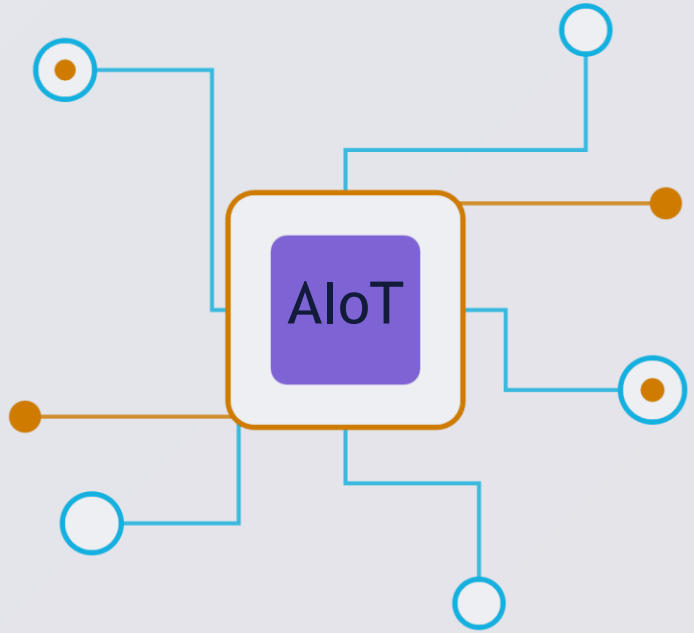
ENDÜSTRI 4.0 · SINIR BILIŞIM (EDGE) MIMARILERI

Otonom AIoT ve IIoT

Akıllı nesneler, yönetimi ve aşamaları



Enerji ve güvenlik paradoksunu çözmek · Ekim 2026

NESNELERIN İNTERNETI'NDEN ZEKÂSINA

Otomasyondan otonomiye geçiş

2030'a kadar

75

milyar

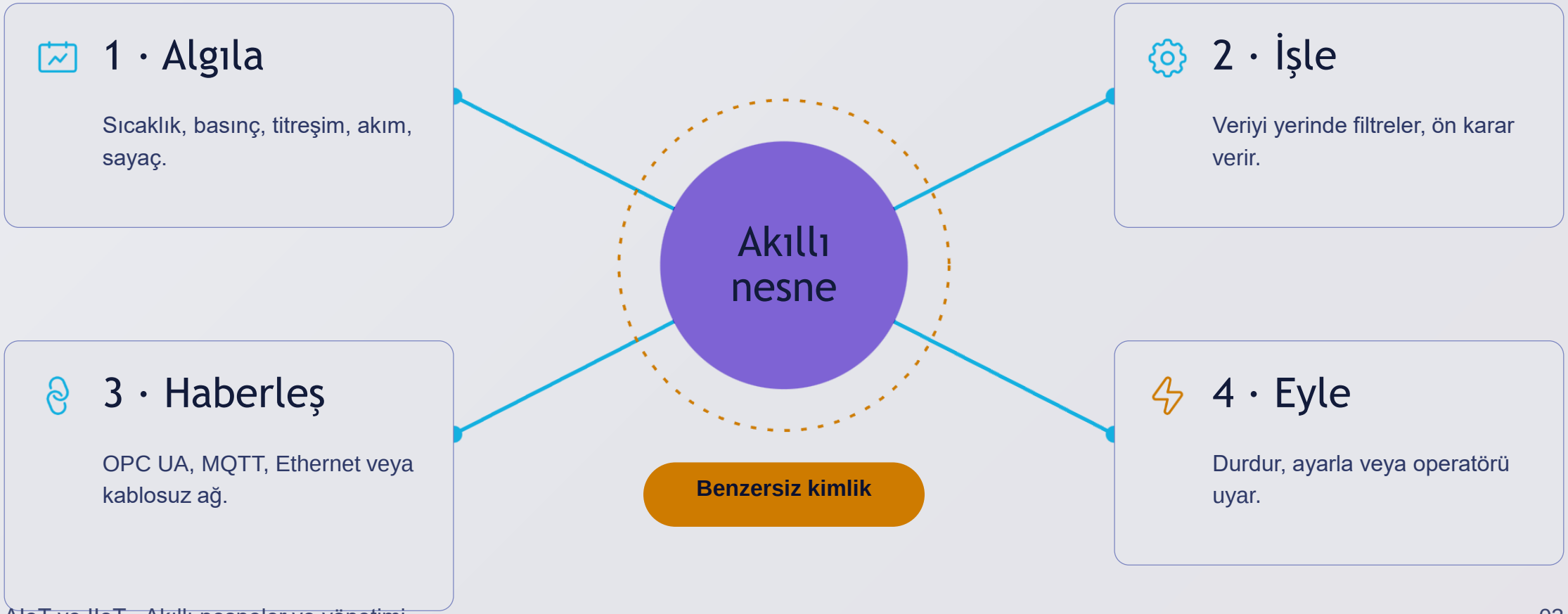
bağlı cihaz

Geleneksel IoT	Otonom AIoT
İşleme Merkezi, bulut tabanlı	**İşleme** Sınırda (edge) ve dağıtık
Hata yönetimi Reaktif: bozulunca müdahale	**Hata yönetimi** Kestirimci: anomali tespiti
Karar mekanizması İnsan kontrollü	**Karar mekanizması** Veri odaklı, otonom
Ölçeklenebilirlik Sınırlı ve darboğazlı	**Ölçeklenebilirlik** Modüler ve esnek

Cihaz sayısı öngörüsü kaynak sunumdan alınmıştır

AKILLI NESNE

Bir nesneyi akıllı yapan dört yetenek



AŞAMALAR

Dijital olgunluğun altı basamağı



Aşamalar: acatech Industrie 4.0 Maturity Index · IIoT/AIoT etiketleri yorumdur

SORUN

Ölümcül döngü: güvenlik ile enerji çatışması

Güvenlik ve enerji ayrı hedefler sayıldığında sistem çöker.

1 · Zayıf güvenlik

Şifreleme yok, saldırı tespiti yok

2 · Siber saldırı

DDoS, Sybil, araya girme (MITM)



4 · Ağ çöküşü

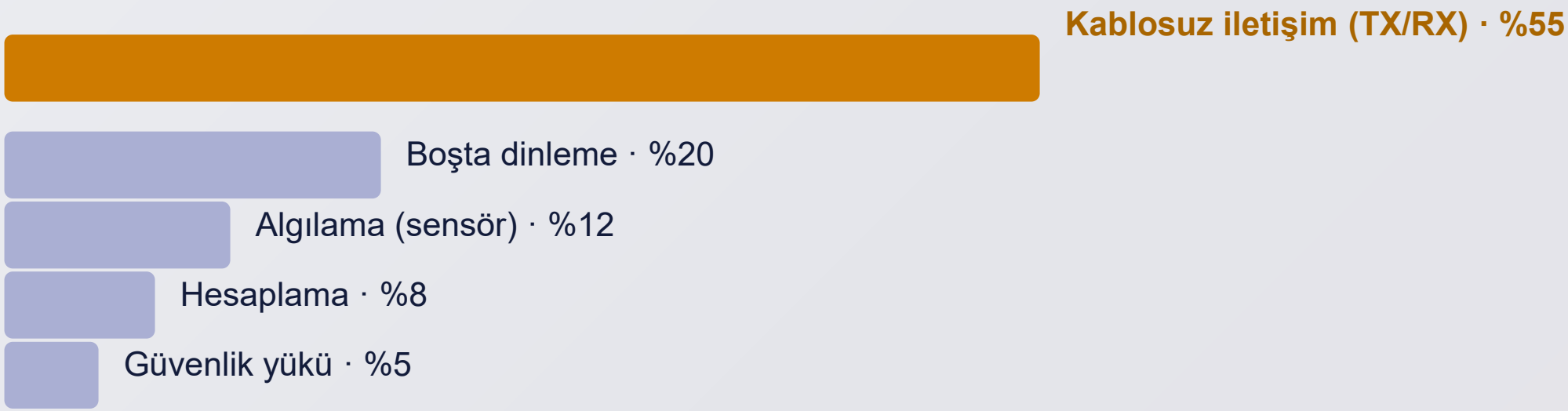
Düğümler ölür, kapsama kaybolur

3 · Enerji tükenmesi

Pil biter, cihaz uyuyamaz

IOT DÜĞÜMÜNDE ENERJI DAĞILIMI

İletişim, işlemden çok daha pahalıdır



Stratejik çıkarım: çözüm veriyi taşımak değil, zekâyı veriye taşımaktır.

Oranlar kaynak sunumdan alınmıştır

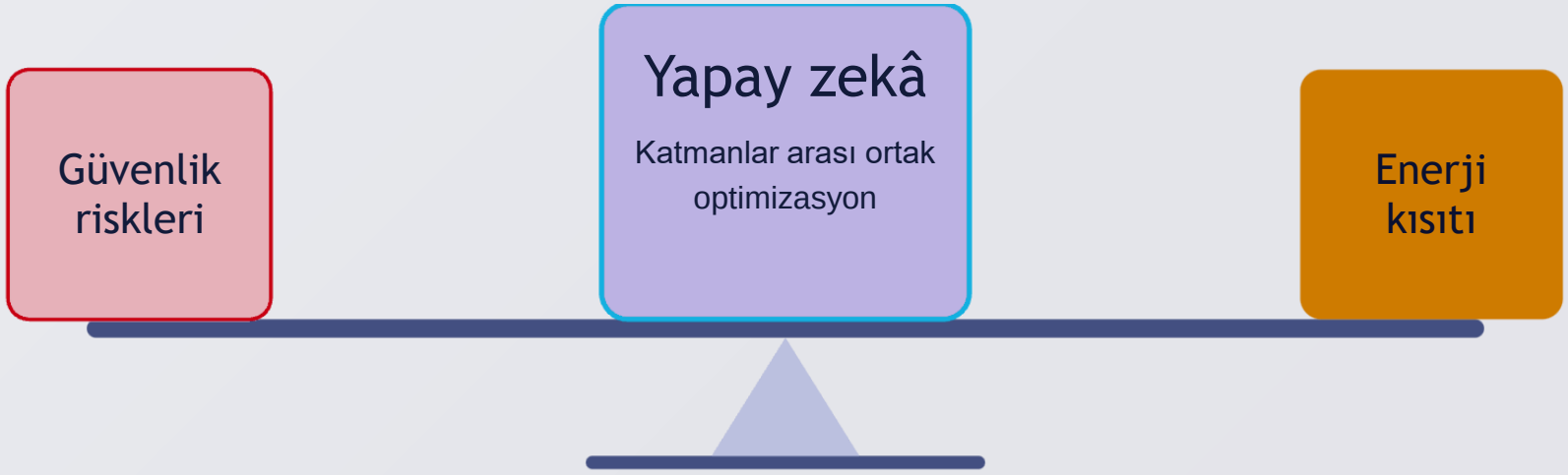
SORUN

Kısıtlı düğümlerde genişleyen saldırı yüzeyi

Ağ katmanı DDoS ve taşkın, araya girme, tekrar oynatma	→	**Sonuç** İletişim felci
Düğüm katmanı Sybil, düğüm ele geçirme, kimlik taklidi	→	**Sonuç** Ağa sızma
Veri katmanı Veri zehirlenmesi, kötü amaçlı yazılım	→	**Sonuç** Yanlış sensör okumaları
Yapay zekâ katmanı Çekişmeli örnekler, model tersine çevirme	→	**Sonuç** Kararların manipülasyonu

ÇÖZÜM

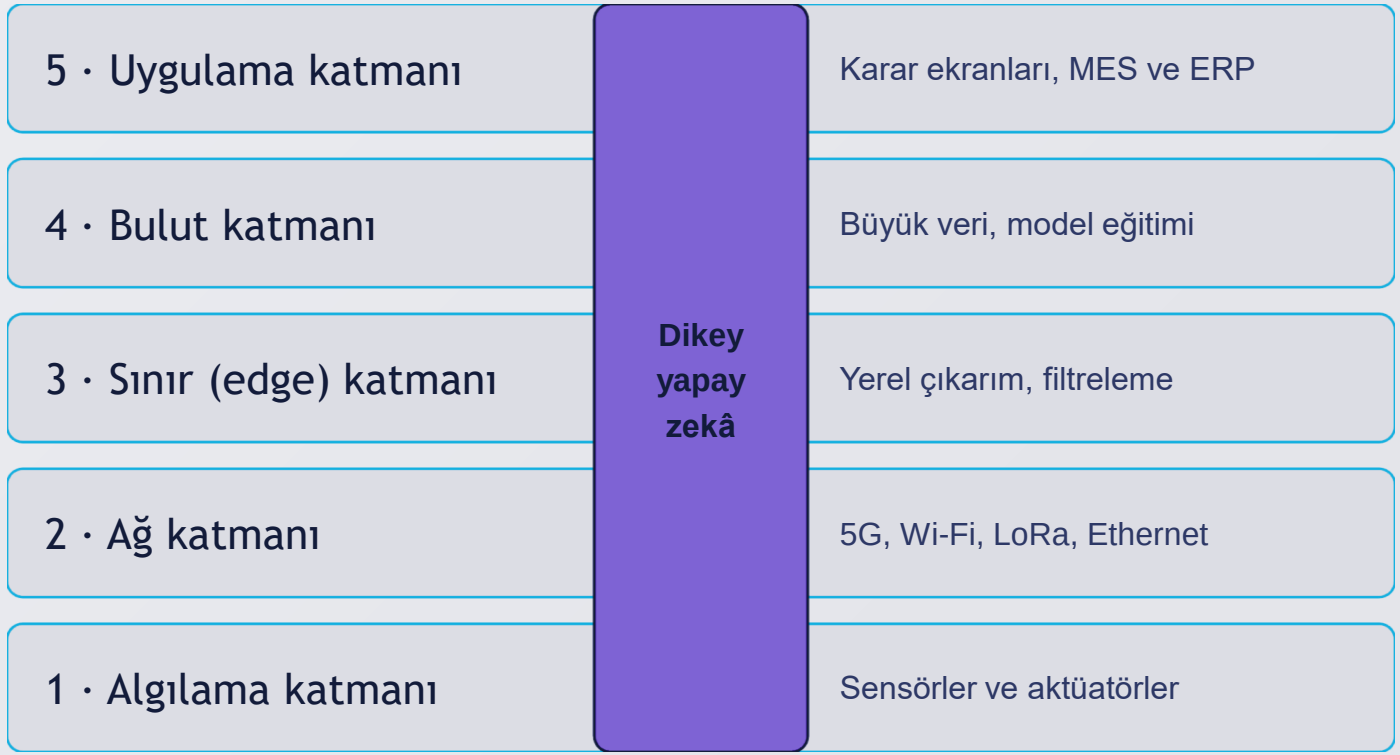
Zeki denge: yapay zekâ çıkmazı nasıl kırar?



Sistem yanıtı: pil seviyesine, kanal durumuna ve tehdit bilgisine bakarak şifreleme düzeyini ve veri iletim sıklığını dinamik ayarlar.

OTONOM AIOT EKOSISTEMI

Beş katmanlı sinir sistemi

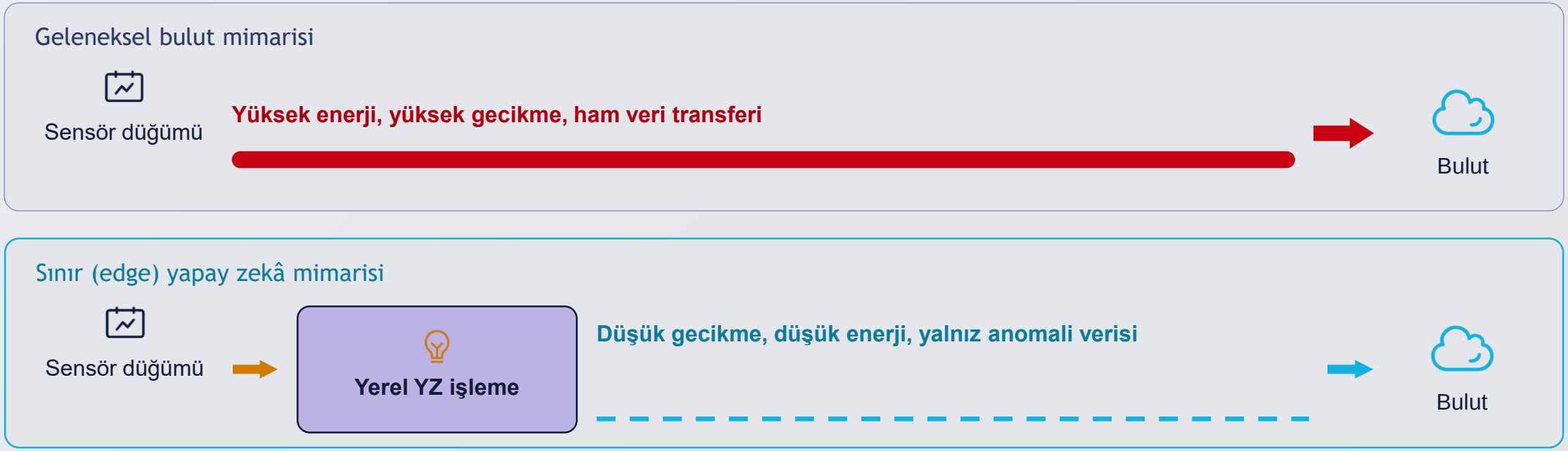


Sistem yanıtı

Yapay zekâ, enerji ve güvenliği optimize etmek için tüm katmanlarda sürekli öğrenir ve karar verir.

SINIR BILIŞIM (EDGE COMPUTING)

Zekâyı kaynağa indirmek



İşlem yükünü düğümlerden sınır sunucularına aktarmak, ağ çapında enerji tasarrufu ve gerçek zamanlı karar sağlar.

DINAMIK KAYNAK YÖNETIMI

Öğrenen ağ, enerjisini kendi yönetir

Yönlendirme ve güç kontrolü

Algoritma: derin Q-ağları (DQN)

%20–40
ağ ömrü artışı

İletim gücünü sistemin anlık durumuna göre optimize eder.

Uyarlanabilir enerji hasadı

Algoritma: LSTM tahmin modeli

Kesintisiz
operasyon

Güneş ve ısı enerjisini tahmin ederek sensör uyku döngülerini ayarlar.

Kestirimci optimizasyon

Algoritma: CNN / Transformer

Olay odaklı
algılama

Trafik yükünü tahmin eder, gereksiz algılamayı durdurup cihazı uyutur.

Ağ ömrü aralığı kaynak sunumdan alınmıştır

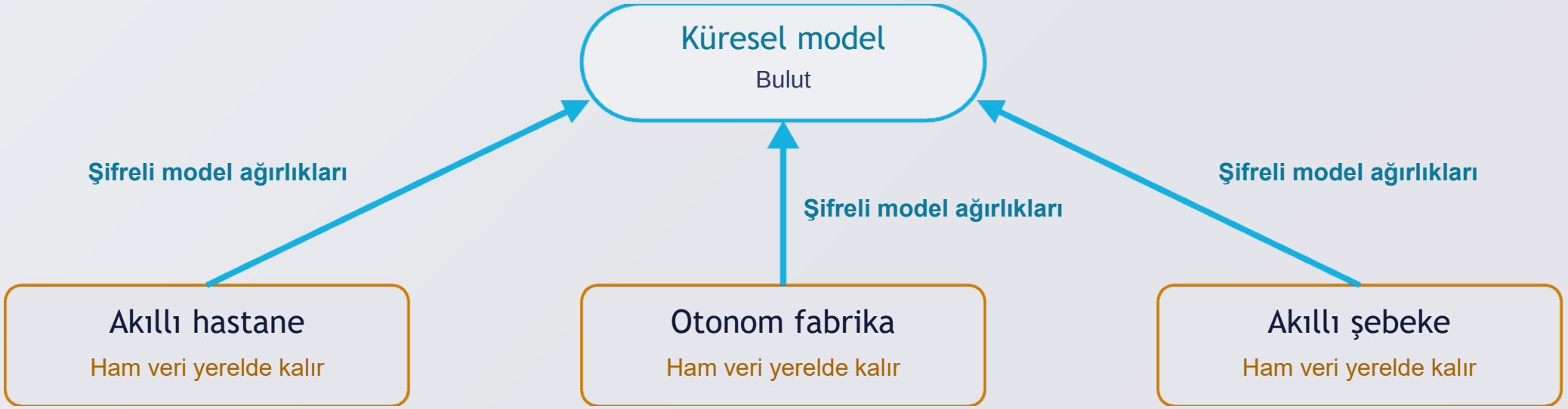
TEŞHIS MATRISI

Yapay zekâ odaklı güvenlik stratejileri

Strateji	Engellediği tehdit	Enerji yükü	Güvenlik seviyesi
ML tabanlı saldırı tespiti (IDS)	DDoS, sızma	Yüksek	Çok yüksek
Hafif blokzincir	Kimlik, dış müdahale	Orta	Yüksek
Hafif kriptografi (ASCON)	Veri gizliliği	Düşük	Yüksek
Federe öğrenme	Gizlilik ihlali	Düşük	Çok yüksek

FEDERE ÖĞRENME

Veriyi değil, aklı paylaşmak



Daha az veri iletilir, enerji korunur; ham veri yerinden çıkmadığı için KVKK ve GDPR uyumu kolaylaşır.

HAFIF KRIPTOGRAFI

Maksimum zırh, minimum yük



Geleneksel şifreleme (AES, RSA)

Yüksek enerji yükü

Kısıtlı IoT donanımını zorlar, pili hızla tüketir.



Hafif şifreleme (ASCON, ECC)

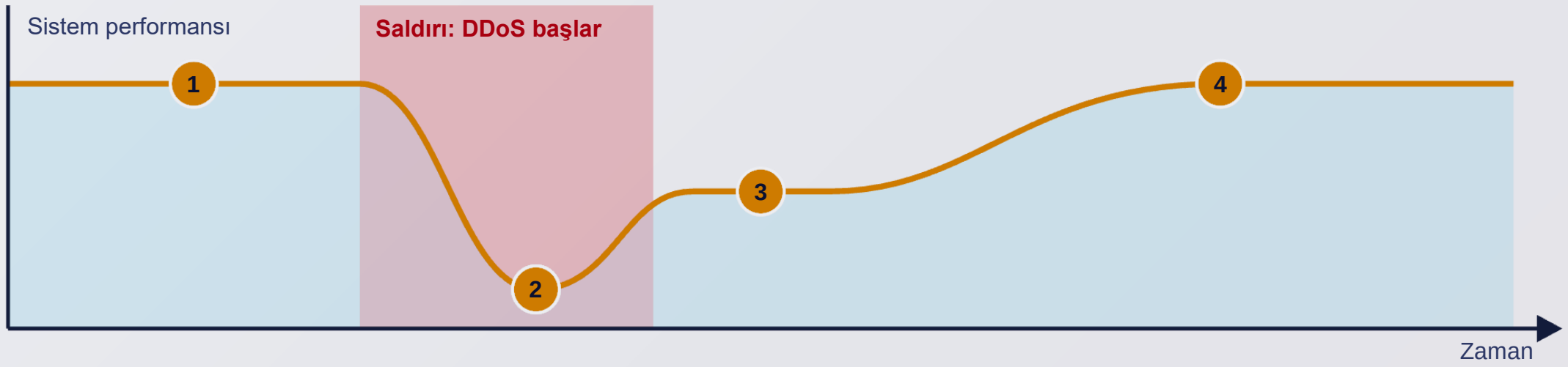
Düşük enerji yükü

Kısıtlı donanım için tasarlanmıştır; küçük devre alanıyla güçlü koruma sağlar.

Uyarlanabilir kripto: yapay zekâ, pil düzeyine ve anlık tehdide göre şifreleme düzeyini değiştirir.

Pil çizimleri temsilidir, ölçüm değildir

Saldırıda emilim, adaptasyon, iyileşme



1 · Normal performans

Sistem beklenen düzeyde çalışır.

2 · Emilim

YZ tabanlı saldırı tespiti anormal trafiği hızla yakalar.

3 · Adaptasyon

Kontrolör enerjiyi kritik savunmaya yönlendirir.

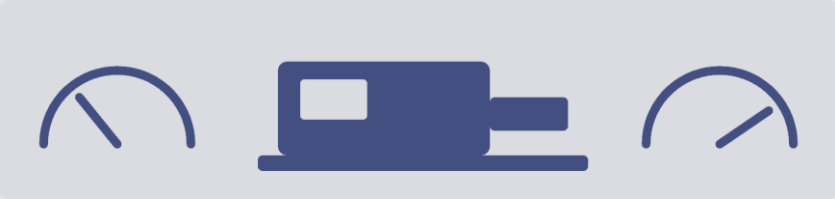
4 · İyileşme

Tehdit izole edilir, yeni imza ağa dağıtılır.

Eğri kavramsaldır, ölçüm değildir

Reaktiften proaktife geçiş

Geleneksel makine paneli



- Reaktif: bozulunca tamir
- Sınırlı veri görünürlüğü
- İnsana dayalı karar
- Periyodik bakım programı

AIoT entegre makine paneli



- Proaktif ve kestirimci
- 7/24 gerçek zamanlı görünürlük
- Veri odaklı otonom karar
- Duruma dayalı bakım

Bu bir teknoloji güncellemesi değil; makinelere anomali tespiti ve kendi kendini onarma yeteneği kazandıran stratejik bir hamledir.

KESTIRIMCI BAKIMIN ANATOMISI

P-F eğrisi: arızayı erken görmek



Düşüş oranı kaynak sunumdan alınmıştır; eğri kavramsaldır

ÖRNEKLER · SEKTÖRLER

Her sektörde aynı mantık, farklı nesne

Otomotiv

Robot ve pres hatları: kestirimci bakım

Gıda ve içecek

Soğuk zincir ve dolum: kalite izleme

Enerji

Türbin ve trafolar: arıza tahmini

Kimya ve proses

Pompa, vana, reaktör: proses ayarı

Lojistik ve depo

Araç ve raflar: dinamik rota

Madencilik

İş makineleri: güvenlik ve yakıt

Tarım

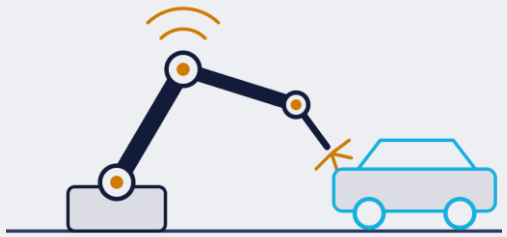
Toprak ve iklim sensörü: akıllı sulama

İlaç

Temiz oda ve seri takibi: izlenebilirlik

ÖRNEK 1 · OTOMOTİV

Robot arızasını duruştan önce yakalamak



Akıllı nesne: gövde hattındaki kaynak robotu.

Kazanım: plansız duruş ve hurda azalır; bakım takvime değil duruma göre yapılır.

IIoT

Algıla

- Eksen motor akımı ve titreşim
- Kaynak akımı, voltajı, çevrim süresi
- Elektrot aşınma sayacı

AIoT

Analiz et

- Normal çalışma imzasından sapma tespiti
- Parça için kalan ömür tahmini
- Hatalı kaynak olasılığı

Karar

Harekete geç

- Bakımı planlı duruşa denk getir
- Parametre düzeltme önerisi sun
- Şüpheli parçayı kontrole ayır

ÖRNEK 2 · GIDA VE IÇECEK

Soğuk zincirde bozulmayı önlemek



Akıllı nesne: soğutuculu araç ve depo.

Kazanım: ürün kaybı azalır; her parti için kesintisiz sıcaklık kaydı oluşur.

IIoT

Algıla

- Depo ve araç içi sıcaklık, nem
- Kapı açılma ve konum bilgisi
- Kompresör çalışma verisi

AIoT

Analiz et

- Sıcaklık sapmasının erken tahmini
- Raf ömrüne etkisinin hesabı
- Kompresör arıza eğilimi

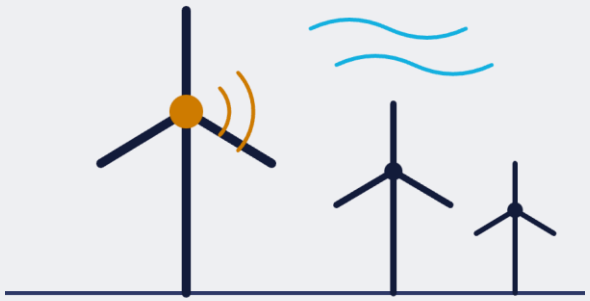
Karar

Harekete geç

- Sürücüye ve depoya anında uyarı
- Riskli partiyi öne al veya ayır
- Soğutucu bakımını öne çek

ÖRNEK 3 · ENERJI

Türbinde arızayı önceden görmek



Akıllı nesne: uzak sahadaki rüzgâr türbini.

Kazanım: plansız saha ziyareti ve üretim kaybı azalır.

IIoT

Algıla

- Dişli kutusu titreşimi ve yağ sıcaklığı
- Rüzgâr hızı, kanat açısı, üretilen güç
- Jeneratör sargı sıcaklığı

AIoT

Analiz et

- Güç eğrisinden sapma tespiti
- Rulman ve dişli arıza tahmini
- Hava durumuna göre üretim tahmini

Karar

Harekete geç

- Bakımı düşük rüzgârlı güne planla
- Kanat açısını otomatik ayarla
- Yedek parçayı önceden sipariş et

ÖRNEK 4 · LOJISTIK VE DEPO

Depoda dinamik görev ve rota



Akıllı nesne: forklift, otonom araç, raf ve palet.

Kazanım: boş sefer ve bekleme azalır; araç ihtiyacı gerçek akışa göre belirlenir.

IIoT

Algıla

- Araç konumu, yük ve batarya durumu
- Raf ve stok alanı doluluğu
- Sipariş ve sevkiyat talepleri

AIoT

Analiz et

- Talep yoğunluğu tahmini
- En az boş seferli rota
- Darboğaz noktalarının tespiti

Karar

Harekete geç

- Görevi en uygun araca ata
- Araç sayısını yüke göre planla
- Şarjı boş zamana kaydır

AKILLI NESNELERIN YÖNETIMI

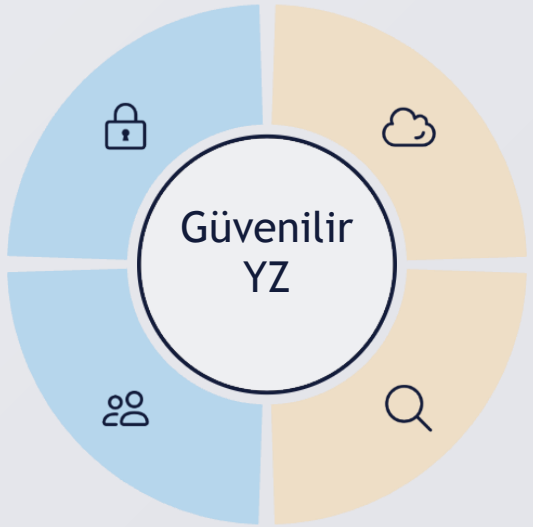
Güvenilir yapay zekâ yönetişimi

1 · Tasarım

Gizlilik odaklı tasarım ve hafif modeller.

2 · Dağıtım

Uçtan uca siber dayanıklılık.



4 · Kontrol

Anlamlı insan müdahalesi: insan döngüde kalır.

3 · İzleme

Açıklanabilir yapay zekâ ile şeffaflık.

Yönetişim, sistemin tüm yaşam döngüsü boyunca hesap verebilir olmasını gerektirir.

GELECEK UFKU

AIoT araştırma ve evrim yol haritası

Yakın dönem

2024–2026

- TinyML tabanlı saldırı tespiti
- IoT için nöral mimari arama
- Hafif blokzincir
- Federe öğrenmede gizlilik

Orta dönem

2026–2028

- Kuantum sonrası kriptografi
- Dijital ikiz simülasyonları
- Katmanlar arası ortak optimizasyon

Uzun dönem

2028 ve sonrası

- Açıklanabilir YZ ile saldırı tespiti
- Yapay zekâ yerleşik 6G AIoT
- Kuantum güvenlikli federe öğrenme

Dönemler kaynak sunumdaki araştırma takvimidir

AÇIK SORUNLAR

Ölçeklenmenin önündeki üç darboğaz

1 · Heterojenlik ve ölçek

- Milyarlarca farklı donanım ve protokolün güvenli birlikte çalışması
- Ortak standart eksikliği (IEEE, IETF)

2 · Yapay zekânın zafiyetleri

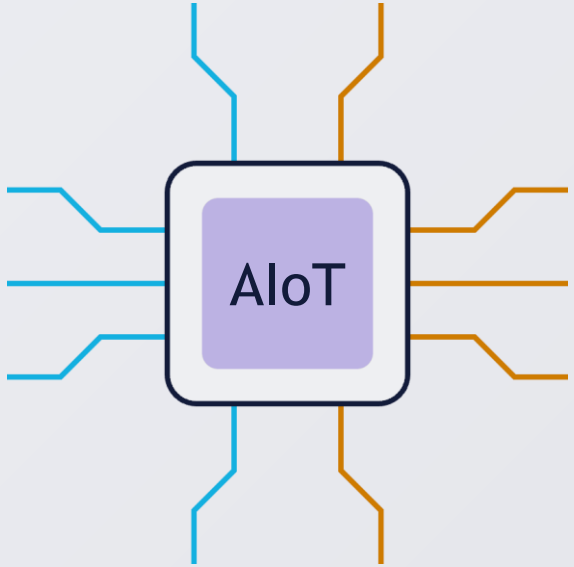
- Yapay zekâya karşı çekişmeli saldırılar
- Federe ağlarda veri zehirlemesi ve model tersine mühendisliği

3 · Yasal uyum ve enerji

- Kısıtlı uç cihazlarda saldırı tespitini gizlilik kurallarına uygun çalıştırmak
- Bunu düşük gecikme ve dengesiz enerjiyle başarmak

SONUÇ

Stratejik bir zorunluluk olarak AIoT



AIoT altyapıları yalnızca daha akıllı yapmaz; enerji israfı ile güvenlik açıkları arasındaki ölümcül döngüyü kırarak makineleri kendi kendini iyileştiren, sürdürülebilir ve otonom ekosistemlere dönüştürür.

Zeki, enerji verimli ve doğası gereği güvenli mimari artık bir araştırma hedefi değil, mühendislik zorunluluğudur.