PaperID: 07

CNN-based IoT Device Identification:
A Comparative Study on Payload vs. Fingerprint

CNN Tabanlı IoT Cihaz Tanımlama:
Yük ile Parmak İzi Yöntemlerinin Karşılaştırması

Kahraman Kostas, PhD
YYEGM, MEB

ICADA

IoT Cihaz Tanımlama Nedir ne işimize yarar?

Makine öğrenmesi kullanarak ağdaki IoT cihazlarının türünü ve kimliğini otomatik olarak belirleme sürecidir.

Güvenlik açıklarını tespit eder.

Olası saldırıları önler.

Zararsız ağ trafiğine ihtiyaç duyar.

Tekil paket özelliklerine ihtiyaç duyar.

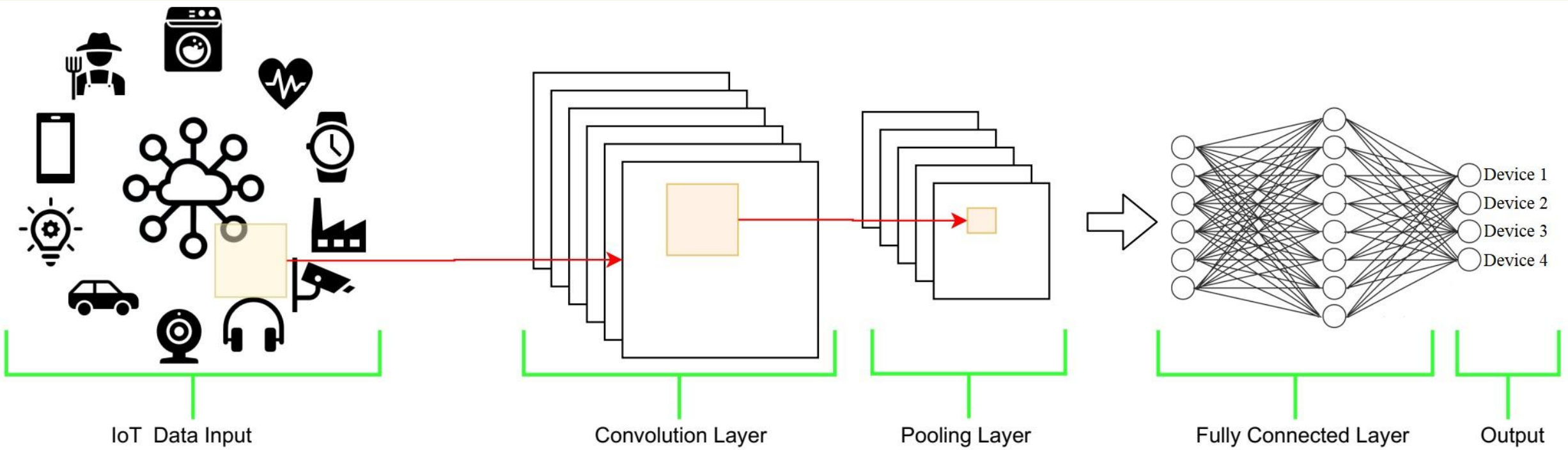
Saldırıları tespit eder.

Aktif saldırıları önler.

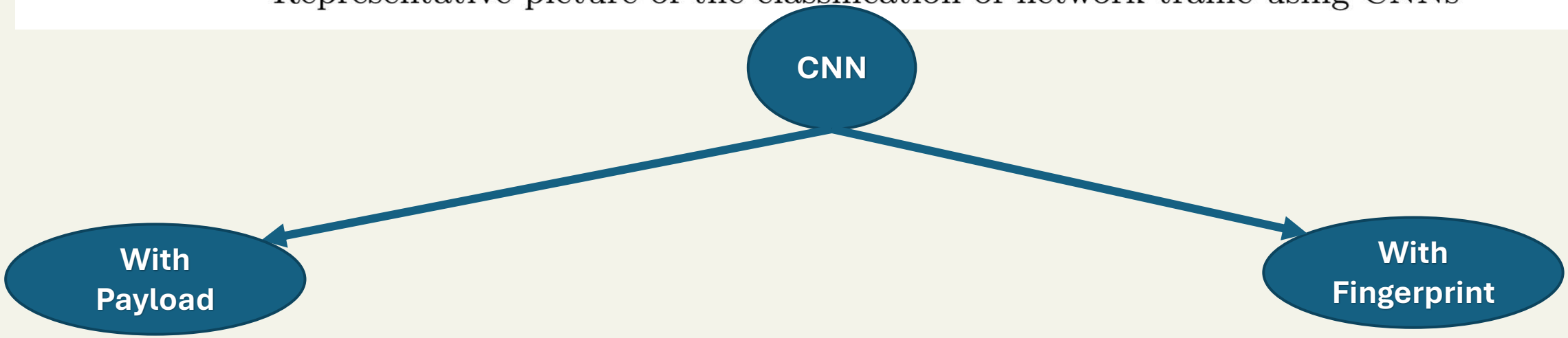
Ağ trafiğinin güvenli kalmasını sağlar.

İlgili/bağımlı özelliklere ihtiyaç duyar.

Convolutional Neural Network - CNN

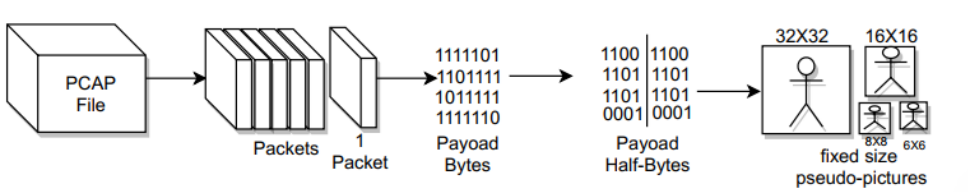


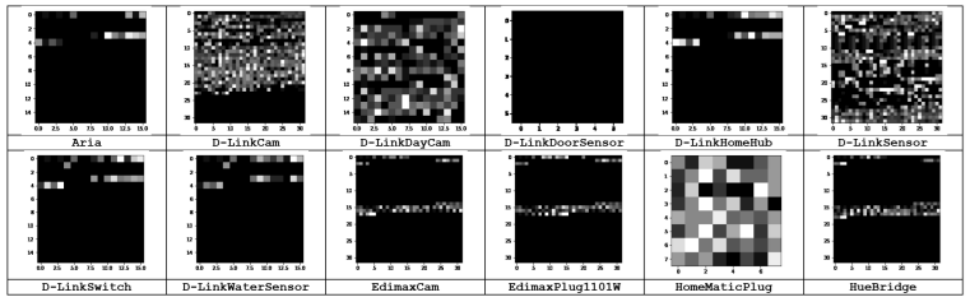
Representative picture of the classification of network traffic using CNNs



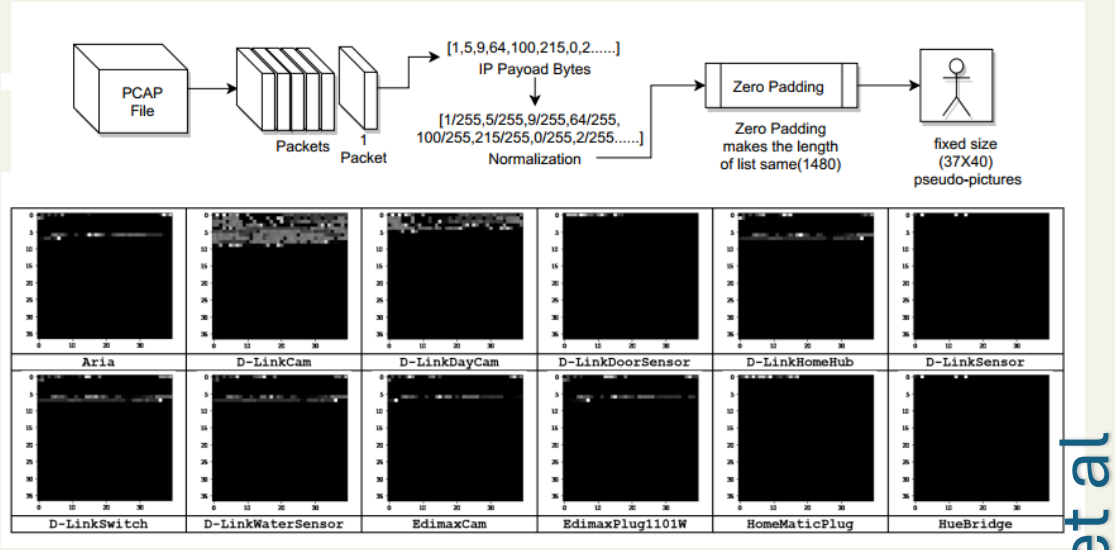
LİTERATÜRE BAKIŞ

Lim et al

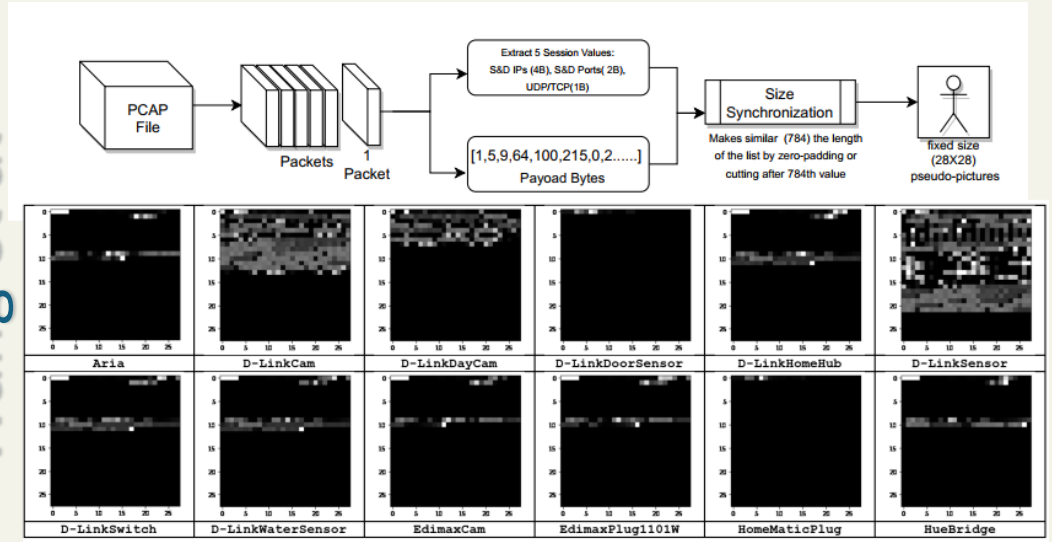




Lotfollahi et al.



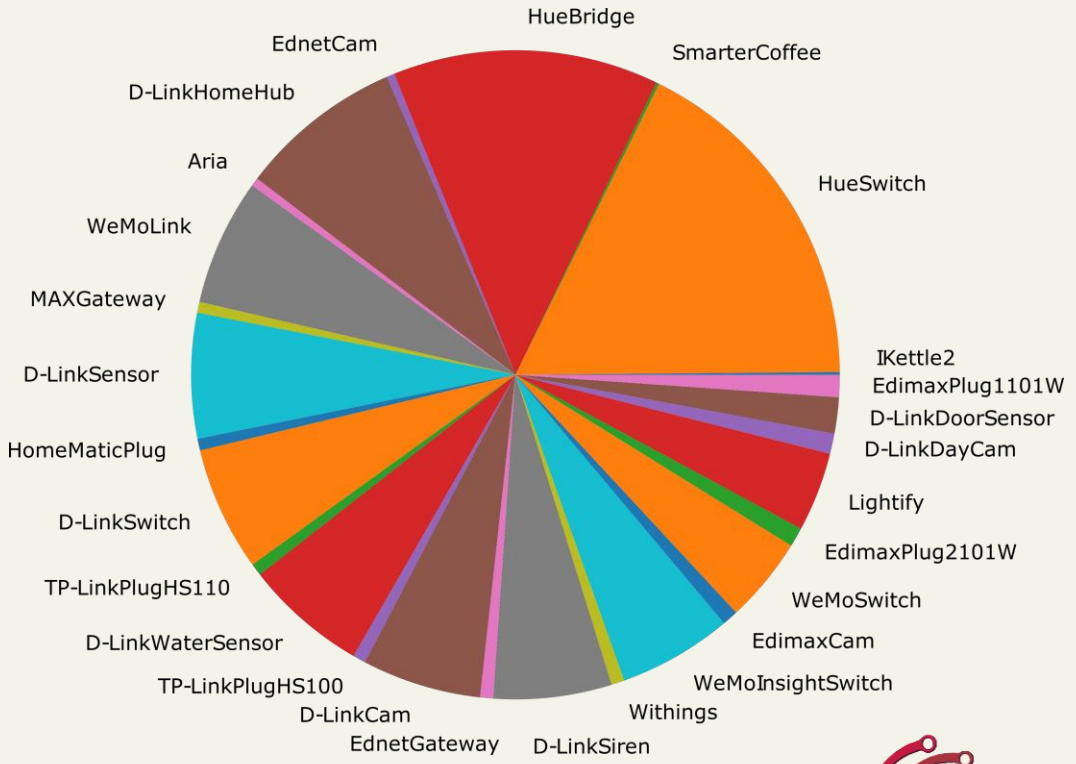
Wang et al



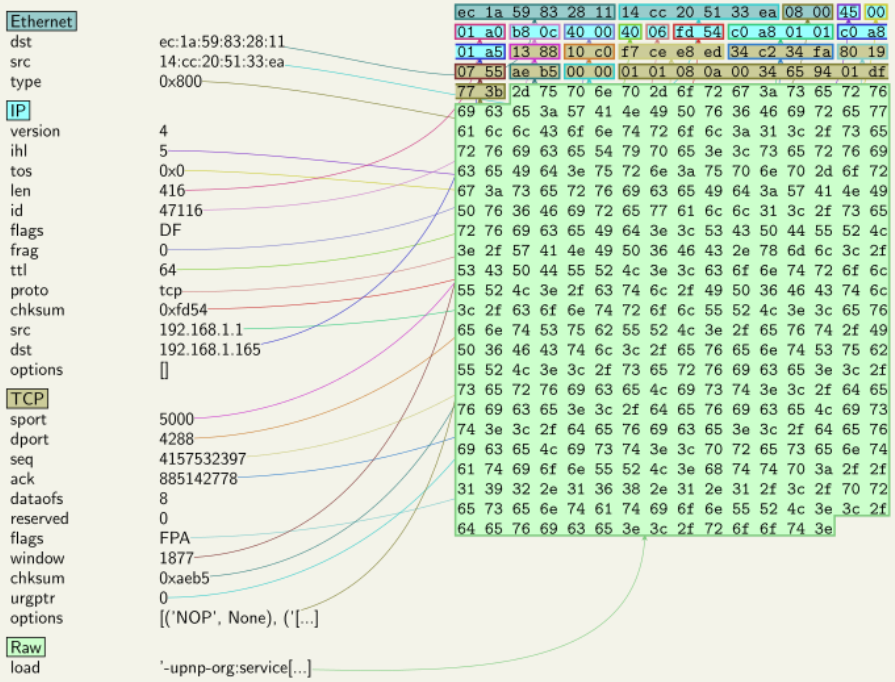
Aalto-yliopisto
Aalto-universitetet
Aalto University

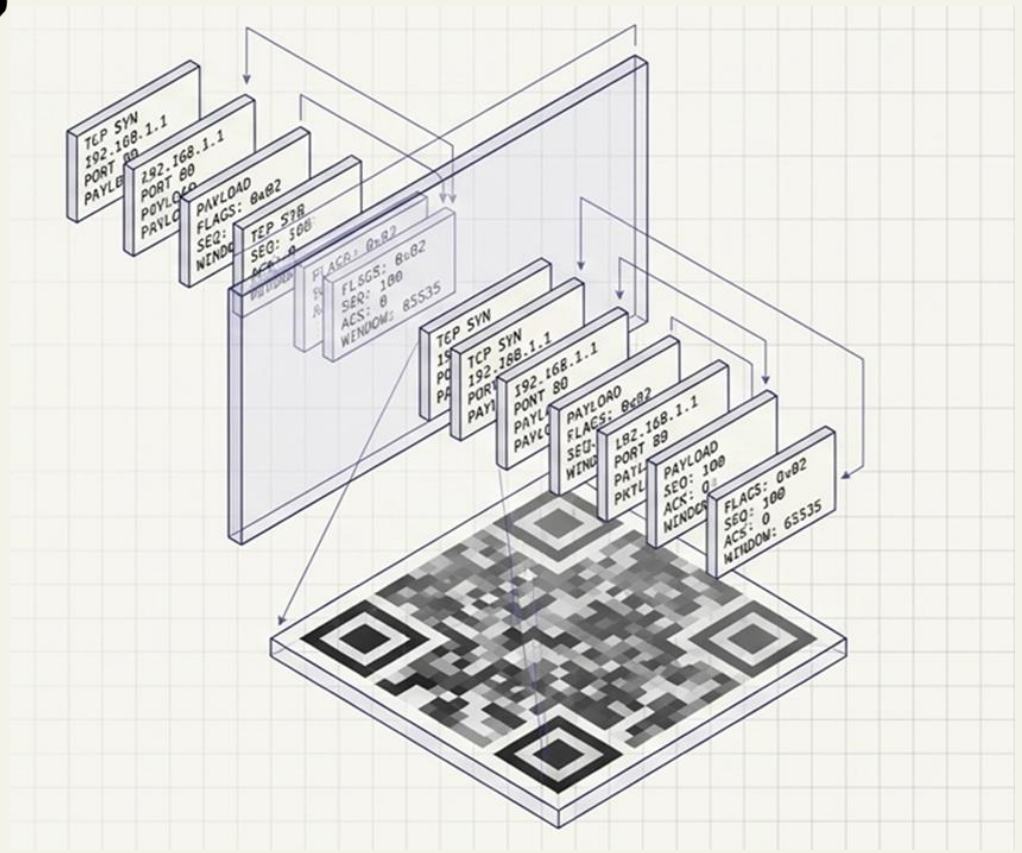
IoT devices captures

- Oldukça yaygın kullanılıyor
- Çok sayıda cihaz içeriyor (27 sınıf 31 cihaz)
- Aynı cihazın birden fazla örneği, benzer marka ve görevde birden fazla cihaz gibi gerçek hayat sorunlarına sahip
- Tüm veriler iyi huylu dolayısıyla cihaz tanımlama için ideal
- Çok büyük başa çıkması zor bir veri seti değil ancak yeterince biri içeriyor



ICADA





IoTDevID

- destination IP counter (int)
- source port number (int)
- destination port number (int)
- packet size (int)
- Entropy of payload
- TCP window size
- packet raw data
- Padding/Router Alert
- ARP/LLC
- IP/ICMP/ICMPv6/EAPoL
- TCP/UDP
- HTTP/HTTPS/ DHCP/BOOTP
- SSDP/DNS/MDNS/NTP

Bir Veri Paketi Nasıl Görüntüye Dönüşür?

Adım 1: Ham Veri

Ham PCAP Dosyası
-> İlk Paket Çıkarımı

Adım 2: Bayt Çıkarımı

Ağ Yükü (Payload) Baytları -> Ondalık Değerlere Dönüştürme

[[12, 255, 0, 78, ...]]

Adım 3: Boyutlandırma

Sıfır Dolgusu (Zero Padding) veya Kırpma (Truncation)
-> 784 Baytlık Standart Boyut

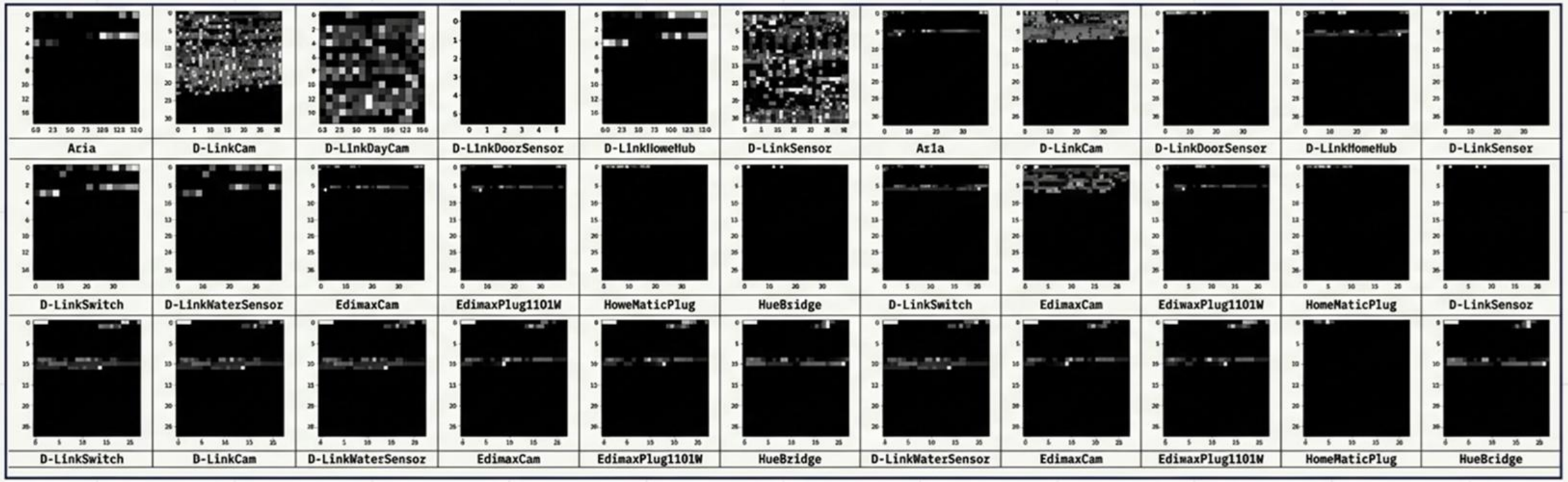
Adım 4: Son Matris

28x28 Sabit Boyutlu Matris

> Literatürdeki farklı yaklaşımlar (Wang et al.), cihaz spesifik imzaların Uygulama Katmanı Yükünde (L7) yattığını gösterir. Aalto veri setindeki IoT paketlerinin büyük çoğunluğu 0-800 bayt aralığındadır, bu nedenle 784 piksellik (28x28) matris optimum standart olarak belirlenmiştir.

Cihazların Benzersiz Dijital Portreleri

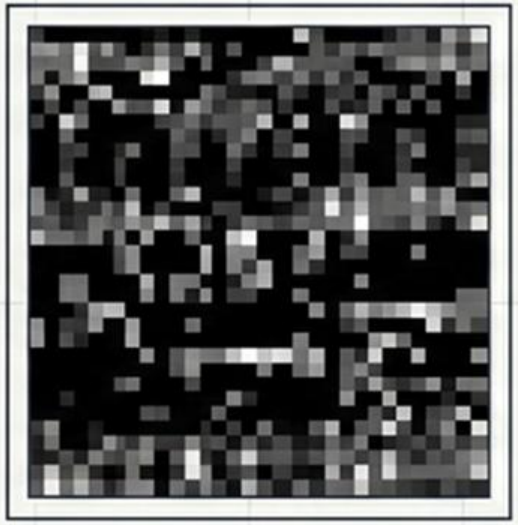
Farklı IoT cihazlarının (Aria, D-LinkCam, HueBridge vb.) ilk paketlerinden üretilen sözde görüntüler (pseudo-images).



İnsan gözü için bir anlam ifade etmeyen bu pikseller (0-255 arası bayt değerleri), bir CNN modeli için her cihaza özgü, taklit edilemez yapısal görsel imzalardır. Derin öğrenme modeli, cihazları bu matrislerdeki kalıplar üzerinden sınıflandırır.

Aalto Veri Seti Üzerinde İki Farklı Yaklaşım

Yük (Payload) Tabanlı CNN



Tüm paket başlıkları silinir. Uygulama katmanı yükünün ilk 771 baytı ve 13 baytlık oturum başlığı birleştirilerek tam bir 28x28 matris (784 bayt) oluşturulur.

Temel Mantık: İçeriğin tamamını derinlemesine incelemek (DPI).

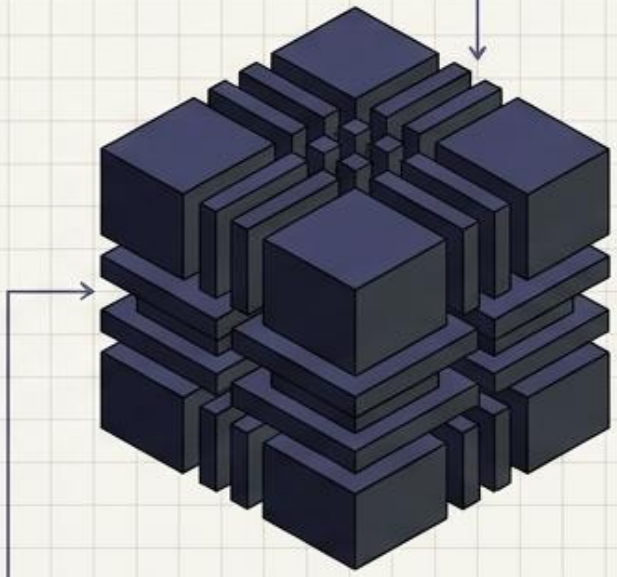
Parmak İzi (Fingerprint) Tabanlı CNN

IoTDevIDv1'den çıkarılan özellik setleri (feature sets) kullanılarak üretilir. Sadece 5x5 boyutunda küçük bir sözde görüntü oluşturulur.

Temel Mantık: Yalnızca kritik davranışsal ve yapısal metadatalara odaklanmak.

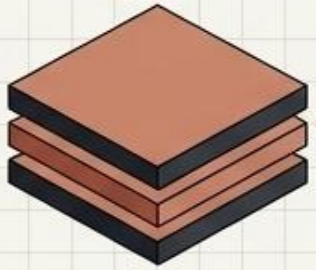
Mimari Yük: Derinlik ve Verimlilik Karşılaştırması

267.678 Parametre



Yük (Payload) Modeli - Girdi: 28x28x1

28.955 Parametre



Parmak İzi (Fingerprint) Modeli - Girdi: 5x5x1

ÖNEMLİ BULGU: Parmak izi (Fingerprint) modeli, girdi verisinin küçüklüğü sayesinde yaklaşık 9 kat daha hafif bir mimariye sahiptir. Bu, donanım kaynakları kısıtlı cihazlar için kritik bir ilk avantajdır.

Sınıflandırma Başarısı: Beklenmedik Bir Beraberlik

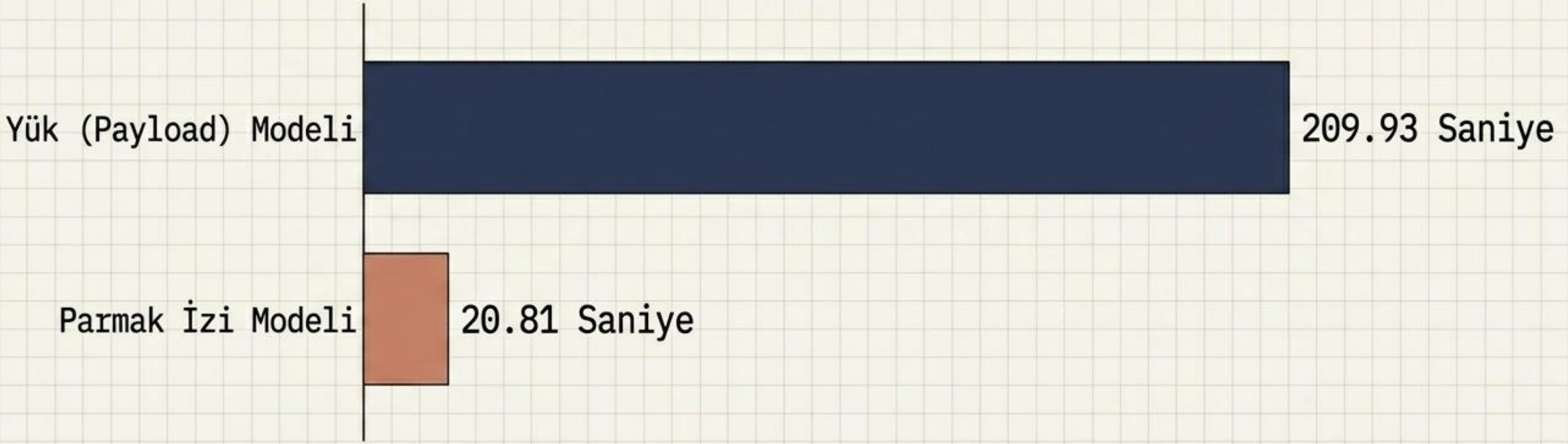
Yük (Payload) Tabanlı CNN

Parmak İzi (Fingerprint) Tabanlı CNN

Mantıken, paketin tam yükünü (DPI) analiz eden modelin çok daha başarılı olması beklenir. Ancak veriler farklı bir tablo çiziyor.

Ham veri yükünün tamamını analiz etmek, meta-özellik tabanlı parmak izi yöntemine kıyasla istatistiksel olarak sadece %0.6'lık marjinal bir doğruluk artışı sağlamıştır.

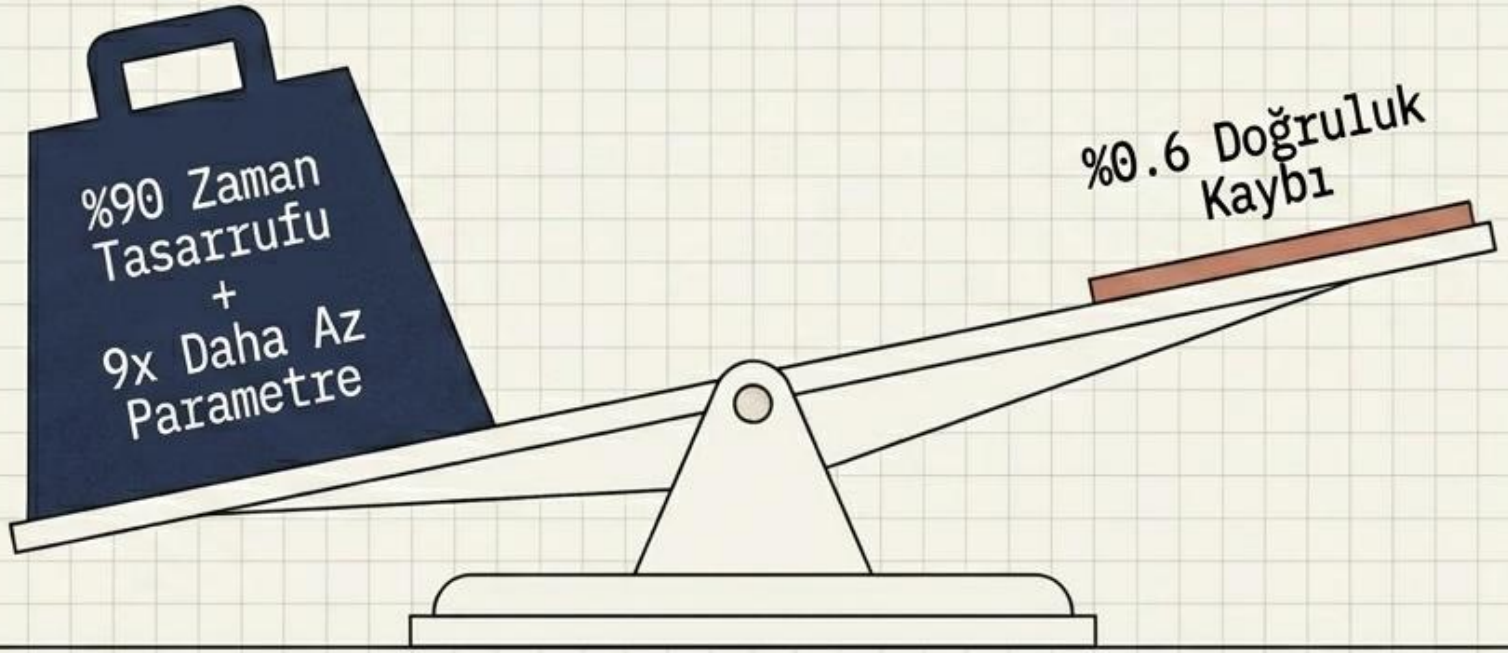
Eğitim Süresi: Parmak İzi Modelinin Çarpıcı Üstünlüğü



Doğruluk oranlarındaki %0.6'lık farka karşılık, eğitim ve işlem süresinde devasa devasa bir asimetri bulunmaktadır.

Parmak izi tabanlı model, tam veri yükü modelinden yaklaşık 10 kat daha hızlıdır. Bu süre zarfında %90'lık devasa bir zaman ve enerji tasarrufu elde edilir.

Karar Anı: Asimetrik Bir Takas (Trade-Off)



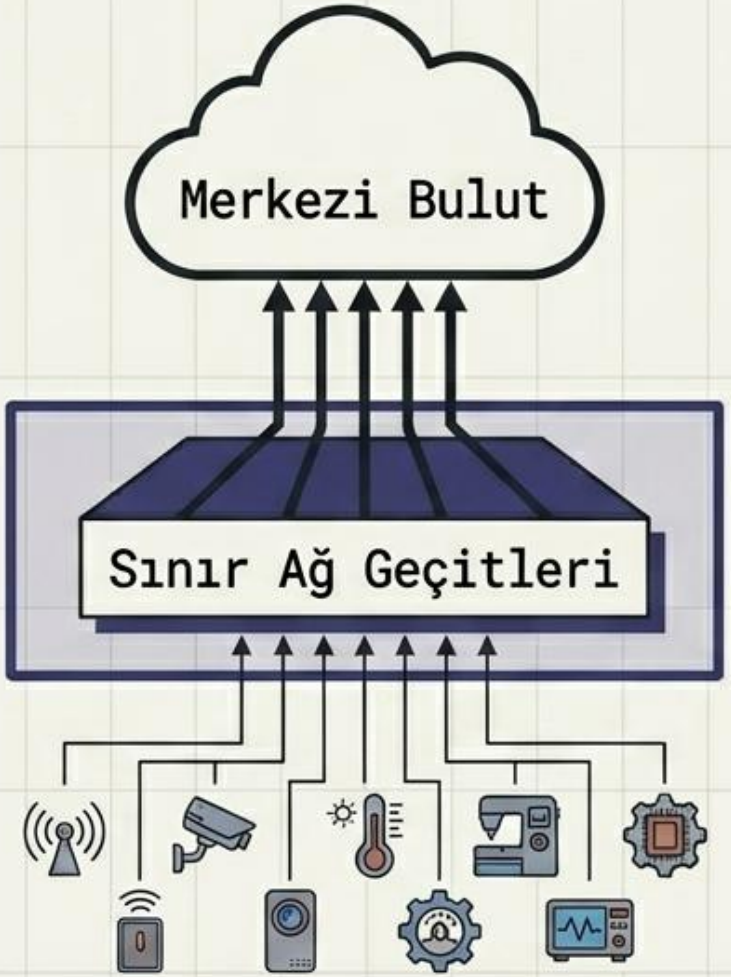
Mühendislikte mükemmel çözüm yoktur, optimize edilmiş takaslar vardır. Gerçek dünya IoT ağlarında, %0.6'lık önemsiz bir doğruluk kaybını göze almak; ağda yaratılacak işlem gücü yükünü ve enerji tüketimini kökten çözer.

Ağ trafiği analizinde veri büyüklüğü her zaman daha iyi sonuç demek değildir. Akıllıca seçilmiş özellik setleri (fingerprints), kaba kuvvet (brute-force) veri analizini geride bırakır.

Tanısal Karşılaştırma Matrisi

Kriter	Yük (Payload) Modeli	Parmak İzi (Fingerprint) Modeli
Girdi Matris Boyutu	28x28 (784 Bayt)	5x5 (25 Bayt)
Toplam Parametre	267.678	28.955
Sınıflandırma Başarısı	%63.1	%62.5
Eğitim Süresi	~210 Saniye	~21 Saniye
Analiz Derinliği	Derin Paket İnceleme (DPI)	Özellik ve Davranış Çıkarımı
Genel Verimlilik	Düşük	Çok Yüksek

Sınır Bilişim (Edge Computing) İçin Stratejik Zorunluluk



Modern IoT güvenliği merkezi sunucularda değil, doğrudan cihazların ağa bağlandığı sınır noktalarda (Edge Gateways) sağlanmalıdır.

Derin paket incelemenin (Payload model) yaratacağı gecikme (latency) ve yüksek bellek ihtiyacı, kısıtlı donanıma sahip yönlendiricilerde uygulanabilir değildir. Parmak İzi (Fingerprint) yaklaşımı, gecikmesiz gerçek zamanlı izleme için pratik tek mimaridir.

Thank you

Kahraman Kostas, PhD
YYEGM, MEB

kahramankostas@gmail.com