler buluta taşınıp burada gerçek zamana yakın bir zamanda analiz edilerek parçaların durumları hakkında bilgiler elde edilerek, kaza veya sistem aksamasına meydan vermeden yıpranan parçalar değişimi veya gerekli bakımlar yapılarak verimlilik artışı sağlanmaktadır.

IoT projesine iyi bir başlangıç yapmak, uzun vadeli başarı için çok önemlidir, ancak IoT "herkese uyan tek boyutlu" bir çözüm değildir.

IoT teknolojilerinin entegrasyonu şirketler arasında önemli ölçüde farklılık gösterir ve endüstriler için doğru IoT çözümünü gerçekleştirmek, doğru bir IoT mimarisi gerektirir. Bu da içinde çözüm odaklı bir düşünce ile yapılabilir.

IoT kullanımı ve bütçesi her yıl artmaktadır. Son yıllarda dijital dönüşüm Endüstri 4.0 ile bu oran daha da yükselmiştir. Aşağıdaki Şekil 2'de Sista'nın veri ve tahminleri doğrultusunda yıllara göre IoT cihaz sayıları görülmektedir.

Diğer taraftan IoT'ye harcanan para her geçen yıl artmaktadır. IDC'ye göre dünya genelinde IoT harcamalarının 2020'de 742 milyar dolara ulaşacağı ve 2022'de 1 trilyon doları geçeceği tahmin edilmektedir.



Şekil 2. Yıllara Göre IoT Cihaz Sayıları

Uygulama Alanları

Sensörlerden veri toplansa da bunların bütüncül bir bakış açısı ile işlenip, anlamlandırılıp cihazlara uygun komutların gönderilmesi gerekmektedir. Bu işlemin etkin ve verimli yapılabilmesi için IoT cihaz ve sensörleri, yenilikçi teknoloji ve uygulamalarla entegre olarak çalışmalıdır.

Etrafımıza baktığımızda hayatımızı kolaylaştırmaya çalışan birçok teknoloji ve uygulama olduğunu görüyoruz. İnsan, makine, doğa başta olmak üzere etrafımızda var olan her şeyle iletişim içinde olmamız; onlardan veri toplamamız, işlememiz, anlamlı sonuçlar üretmemiz ve bu sonuçları sistemler ve insan hayatını kolaylaştırmak için kullanmamız gerekiyor. Günümüzde yapay zeka, büyük veri analizi, dijital dönüşüm, Endüstri 4.0 bunları sağlamakta kullanılan ana araç ve yöntemler. Bu çözümlerin büyük oranda kesişim kümeleri bulunmaktadır. Bunların her birini kısaca tanıttıktan sonra IoT ile ilişkilerini açıklamak faydalı olacaktır.

Yapay Zeka

Temelinde IoT, İnternet bağlantısı aracılığıyla durum hakkında veri toplamak ve komut vermek istenen makinelere yerleştirilmiş sensörlerdir. IoT, bu veri toplama ve komut verme bağlantısında; oluşturma, iletişim, toplama, analiz etme ve harekete geçme adı verilen beş temel adımı takip eder. Harekete geçirme kaçınılmaz olarak analize bağlıdır. Bu nedenle, IoT'nin hangi davranışı sergileyeceği analiz aşamasında belirlenir. Yapay Zeka (Arficial Intelligency-AI) teknolojisinin rolü bu noktada ortaya çıkmaktadır.

IoT sensörleri veri sağlarken AI bunları hızlı ve verimli bir şekilde analiz edip doğru kararın verilmesinde kilit rol oynar. Burada tek bir sensörden gelen değil yüzlerce sensörden gelen, farklı formattaki verinin analiz edilip, ona göre en iyi kararın verileceği göz önünde bulundurulmalıdır. İşte bu büyük ve karmaşık verinin işlenmesinde AI kullanılmaktadır.

Şekil 3. IoT ve Yapay Zeka

Tesla'nın sürücüsüz arabaları, IoT ve AI'nın birlikte çalışmasına iyi bir örnektir. Yapay zekanın gücüyle, sürücüsüz arabalar, çeşitli koşullarda yayaların ve çevresel etmenlerin davranışını tahmin eder. Örneğin, yol koşullarını, trafik durumunu, hava durumunu ve diğer faktörleri algılayarak her seferinde en etkin sürüş hızını belirleyebilirler. Burada önceki deneyimlerden de yararlanılacağı unutulmamalıdır.

Endüstri 4.0

Alman Ticaret ve Yatırım kurumu (GTAI), Endüstri 4.0'ın, "entegre sistemlerin sibernetik sistemlere teknolojik evrimini" temsil eden bir yaklaşım olduğunu belirtiyor. Bu tanım, Endüstri 4.0, üretim sistemleri ve onları oluşturan nesnelerin basitçe birbirine bağlanması olarak düşünülmemelidir. Bunun yerine dijital alanda fiziksel bilginin toplanması, analiz edilmesi ve doğru eylemin gerçekleştirilmesi olarak anlaşılmalıdır. IoT, Endüstri 4.0'ın temel sütunu olarak görülmelidir. Daha çok endüstriyel otomasyona odaklanan adı sık sık insansız fabrikalarla ifade edilen Endüstri 4.0 için temel veri toplama kaynağı cihazlar ve onların sensörleridir.

Aşağıdaki tabloda endüstriyel kontrol sistemleri ve bilgisayar ağları arasındaki temel farklılıklar yer almaktadır. Bu karşılaştırma IoT sistemleri için de geçerlidir.

Tablo 1. Bilgisayar Sistemleri ve Endüstriyel Kontrol Sistemleri

Kategori	Endüstriyel Kontrol Sistemi	Bilgisayar Ağı
Performans Gereksinimleri	• Gerçek Zamanlı • Düşük performans kabul edilebilir • Gecikme veya değişkenlik kabul edilemez • Erişim kontrol edilebilmeli	• Gerçek zamanlı değil • Tepki tutarlı olmalı • Yüksek performans ister • Yüksek gecikme veya değişkenlik kabul edilebilir • Sıkı erişim kontrolü gerekir
Elde Edilebilirlik Gereksinimleri	• İşlemlerden dolayı yeniden başlatma kabul edilmeyebilir • Yüksek elde edilebilirlik için yedek sistem gerekir • Devre dışı durumu planlanmalı	• Yeniden başlatma kabul edilebilir • Erişilebilirlik problemleri kabul edilebilir.
Risk Yönetimi Gereksinimleri	• Fiziksel dünyayı kontrol eder • İnsan güvenliği kritik • Hata toleransı kabul edilemez. • Önemli risk düzenleyici kurum gereksinimleri, çevresel etkiler vb.	• Veri yönetimi • Veri gizliliği ve bütünlüğü kritik • Hata toleransı yüksek • Önemli risk iş süreçlerinin aksaması
Kaynak Sınırlılığı	• Sistem endüstriyel prosesleri desteklemek için tasarlanır. • Güvenlik çözümleri gibi ek çözümler için yeterince bellek ve işlemci gücü yoktur.	• Sistem ek çözümleri bünyesinde barındıracak şekilde tasarlanmıştır.
Haberleşmeler	• Birçok standart ve özel protokolü destekler. • Kablolu, kablosuz, radyo gibi pek çok haberleşme ortamını destekler. • Ağ yapıları karmaşıktır.	• Standart TCP/IP protokol ailesi üzerinden çalışır.
Değişim Yönetimi	• Yazılım değişiklikleri başka bir ortamda test edildikten sonra ve planı olarak yapılmalı. • Artık desteklenmeyen bazı işletimi sistemleri olabilir.	• Yazılım değişiklikleri güvenlik politikalarına uygun olarak düzenli şekilde yapılabilir. • Güncellemeler genellikle otomatiktir.
Kategori	• Endüstriyel Kontrol Sistemi	• Bilgisayar Ağı
Servis Desteği	• Genellikle servis desteği sadece üretici tarafından verilebilir.	• Değişik firmalardan servis desteği alınabilir.
Ürün Yaşam Süresi	• Yaşam süresi 10-15 yıldır	• Yaşam süresi 3-5 yıldır
Ürünlerin Çalışma Ortamı	• Ürünler uzak, izole ve fiziksel olarak erişilmesi zor olan yerde bulunabilirler	• Ürünler kapalı ortamlarda ve kolay erişilen yerde bulunur

IoT ve Büyük Veri

IoT, makine parçaları veya çevre sensörlerden çıkan veriden çok daha büyük miktarda veri üretir. Bu, IoT'nin büyük veri analitiği projelerinin önemli bir itici gücü olduğu anlamına gelir çünkü şirketlerin geniş veri kümeleri oluşturmasına ve bunları analiz etmesine olanak tanır. Geliştiricilere bileşenlerinin gerçek dünyadaki durumlarda nasıl davrandığına dair büyük miktarda veri sağlanması, çok daha hızlı iyileştirmeler yapmalarına yardımcı olur. Örneğin bir şehirdeki sensörlerden toplanan veriler, şehir planlamacılarının trafiği daha verimli bir şekilde planlamasına yardımcı olabilir.

Bu veriler ses, video, sıcaklık veya diğer sensör okumaları, gibi birçok farklı formatta bulunabilirler ve iyi bir çıkarım için kullanılabilirler. IDC'nin Analistleri, IoT meta veri kategorisini, yönetilmesi ve kullanılması gereken, büyüyen bir veri kaynağı olarak ifade etmektedir. "Meta veriler, yapılandırılmamış içeriğe yapı getirmek için MongoDB gibi NoSQL veritabanlarına dışarıdan rastgele veriler eklenen verilere yeni anlayışla, zeka katacak, anlamlandıracak başlıca sistem adaylarıdır.

Şekil 4. IoT ve Büyük Veri

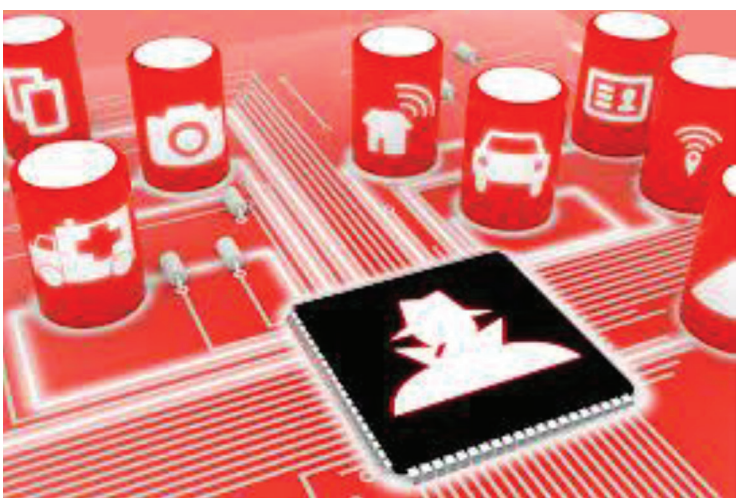
Özellikle IoT, büyük miktarlarda gerçek zamanlı veri sağlayacaktır. Cisco, IoT uygulamalarını destekleyen makineden makineye bağlantıların toplam 27,1 milyar cihazın yarısından fazlasına ulaşacağını ve 2021 yılına kadar küresel IP trafiğinin yüzde 5'ini oluşturacağını öngörüyor. Bu yüzden IoT cihazlarından gelen verilerin analizinin kapsamlı bir şekilde ele alınması gerekiyor.

IoT ve Güvenlik

Güvenlik, IoT ile ilgili en büyük sorunlardan biridir. Sensörler, çoğu son derece hassas verileri toplar. Örneğin bir akıllı ev uygulamasında kendi evinizde söylediklerinizi ve yaptıklarınız sensörler aracılığı ile toplanır ve iletilir. Bunu güvende tutmak, tüketici güveni için hayati önem taşımaktadır. Ancak IoT'nin güvenlik geçmişi son derece zayıf ve iyileştirmeye ihtiyacı var.

1980'li yılların ortalarından sonra İnternet'in yaygınlaşması ile birlikte bilgisayar ve ağ güvenlik olayları da görülmeye başlıyor. Sonrasında sürekli iyileştirmelerle günümüze kadar geliyor. Her ne kadar İnternet ortamı güvensiz dense de gerekli güvenlik önlemlerini alarak e-bankacılık, e-ticaret, e-devlet gibi çok kritik faaliyetleri İnternet üzerinden güvenli bir şekilde yapabiliyoruz. Ama malesef buradaki güvenlik önlemlerini ve tecrübeleri IoT sistemlerine bire bir uygulamak mümkün değil çünkü sistemlerin yapıları birbirinden çok farklı. Örneğin bir IoT sensöründe yüksek güçlü bir işlemci, hafıza olmadığı için güçlü bir şifreleme algoritması çalıştırılamaz, iletilecek veri miktarı çok yüksek olmadığı için TCP/IP gibi karmaşık ve büyük başlıklı bir iletişim protokolü kullanılamaz. Onun yerine daha az kaynak kullanan daha basit protokoller kullanılır. Sensör türleri ve iletişim kanalları farklı olduğu için çok sayıda özel protokol ve çözüm bulunmaktadır. Genellikle bunlar da yeterince güvenlik testinden geçmemiştir.

Yazılımlarda geliştirme doğasından gelen açıklıklar çıkar. Geliştiriciler de bunun için yama çıkarak açıklığı kapatırlar, ancak birçok IoT cihazı yamalanabilme yeteneğinden yoksundur, bu da kalıcı olarak risk altında oldukları anlamına gelir. Bilgisayar korsanları artık yönlendiriciler ve web kameraları gibi IoT cihazlarını aktif olarak hedefliyor çünkü doğalarında var olan güvenlik eksiklikleri onları tehlikeye atmayı ve büyük botnetlere dönüştürmeyi kolaylaştırıyor.



Şekil 5. IoT ve Güvenlik

Tasarım ve yazılım kusurları, buzdolapları, fırınlar ve bulaşık makineleri gibi akıllı ev cihazlarını bilgisayar korsanlarına açık hale getirmiştir. Araştırmacılar, kolaylıkla hacklenebilecek 100.000 web kamerası saptamış; İnternete bağlı bazı akıllı saatlerin, hackerlerin konumunu izlemesine, konuşmaları dinlemesine ve hatta kullanıcıyla iletişim kurmasına olanak tanıyan güvenlik açıkları içerdiği tespit edilmiştir.

Hükümetler buradaki riskler konusunda endişeleniyor ve bu konuda temel düzeyde regülasyonlar oluşturuyorlar. Bu regülasyonlarla cihazların benzersiz parolalara sahip olmasını, şirketlerin herkesin bir güvenlik açığını bildirebilmesi için herkese açık bir iletişim noktası sunmasını (ve bunlara göre hareket geçilmesini) ve üreticilerin cihazların ne kadar süreyle güvenlik güncellemelerini alacağını açıkça belirtmesini istiyorlar. Gelecekte bu alanda daha sıkı regülasyonlar uygulanması beklenmektedir.

Bu açıklıkların hepsi iş dünyası için de geçerli, ancak risk endüstriyel kontrol sistemlerinde daha yüksektir. Çünkü oradaki bir açıklık kritik altyapıların devre dışı kalmasına veya fiziksel olarak ciddi zarar görmesine neden olabilir. Endüstriyel makinelerin IoT ağlarına bağlanması, bilgisayar korsanlarının bu cihazları keşfetmesi ve bunlara saldırması riskini artırır. Endüstriyel casusluk veya kritik altyapıya yönelik yıkıcı bir saldırı, potansiyel risklerdir. Bu, işletmelerin bu ağların izole edildiğinden ve korunduğundan, sensörlerin, ağ geçitlerinin ve diğer bileşenlerin güvenliği ile veri şifrelemenin bir gereklilik olduğundan emin olmaları gerekir.

IoT, dijital dünya ile fiziksel dünya arasındaki boşluğu doldurur, bu da cihazlara saldırmanın fiziksel dünyada tehlikeli sonuçları olabileceği anlamına gelir. Bir elektrik santralındaki sıcaklığı kontrol eden sensörlere girmek, operatörleri felaketle sonuçlanan bir karar vermeye yönlendirebilir; sürücüsüz bir arabanın kontrolünü ele geçirmek de felaketle sonuçlanabilir. Bu yazının doğrudan konusu olmazsa bile bu tür açıklıklar sonucu oluşan zararlardan kimin sorumlu olacağına yönelik hukuksal süreçlerin üzerinde de çalışılması gerekir.

Güvenliğin diğer önemli bir boyutu veri mahremiyetidir. Yaptığınız her şey hakkında veri toplayan tüm bu sensörlerle IoT, potansiyel olarak veri gizliliği ve mahremiyeti için önemli bir baş ağrısıdır. Akıllı evi ele alalım: Ne zaman uyandığınızı (akıllı kahve makinesi etkinleştirildiğinde) ve dişlerinizi ne kadar iyi fırçaladığınızı (akıllı diş fırçanız sayesinde), hangi radyo istasyonunu dinlediğinizi (akıllı hoparlörünüz sayesinde) söyleyebilir, ne tür yiyecekler yediğiniz

Şekil 6. IoT ve Veri Mahremiyeti

(akıllı fırınınız veya buzdolabınız sayesinde), çocuklarınızın ne düşündüğü (akıllı oyuncakları sayesinde) ve sizi kimin ziyaret edip evinizin önünden geçeceği (güvenlik kameraları sayesinde) kayıt altına alınacaktır. Şirketler ilk etapta size akıllı nesneyi satarak para kazanacak olsa da, IoT iş modeli muhtemelen bu verilerin en azından bir kısmını satmayı da içerir. Bu yüzden veri mahremiyeti IoT sistemlerinde dikkatle ele alınması gereken husustur.

Sonuç

Sistemleri izleme, iş süreçlerini iyileştirme, daha doğru karar vermeyi sağlamada temel teknolojilerden bir olan IoT, fabrikalar, arabalar, bilgi sistemleri, sağlık sistemleri, taşıma sistemleri, haberleşme sistemleri, endüstriyel kontrol sistemleri gibi kritik altyapılarda artarak kullanılacaktır. Her ne kadar bu sistemlerin işlemci, bellek, iletişim protokolü gibi sınırlamaları olsa da bilgisayar sistemlerinde elde edilen tecrübelerle alana yönelik yeni çözümler artarak devam edecektir.

IoT, yapay zeka, büyük veri analizi, dijital dönüşüm Endüstri 4.0 alanındaki gelişmeleri de kullanarak hızlı ve etkili çözümler sunacaktır.

IoT sistemlerinde çok kritik veriler toplanıp, iletileceği için veri güvenliği ve mahremiyeti büyük önem arz etmektedir. IoT cihazlarındaki kaynak sınırlılığı, bilgi sistemlerinde kullandığımız güvenlik ve mahremiyet çözümlerini burada kullanmamızı engellemektedir. Bu da bilgisayar korsanlarının bu alana yönelmesini sağlamaktadır. Güvenlik risklerinin minimize edilmesi için IoT ürün geliştirme ve entegrasyon projelerinde, güvenlik ve mahremiyet, projenin en başında sürece dahil edilmeli ve tüm ürün, proje yaşam döngülerinde etkili bir şekilde uygulanmalıdır.