ioT - FİNAL

1 - iOT ve Location ilişkisinden bahsediniz

- Konum bilgisi, IoT sistemlerinde "bağlam" (context) oluşturur ve cihazların, nesnelerin veya olayların fiziksel dünyadaki yerini anlamayı sağlar.
- IoT, konum bilgisiyle kişiselleştirilmiş hizmetler sunar. Örneğin, bir akıllı telefon uygulamasının kullanıcının bulunduğu konuma göre restoran önerileri sunması veya bir navigasyon cihazının trafik durumuna göre rota önermesi.
- **Konum Belirleme (Localization):** konum genellikle önceden bilinmez ve cihazların veya nesnelerin konumunu belirlemek için yerelleştirme (localization) teknikleri kullanılır.
- - **Global Konum**:
    - **GPS (Küresel Konumlandırma Sistemi)**: En yaygın kullanılan yöntemdir. Cihazın enlem (latitude) ve boylam (longitude) bilgilerini sağlar. Ancak, GPS iç mekanlarda veya yoğun yapılarda sınırlıdır.
    - **UTM (Universal Transverse Mercator)**: Dünya yüzeyini bölgeler ve enlem bantları olarak böler, daha spesifik konum belirleme için kullanılır.
- **Göreceli Konum (Relative Positioning)**:
  - GPS gibi küresel bir referansa bağlı olmadan, cihazlar arasındaki mesafeleri veya yerel bir koordinat sistemine göre konumları hesaplar. Örneğin, bir IoT ağındaki sensör düğümleri (nodes) arasındaki mesafeler ölçülerek konum tahmini yapılır.
  - Bu yöntem, genellikle düşük güç tüketimi gerektiren veya GPS sinyalinin zayıf olduğu durumlarda tercih edilir (örneğin, iç mekan navigasyonu).
- **Sembolik Konum Bilgisi**:
  - Konum, koordinat yerine sembolik ifadelerle tanımlanabilir. Örneğin, "Ofis 354" veya "Otoyol 23'teki 17. mil işareti". Bu, özellikle insan odaklı uygulamalarda kullanışlıdır.
  - **IoT'de Konum Tabanlı Uygulamalar**:
  - **Akıllı Şehirler**: Trafik yönetimi, park yeri bulma, atık toplama gibi süreçlerde konum bilgisi kullanılır.
  - **Sağlık**: Hastaların veya medikal cihazların konumunu izlemek (örneğin, hastanelerde ekipman takibi).
  - **Tarım**: Tarım alanlarında sensörlerin konumlarına göre sulama veya gübreleme optimizasyonu.
  - **Perakende**: Mağaza içinde müşterilerin hareketlerini izleyerek kişiselleştirilmiş kampanyalar sunma.
- **Teknolojik Zorluklar ve Çözümler**:
  - **İç Mekan Konumlandırma**: GPS'in iç mekanlarda çalışmaması nedeniyle, Wi-Fi tabanlı konumlandırma, Bluetooth Low Energy (BLE) veya Ultra-Wideband (UWB) gibi teknolojiler kullanılır.
  - **Enerji Verimliliği**: IoT cihazları genellikle pil ile çalışır, bu nedenle düşük güç tüketimli konum belirleme yöntemleri (örneğin, BLE beacon'lar) tercih edilir.
  - **Gizlilik ve Güvenlik**: Konum bilgisi hassas bir veri türüdür. IoT sistemlerinde, konum verilerinin güvenliği için şifreleme ve anonimleştirme teknikleri kullanılır.

2- Ranging teknikleri nelerdir? açıklayınız?

Ranging, iki cihaz veya nesne arasındaki mesafeyi belirlemek için kullanılan yöntemlerdir. IoT'de konumlandırma (localization) için kritik olan bu teknikler, farklı sinyal türleri (radyo, ses vb.) ve ölçüm prensipleri kullanır. Slaytta belirtilen dört ana ranging tekniği şunlardır:

1. **Time of Arrival (ToA - Varış Zamanı)**:
   - **Mantık**: Bir sinyalin göndericiden alıcıya ulaşma süresi ölçülerek mesafe hesaplanır. Sinyalin hızı biliniyorsa (örneğin, radyo sinyali 300 km/s, ses dalgası 343 m/s), mesafe = hız × zaman formülüyle bulunur.
   - **Tek Yönlü ToA (One-way ToA)**:
     - Sinyal sadece tek yönde (göndericiden alıcıya) ölçülür.

    - Gönderici ve alıcının saatlerinin çok hassas bir şekilde senkronize olması gerekir, çünkü küçük bir zaman farkı büyük mesafe hatalarına yol açar.
    - Örnek: GPS, bu yöntemi kullanır.
  - **Çift Yönlü ToA (Two-way ToA)**:
    - Sinyal göndericiden alıcıya gider ve geri döner (round-trip). Gönderici, sinyalin toplam gidiş-dönüş süresini ölçer.
    - Saat senkronizasyonu gerekmez, çünkü süre göndericide ölçülür.
    - Örnek: Bir IoT cihazının başka bir cihaza ping atması ve yanıt süresini ölçmesi.
  - **Avantajlar**: Doğru mesafe ölçümü sağlar.
  - **Dezavantajlar**: Tek yönlü ToA için senkronizasyon gereklidir; radyo sinyalleri için çok hassas zaman ölçümleri gerekir (örneğin, 10 m için 30 nanosaniye).
2. **Time Difference of Arrival (TDoA - Varış Zamanı Farkı)**:
  - **Mantık**: İki farklı hızda sinyal (örneğin, radyo ve ses sinyali) gönderilir ve bu sinyallerin alıcıya ulaşma zamanları arasındaki fark ölçülerek mesafe hesaplanır.
  - **Nasıl Çalışır**: Örneğin, bir cihaz önce radyo sinyali (hızlı) gönderir, ardından bir ses sinyali (yavaş) gönderir. Alıcı, bu iki sinyalin varış zamanları arasındaki farkı ölçer ve mesafeyi hesaplar.
  - **Avantajlar**: Saat senkronizasyonu gerektirmez, bu da IoT cihazları için pratiktir. Mesafe ölçümleri çok hassas olabilir.
  - **Dezavantajlar**: Farklı sinyal türleri için ek donanım (örneğin, mikrofon veya hoparlör) gerekir.
  - **Örnek Kullanım**: İç mekan konumlandırma sistemlerinde, örneğin bir mağazada müşteri hareketlerini izlemek.
3. **Angle of Arrival (AoA - Varış Açısı)**:
  - **Mantık**: Sinyalin geldiği yön (açı) ölçülerek cihazın konumu belirlenir. Bu, genellikle bir anten dizisi veya mikrofon dizisi ile yapılır.
  - **Nasıl Çalışır**: Antenler veya mikrofonlar arasındaki küçük zaman, genlik veya faz farkları analiz edilerek sinyalin açısı hesaplanır. Bu açı, cihazın yönünü gösterir.
  - **Avantajlar**: Birkaç derecelik hassasiyetle yüksek doğruluk sağlar.
  - **Dezavantajlar**: Anten veya mikrofon dizisi gibi ek donanımlar gerekir, bu da maliyeti artırır.
  - **Örnek Kullanım**: Akıllı ev sistemlerinde cihazların yönünü belirlemek veya otonom araçlarda engel tespiti.
4. **Received Signal Strength (RSS - Alınan Sinyal Gücü)**:
  - **Mantık**: Sinyalin gücü mesafeyle azalır. Alıcı cihaz, sinyal gücünü (RSSI - Received Signal Strength Indicator) ölçerek mesafeyi tahmin eder.
  - **Nasıl Çalışır**: Sinyal gücü, genellikle mesafenin karesiyle (veya daha karmaşık ortamlarda 3-5. kuvvetiyle) azalır. Friis denklemi, ideal koşullarda bu ilişkiyi tanımlar, ancak gerçek dünyada yansımalar, gürültü ve engeller nedeniyle sapmalar olur.
  - **Avantajlar**: Birçok IoT cihazı zaten RSSI ölçebildiği için ek donanıma gerek yoktur. Basit ve düşük maliyetlidir.
  - **Dezavantajlar**: Çevresel faktörler (duvarlar, yansımalar) nedeniyle doğruluk düşüktür. RSSI değerleri cihazdan cihaza değişebilir.
  - **Örnek Kullanım**: Wi-Fi veya Bluetooth tabanlı iç mekan konumlandırma sistemleri.

  Çevresel gürültü, sinyal yansımaları ve cihazlar arası senkronizasyon gibi faktörler, bu tekniklerin doğruluğunu etkileyebilir. Bu nedenle, genellikle birden fazla teknik bir arada kullanılarak (örneğin, ToA ve RSS) daha güvenilir sonuçlar elde edilir.

3- gps çalışma prensibi, gps trilateraion nedir?

GPS (Global Positioning System), dünya çapında konum belirlemek için kullanılan bir uydu tabanlı navigasyon sistemidir. NAVSTAR olarak da bilinir ve en az 24 uydudan oluşan bir küresel navigasyon uydu sistemi (GNSS) örneğidir. 1973'te geliştirilmeye başlanmış, 1995'te tam operasyonel hale gelmiştir.

Nasıl Çalışır? (Mantık):

1. **Uydu Ağı**:

- GPS, yaklaşık 11.000 mil yükseklikte yörüngede dönen en az 24 uydu içerir. Uydular, 6 yörüngede (her yörüngede 4 uydu) eşit dağıtılmıştır ve dünya çevresinde günde iki kez döner (saatte yaklaşık 7.000 mil hızla).
- Dünya üzerindeki herhangi bir noktadan genellikle en az 8 uydu aynı anda görülebilir.

2. **Sinyal Gönderimi**:
   - Her uydu, 1575.42 MHz frekansında kodlanmış radyo sinyalleri (pseudorandom code) yayınlar. Bu sinyaller:
     - Uydunun kimliği,
     - Uydunun konumu,
     - Uydunun durumu,
     - Sinyalin gönderildiği tarih ve saat bilgisini içerir.
   - Sinyaller, ışık hızında (yaklaşık 186.000 mil/saniye) hareket eder.
3. **Mesafe Ölçümü (Ranging)**:
   - GPS alıcısı (örneğin, akıllı telefon veya IoT cihazı), uydudan gelen sinyali alır ve sinyalin gönderildiği zaman ile alındığı zaman arasındaki farkı (Δ) hesaplar.
   - Bu zaman farkı, sinyalin seyahat süresini verir. Mesafe = hız (ışık hızı) × zaman (Δ) formülüyle hesaplanır.
   - Alıcı, her uydu için bu mesafeyi hesaplar ve kendisini uydunun merkezinde olduğu bir kürenin yüzeyinde bir yerde konumlandırır.
4. **Konum Belirleme**:
   - Tek bir uydu, alıcıyı bir küre üzerinde konumlandırır.
   - İki uydu, bu kürelerin kesişiminde bir çember oluşturur.
   - Üç uydu, kesişimde genellikle iki noktaya indirger (biri genellikle mantıksızdır ve elenir).
   - Dört uydu, tam ve doğru bir konum sağlar (trilateration ile).
5. **Zamanlama ve Doğruluk**:
   - GPS uyduları, atomik saatlerle donatılmıştır ve çok hassas zamanlama sağlar. Ancak, alıcıların saatleri (örneğin, telefonlardaki) daha az hassastır.
   - Saat hatalarını düzeltmek için dördüncü uydu kullanılır. Örneğin, 1 ms'lik bir saat hatası, 300 km'lik bir konum hatasına yol açabilir.
   - Uyduların yörünge ve saat bilgileri, Colorado Springs'teki Ana Kontrol İstasyonu (MCS) tarafından sürekli güncellenir.
6. **Hizmet Seviyeleri**:
   - **Standart Konumlandırma Servisi (SPS)**: Herkese açık, ücretsiz, genellikle 3-10 metre doğruluk sağlar.
   - **Hassas Konumlandırma Servisi (PPS)**: Askeri kullanım için, çift sinyal kullanarak daha yüksek doğruluk sunar.

GPS Trilateration: Trilateration, GPS'in bir alıcının (örneğin, IoT cihazı veya telefon) konumunu belirlemek için kullandığı matematiksel yöntemdir. Mesafe ölçümleriyle (ranging) bir cihazın 3D konumunu (enlem, boylam, yükseklik) hesaplar. Alıcının en az üç uydudan mesafe ölçümlerini kullanarak konumunu (x, y, z) hesaplayan yöntemdir. Her uydu, alıcıyı bir küre üzerine yerleştirir; kürelerin kesişimi konumu belirler. Dördüncü uydu, saat hatalarını düzeltir.

4- indoor localization (İÇ MEKAN KONUMLANDIRMA) nedir?
bir cihazın veya nesnenin iç mekan ortamında (örneğin, bir bina içinde) tam yerini veya diğer nesnelere göre relatif konumunu belirleme sürecidir. Dış mekanlarda GPS gibi sistemler etkili olsa da, iç mekanlarda sinyal zayıflaması veya engeller nedeniyle GPS genellikle yetersiz kalır. Bu nedenle, iç mekan konumlandırma, IoT uygulamalarında özel teknikler gerektirir. İç mekanlarda GPS sinyalleri duvarlar, mobilyalar veya diğer engeller nedeniyle zayıflar veya kaybolur. Bu nedenle, alternatif teknolojiler ve ranging teknikleri (önceki soruda bahsedilen ToA, TDoA, AoA, RSS) kullanılır. Konum, genellikle bir cihazın sabit referans noktalarına (örneğin, Wi-Fi erişim noktaları, Bluetooth beacon'lar) olan mesafesini veya açısını ölçerek hesaplanır. **Amaç, cihazın koordinatlarını (x, y, z) veya sembolik bir konumu (örneğin, "3. kat, ofis 105") belirlemektir.**

Kullanılan Teknolojiler:

1. **Wi-Fi**: Wi-Fi erişim noktalarının sinyal gücü (RSSI) veya zaman farkı (TDoA) ölçülerek konum tahmini yapılır. Yaygın ve düşük maliyetlidir, ancak doğruluk 2-5 metre arasında değişir.
2. **Bluetooth Low Energy (BLE)**: BLE beacon'lar, düşük güç tüketimiyle konum bilgisi sağlar. Örneğin, bir mağazada müşterinin hangi reyonda olduğunu tespit edebilir.
3. **Ultra-Wideband (UWB)**: Çok yüksek doğruluk (10-30 cm) sunar. ToA ve AoA tekniklerini kullanır, ancak daha pahalıdır. Örnek: Akıllı telefonlarda hassas takip (Apple AirTag).
4. **Akustik Sinyaller**: Ses dalgalarıyla mesafe ölçümü yapılır (TDoA). İç mekanlarda hassas olabilir, ancak ek donanım gerektirir.
5. **İnertial Sensörler**: Cihazın ivmeölçer ve jiroskop verileriyle hareket takibi yapılır. Ancak, zamanla hata birikir (drift).
6. **Manyetik Alan veya Işık Tabanlı Sistemler**: Ortamın manyetik alan haritası veya görünür ışık iletişimi (VLC) ile konum belirlenir, ancak özel altyapı gerekir.

Nasıl Çalışır? (Basit Mantık):

- Bir IoT cihazı, çevresindeki sabit referans noktalarından (örneğin, Wi-Fi router'lar veya beacon'lar) sinyaller alır.
- Sinyallerin gücü (RSS), varış zamanı (ToA/TDoA) veya açısı (AoA) analiz edilir.
- Bu veriler, trilaterasyon (mesafelerle konum hesaplama) veya triangulasyon (açılarla konum hesaplama) gibi yöntemlerle işlenerek cihazın konumu belirlenir.
- Örneğin, bir alışveriş merkezinde telefonunuz, yakındaki üç Wi-Fi noktasına olan mesafesini ölçer ve bu verilerle sizin hangi mağazada olduğunuzu hesaplar.

5- Kapalı alanlarda konum bilgisi bulmanın zorlukları nelerdir?
Kapalı alanlarda konum bilgisi bulma, GPS gibi dış mekan teknolojilerinin sinyal zayıflaması veya engeller nedeniyle yetersiz kalması sebebiyle karmaşıktır. IoT cihazlarının iç mekanlarda hassas ve güvenilir konum bilgisi sağlaması için bir dizi teknik ve çevresel zorlukla başa çıkılması gerekir. Başlıca zorluklar şunlardır:

1. **Sinyal Engelleri ve Zayıflaması**:
   - **Açıklama**: İç mekanlarda duvarlar, mobilyalar, camlar, metal yapılar veya diğer engeller sinyalleri (örneğin, Wi-Fi, Bluetooth, UWB) bozar, yansıtır veya zayıflatır. Bu, sinyal gücünün (RSSI) veya varış zamanının (ToA/TDoA) doğru ölçülmesini zorlaştırır.
   - **Örnek**: Bir alışveriş merkezinde, Wi-Fi sinyalleri kalın beton duvarlardan geçerken zayıflayabilir, bu da konum doğruluğunu azaltır.
   - **Etkisi**: Mesafe tahmini hatalı olur, cihazın konumu yanlış hesaplanır.
2. **Çok Yollu Yayılım (Multipath Propagation)**:
   - **Açıklama**: İç mekanlarda sinyaller, yansımalar nedeniyle birden fazla yoldan alıcıya ulaşır (örneğin, duvardan yansıma, tavandan sekme). Bu, sinyalin varış zamanını veya gücünü bozar ve konum hesaplamasını karmaşıklaştırır.
   - **Örnek**: Bir ofiste, Bluetooth sinyali bir masadan yansıyarak alıcıya farklı bir mesafede gibi görünebilir.
   - **Etkisi**: Konum tahmininde tutarsızlıklar oluşur.
3. **Doğruluk ve Hassasiyet Sınırlamaları**:
   - **Açıklama**: İç mekan konumlandırma sistemleri (Wi-Fi, BLE, vb.) genellikle GPS'ten daha düşük doğruluk sağlar. Örneğin, Wi-Fi tabanlı sistemler 2-5 metre doğruluk sunarken, UWB 10-30 cm doğruluk sağlar, ancak maliyetlidir.
   - **Örnek**: Bir hastanede, bir cihazın hangi odada olduğunu belirlemek için birkaç santimetre hassasiyet gerekebilir, ancak Wi-Fi bunu sağlayamayabilir.
   - **Etkisi**: Uygulamaların (örneğin, otonom robotlar) güvenilirliği azalabilir.
4. **Altyapı ve Maliyet Gereksinimleri**:
   - **Açıklama**: İç mekan konumlandırma için sabit referans noktaları (örneğin, Wi-Fi erişim noktaları, Bluetooth beacon'lar, UWB anchor'lar) kurulması gerekir. Bu, ek donanım ve kurulum maliyeti anlamına gelir.
   - **Örnek**: Bir depoda varlık takibi için yüzlerce beacon yerleştirmek pahalı ve zaman alıcı olabilir.

- **Etkisi**: Küçük ölçekli projelerde veya bütçe kısıtlaması olan yerlerde uygulanması zorlaşır.

5. **Cihaz Kısıtlamaları**:
   - **Açıklama**: IoT cihazları genellikle düşük güç tüketimli ve sınırlı işlem kapasitesine sahiptir. Hassas konumlandırma için karmaşık algoritmalar veya ek sensörler (örneğin, AoA için anten dizileri) gerekir, bu da cihaz tasarımını zorlaştırır.
   - **Örnek**: Bir BLE beacon, sürekli sinyal gönderirken pil ömrünü hızlı tüketebilir.
   - **Etkisi**: Düşük güç tüketimi ve doğruluk arasında denge kurmak zorlaşır.
6. **Gizlilik ve Güvenlik Endişeleri**:
   - **Açıklama**: Konum bilgisi hassas bir veridir ve iç mekanlarda kullanıcıların veya cihazların hareketlerini izlemek, gizlilik ihlali riski taşır. Ayrıca, sinyallerin ele geçirilmesi (spoofing) güvenlik tehdidi oluşturabilir.
   - **Örnek**: Bir mağazada müşteri hareketlerini izleyen bir sistem, verilerin kötü niyetli kişilerce ele geçirilmesine açık olabilir.
   - **Etkisi**: Şifreleme ve anonimleştirme gibi güvenlik önlemleri, sistem karmaşıklığını artırır.
7. **Çevresel Değişkenlik**:
   - **Açıklama**: İç mekan ortamları dinamiktir; insanlar, taşınan eşyalar veya değişen düzen, sinyal yayılımını etkiler. Örneğin, bir ofiste masaların yerinin değişmesi, Wi-Fi sinyallerinin davranışını değiştirebilir.
   - **Örnek**: Bir alışveriş merkezinde kalabalık saatlerde sinyal bozulmaları artabilir.
   - **Etkisi**: Sistemlerin sürekli kalibrasyon veya uyarlama yapması gerekir.
8. **Farklı Teknolojilerin Uyumluluğu**:
   - **Açıklama**: İç mekan konumlandırma için kullanılan teknolojiler (Wi-Fi, BLE, UWB, akustik) farklı cihazlarla uyumluluk sorunları yaratabilir. Ayrıca, kullanıcı cihazlarında Bluetooth veya diğer özelliklerin açık olması gerekir.
   - **Örnek**: Bir müşterinin telefonunda Bluetooth kapalıysa, beacon tabanlı bir sistem çalışmaz.
   - **Etkisi**: Kullanıcı deneyimi ve sistem güvenilirliği azalabilir.

6- Beacon nedir? kullanım amacı nedir?

Beacon, genellikle Bluetooth Low Energy (BLE) teknolojisini kullanarak sinyal yayınlayan küçük, düşük güç tüketimli kablosuz cihazlardır. Bu cihazlar, belirli bir alanda (genellikle 10-100 metre aralığında) çevredeki IoT cihazlarına veya akıllı telefonlara sinyal gönderir. Sinyaller, benzersiz bir kimlik (ID) içerir ve alıcı cihazlar bu sinyalleri algılayarak konum, yakınlık veya bağlam tabanlı bilgiler elde eder.

- Küçük, taşınabilir ve genellikle pil ile çalışır (bazen yıllar boyunca çalışabilir).
- BLE protokolünü kullanır, bu da düşük enerji tüketimi sağlar.
- Tek yönlü iletişim kurar; yani sinyal gönderir ama genellikle veri almaz.
- Yaygın örnekler: iBeacon (Apple), Eddystone (Google) gibi protokoller.

Beacon'lar, IoT ekosisteminde özellikle **iç mekan konumlandırma (indoor localization)**, **yakınlık tabanlı hizmetler** ve **bağlam tabanlı etkileşimler** için kullanılır. Başlıca kullanım amaçları şunlardır:

1. **İç Mekan Konumlandırma ve Navigasyon**:
   - GPS'in zayıf olduğu iç mekanlarda (örneğin, alışveriş merkezleri, havaalanları, müzeler), beacon'lar cihazların konumunu belirlemek için kullanılır.
   - Örnek: Bir müzede, ziyaretçinin hangi sergide olduğunu tespit ederek o esere dair bilgi gönderen bir uygulama.
2. **Yakınlık Tabanlı Bildirimler (Proximity Marketing)**:
   - Beacon'lar, bir cihazın belirli bir alana yaklaştığını algılayarak hedeflenmiş bildirimler veya reklamlar gönderir.
   - Örnek: Bir mağazada, müşteri belirli bir reyona yaklaştığında indirim kuponu gönderen bir mobil uygulama.
3. **Varlık Takibi (Asset Tracking)**:
   - Depolarda, hastanelerde veya fabrikalarda ekipman, ürün veya araçların yerini izlemek için kullanılır.
   - Örnek: Bir hastanede tekerlekli sandalyelerin veya tıbbi cihazların konumunu gerçek zamanlı takip etme.
4. **Bağlam Tabanlı Otomasyon**:

- Beacon’lar, bir cihazın belirli bir alana girdiğini algılayarak otomatik eylemler tetikler.
- Örnek: Akıllı bir evde, kullanıcının odaya girmesiyle ışıkları açan veya klimayı çalıştıran bir sistem.

7- IoT Communication Protocols'leri (COAPP, MQTT, AMQP) açıklayın ve kıyaslayın.

AMQP (Advanced Message Queuing Protocol)

- **Tanım**: AMQP, daha karmaşık ve kurumsal düzeyde mesajlaşma sistemleri için tasarlanmış bir protokoldür. Mesaj kuyruklama (queuing) modeline dayanır ve TCP üzerinden çalışır. Güvenilirlik ve birlikte çalışabilirlik (interoperability) odaklıdır.
- **Mantık**: AMQP, mesajları kuyruklara yerleştirir ve bu kuyruklar üzerinden cihazlar veya uygulamalar mesajları alır. Mesaj yönlendirme, sıralama ve güvenilirlik için gelişmiş özellikler sunar.
- **Özellikler**:
  - Yüksek güvenilirlik ve sağlamlık (mesaj kaybını önler).
  - Esnek mesaj yönlendirme (örneğin, kuyruklar ve exchange mekanizmaları).
  - Daha fazla kaynak tüketir (CPU, bellek), bu nedenle güçlü cihazlar için uygundur.
  - Genellikle bir mesaj broker’ı (örneğin, RabbitMQ) gerektirir.
- **Kullanım Alanları**: Büyük ölçekli IoT sistemleri, finansal işlemler, kurumsal veri entegrasyonu.
- **Örnek**: Bir lojistik firmasında, AMQP ile araçların konum verileri bir kuyruğa gönderilir ve merkezi bir sistem bu verileri işler.

Kriter	CoAP	MQTT	AMQP
Model	İstemci-Sunucu (REST tabanlı)	Yayın/Abone (Publish/Subscribe)	Mesaj Kuyruklama
Protokol Katmanı	UDP	TCP	TCP
Hafiflik	Çok hafif, düşük kaynak tüketimi	Hafif, düşük bant genişliği	Daha ağır, yüksek kaynak tüketimi
Güvenilirlik	Düşük (UDP), onaylı mesaj seçeneği	Yüksek (TCP, QoS seviyeleri)	Çok yüksek (TCP, kuyruklama)
Kaynak Kısıtlı Cihazlar	Çok uygun (sensörler, düşük güç)	Uygun (sensörler, düşük bant)	Daha az uygun (güçlü cihazlar için)
Kullanım Alanı	Akıllı ev, sensör ağları	Gerçek zamanlı veri toplama	Kurumsal, büyük ölçekli sistemler
Mesaj Yönlendirme	Basit (multicast destekler)	Konu tabanlı (topic-based)	Gelişmiş kuyruk ve exchange
Kurulum Karmaşıklığı	Düşük (broker gerekmez)	Orta (broker gerekir)	Yüksek (broker ve yapılandırma)
Örnek Uygulama	Akıllı termostat kontrolü	Sıcaklık sensörü veri aktarımı	Lojistikte araç takibi

Hangi Protokol Seçilmeli?:

- Eğer düşük güçlü, kısıtlı cihazlarla çalışılıyorsa (örneğin, bir akıllı ev sistemi): **CoAP**.
- Eğer gerçek zamanlı, düşük bant genişlikli veri aktarımı gerekiyorsa (örneğin, sensör ağları): **MQTT**.
- Eğer büyük ölçekli, güvenilir ve karmaşık bir sistem gerekiyorsa (örneğin, kurumsal IoT): **AMQP**.

8- IoT'de meydana gelen güvenlik atakları, saldırılar, açıklar nelerdir? nasıl engellenir?
Güvenlik Atakları ve Açıklar:

- Kimlik hırsızlığı ve yetkisiz erişim (zayıf şifreler),
- Veri sızıntısı (şifresiz iletişim),

- MitM saldırıları (ağ dinleme),
- DDoS saldırıları (botnet'ler),
- Yazılım/donanım açıkları (güncellenmemiş sistemler),
- Fiziksel saldırılar (cihaz manipülasyonu),
- Sinyal karıştırma ve kimlik sahteciliği.

Korunma Yöntemleri:

- Güçlü kimlik doğrulama, veri şifreleme, düzenli yazılım güncellemeleri,
- Ağ güvenliği (WPA3, VLAN), fiziksel koruma,
- Anomali tespiti, minimal veri toplama, güvenli protokoller ve tasarım.

IoT'de Meydana Gelen Güvenlik Atakları, Saldırılar ve Açıklar

IoT sistemleri, sensörler, akıllı cihazlar ve ağlardan oluşan geniş bir ekosistem içerir. Bu cihazların düşük işlem gücü, sınırlı bellek ve internet bağlantısı, onları çeşitli güvenlik tehditlerine açık hale getirir. Başlıca güvenlik atakları, saldırılar ve açıklar şunlardır:

1. **Kimlik Hırsızlığı ve Yetkisiz Erişim (Unauthorized Access)**:
   - **Açıklama**: Saldırganlar, zayıf şifreler veya varsayılan kimlik bilgileri (örneğin, "admin/admin") kullanarak IoT cihazlarına erişir.
   - **Örnek**: Bir akıllı ev kamerasının varsayılan şifresi değiştirilmezse, saldırganlar kamerayı ele geçirip görüntüleri izleyebilir.
   - **Etkisi**: Cihaz kontrolünün kaybı, veri hırsızlığı veya kötü amaçlı kullanım.
2. **Veri Sızıntısı ve Gizlilik İhlali**:
   - **Açıklama**: IoT cihazları, konum, sağlık veya kullanım alışkanlıkları gibi hassas veriler toplar. Bu veriler şifrelenmezse veya güvenli olmayan kanallardan iletilirse sızabilir.
   - **Örnek**: Bir akıllı termostatın sıcaklık verileri, şifresiz bir ağ üzerinden gönderilirse ele geçirilebilir.
   - **Etkisi**: Kullanıcı gizliliğinin ihlali, veri kötüye kullanımı.
3. **Man-in-the-Middle (MitM) Saldırıları**:
   - **Açıklama**: Saldırgan, cihaz ile sunucu arasındaki iletişimi dinler veya manipüle eder. Örneğin, şifresiz Wi-Fi ağlarında veri paketleri yakalanabilir.
   - **Örnek**: Bir IoT cihazının komutları (örneğin, "kapıyı aç") değiştirilerek yetkisiz erişim sağlanabilir.
   - **Etkisi**: Yanlış komutlar, veri manipülasyonu veya sistem kontrolünün kaybı.
4. **Dağıtık Hizmet Engelleme (DDoS) Saldırıları**:
   - **Açıklama**: Çok sayıda IoT cihazı ele geçirilerek (örneğin, bir botnet oluşturularak) bir sunucuya aşırı trafik gönderilir, sistemin çökmesi hedeflenir.
   - **Örnek**: 2016'daki Mirai botnet saldırısı, ele geçirilen IoT cihazlarıyla (kameralar, router'lar) büyük bir DDoS saldırısı düzenledi.
   - **Etkisi**: Sunucuların veya hizmetlerin devre dışı kalması.
5. **Yazılım ve Donanım Açıkları (Vulnerabilities)**:
   - **Açıklama**: IoT cihazlarının eski veya güncellenmemiş yazılımları, güvenlik açıkları içerir. Ayrıca, donanım tasarımı hataları (örneğin, fiziksel erişim noktaları) risk oluşturur.
   - **Örnek**: Bir akıllı kapı kilidinin güncellenmeyen yazılımı, bilinen bir açıktan yararlanılarak açılabilir.
   - **Etkisi**: Cihazın ele geçirilmesi veya kötüye kullanımı.
6. **Fiziksel Saldırılar**:
   - **Açıklama**: IoT cihazlarına fiziksel erişim sağlanarak manipüle edilir (örneğin, cihazın devre kartına müdahale).
   - **Örnek**: Bir akıllı sayacın fiziksel olarak açılıp veri manipülasyonu yapılması.
   - **Etkisi**: Cihazın işlevselliğinin bozulması veya veri hırsızlığı.
7. **Sinyal Karıştırma (Jamming)**:

- **Açıklama**: IoT cihazlarının iletişim sinyalleri (örneğin, Wi-Fi, Bluetooth) bozularak iletişim engellenir.
- **Örnek**: Bir güvenlik sensörünün sinyali bozularak alarm sistemi devre dışı bırakılabilir.
- **Etkisi**: Cihazın işlev görememesi.

8. **Kimlik Sahteciliği (Spoofing)**:
   - **Açıklama**: Saldırgan, sahte bir cihaz veya ağ gibi davranarak sistemin güvenini kazanır.
   - **Örnek**: Sahte bir Bluetooth beacon, kullanıcıları yanlış bir konuma yönlendirebilir.
   - **Etkisi**: Yanlış veri aktarımı veya sistem manipülasyonu.

Bu Saldırılar ve Açıklar Nasıl Engellenir?

IoT güvenliğini artırmak için hem cihaz hem de ağ seviyesinde çeşitli önlemler alınabilir. İşte temel korunma yöntemleri:

1. **Güçlü Kimlik Doğrulama ve Yetkilendirme**:
   - **Çözüm**: Varsayılan şifreleri değiştirme, güçlü ve benzersiz şifreler kullanma, çok faktörlü kimlik doğrulama (MFA) uygulama.
   - **Örnek**: Bir akıllı ev cihazında, kullanıcıdan biyometrik doğrulama veya tek kullanımlık şifre istenmesi.
   - **Etkisi**: Yetkisiz erişim riskini azaltır.
2. **Veri Şifreleme**:
   - **Çözüm**: Cihazlar ve sunucular arasındaki veri aktarımında uçtan uca şifreleme (örneğin, TLS, AES) kullanma.
   - **Örnek**: Bir IoT sensörünün verileri, HTTPS veya MQTT üzerinden şifreli olarak iletilir.
   - **Etkisi**: Veri sızıntısı ve MitM saldırılarını önler.
3. **Yazılım Güncellemeleri ve Yama Yönetimi**:
   - **Çözüm**: IoT cihazlarının yazılımlarını düzenli olarak güncelleme, bilinen açıkları kapatacak yamalar uygulama.
   - **Örnek**: Bir akıllı termostat üreticisinin, yeni bir güvenlik açığını kapatmak için OTA (Over-The-Air) güncelleme yayınlaması.
   - **Etkisi**: Yazılım açıklarından kaynaklanan riskler azalır.
4. **Ağ Güvenliği**:
   - **Çözüm**: Güvenli ağ protokolleri (örneğin, WPA3 ile Wi-Fi), ağ segmentasyonu ve güvenlik duvarları kullanma.
   - **Örnek**: IoT cihazlarını ayrı bir VLAN'a yerleştirerek diğer cihazlardan izole etme.
   - **Etkisi**: DDoS ve sinyal karıştırma saldırılarını zorlaştırır.
5. **Fiziksel Güvenlik**:
   - **Çözüm**: IoT cihazlarını fiziksel olarak korumalı alanlara yerleştirme, tamper-proof (kurcalamaya karşı korumalı) donanım kullanma.
   - **Örnek**: Bir akıllı sayacın fiziksel erişime karşı kilitli bir kutuya yerleştirilmesi.
   - **Etkisi**: Fiziksel saldırı riskini azaltır.
6. **Anomali Tespiti ve İzleme**:
   - **Çözüm**: IoT ağını sürekli izleyerek anormal davranışları (örneğin, anormal veri trafiği) tespit eden sistemler kullanma.
   - **Örnek**: Bir IoT ağında, anormal veri gönderimi yapan bir cihazın otomatik olarak karantinaya alınması.
   - **Etkisi**: DDoS veya kimlik sahteciliği gibi saldırılar erken tespit edilir.
7. **Minimal Veri Toplama ve Anonimleştirme**:
   - **Çözüm**: Yalnızca gerekli verileri toplama, hassas verileri anonimleştirme veya maskeleme.
   - **Örnek**: Bir akıllı saat, konum verilerini paylaşırken yalnızca genel bir bölge bilgisi gönderir.
   - **Etkisi**: Gizlilik ihlali riskini azaltır.
8. **Güvenli Protokoller ve Tasarım**:

- **Çözüm**: IoT cihazlarında güvenli protokoller (örneğin, CoAP, MQTT) kullanma, güvenlik odaklı tasarım (security by design) uygulama.
- **Örnek**: Bir IoT cihazının, fabrika çıkışında güvenli bir önyükleme (secure boot) mekanizmasıyla gelmesi.
- **Etkisi**: Sistem açıklarını en aza indirir.

9- IoT security'den bahsedin.
IoT güvenliği, aşağıdaki temel alanlarda ele alınır:

1. **Cihaz Güvenliği**:
   - IoT cihazları genellikle düşük işlem gücü ve belleğe sahiptir, bu da karmaşık güvenlik mekanizmalarını zorlaştırır.
   - **Örnek**: Bir akıllı termostatın varsayılan şifresinin değiştirilmemesi, cihazın ele geçirilmesine yol açabilir.
   - **Önlemler**:
     - Güvenli önyükleme (secure boot) ve donanım tabanlı güvenlik (örneğin, TPM - Trusted Platform Module).
     - Cihazın fiziksel kurcalamaya karşı korumalı (tamper-proof) olması.
     - Düzenli yazılım güncellemeleri ve yamalar.
2. **Veri Güvenliği**:
   - IoT cihazları, konum, sağlık veya kullanım alışkanlıkları gibi hassas veriler toplar. Bu verilerin toplanması, iletimi ve depolanması sırasında korunması gerekir.
   - **Örnek**: Bir akıllı saat, kullanıcının konum verilerini şifresiz bir ağ üzerinden gönderirse, bu veriler ele geçirilebilir.
   - **Önlemler**:
     - Uçtan uca şifreleme (örneğin, TLS, AES).
     - Minimal veri toplama (sadece gerekli verilerin toplanması).
     - Verilerin anonimleştirilmesi veya maskelenmesi.
3. **Ağ Güvenliği**:
   - IoT cihazları, Wi-Fi, Bluetooth veya hücresel ağlar üzerinden iletişim kurar. Bu ağlar, saldırılara (örneğin, Man-in-the-Middle) karşı korunmalıdır.
   - **Örnek**: Şifresiz bir Wi-Fi ağı üzerinden iletişim kuran bir IoT cihazı, veri sızıntısına yol açabilir.
   - **Önlemler**:
     - Güvenli protokoller (örneğin, WPA3, HTTPS).
     - Ağ segmentasyonu (IoT cihazlarını ayrı bir VLAN'a yerleştirme).
     - Güvenlik duvarları ve izinsiz giriş tespit sistemleri (IDS).
4. **Kimlik Doğrulama ve Yetkilendirme**:
   - IoT cihazlarının ve kullanıcıların kimliklerinin doğrulanması, yetkisiz erişimi önler.
   - **Örnek**: Bir akıllı kapı kilidinin zayıf şifresi, yetkisiz erişime izin verebilir.
   - **Önlemler**:
     - Güçlü, benzersiz şifreler ve çok faktörlü kimlik doğrulama (MFA).
     - Cihazlar arası kimlik doğrulama için sertifikalar veya token'lar.
5. **Yazılım ve Donanım Güvenliği**:
   - IoT cihazlarının yazılımları ve donanımları, bilinen açıklara karşı korunmalıdır.
   - **Örnek**: Güncellenmemiş bir IoT cihazı, bilinen bir yazılım açığından yararlanılarak ele geçirilebilir.
   - **Önlemler**:
     - Otomatik yazılım güncellemeleri (OTA - Over-The-Air).
     - Güvenlik odaklı tasarım (security by design) ve açıkların düzenli taranması.

IoT Güvenliğinin Önemi

- **Gizlilik**: Kullanıcıların kişisel verileri (örneğin, konum, sağlık) korunmalıdır.
- **Bütünlük**: IoT sistemlerinin doğru ve güvenilir çalışması sağlanmalıdır.

- **Erişilebilirlik**: DDoS gibi saldırılar, sistemlerin kullanılabilirliğini tehdit eder; bu önlenmelidir.
- **Güvenlik Riskleri**: IoT cihazları, botnet oluşturma (örneğin, Mirai saldırısı), veri hırsızlığı veya fiziksel zarar (örneğin, akıllı kilitlerin açılması) gibi tehditlere açıktır.

IoT Güvenlik Tehditleri (Özet):

Önceki soruda detaylı ele alındığı için kısa bir özet:

- Yetkisiz erişim (zayıf şifreler).
- Veri sızıntısı (şifresiz iletişim).
- Man-in-the-Middle (MitM) saldırıları.
- DDoS saldırıları (botnet'ler).
- Yazılım/donanım açıkları.
- Fiziksel saldırılar ve sinyal karıştırma.

IoT Güvenliğini Sağlama Yöntemleri

1. **Güvenli Tasarım (Security by Design)**:
   - Cihazlar, geliştirme aşamasından itibaren güvenlik odaklı tasarlanmalıdır.
   - Örnek: Güvenli önyükleme mekanizmaları ve donanım tabanlı şifreleme.
2. **Şifreleme ve Güvenli Protokoller**:
   - Veri aktarımı için TLS, HTTPS, MQTT gibi güvenli protokoller kullanılmalıdır.
   - Örnek: Bir IoT sensörünün verileri, şifreli bir kanaldan sunucuya gönderilir.
3. **Kimlik Doğrulama ve Yetkilendirme**:
   - Güçlü şifreler, MFA ve cihaz sertifikaları kullanılmalıdır.
   - Örnek: Bir akıllı ev cihazı, yalnızca yetkilendirilmiş kullanıcılar tarafından kontrol edilebilir.
4. **Düzenli Güncellemeler**:
   - Yazılım ve donanım açıklarını kapatmak için OTA güncellemeleri yapılmalıdır.
   - Örnek: Bir akıllı kameranın yazılımı, yeni bir güvenlik açığını kapatmak için güncellenir.
5. **Ağ Güvenliği**:
   - Güvenli ağlar (WPA3), ağ segmentasyonu ve güvenlik duvarları kullanılmalıdır.
   - Örnek: IoT cihazları, ev ağında ayrı bir VLAN'da izole edilir.
6. **Anomali Tespiti ve İzleme**:
   - Anormal davranışları tespit eden sistemler (örneğin, IDS) kullanılmalıdır.
   - Örnek: Bir IoT cihazının anormal veri trafiği, bir botnet belirtisi olarak tespit edilir.
7. **Fiziksel Güvenlik**:
   - Cihazlar, fiziksel erişime karşı korunmalıdır (örneğin, tamper-proof tasarımlar).
   - Örnek: Bir akıllı sayaç, kurcalamaya karşı kilitli bir kutuda saklanır.
8. **Kullanıcı Eğitimi**:
   - Kullanıcılar, varsayılan şifreleri değiştirme ve güvenli ağ kullanımı konusunda bilgilendirilmelidir.
   - Örnek: Bir kullanıcı, akıllı ev cihazının şifresini benzersiz bir şekilde ayarlar.