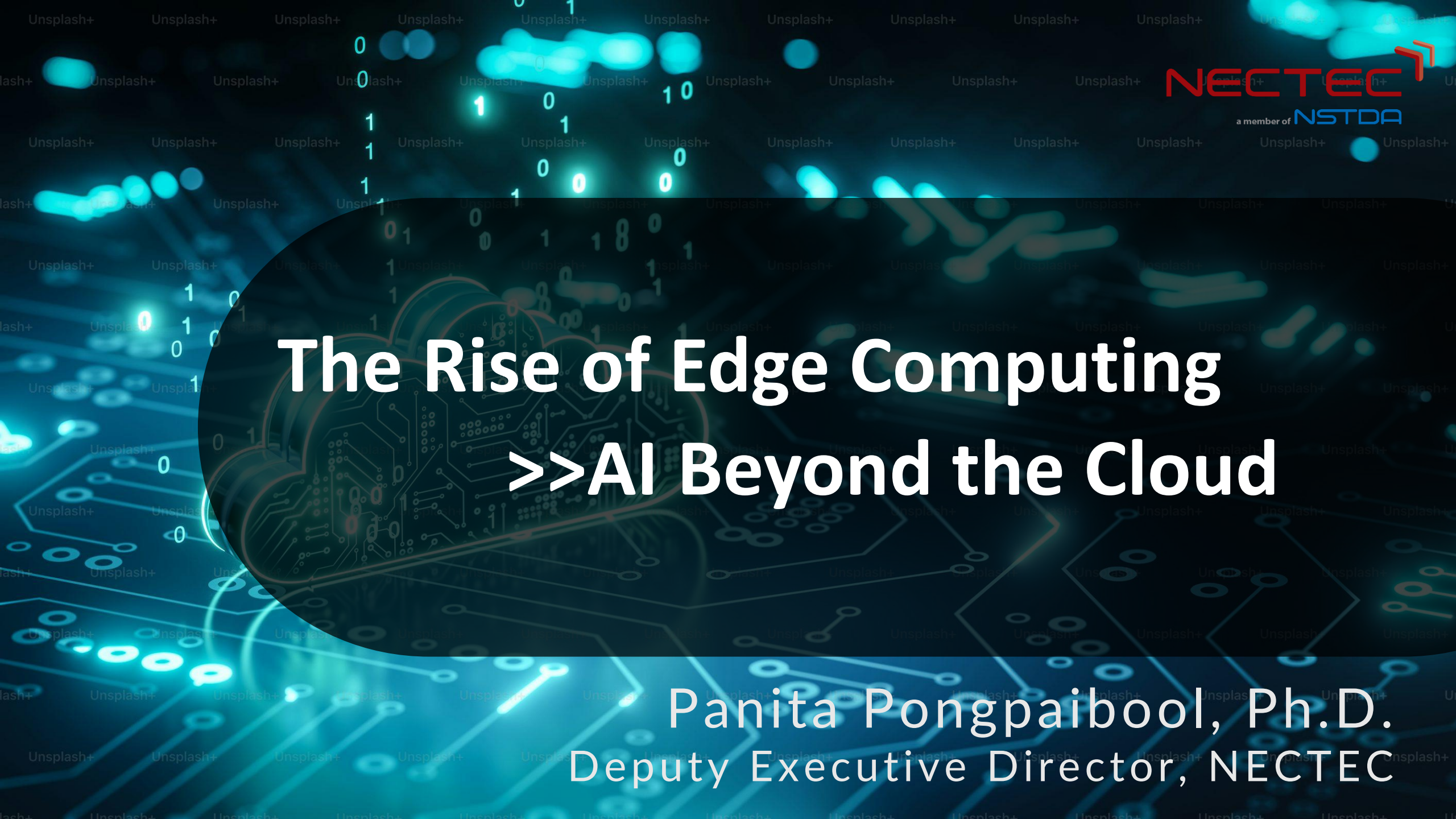


The Rise of Edge Computing >>AI Beyond the Cloud

Panita Pongpaibool, Ph.D.
Deputy Executive Director, NECTEC

Credit

ดร.เอมอัชนา นิรันตสุขรัตน์

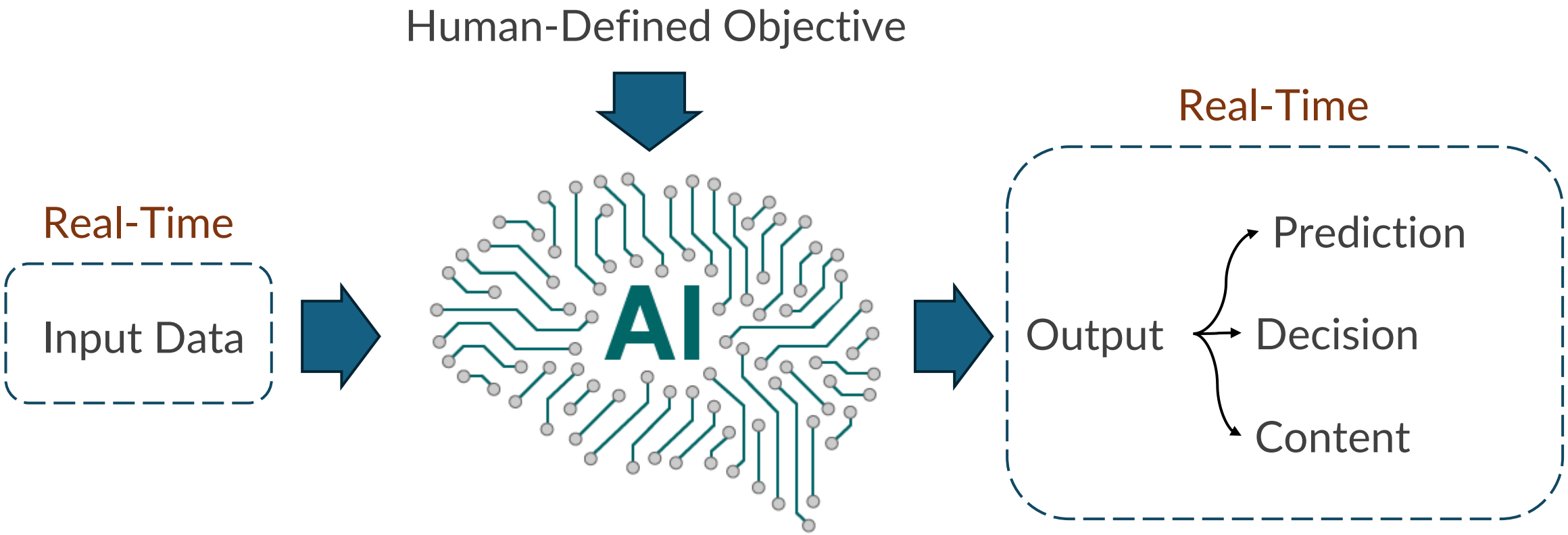
หัวหน้าทีมระบบไซเบอร์-กายภาพ
เนคเทค สวทช.

Definition of AI

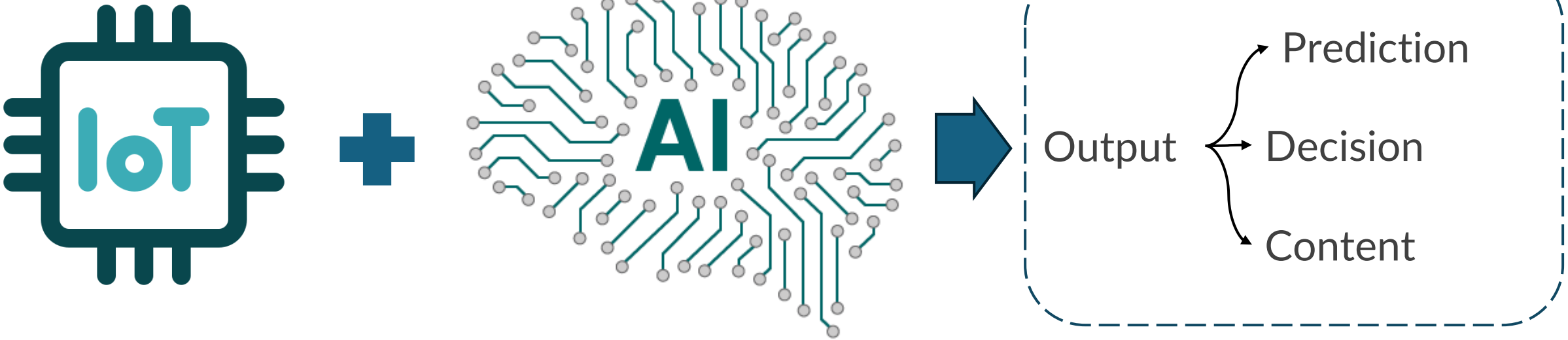
Artificial Intelligence

A technical and scientific field devoted to the engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives

Definition of AI

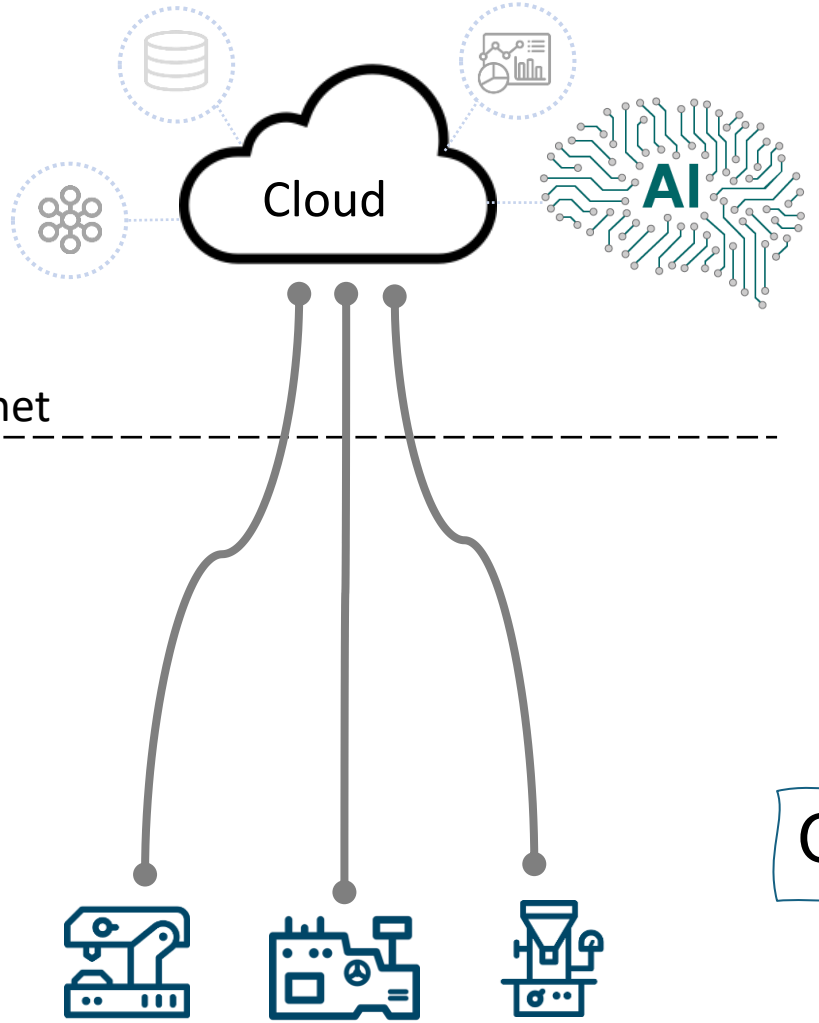


AIoT



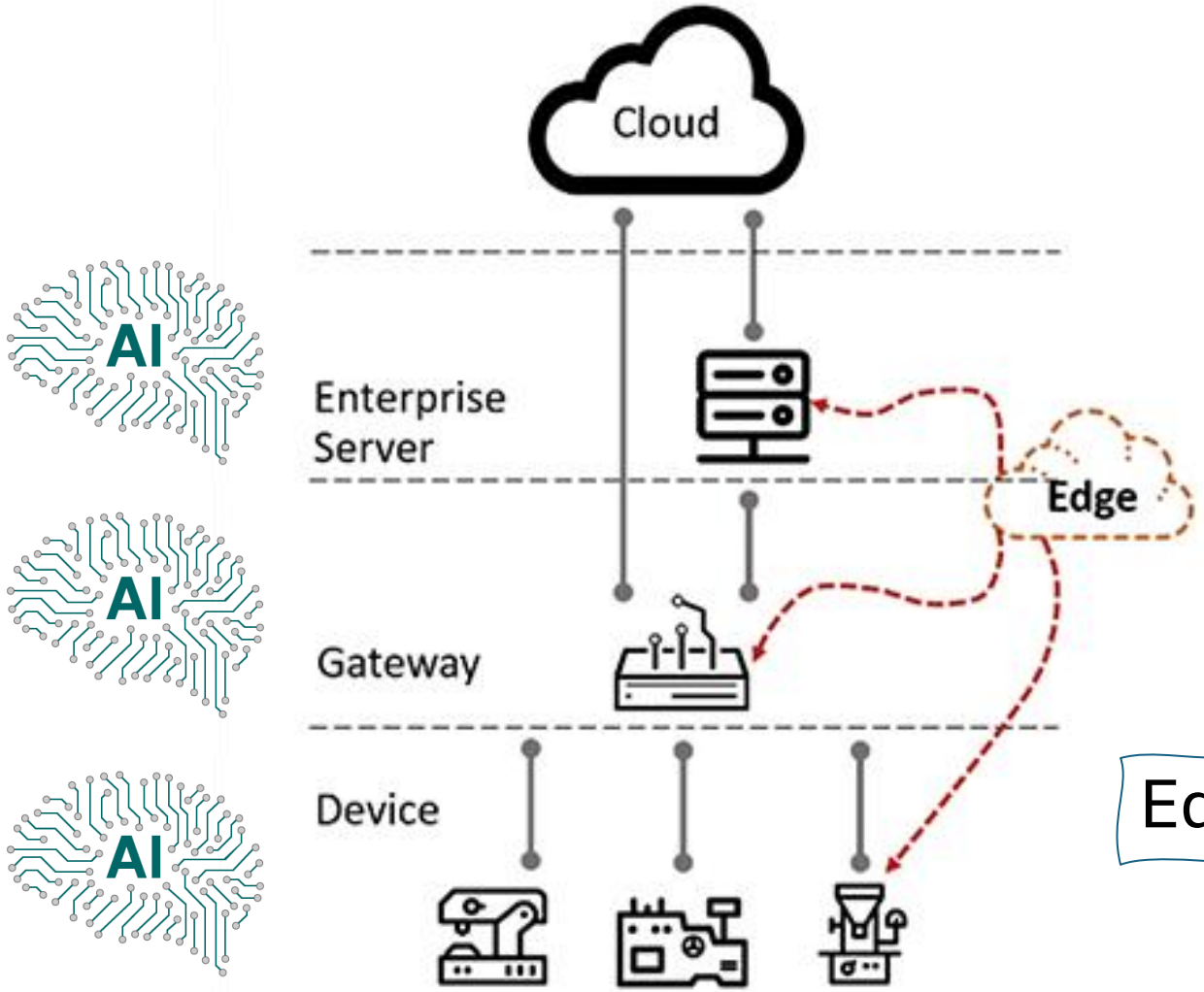
Conventional Approach : Cloud Computing

- Network bottleneck
- High-speed network cost
- Data privacy & security



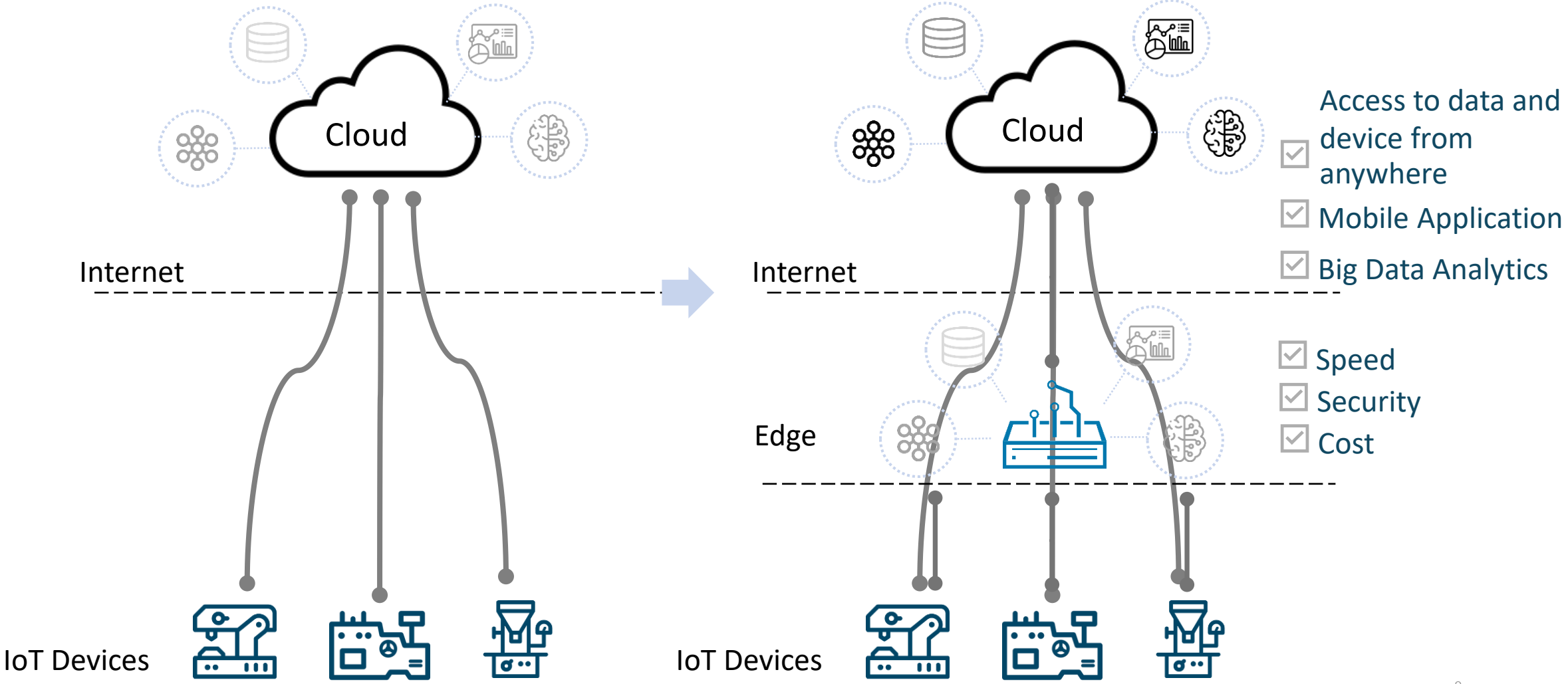
Cloud = centralized

Edge Computing

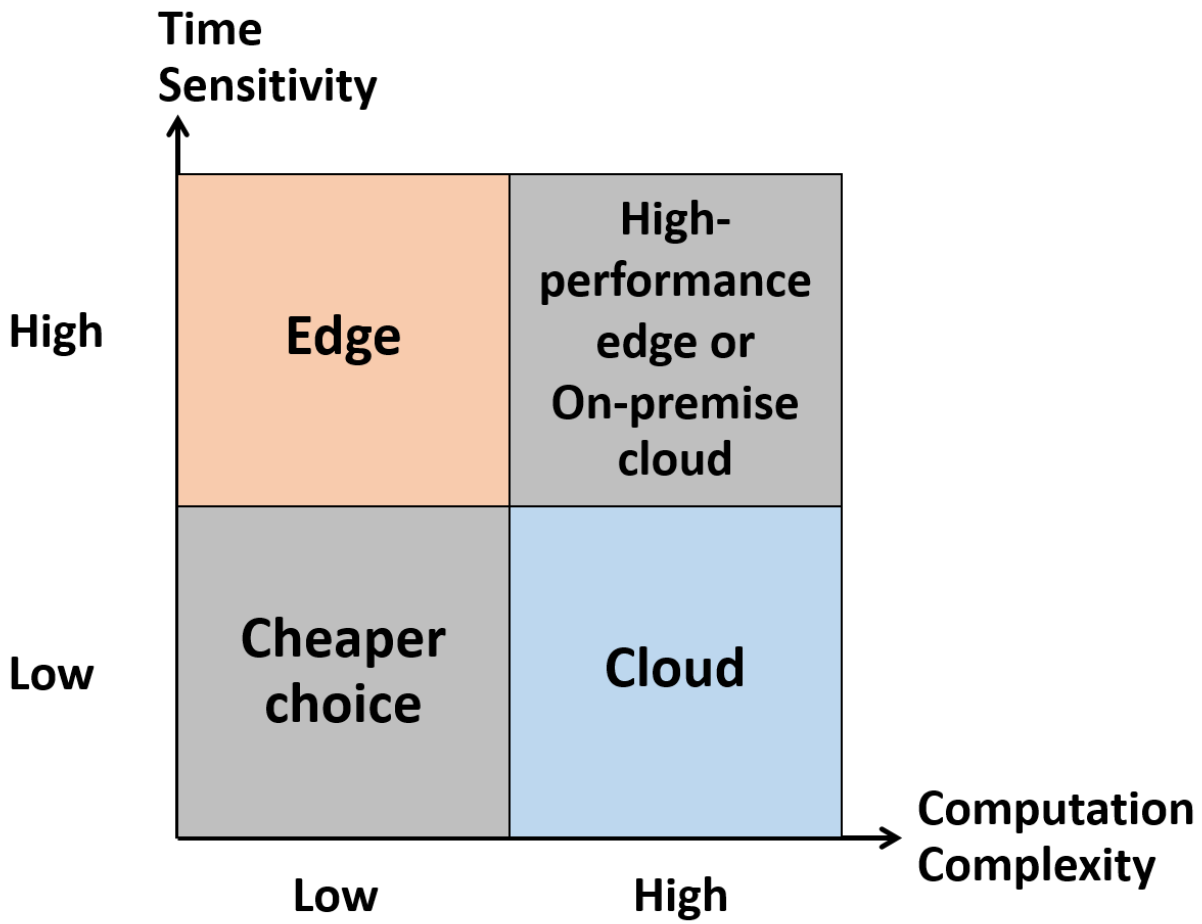


Edge = decentralized

Edge-Cloud Computing



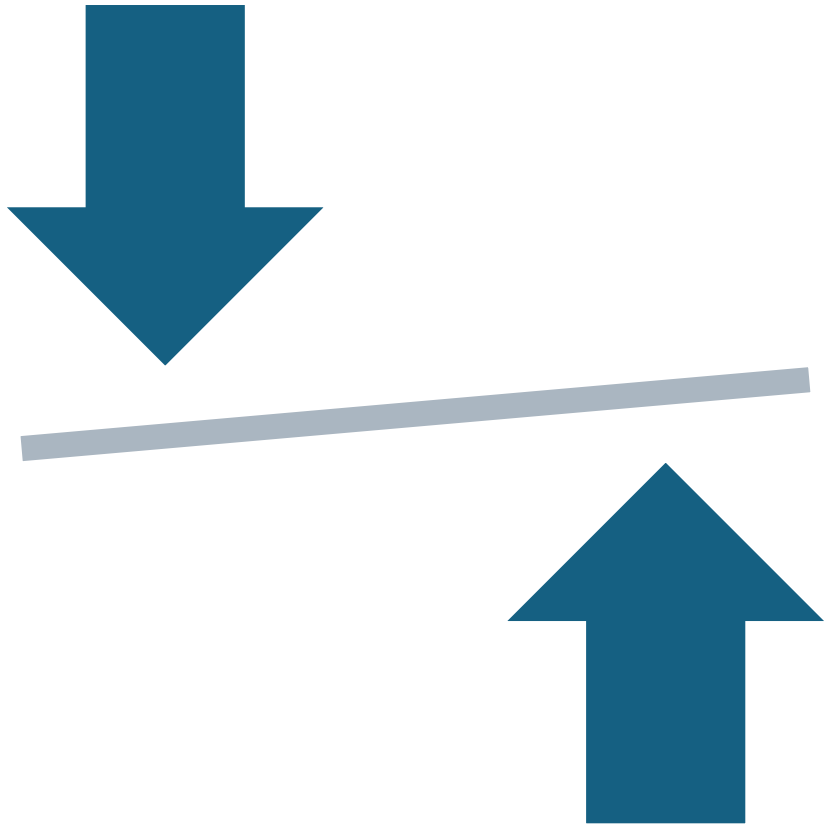
Edge vs Cloud



Pro vs. Con of Edge

Limitations

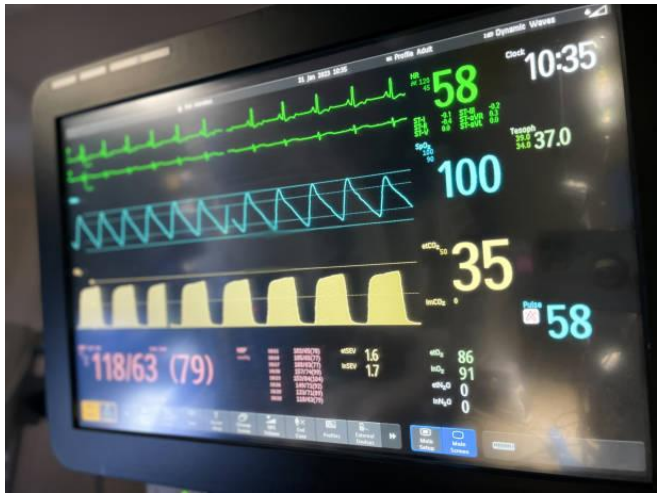
- Computing power
- Limited storage
- Diverse hardware
- Hard to maintain



Benefits

- Low delay/response time
- Low bandwidth
- Data privacy
- Cheaper device cost

Edge in Daily Life



Vital sign monitors

CCTV

Smart phones, computers

Home routers

Vacuum robots

Real-time AI at the Edge

Rescue Drones

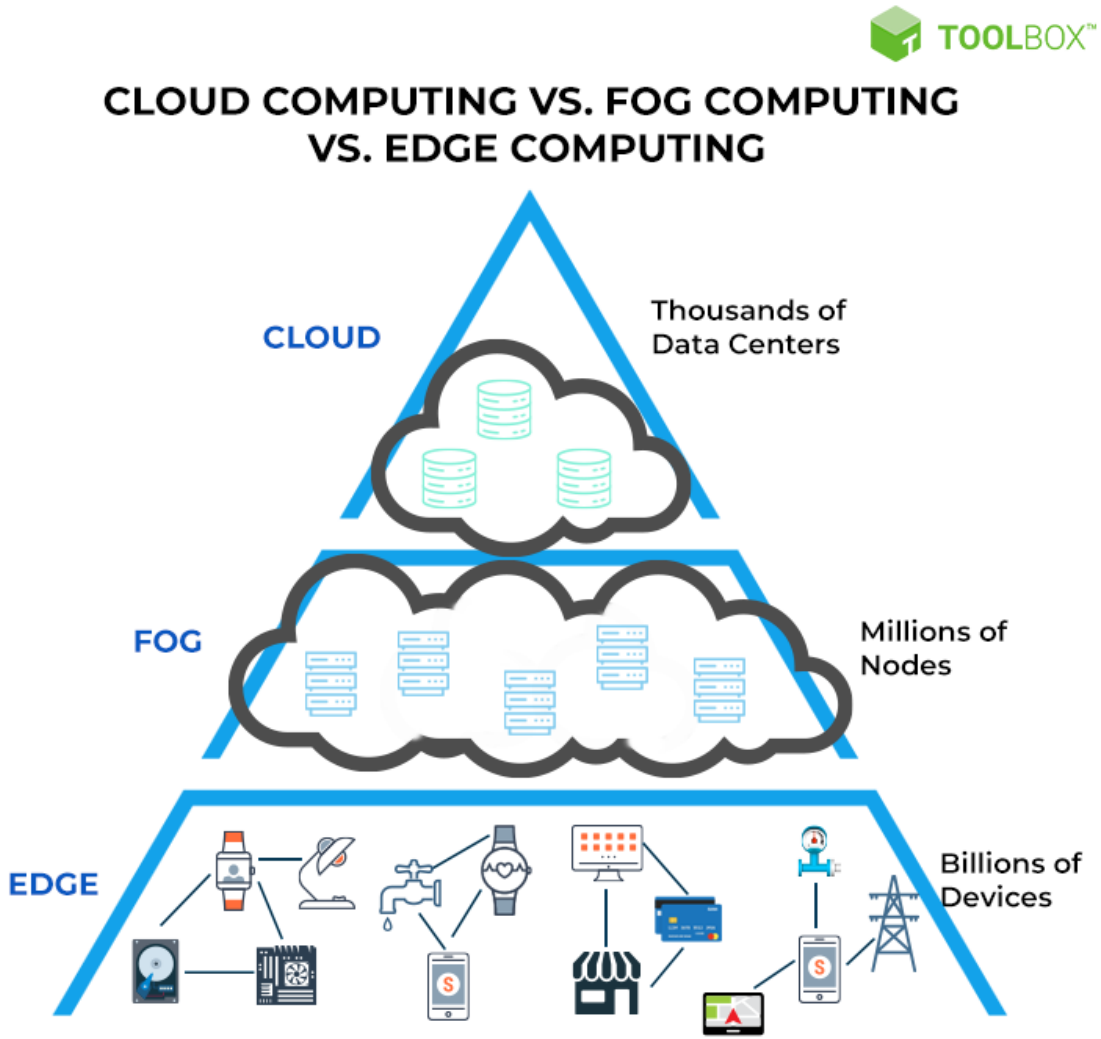
Service robots

AGV

Bin-picking robots

Self-driving cars

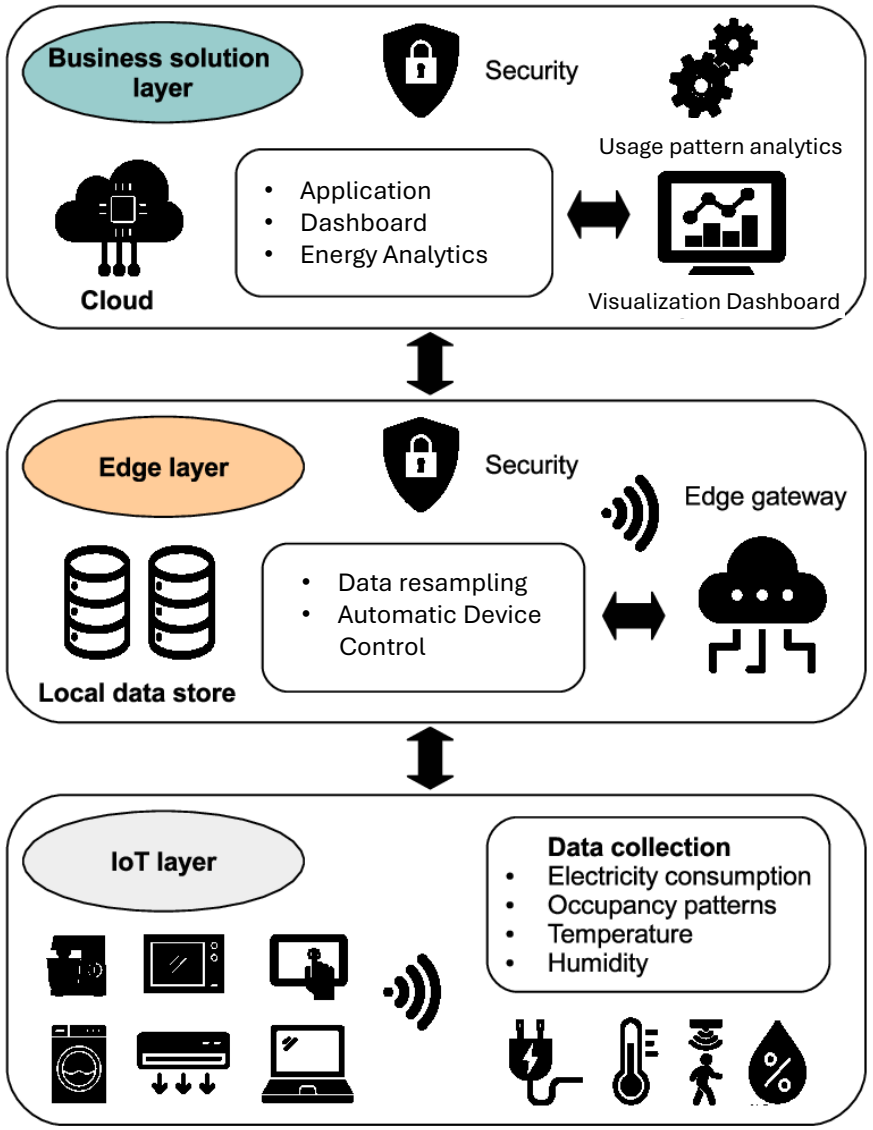
Edge-Fog-Cloud Computing



https://www.spiceworks.com/tech/cloud/articles/edge-vs-fog-computing/

EDGE COMPUTING	FOG COMPUTING
Less scalable than fog computing.	Highly scalable when compared to edge computing.
Millions of nodes are present.	Billions of nodes are present.
Nodes are installed far away from the cloud.	Nodes are installed closer to the cloud.
Edge computing is a subdivision of fog computing.	Fog computing is a subdivision of cloud computing.
The bandwidth requirement is very low. Because data comes from the edge nodes themselves.	The bandwidth requirement is high. Data originating from edge nodes is transferred to the cloud.
Operational cost is higher.	Operational cost is comparatively lower.
High privacy. Attacks on data are very low.	The probability of data attacks is higher.
Edge devices includes IoT devices or client's network.	Fog is an extended layer of cloud.
The power consumption of nodes is low.	The power consumption of nodes filter important information from the massive amount of data collected from the device and saves it in the filter high.
Edge computing helps devices to get faster results by processing the data simultaneously received from the devices.	Fog computing filters important information from the massive amount of data collected from the device.

Example of Hybrid Architecture: BMS



Hybrid Edge-Cloud Design for AI

Prioritize local processing

Only send aggregated or anonymized results to the cloud

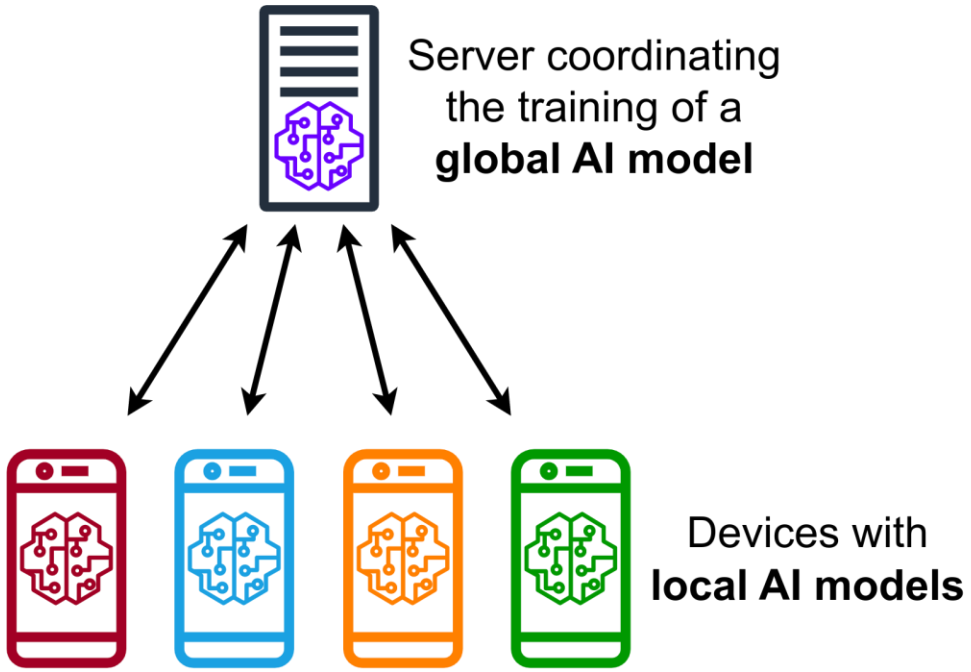
Employ federated learning

Train models locally and share only model updates with a central server

Use differential privacy

Add mathematical noise to outputs or model updates

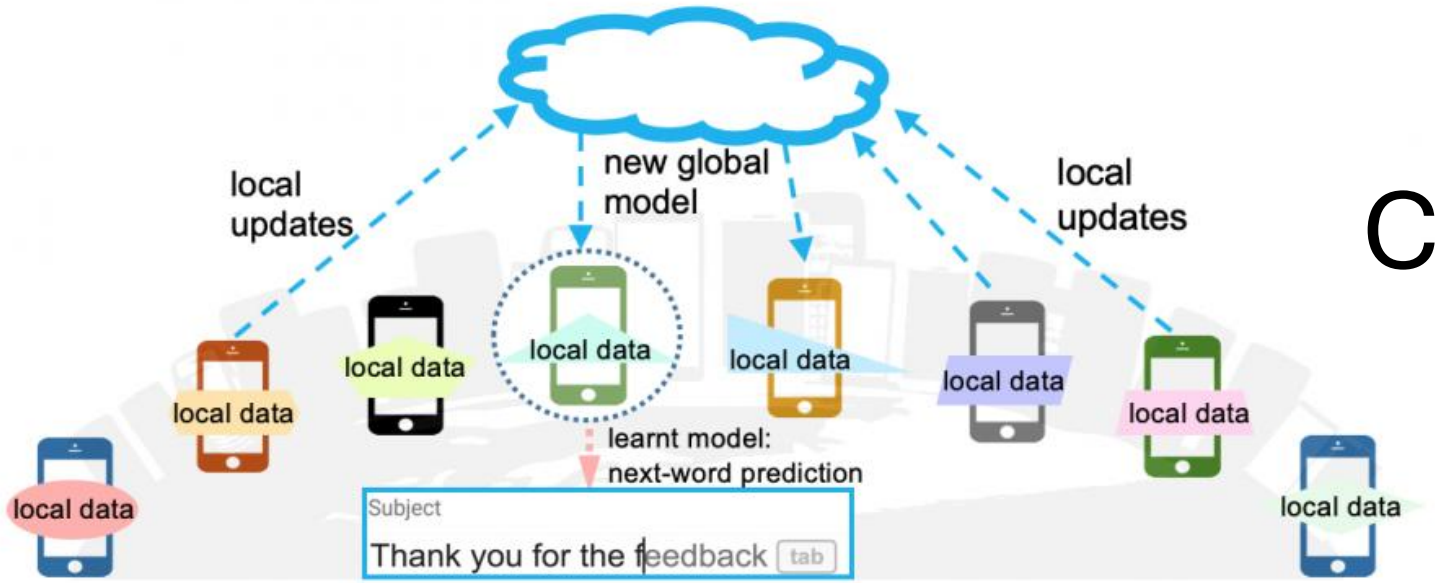
Federated Learning



privacy-preserving model training in heterogeneous, distributed networks

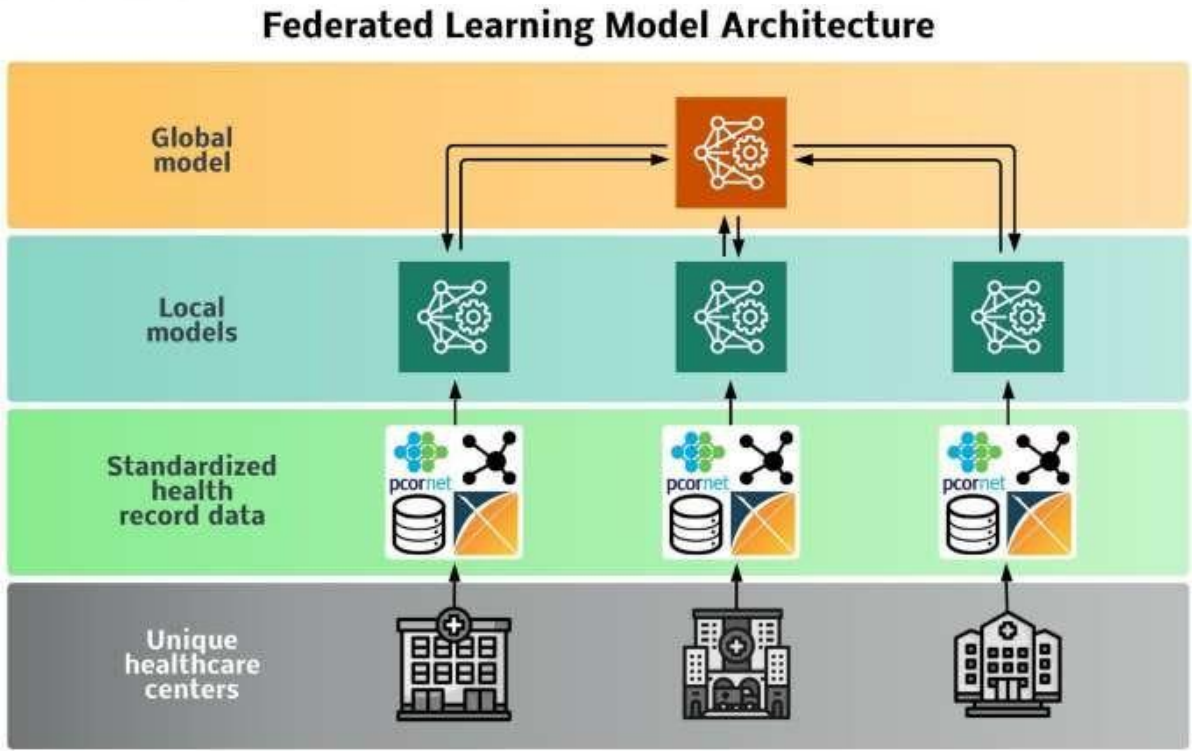
Principles:

1. **Local Data Stays Local**
2. **Collaborative Model Training**
3. **Privacy by Design**
4. **Efficiency and Scalability**



Cross device model

Cross silo model



Benefit of FL

Hyper-Personalized

Low Cloud Infra Overheads

Minimum Latencies

Privacy Preserving

Enhanced Privacy and Security

- Data localization
- Encryption and differential privacy

Reduce Bandwidth Requirement

- Model update compression
- Asynchronous communication

Decentralized Learning

- Leverage edge computing
- Scalability and flexibility
- Empower local intelligence

Challenges in FL

Expensive Communication

Systems Heterogeneity

Statistical Heterogeneity

Privacy Concerns

Hybrid Edge-Cloud Design for AI

Prioritize local processing

Only send aggregated or anonymized results to the cloud

Employ federated learning

Train models locally and share only model updates with a central server

Use differential privacy

Add mathematical noise to outputs or model updates

AI Model Security

Model integrity

Protect against tampering of the AI models deployed at the edge

Adversarial robustness

Edge models are more exposed to adversarial input attacks.
Testing and hardening are important.

Monitoring & logging

Track model behavior locally and centrally to
detect anomalies or misuse.

Life Cycle Management

Patching & updates

OTA updates should be secure and regular.

Secure decommissioning

Wipe all sensitive data and cryptographic keys from retired devices.

Audit & compliance

Ensure deployments meet data protection regulations (GDPR, HIPAA, PDPA, etc.).

Limitations of Existing Edge Development Platforms

Dimension	Limitation
Flexibility	• Hard to update or switch AI models • Often tied to specific hardware or SDK
Model Lifecycle	• No simple versioning, rollback, or A/B testing • Retraining & redeployment is complex
Scalability & Maintenance	• Difficult to manage thousands of edge nodes • Updates and monitoring are resource-intensive
Cost	• New hardware often required for new use cases • High maintenance and operational costs
Security & Compliance	• Irregular patching and OTA updates • Risk of data privacy and regulatory issues

Why We Need
a New Edge Development Platform

Existing Platforms: Limitations

Next Step:

Edge Development Platform

Future Needs: New Platform

- **Flexible**
- **Easy model update**
- **Central management**
- **Lower cost**
- **Security**

Introducing

Edge-AI customization made easy

https://daysie.io

https://www.youtube.com/watch?v=rpSyE9-2IRA

เมฆหรือหมอก Cloud or Fog

เมฆและหมอกหลอกตาน่าครุ่นคิด
อันไอน้ำกระจิริดมหาศาล
ยามอยู่เดี่ยวมองไปไม่เห็นธาร
รวมกันอยู่ดูดังม่านขาววาวตา
เมฆหรือหมอกหลอกตาน่าฉงน
อันหนึ่งอยู่เบื้องบนโพ้นขอบฟ้า
อันหนึ่งอยู่ต่ำเตี้ยเรี่ยยอดหญ้า
ต่างคุณค่าต่างหน้าที่ต่างมีคุณ
ดังมนุษย์เกิดมาครบสามสิบสอง
มีสมองสองมือเท้าก้าวเกื้อหนุน
ทำประโยชน์ที่แตกต่างอย่างสมดุล
จิตการุณกูลเกื้อเอื้ออาทร

พนิตา พงษ์ไพบูลย์

คอลัมน์ ทันกระแส IoT, Post Today, November 9, 2017