



**SAKARYA ÜNİVERSİTESİ**  
**Bilgisayar ve Bilişim Bilimleri Fakültesi**  
**Bilgisayar Mühendisliği Bölümü**

**BSM 313**  
**NESNELERİN İNTERNETİ VE UYGULAMALARI**

(Internet of Things (IoT) and Applications)

**NESNELERİN İNTERNET'İNDE GÜVENLİK**

**Prof. Dr. Cüneyt BAYILMIŞ**



# Nesnelerin İnternetinde Güvenlik

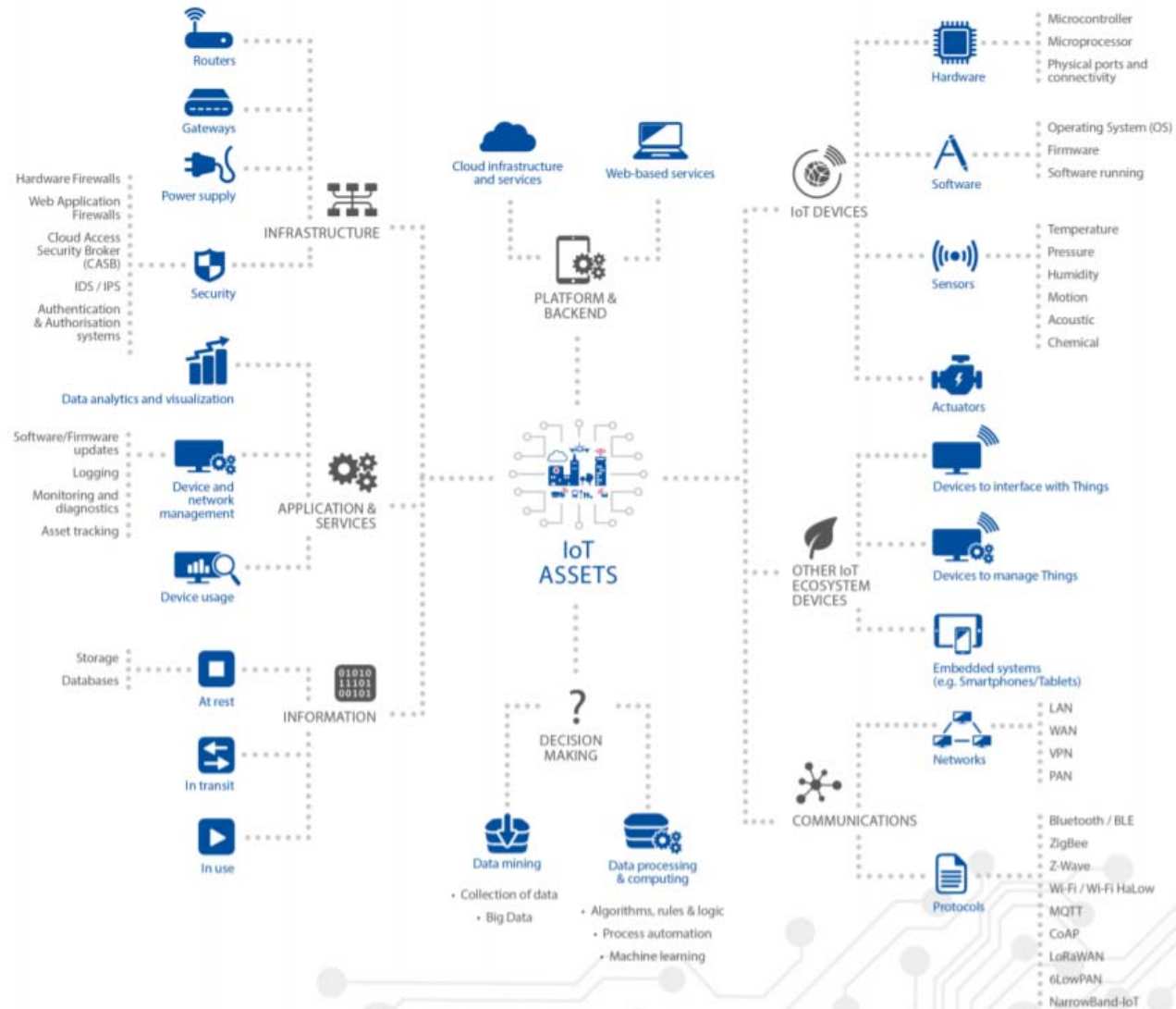
## (Security in IoT)

- ❑ Günümüzde iş, sosyal ve sağlık alanındaki uygulamaları ile hayatımızın her noktasında yer almakta olan IoT uygulamaları dikkate alındığında güvenlik büyük bir önem arz etmektedir.
- ❑ Değişik iletişim protokolleri aracılığıyla birbirleri ile haberleşebilen, algılama ve veri işleme yeteneğine sahip nesnelerin/cihazların oluşturduğu küresel bir ağ IoT mimarisi dikkate alındığında, sensörlerden, gömülü sistemlere, haberleşme teknolojilerinden bulut sistemlere tüm süreçlerde güvenlik ele alınmalıdır.



# IoT Uygulamalarındaki Bileşenler

## (Büyük Resim)



# Nesnelerin İnternetinde Güvenliğin Önemi

---

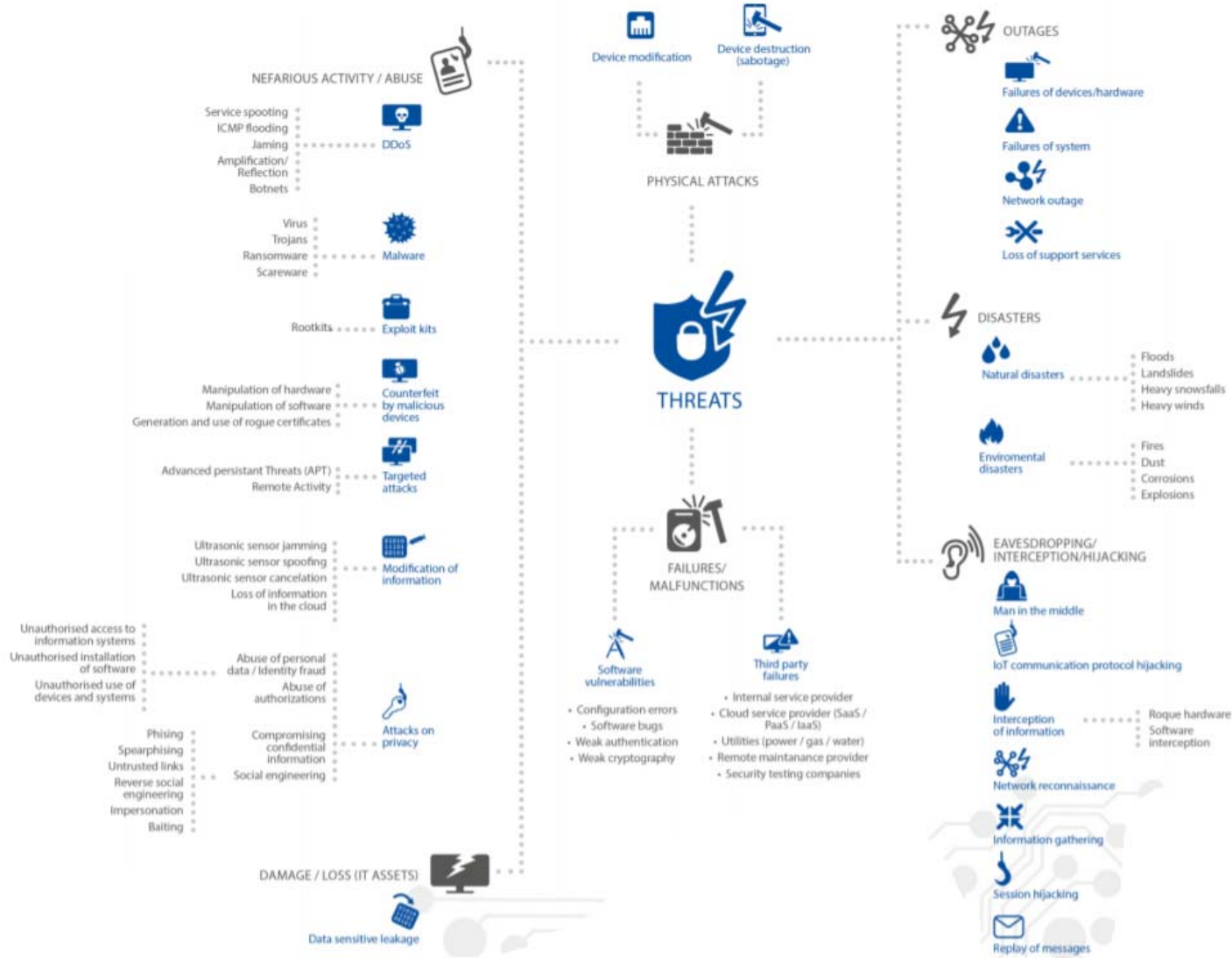
- ❑ Tamamen güvenli denebilecek IoT nesnesi (uygulaması) yoktur denmesi hatalı olmayabilir.
- ❑ Bunun nedenleri arasında şunlar sayılabilir:
  - IoT uygulamalarının 3. parti (third party) bileşen, donanım ve yazılımlar içermesi,
  - IoT uygulamalarının, ağlara (internet, WiFi, vb.) ve harici servislere bağımlılığı,
  - IoT uygulamalarında kullanılan protokollerin zafiyetleri,
  - IoT nesnelerinin tasarımında güvenliğe önem verilmemesi,
  - Güvenlikten önce IoT uygulamasının fonksiyonelliğine önem verilmesi,
  - Güvenlikle ilgili yatırımların sınırlı olması,
  - Sorumluklara yönelik yasal çerçevenin tam olarak ortaya konulmaması (eksikliği)

# IoT Güvenliğindeki Temel Zorluklar

---

- ❑ IoT nesnelerinin sınırlı kaynaklara sahip olması,
- ❑ Çok geniş saldırı yüzeyi ve IoT nesnelerinin geniş bir alanda konuşlandırılmaları,
- ❑ Standart ve yönetmeliklerin eksikliği,
- ❑ Tasarım süreçlerinde güvenliğin en öncelikli olmaması ve güvenliksiz (güvenlik süreçlerinin dikkate alınmadığı) geliştirme
- ❑ IoT güvenliği alanında uzman eksikliği,
- ❑ IoT cihazlarına güvenlik güncellemelerinin uzaktan yüklenme zorluğu,
- ❑ Sorumlulukların/yükümlülüklerinin açıkça belirtilmemesi,

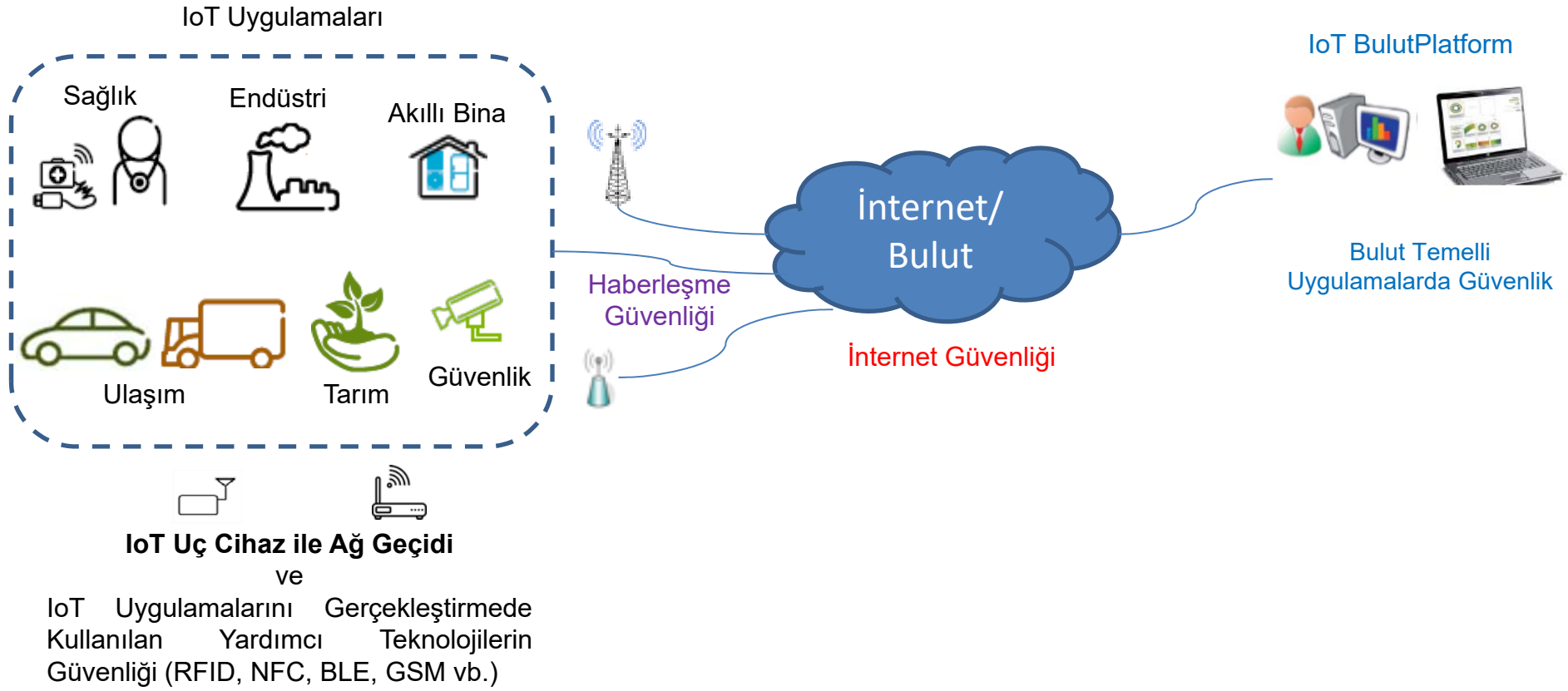
# IoT Uygulamalarındaki Bileşenlere Yönelik Tehditler



# OWASP IoT Güvenlik Riskleri

- ❑ OWASP (Open Web Application Security Project) dünya üzerindeki kurulu olan birçok platformda bulunan zafiyetlerin güncel sürümlerini yayınlamaktadır.
- ❑ IoT cihazların potansiyel güvenlik riskleri
  - Zayıf, tahmin edilebilir veya gömülü kodlanmış şifreler
  - Güvensiz ağ servisleri
  - Güvensiz ekosistem arayüzleri
  - Güvenli güncelleme mekanizması eksikliği
  - Güvensiz veya eski bileşenlerin kullanımı
  - Yetersiz gizlilik koruması
  - Güvensiz veri aktarımı ve depolanması
  - Cihaz yönetimi eksikliği
  - Güvensiz varsayılan ayarlar
  - Fiziksel güçlendirme eksikliği

# Nesnelerin İnternet'i Bileşenleri Seviyesinde Güvenlik İhtiyacı



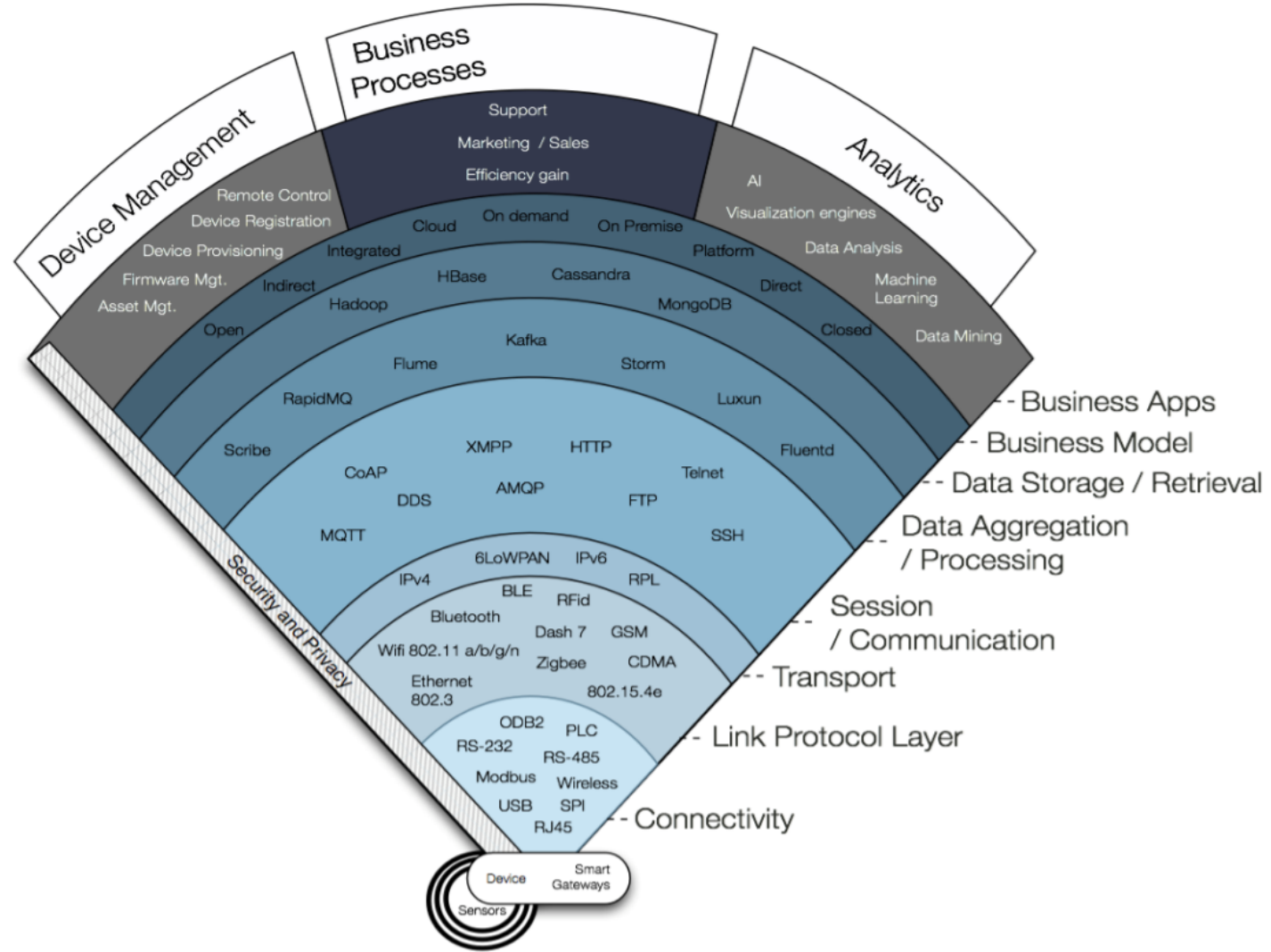
IoT uygulamalarının büyük bir çoğunluğu bulutta ya da IoT nesnesi üzerinde hassas bilgi içermektedir.

IoT uygulamalarında güvenlik konusunda birçok zaafiyet bulunmaktadır.





# IoT Nesnesi ile Kullanılan Teknoloji, Protokol ve Yazılımlar



# IoT Bileşenleri Seviyesinde Saldırı Türleri ve Riskler

❑ IoT nesneleri kapsamında akıllı telefon, gömülü sistem vb. birçok cihaz ile bu cihazların internete çıkmasını sağlayan ağ geçitleri akla gelmektedir.



❑ IoT uç cihaz ve ağ geçidi seviyesinde saldırı türleri ve riskler

- Veri sızıntısı (**data leakage**),
- Cihazlar üzerindeki savunmasız yazılımlar,
- Düşüm yayımı bozma (**jamming**),
- Fiziksel hasar (**efficiency**),
- Kötü niyetli düşüm yazılımı (**malicious node adware**)
- Hizmet engelleme saldırıları (**DoS**)

# IoT Bileşenleri Seviyesinde Saldırı Türleri ve Riskler

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

❑ Bağlantı (connectivity) seviyesinde güvenlik riskleri ve saldırılar (haberleşme ve internet)



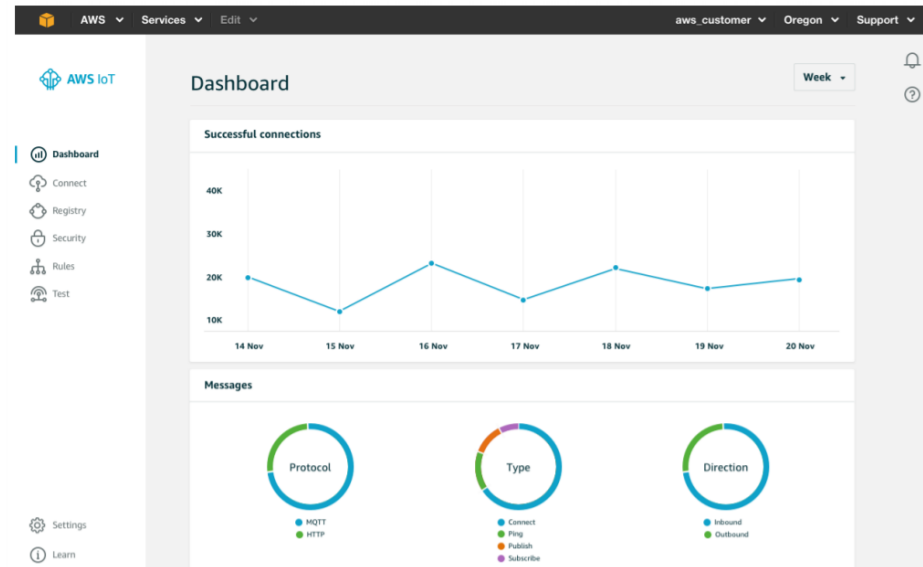
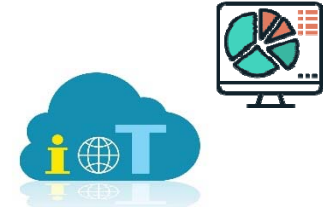
- Hizmet engelleme saldırıları (DoS)
- Ortadaki adam saldırısı (man in the middle attacks),
- İletişim güvenliği,
- İzinsiz erişim (unauthorized access),
- Sahte ağ mesajı
- Yönlendirme atakları

# IoT Bileşenleri Seviyesinde Saldırı Türleri ve Riskler

❑ IoT bulut bileşenleri olarak, veri depolama, web temelli servisler, cihaz yönetimi ve konfigürasyonu akla gelmektedir.

❑ IoT bulut seviyesinde güvenlik riskleri ve saldırılar

➤ Savunmasız web uygulamaları ve API'ler



# Birincil Güvenlik İlkeleri

---

❑ IoT uygulaması geliştirirken dikkat edilmesi gereken birincil güvenlik ilkeleri

- Mesaj gizliliği (*confidentiality*),
- Veri bütünlüğü (*data integrity*),
- Veri tazeliği/güncelliği (*data freshness*),
- Verimlilik (*efficiency*),
- Kendi kendini idare etme (*autonomy*)
- Kimlik doğrulama (*authentication*)

# Güvenlik Çözümleri

❑ Bir IoT sistem, sahada konuşlanmış, birbirleri ve internet ile haberleşen çok sayıda IoT nesnesinden oluşmaktadır.

❑ IoT uygulamalarında güvenliğin dört temel bileşenden oluştuğu kabul edilebilir

- IoT nesnesi kimlik doğrulama,
- Güvenli iletişim bağlantıları,
- Güvenli yazılımlar,
- Güvenli depolama



# KAYNAKLAR

---

## ❖ Temel Kaynaklar

- Prof. Dr. Cüneyt BAYILMIŞ ve Prof. Dr. Kerem KÜÇÜK, “**Nesnelerin İnternet’i: Teori ve Uygulamaları**”, Papatya Yayınevi, 2019.

## ❖ Diğer Kaynaklar

- **owasp.org**
- **C. Skoulodi, A. Malatras, ‘Introduction to IoT Security’, ENISA IoT Security Team, European Union Agency for Network and Information Security**
- P. Panahi, **C. Bayilmis**, U. Cavusoglu, S. Kacar, “Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications”, Arabian Journal for Science and Engineering, Vol. 46, 4015-4037, 2021.

