MUH441 Bilişimde Güvenlik – 1

Prof. Dr. Hasan Hüseyin BALIK

(14. Hafta)

İçerik

- 3.Yazılım Güvenliği ve Güvenilir sistemler
  - 3.1.Arabellek Taşması
  - 3.2.Yazılım Güvenliği
  - 3.3.İşletim Sistemi Güvenliği
  - 3.4. Bulut Güvenliği
  - 3.5. IoT Güvenliği

3.4. IoT Güvenliği

3.4.İçerik

- Nesnelerin İnterneti
- IoT Güvenliği

Nesnelerin İnterneti (IoT)

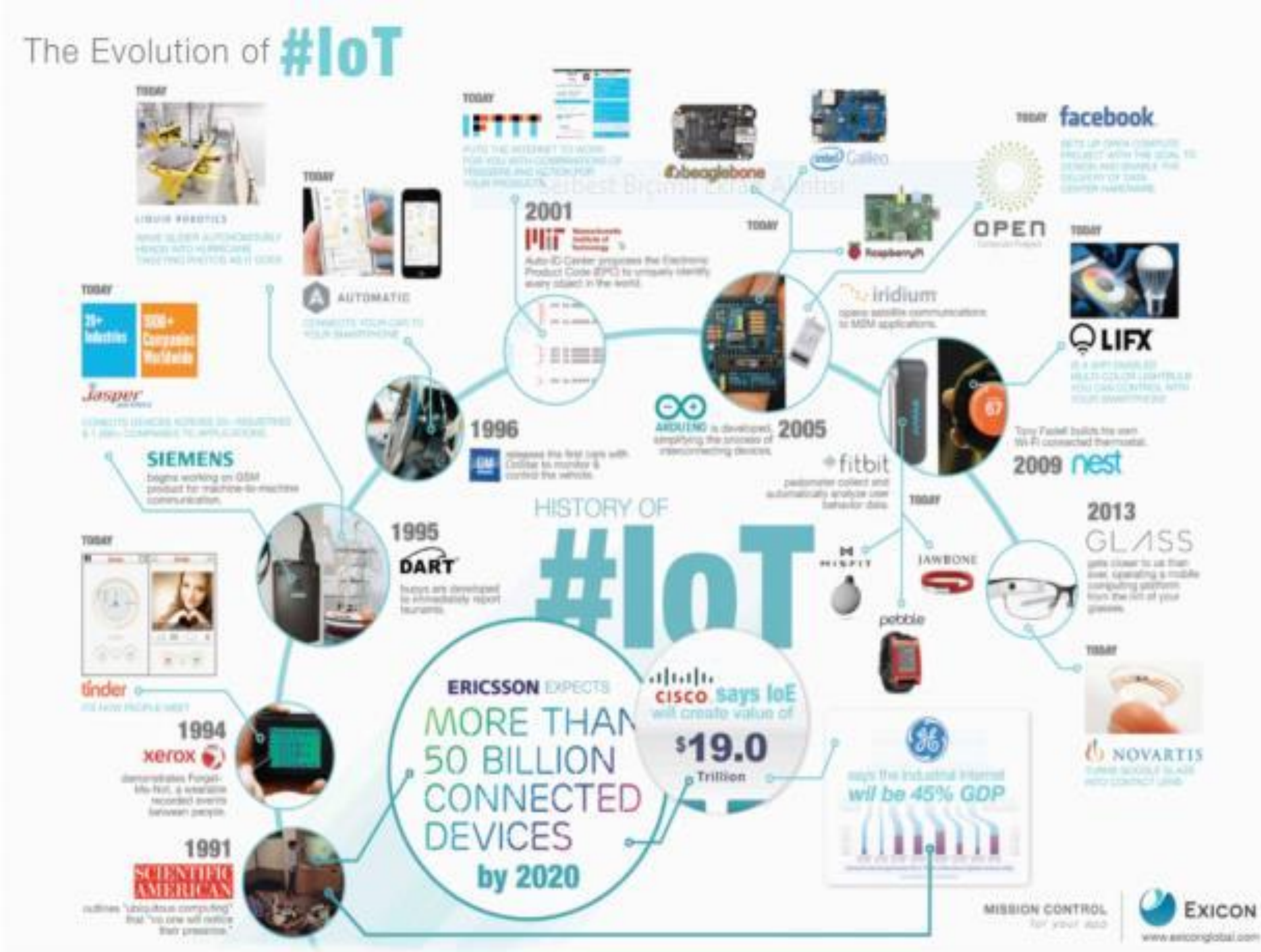
- IoT, cihazlardan küçük sensörlere kadar uzanan akıllı cihazların genişleyen ara bağlantısını ifade eden bir terimdir
  - Baskın bir tema, kısa menzilli mobil alıcı-vericilerin çok çeşitli araçlara ve günlük öğelere yerleştirilmesi, insanlarla nesneler arasında ve nesnelerin kendi aralarında yeni iletişim biçimlerine olanak sağlamasıdır.
  - İnternet, genellikle bulut sistemleri aracılığıyla karşılıklı bağlantıyı destekler
- Nesneler, daha büyük bir sistemin genel yönetimini oluşturmak için sensör bilgilerini iletir, çevrelerine göre hareket eder ve bazı durumlarda kendilerini değiştirir.
- IoT, öncelikle derinlemesine gömülü cihazlar tarafından yönlendirilir
  - Bu cihazlar, birbirleriyle iletişim kuran ve kullanıcı arayüzleri aracılığıyla veri sağlayan düşük tekrarlı veri yakalama ve düşük bant genişliğine sahip veri kullanım cihazlarıdır.
  - Yüksek çözünürlüklü video güvenlik kameraları, video VoIP telefonları ve birkaç diğerleri gibi gömülü aygıtlar, yüksek bant genişliğine sahip akış yetenekleri gerektirir

Evrim

Desteklenen son sistemlerle ilgili olarak, İnternet, IoT ile sonuçlanan kabaca dört kuşak dağıtımdan geçti

Bilgi Teknolojisi (BT)	Kurumsal BT çalışanları tarafından öncelikle kablolu bağlantı kullanılarak BT cihazı olarak satın alınan bilgisayarlar, sunucular, yönlendiriciler, güvenlik duvarları vb
Operasyonel Teknoloji (OT)	Tıbbi makineler, SCADA, proses kontrolü ve kiosklar gibi BT dışı şirketler tarafından inşa edilen yerleşik BT'ye sahip makineler/cihazlar, kurumsal OT çalışanları tarafından cihaz olarak satın alındı ve öncelikle kablolu bağlantı kullanıldı
Kişisel Teknoloji	Tüketiciler (çalışanlar) tarafından yalnızca kablosuz bağlantı ve genellikle birden çok kablosuz bağlantı biçimi kullanılarak BT cihazı olarak satın alınan akıllı telefonlar, tabletler ve e-Kitap okuyucular
Sensör/Aktüatör Teknolojisi	Tüketiciler, BT ve OT çalışanları tarafından, daha büyük sistemlerin bir parçası olarak genellikle tek bir biçimde, özel olarak kablosuz bağlantı kullanarak satın alınan tek amaçlı cihazlar

Genellikle IoT olarak düşünülen ve milyarlarca gömülü cihazın kullanımıyla öne çıkan dördüncü nesildir


The Evolution of #IoT
TODAY
IFTTT
2001
beaglebone
Galileo
TODAY facebook
OPEN
Raspberry Pi
iridium
LIFX
AUTOMATIC
Jasper
SIEMENS
1996
2005
fitbit
2009 nest
HISTORY OF
#IoT
1995
DART
2013
GLASS
MISFIT
JAWBONE
pebble
tinder
1994
xerox
1991
SCIENTIFIC AMERICAN
ERICSSON EXPECTS
MORE THAN
50 BILLION
CONNECTED
DEVICES
by 2020
cisco says IoE
will create value of
$19.0
Trillion
will be 45% GDP
NOVARTIS
MISSION CONTROL
EXICON

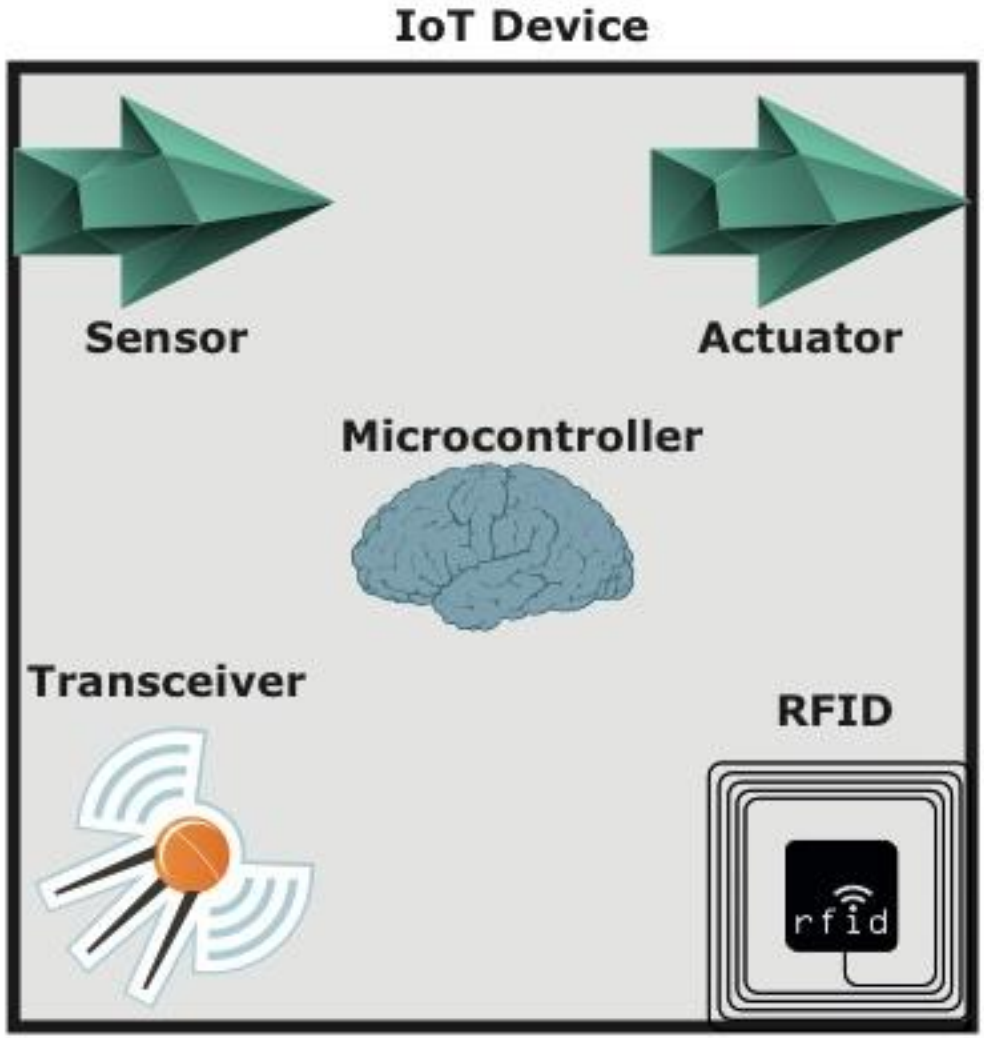
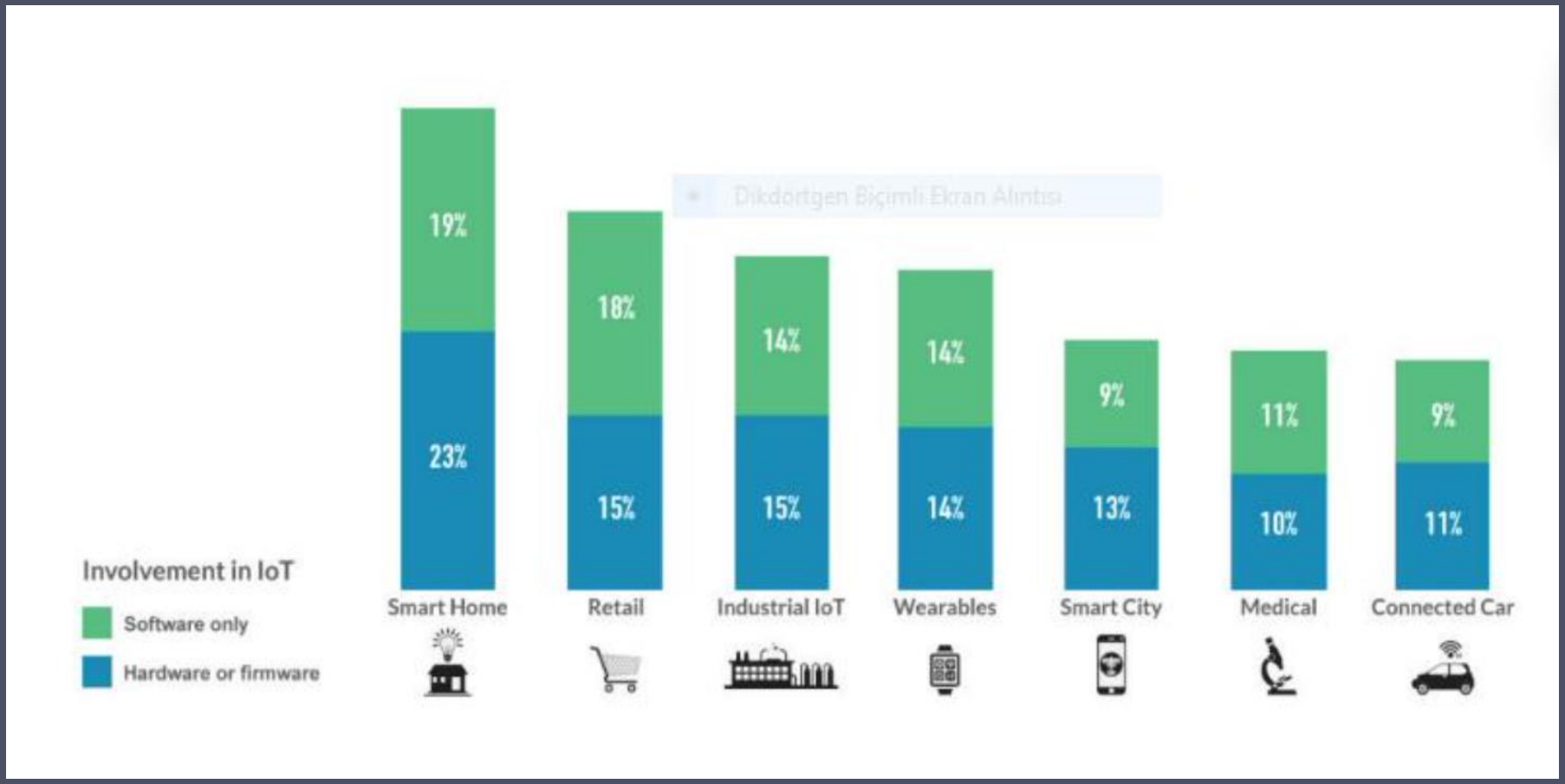


Figure 13.8 IoT Components


Involvement in IoT
Software only
Hardware or firmware
19%
23%
Smart Home
18%
15%
Retail
14%
15%
Industrial IoT
14%
14%
Wearables
9%
13%
Smart City
11%
10%
Medical
9%
11%
Connected Car

Çizelge 1. KAA katman mimarisi (layered architecture for WSN)

UYGULAMA KATMANI	Veri birleştirme, son kullanıcıyla etkileşim yapılır.
TAŞIMA KATMANI	Güvenilir veri taşıma işlemi bu katmanda yapılır.
AĞ KATMANI	Yönlendirme, ağ topoloji yönetimi yapılır.
VERİ BAĞI KATMANI	Hata Kontrolü, Veri çerçevesi tespit etme, çoğullama
FİZİKSEL KATMAN	Modülasyon, frekans ve kanal seçimi, sinyal işleme

Çizelge 2. Nesnelerin İnternetinde katman mimarisi (layered architecture for the Internet of Things)

UYGULAMA KATMANI	Son kullanıcıyla etkileşim kuran soyutlanmış çözümler.
ORTA KATMAN	API, Web Servis ve Bulut vb.
AĞ KATMANI	Kablolu ve kablosuz sistemlerden oluşur. Algılama katmanından gelen veriyi işleme ve iletme işlemleri.
ALGILAMA KATMANI	Ortam verisini algılama işlemleri. mekaniksel, elektriksel, elektronik ve kimyasal algılayıcılar

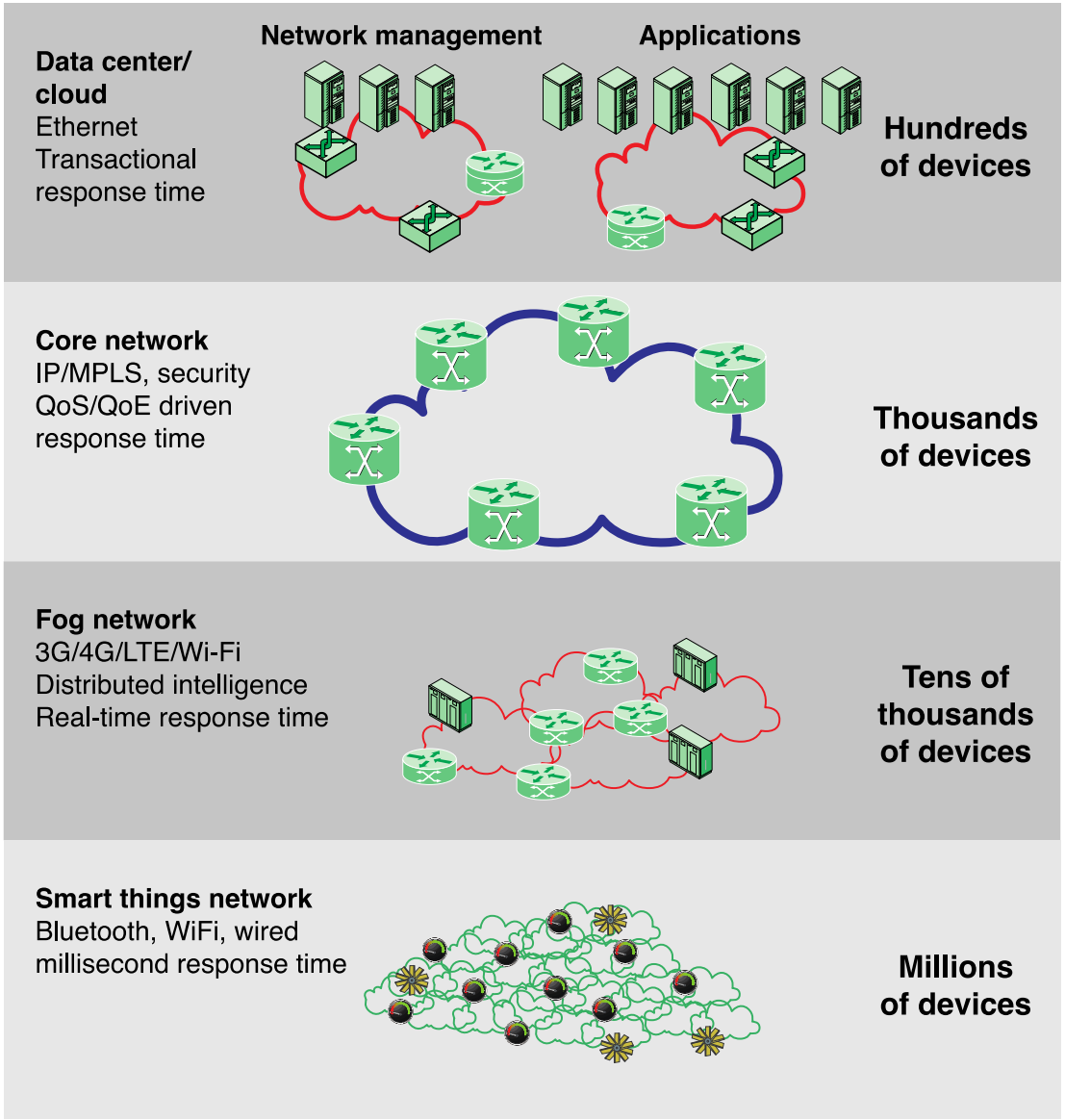


Figure 13.9 The IoT/Cloud Context

Edge-Kenar

Tipik bir kurumsal ağın ucunda (edge), sensörlerden ve belki de aktüatörlerden oluşan IoT özellikli cihazlardan oluşan bir ağ bulunur

- Bu cihazlar birbirleriyle iletişim kurabilir
- Bir sensör kümesinin tümü, verilerini daha üst düzey bir varlık tarafından toplanacak verileri toplayan bir sensöre iletebilir

Bir ağ geçidi (gateway), IoT özellikli cihazları üst düzey iletişim ağlarıyla birbirine bağlar

- Haberleşme ağlarında kullanılan protokoller ile cihazların kullandığı protokoller arasında gerekli çeviriyi yapar.
- Ayrıca temel bir veri toplama işlevi de gerçekleştirebilir

Fog-Sis

- Birçok IoT dağıtımında, dağıtılmış bir sensör ağı tarafından büyük miktarda veri üretilebilir
- Tüm bu verileri kalıcı olarak (veya en azından uzun bir süre için) IoT uygulamalarının erişebileceği merkezi depolamada depolamak yerine, genellikle sensörlere mümkün olduğunca yakın veri işleme yapmak istenir
- Bazen uç bilgi işlem düzeyi olarak adlandırılan şeyin amacı, ağ veri akışlarını depolama ve daha yüksek düzey işleme için uygun bilgilere dönüştürmektir.
- Bu seviyelerdeki işleme elemanları, yüksek hacimli verilerle başa çıkabilir ve veri dönüştürme işlemleri gerçekleştirerek çok daha düşük hacimli verilerin depolanmasına neden olabilir.
- Aşağıdakiler, sis hesaplama işlemlerinin örnekleridir:

Ölçme	Biçimlendirme	Genişletme/kod çözme	Damıtma/indirgeme	Değerlendirme

Fog-Sis

- Genellikle sis bilgi işlem cihazları, fiziksel olarak IoT ağının kenarına, sensörlerin ve diğer veri üreten cihazların yakınına yerleştirilir
- Sis bilgi işlem ve sis hizmetlerinin IoT'nin ayırt edici bir özelliği olması beklenir
- Sis bilgi işlemi, modern ağ oluşturmada bulut bilişimden zıt bir eğilimi temsil eder.
    - Bulut bilgi işlem ile, büyük, merkezi depolama ve işleme kaynakları, nispeten az sayıda kullanıcıya bulut ağ oluşturma tesisleri üzerinden dağıtılmış müşterilerin kullanımına sunulur.
    - Sis bilgi işlemiyle, çok sayıda bireysel akıllı nesne, IoT'deki uç cihazlara yakın işleme ve depolama kaynakları sağlayan sis ağı tesisleriyle birbirine bağlanır
- Sis bilgi işlemi, güvenlik, gizlilik, ağ kapasitesi kısıtlamaları ve gecikme gereksinimleri dahil olmak üzere binlerce veya milyonlarca akıllı cihazın etkinliğinin ortaya çıkardığı zorlukları ele alır
- Sis bilişimi terimi, sisin yere kadar alçakta durma eğilimindeyken bulutların gökyüzünde yüksekte olması gerçeğinden esinlenmiştir

Core-Çekirdek

- *Omurga ağı* olarak da adlandırılan *çekirdek ağ*, coğrafi olarak dağılmış sis ağlarını birbirine bağlamanın yanı sıra kurumsal ağın parçası olmayan diğer ağlara erişim sağlar
- Tipik olarak çekirdek ağ, daha fazla yedeklilik ve kapasite için çok yüksek performanslı yönlendiriciler, yüksek kapasiteli iletim hatları ve birden çok birbirine bağlı yönlendirici kullanır
- Çekirdek ağ ayrıca büyük veritabanı sunucuları ve özel bulut tesisleri gibi yüksek performanslı, yüksek kapasiteli sunuculara da bağlanabilir
- Çekirdek yönlendiricilerden bazıları, kenar yönlendiricileri olarak hizmet vermeden yedeklilik ve ek kapasite sağlayan tamamen dahili olabilir.

Bulut ve Sis Özelliklerinin Karşılaştırılması

	Cloud/Bulut	Fog/Sis
İşleme/depolama kaynaklarının konumu	Merkez	Kenar
Gecikme	Yüksek	Düşük
Erişim	Sabit veya kablosuz	Çoğunlukla kablosuz
Mobilite/Haraketlilik	Uygulanamaz	Evet
Kontrol	Merkezi/hiyerarşik (tam denetim)	Dağıtık/hiyerarşik (kısmi kontrol)
Servise erişim	Çekirdek (core) aracılığıyla	Kenarda (edge)/elde taşınan cihazlar ile
Kullanılabilirlik	%99,99	Son derece değişken/yüksek düzeyde gereksiz
Kullanıcı/cihaz sayısı	Onlarca/yüz milyonlarca	Onlarca milyar
Ana içerik oluşturucu	İnsan	Cihazlar/sensörler
İçerik üretimi	Merkezi konum	Herhangi yer
İçerik tüketimi	uç cihaz	Herhangi yer
Yazılım sanal altyapısı	Merkezi kurumsal sunucular	Kullanıcı cihazları

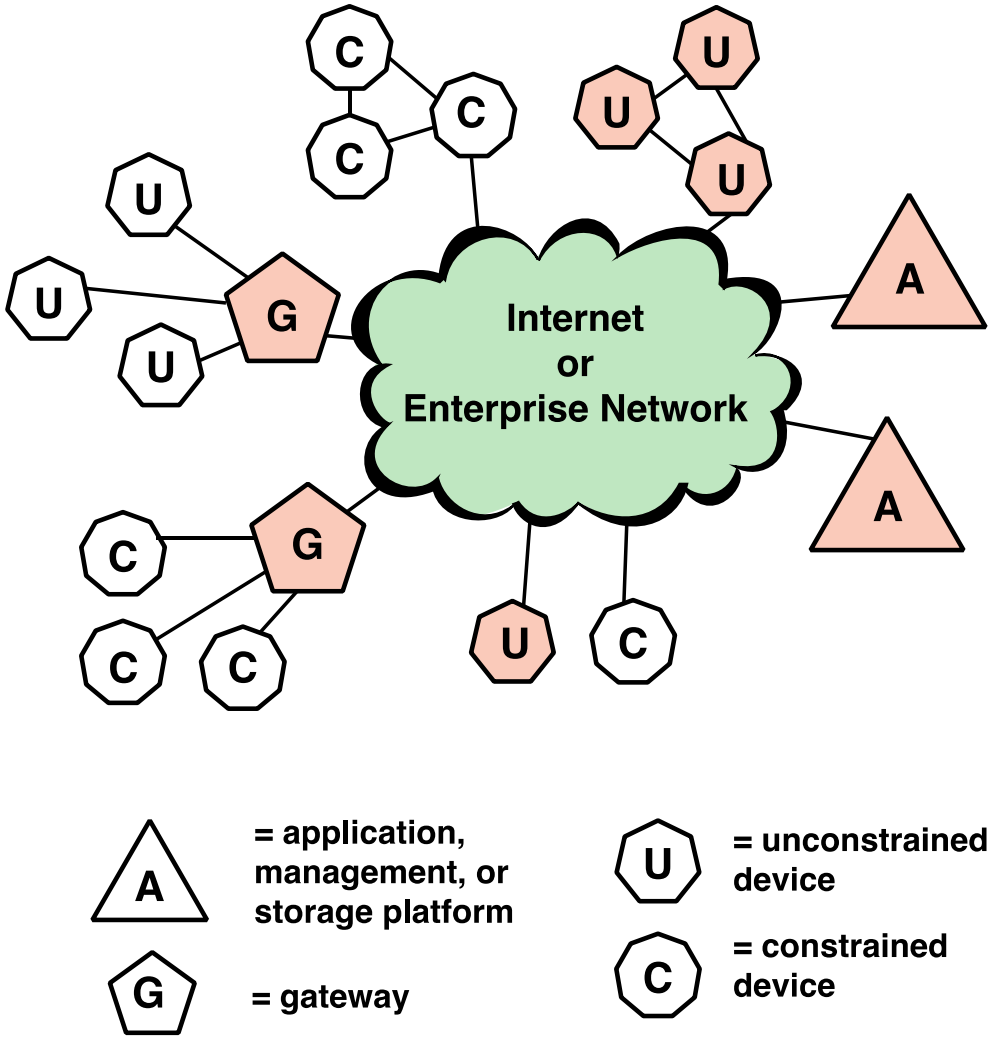


Figure 13.10 IoT Security: Elements of Interest

Yama Güvenlik Açığı

IoT cihazları da dahil olmak üzere gömülü sistemlerin güvenliği ile ilgili bir kriz noktası vardır

Gömülü cihazlar güvenlik açıklarıyla dolu ve bunları düzeltmenin iyi bir yolu yoktur

Çip üreticileri, ürünlerini olabildiğince hızlı ve ucuza üretmek için çaba sarfederler

Cihaz üreticilerinin odak noktası, cihazın kendisinin işlevselliğidir

Son kullanıcının sisteme yama uygulama imkanı olmayabilir veya olsa bile, yama işleminin ne zaman ve nasıl yapılacağı hakkında çok az bilgisi olabilir

Sonuç olarak, IoT'deki yüz milyonlarca internete bağlı cihaz saldırılara karşı savunmasızdır

Bu kesinlikle sensörlerle ilgili bir sorundur ve saldırganların ağa yanlış veriler eklemesine izin verir

Saldırganın makinelerin ve diğer cihazların çalışmasını etkileyebileceği aktüatörlerle potansiyel olarak daha ciddi bir tehdittir

IoT Güvenliği ve Gizlilik Gereksinimleri

- ITU-T Önerisi Y.2066, IoT için güvenlik gereksinimlerinin bir listesini içerir
- Gereksinimler, nesnelerin verilerinin yakalanması, depolanması, aktarılması, toplanması ve işlenmesi sırasındaki işlevsel gereksinimler ve ayrıca nesneleri içeren hizmetlerin sağlanması olarak tanımlanır
- Gereksinimler:
  - İletişim güvenliği
  - Veri yönetimi güvenliği
  - Hizmet sağlama güvenliği
  - Güvenlik politikaları ve tekniklerinin entegrasyonu
  - Karşılıklı kimlik doğrulama ve yetkilendirme
  - Güvenlik denetimi

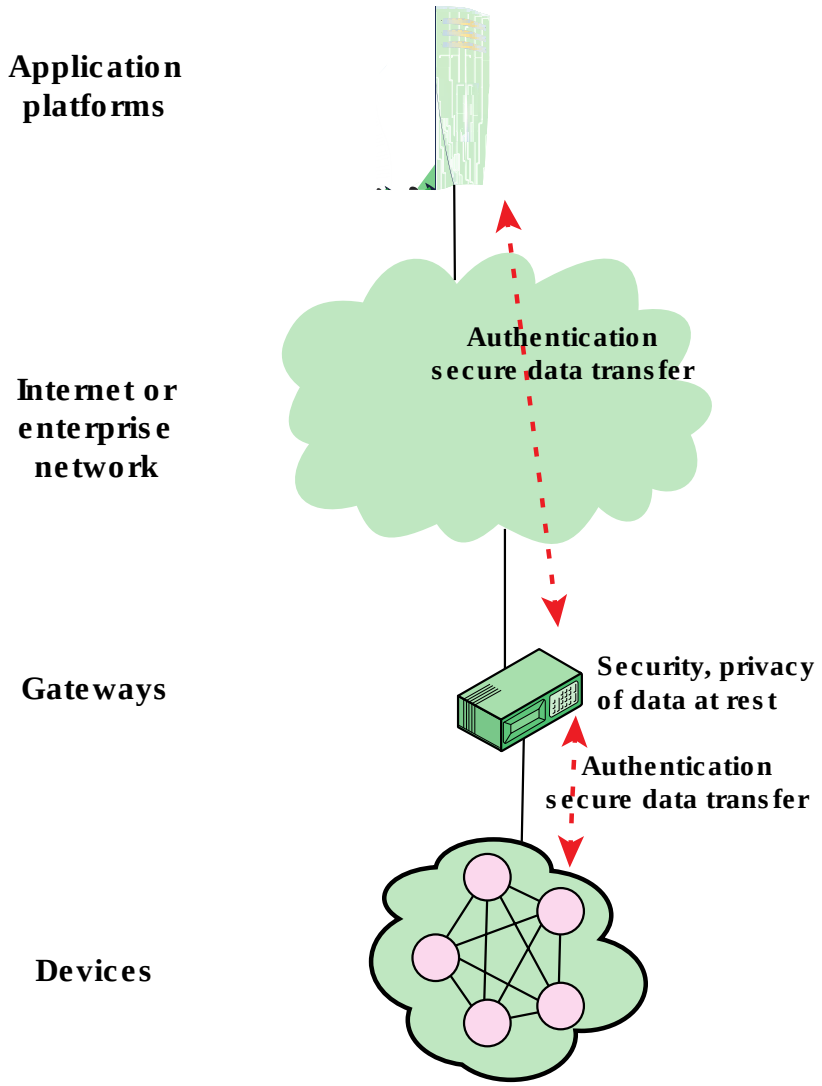


Figure 13.11 IoT Gateway Security Functions

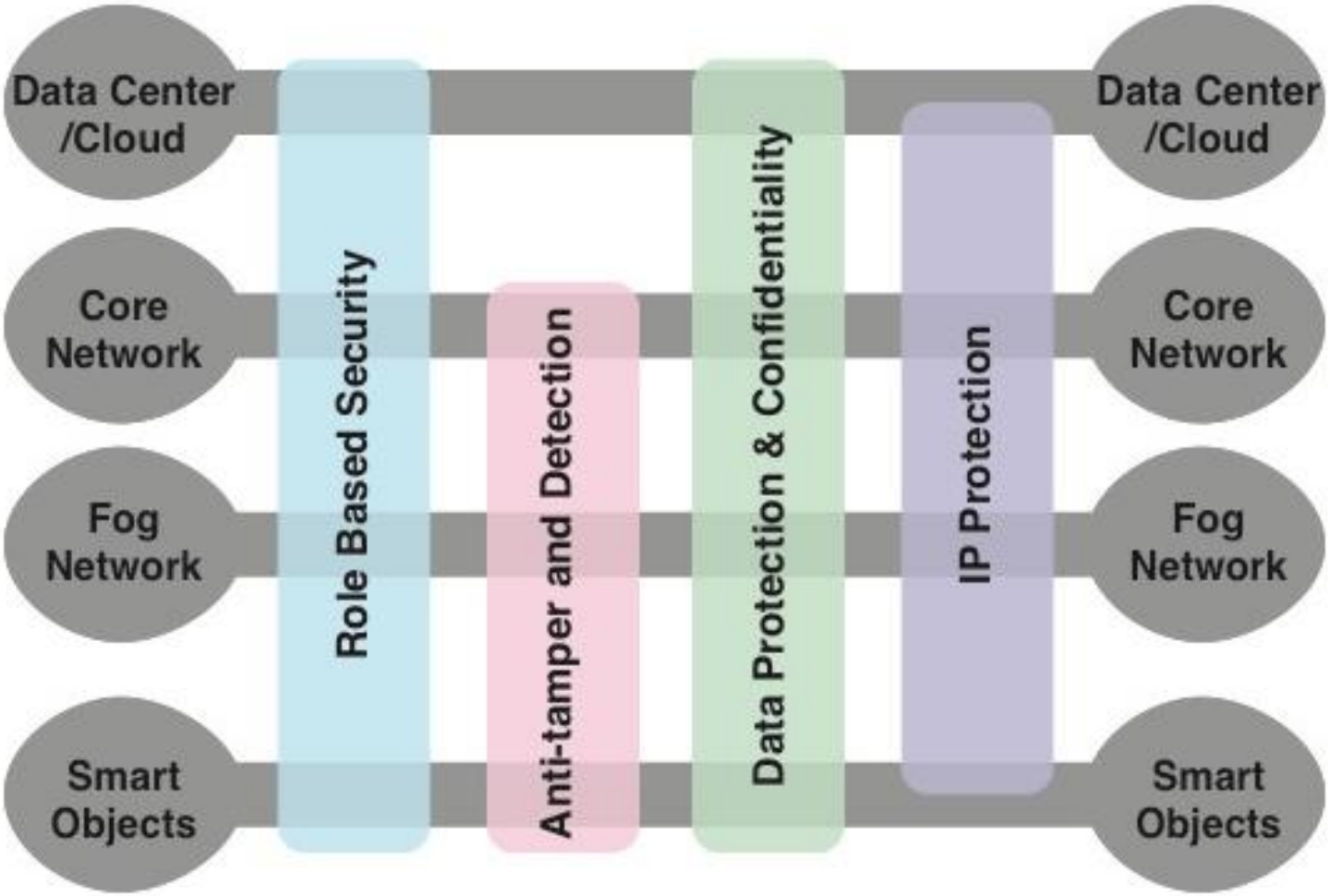


Figure 13.12 IoT Security Environment

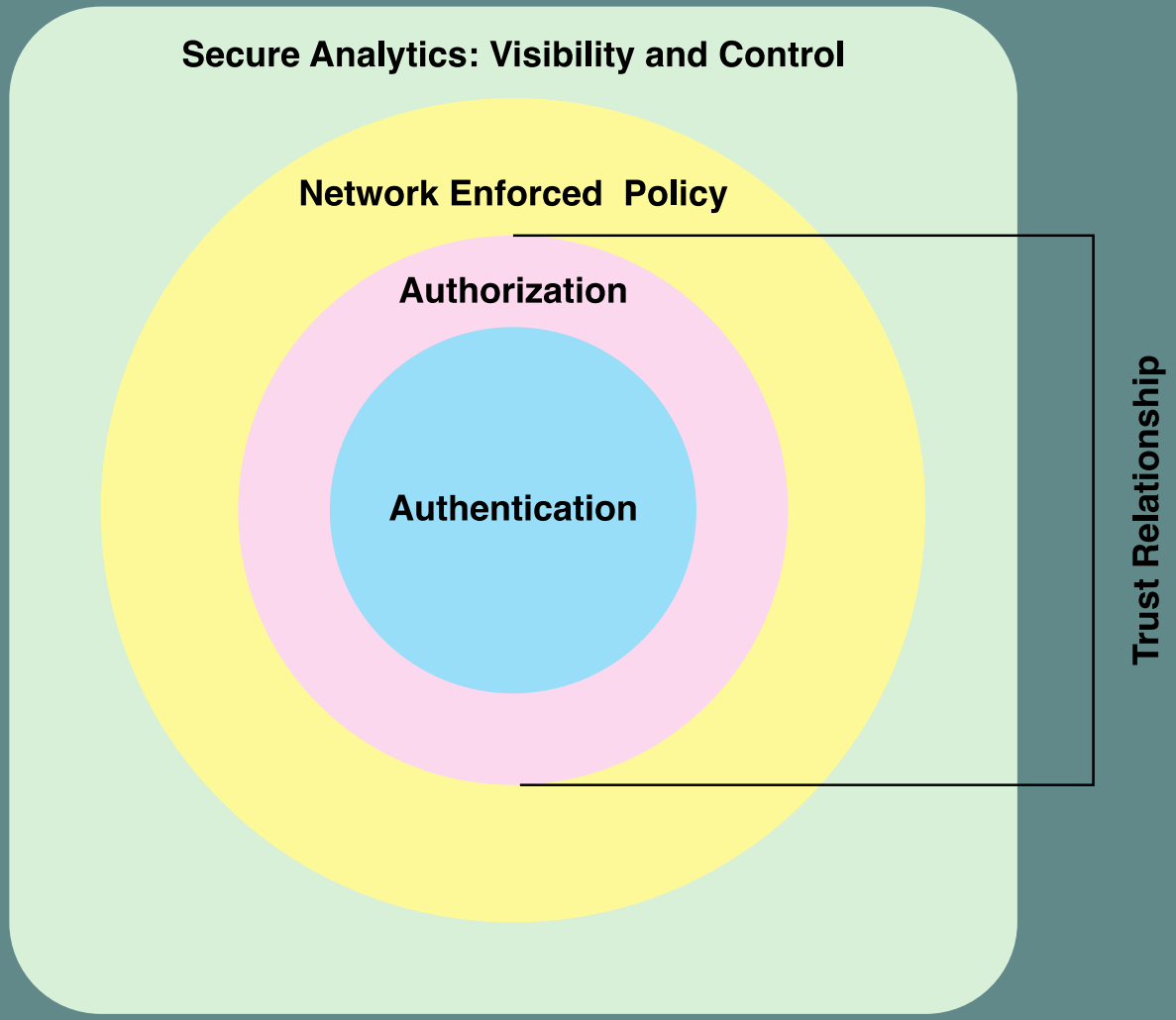


Figure 13.13 Secure IoT Framework

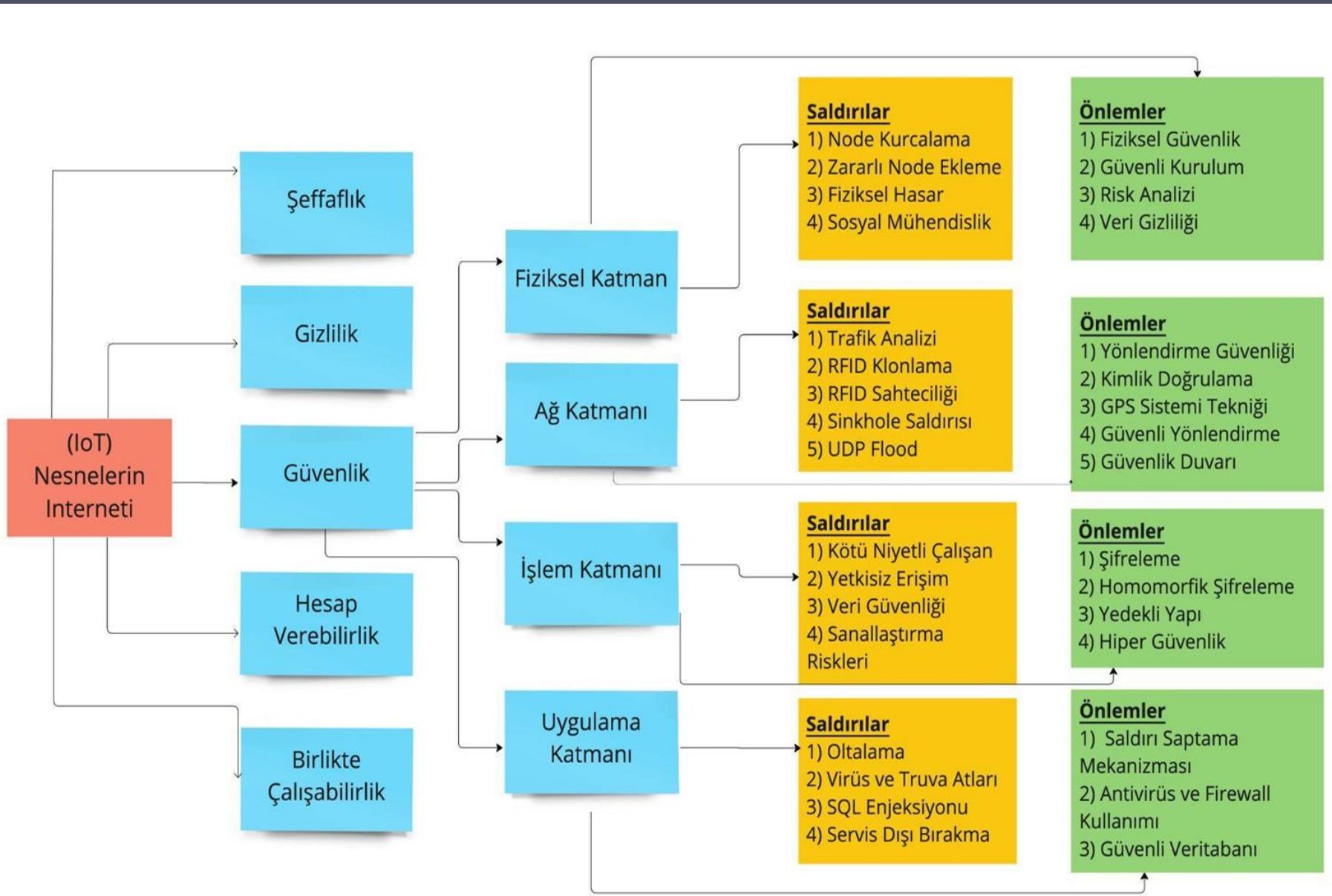
MiniSec

- MiniSec, TinyOS işletim sisteminin bir parçası olan açık kaynaklı bir güvenlik modülüdür
- Yüksek düzeyde güvenlik sunarken aynı zamanda enerji tüketimini düşük tutan ve çok az bellek kullanan bağlantı seviyesinde bir modül olacak şekilde tasarlanmıştır
- MiniSec gizlilik, kimlik doğrulama ve yeniden oynatma koruması sağlar
- MiniSec biri tek kaynaklı iletişim için uyarlanmış ve diğeri çok kaynaklı yayın iletişimi için uyarlanmış iki çalışma moduna sahiptir

MiniSec

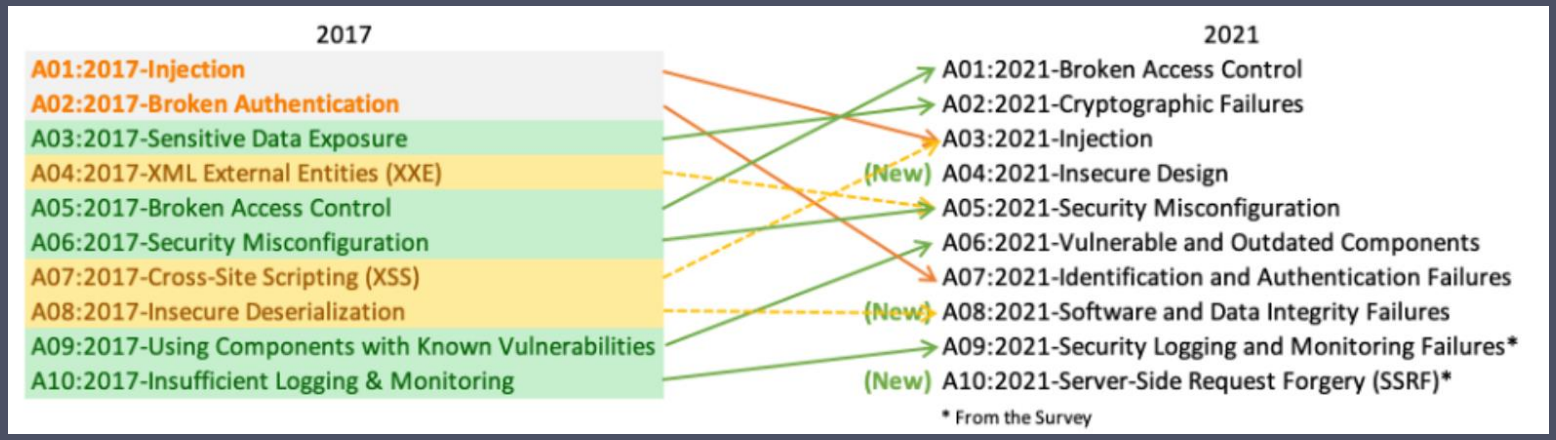

Veri doğrulama
Kayıp mesajlara karşı dayanıklılık
Gizlilik
MiniSec listelenen gereksinimleri karşılamak üzere tasarlanmıştır:
Düşük enerji yükü
Tekrar (replay) koruması
Tazelik

IoT Katmanlarına Göre Saldırılar



IOT VE SQL INJECTION SALDIRISI

- Cihazların ağ ortamında olması birçok güvenlik tehdidini beraberinde getirmektedir
- SQL Enjeksiyonu yöntemini; güvenlik saldırı türü olarak ele almış ve kötü niyetli bir kullanıcının arka planda veri tabanına SQL komutunun bir parçası olarak gönderdiği kullanıcı girdisi olarak tanımlamıştır.
- OWASP



SQL INJECTION TÜRLERİ

SQLI Saldırı Türleri	Amaç
1. Totoloji	Kontrolü atlamak için mantıksal olarak doğru ifadeyi kullanır
2. Uygunsuz sorgular	Hata mesajlarında döndürülen bilgileri kullanır
3. Birleşim sorguları	Orijinal sorguya kötü niyetli bir birleştirme sorgusu kodunun eklenmesine dayanır

SQLI Saldırı Türleri	Amaç
4. Piggybacking	Başka bir sorgu eklemek için noktalı virgül ";" karakterini kullanır
5. Zamanlama saldırıları	Zamanı kullanarak veri tabanı yapısını sınar
6. Boolean-tabanlı enjeksiyon	Mantıksal işlemlerle veri tabanı yapısını sınar

1. Totoloji

```
SELECT * FROM users
WHERE username = "admin" AND password = "" OR 1 = 1;
```

- Totoloji, koşullar ne olursa olsun her zaman doğru olan bir ifadedir.
- Bu yöntemin temel amacı, SQL sorgusuna doğru olarak yorumlanacak bir ifade eklemektir
- En yaygın olarak kullanıcı kimlik doğrulamasını atlamak veya bir veritabanı tablosunda kayıtlı verileri görüntülemek için kullanılır

2. Uygunsuz (Illegal) Sorgular

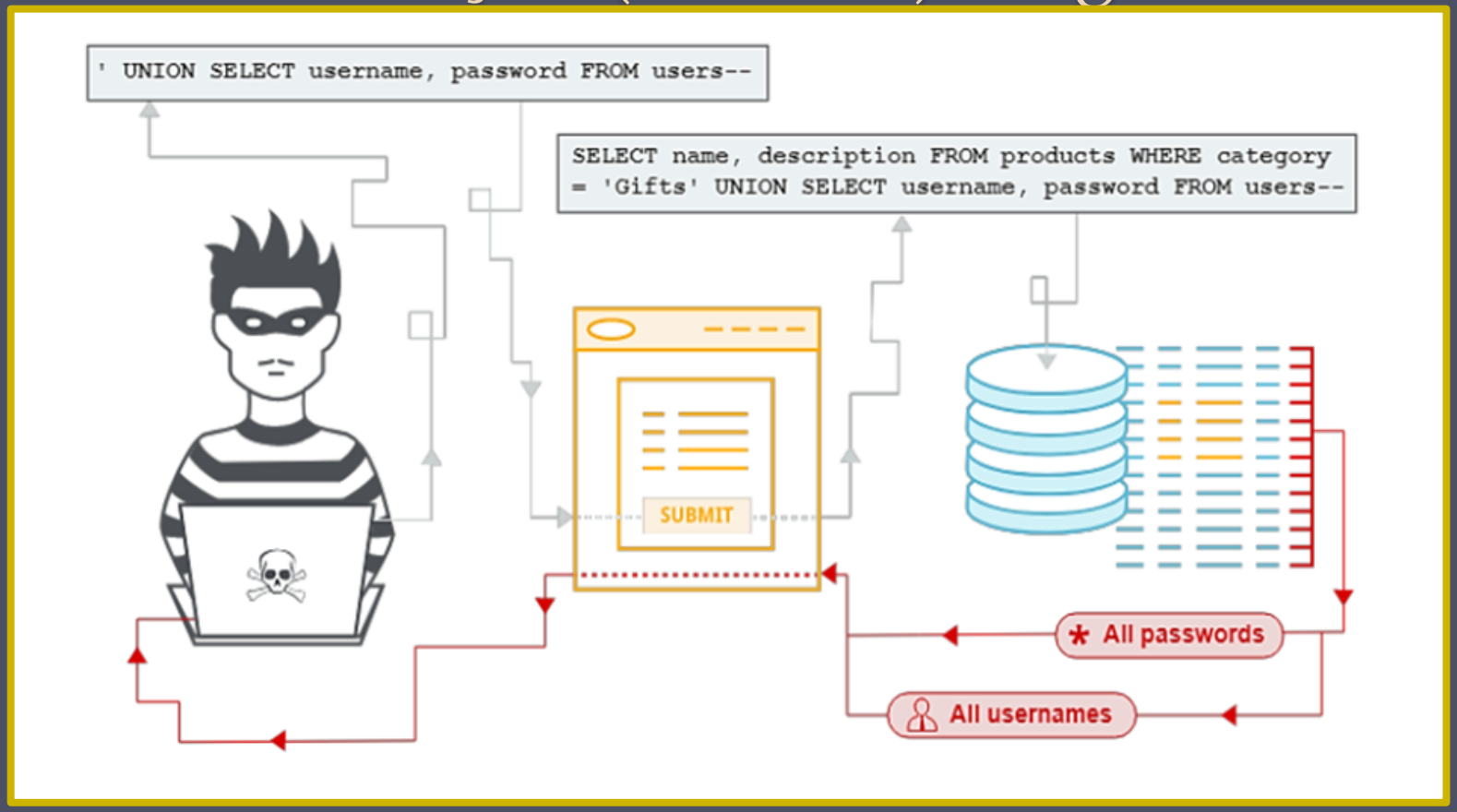
- Bu saldırının temel amacı, saldırganın uygulama tarafından kullanılan veritabanı hakkında önemli bilgiler toplamasıdır.
- Genellikle veritabanı yapısı, tablo adları, öznitelik veri türleri veya veritabanı türleri ve sürümleri hakkındaki bilgilerdir. Veritabanı hakkında toplanan bilgiler genellikle sonraki saldırılarda kullanılır.

```
SELECT * FROM users
WHERE username = ""AND EXTRACTVALUE ("" ,CONCAT ( " :" ,
(SELECT table_name FROM information_schema . tables WHERE
table_schema = database () LIMIT 0, 1))) -- " AND password = ""
```

- Sözdizimi, mantık veya yanlış veri türü nedeniyle hatalara neden olan koşullar genellikle sorgu olarak geçirilir.
- Sözdizimi hataları savunmasız parametreleri tanımlamak için kullanılır. Mantıksal hatalar tablo adları ve öznitelikler hakkında bilgi görüntüler.

```
Error: XPATH syntax error: ‘: users’
```

3. Birleşim (UNION) Sorguları



- Bu yöntem genellikle diğer tablolardan veri toplar. UNION deyimi kullanılarak birden fazla SQL sorgusu oluşturulabilir.
- Bir saldırgan, başlangıçta o tablodan bilgi sağlamak için tasarlanmamış olmasına rağmen başka bir tablodan veri talep edebilir. Bu etki, UNION komutu kullanılarak bağlanan birden fazla SELECT komutu eklenerek elde edilir.

4. Piggybacking/sırtlama

- Piggybacking sorgusu 'bir başkasının üzerinde ya da sanki arkasındaymış gibi' olarak tanımlanabilir
- Bu saldırının ana hedefi verilere erişim ve veri modifikasyonudur. En zararlı saldırılardan biridir çünkü bu şekilde herhangi bir SQL komutunu çalıştırmak mümkündür.
- Tek bir dizede birden fazla komuta izin veren veritabanları bu tür saldırılara karşı savunmasızdır

```
SELECT * FROM users
WHERE login = 'admin' AND pass = 1 "; drop table users
```

- Bu sorgunun çalıştırılması kullanıcılar tablosunu veritabanından silecektir. Aynı şekilde, belirli verilerin girilmesi, değiştirilmesi veya silinmesi gibi başka bir komutun iletilmesi de mümkündür.
- '"; SHUTDOWN -" komutunu göndererek servisin kullanılabilirliğini hedef alan bir DoS saldırısı gerçekleştirmek de mümkündür

ÖNLEMLER

- SQL sunucuda oluşacak hataların web formlarında görüntülenmesi engellenmelidir.
- Uygulamada web formlarına sorgu yazmak yerine, bu sorguları veri tabanı kısmında saklı yordam (Stored Procedure) olarak yazılması sağlanmalıdır.
- Kullanıcıların bilinçlendirilmesi ve teknik önlemler
- SQL enjeksiyon yönteminde kullanılabilecek sözcüklerin bir fonksiyon ile filtrelenmesi önemlidir.