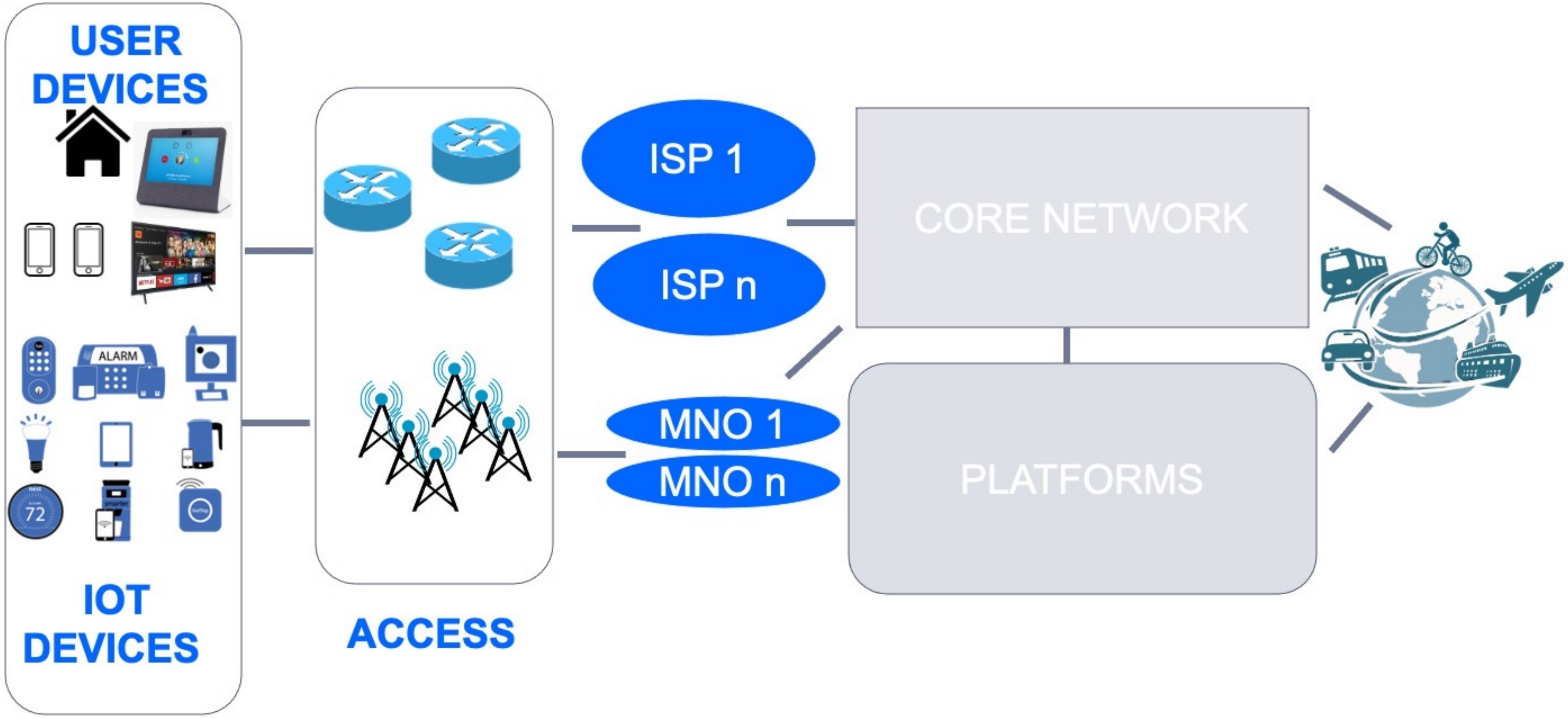
Telefónica

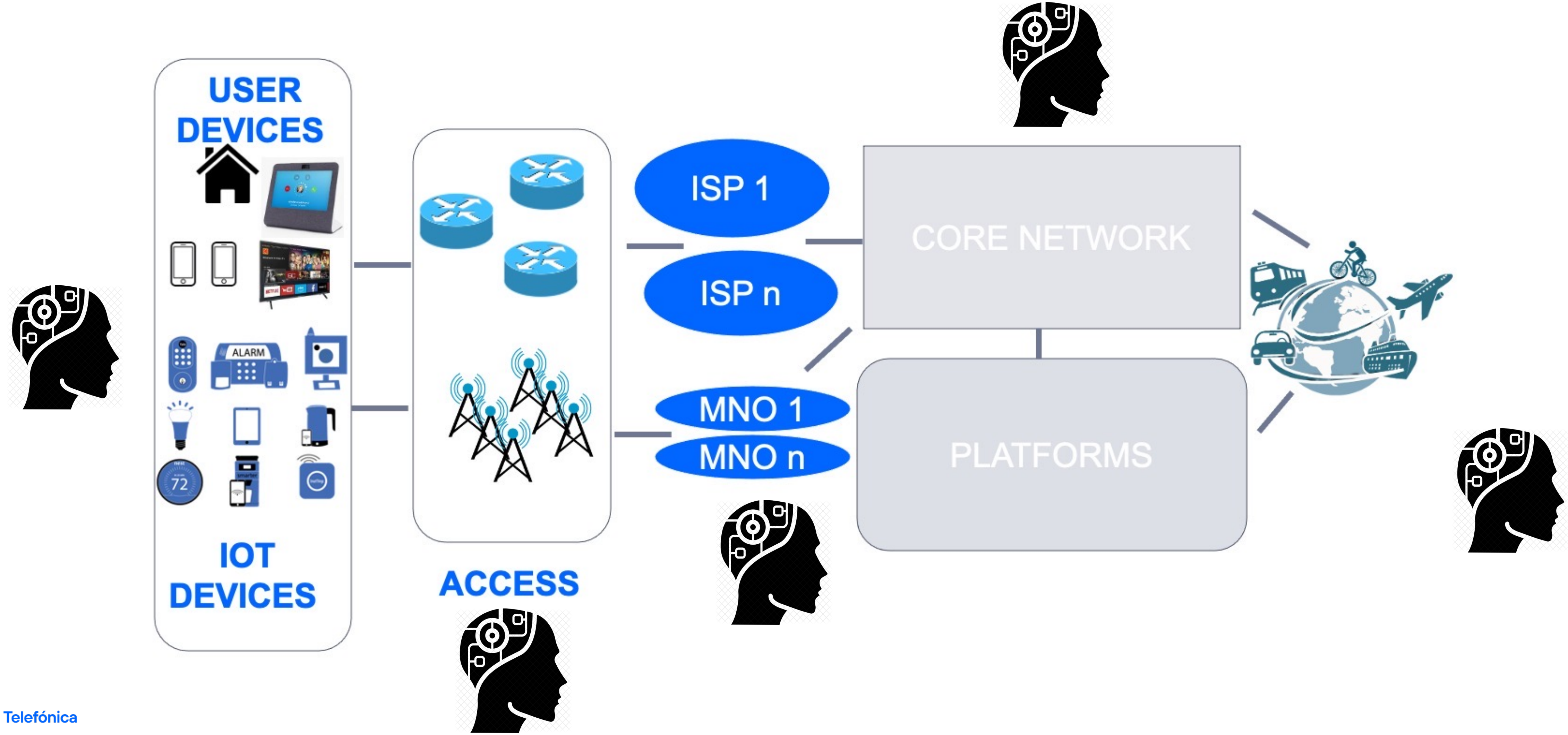
Artificial Intelligence and Decentralized Privacy Preserving Mechanisms for Telco Industry

Diego Perino
Telefonica Research

Telco "Networks" are complex!



Artificial Intelligence to the rescue ? !



USER DEVICES

IOT DEVICES

ACCESS

ISP 1

ISP n

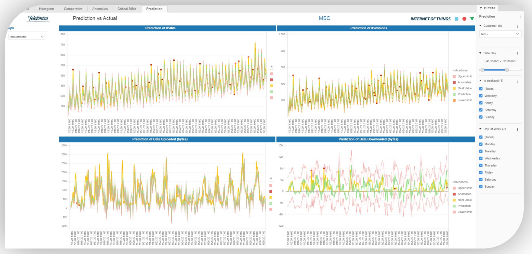
MNO 1

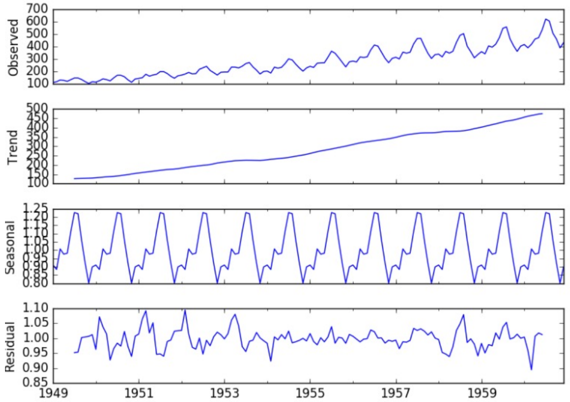
MNO n

CORE NETWORK

PLATFORMS

Intelligence for Networks…



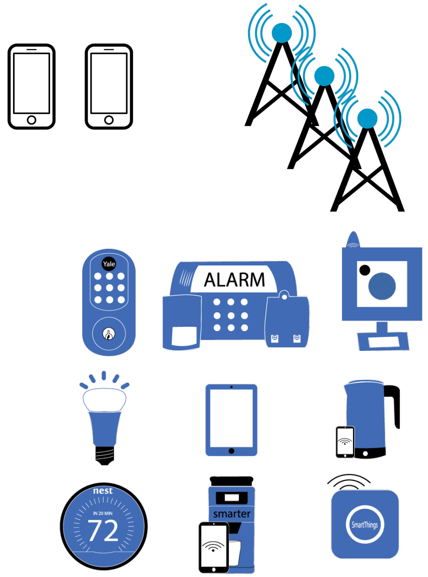


Platforms

- Cloud and Edge management
- IoT devices operations and added value services

Quality of Service/Experience

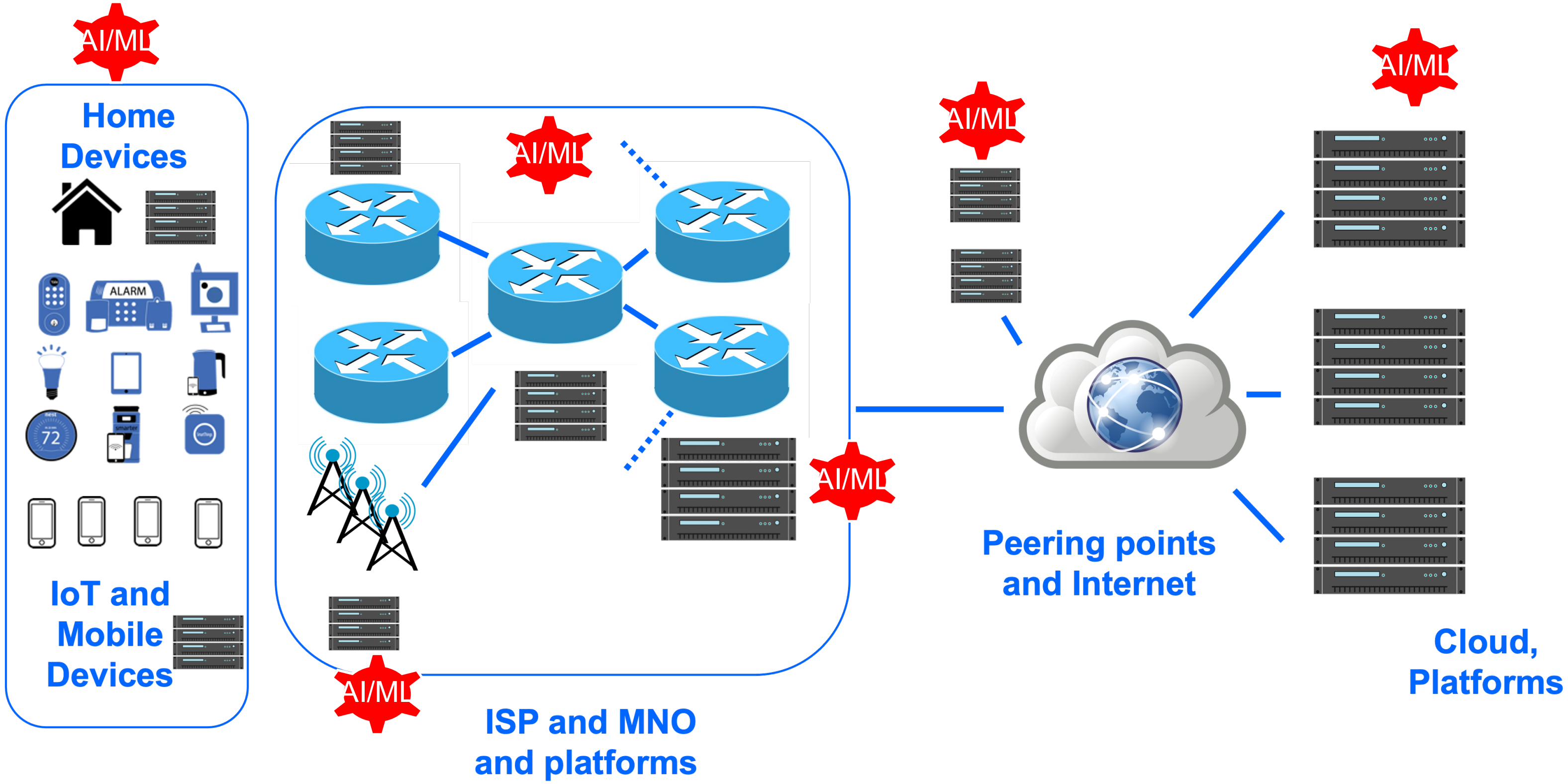
- Predict and Monitor Quality
- Detect Anomalies and React



Edge/Core networks

- Network Planning
- Network Operations
- Network Management

…networks for Intelligence



Networks for AI-based applications (e.g., XR)

- Provide processing capabilities everywhere

Networks as distributed Learning Infrastructure

- Distributed Learning, Federated Learning

Sustainable mobile broadband to unconnected people

Infrastructure with open-access technology and a revenue-sharing model

Thousands of small communities (2-3-4G)

MOUNTAIN 61%

COAST 14%

RAINFOREST 15%

Different power supply

SOLAR PANELS

POWER GRID

BATTERY

Heterogeneous third-party backhaul networks

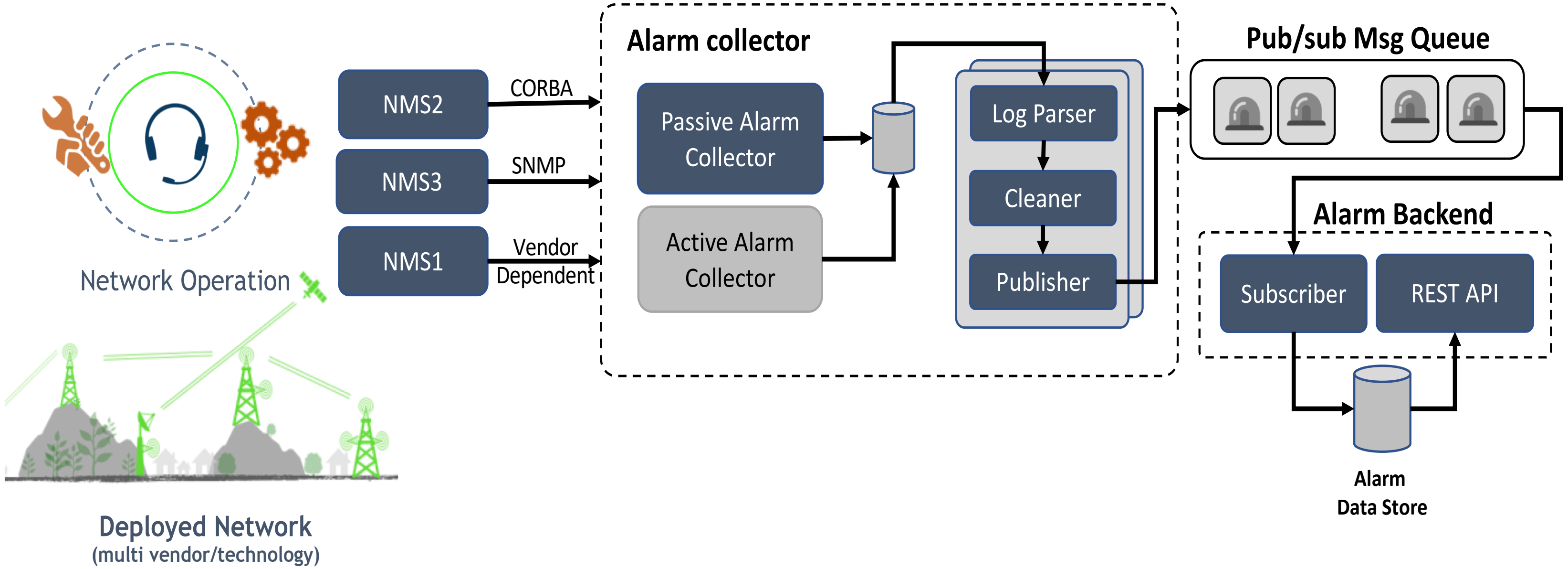
RADIO LINKS

SATELLITE

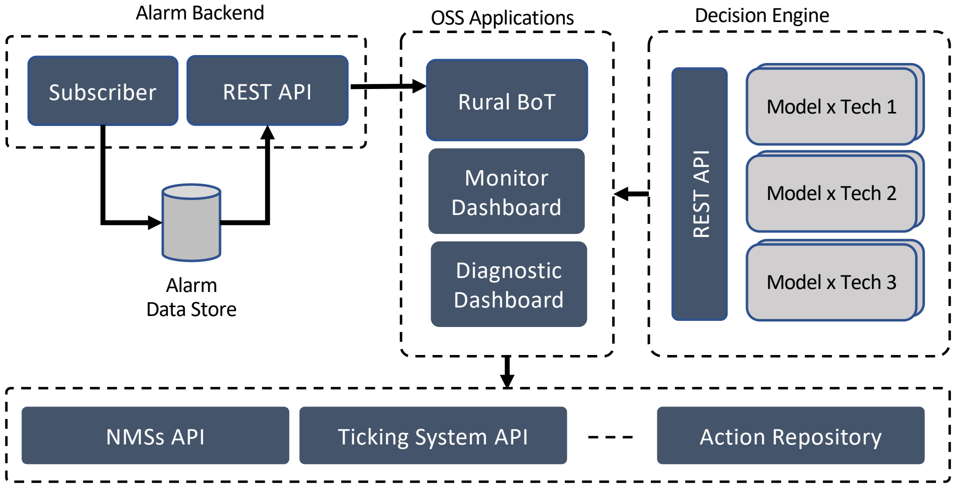
FIBER

Predefined route for operations (some site have no direct road access)

Micro-cell network operation

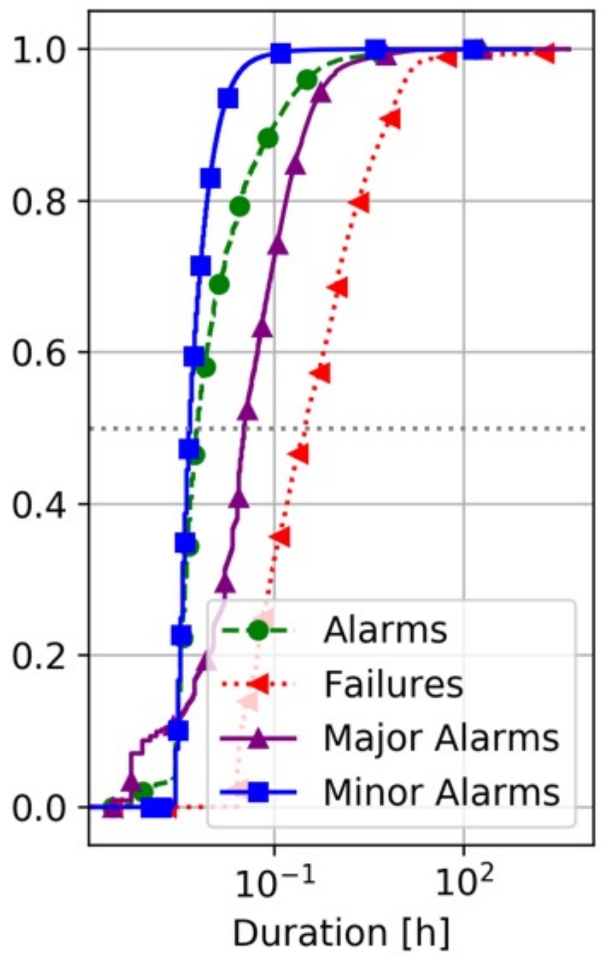


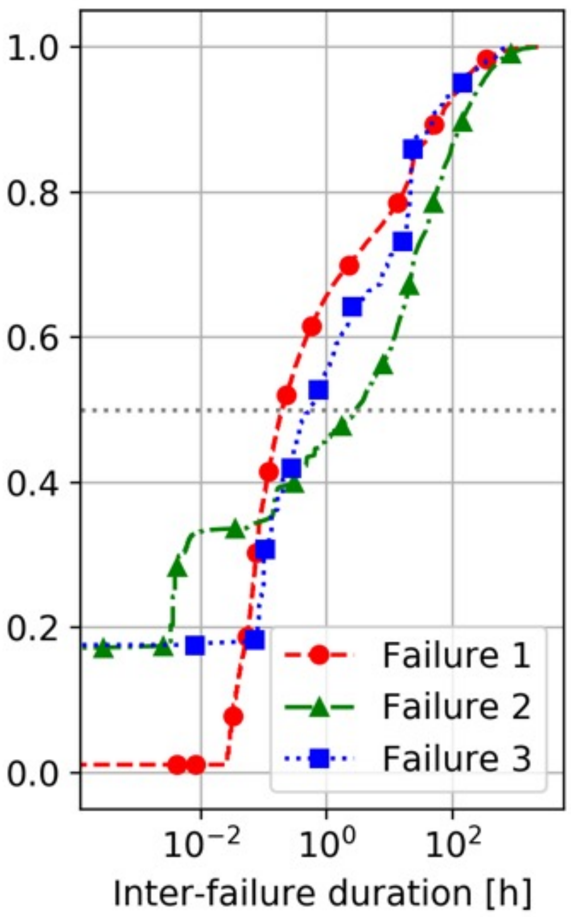
- Different KPIs for different vendors/radio technologies
- Alarms stored with active/cleared state



- Several apps for network management

Micro-cell network operation: 5 months data analysis

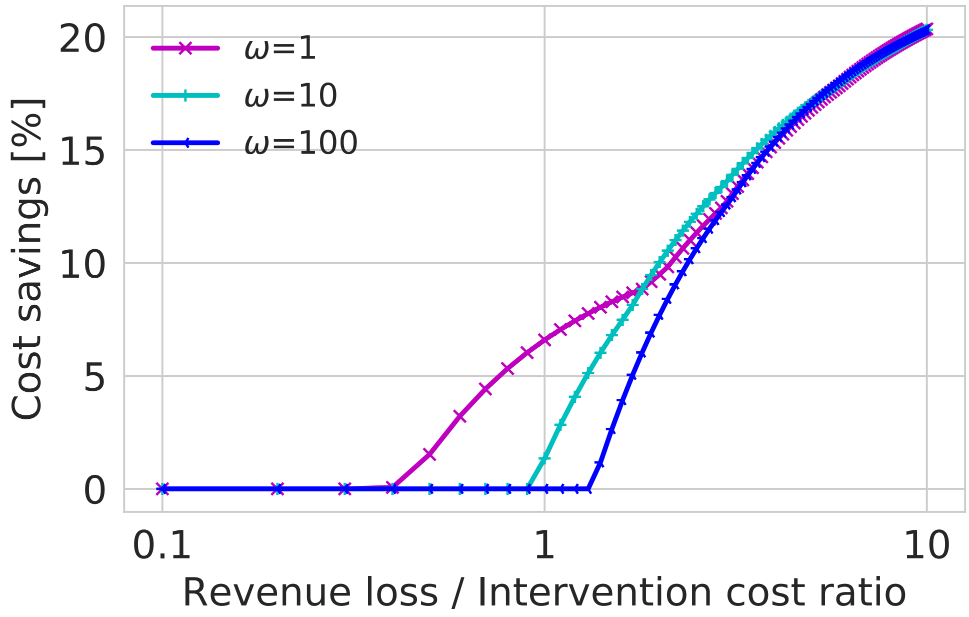


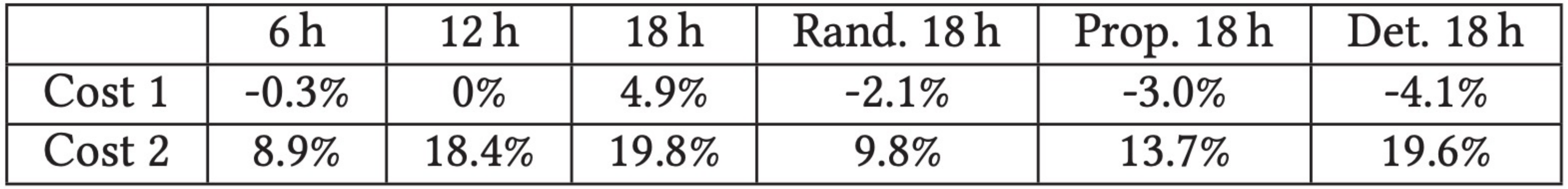


- Most failures are temporal: backhaul saturation or battery outages
- Control and predictive mechanism to avoid costly and unnecessary intervention
- It is critical to understand the nature of the failure

Conclusions and lessons learnt

- We need a good understanding of the status of the network, failures and field operation teams to contain costs
- Failures are mostly temporal and mainly caused by power outages or congestion issues
- Need of control and predictive mechanisms, and to understand the cause of the failure
- ML (and DL) and analytics can actually help to reduce costs (5-20% and design better rule-based systems)





	6 h	12 h	18 h	Rand. 18 h	Prop. 18 h	Det. 18 h
Cost 1	-0.3%	0%	4.9%	-2.1%	-3.0%	-4.1%
Cost 2	8.9%	18.4%	19.8%	9.8%	13.7%	19.6%

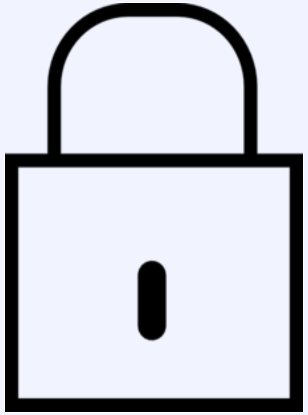
Diego Perino, Xiaoyuan Yang, Joan Serra, Andra Lutu, Ilias Leontiadis, Experience: Advanced Network Operations in (Un)-Connected Remote Communities, in proc. of ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), September 2020

Challenges for current and future networks

- Global, holistic, end-to-end approach
- Usability and explainability
- Data/ground truth availability and quality
- Co-existence with traditional solutions
- Robustness
- Sustainability
- Accountability, Transparency and Fairness

…

How to get the benefits of AI while preserving user privacy and security?



Privacy Preserving Artificial Intelligence

Differential Privacy

Secured Multi-Party Computation

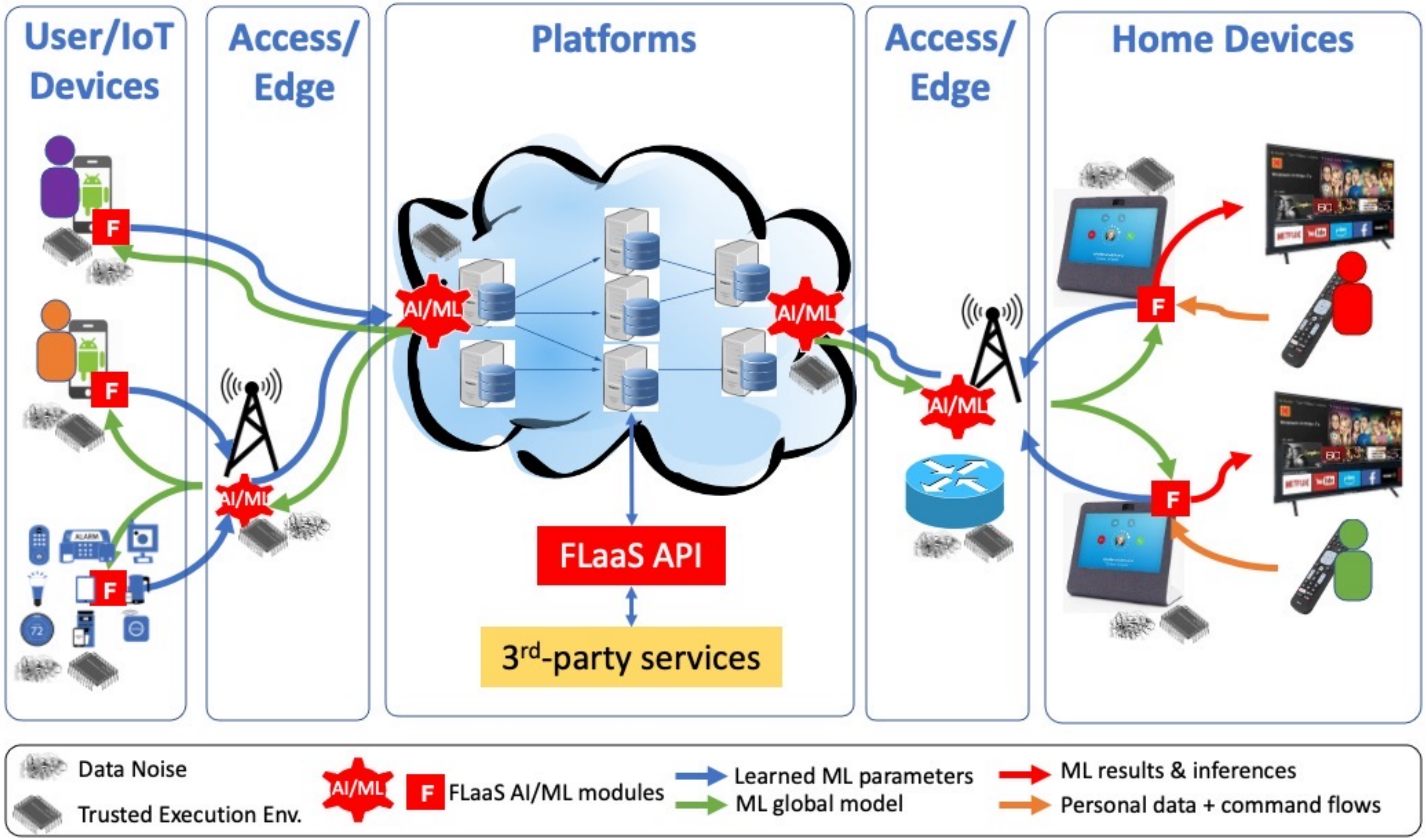
Fully Homomorphic Encryption

Federated Learning

Trusted Execution Environments

…

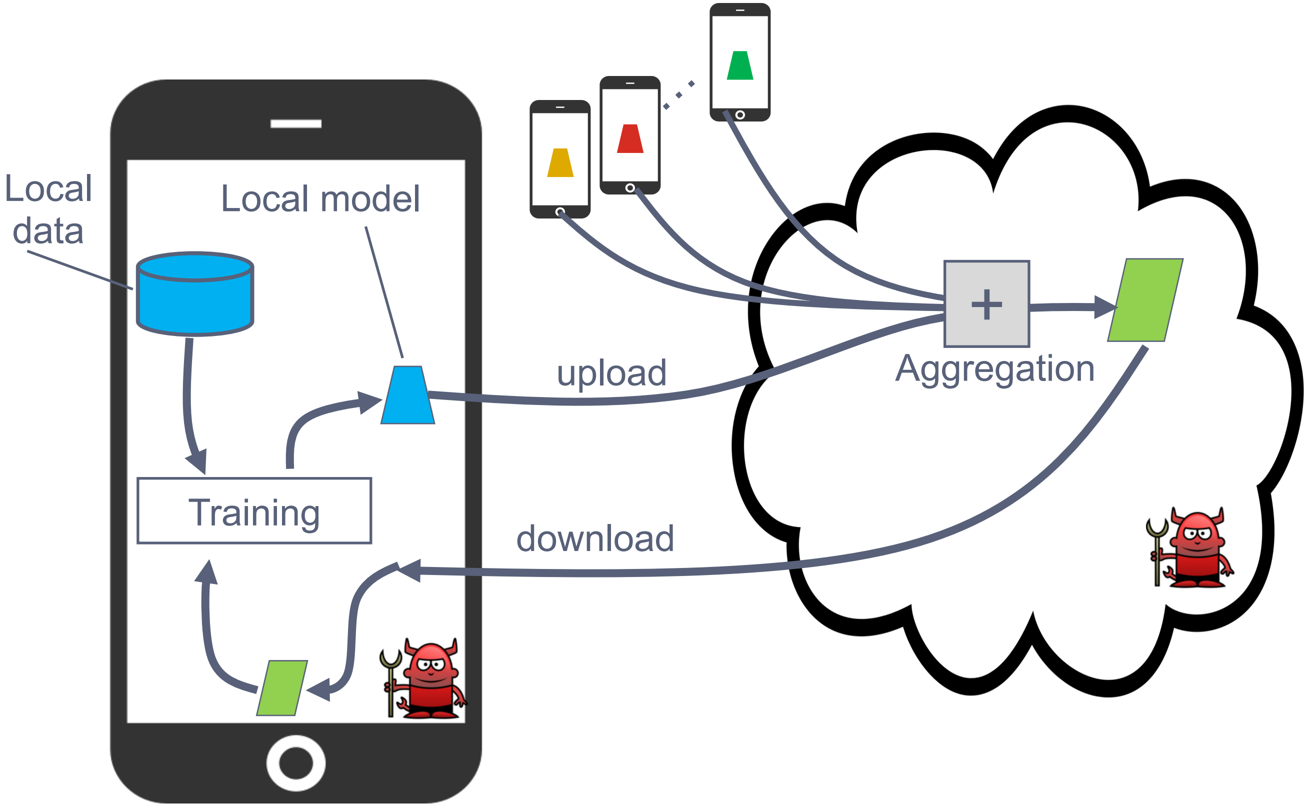
Example: Federated Learning as a Service (FLaaS)



Federated Learning may lead to privacy issues

-Models/gradients memorize datasets

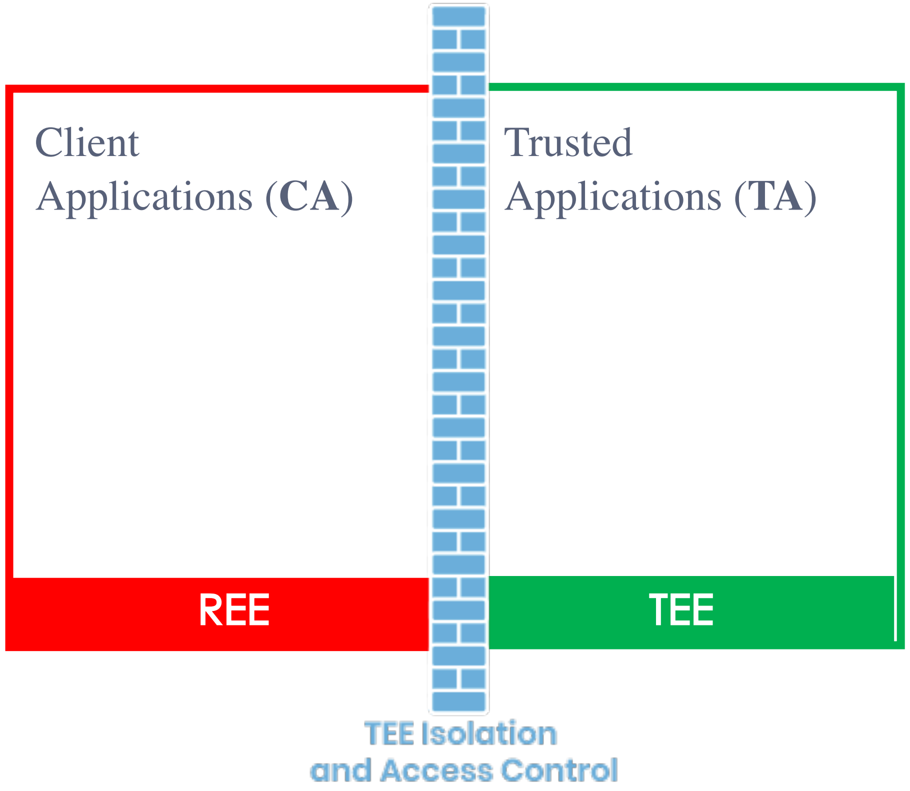
- Privacy-related attack
  - ○ Data reconstruction attack (DRA)
  - ○ Property inference attack (PIA)
  - ○ Membership inference attack (MIA)



Trusted Execution Environments

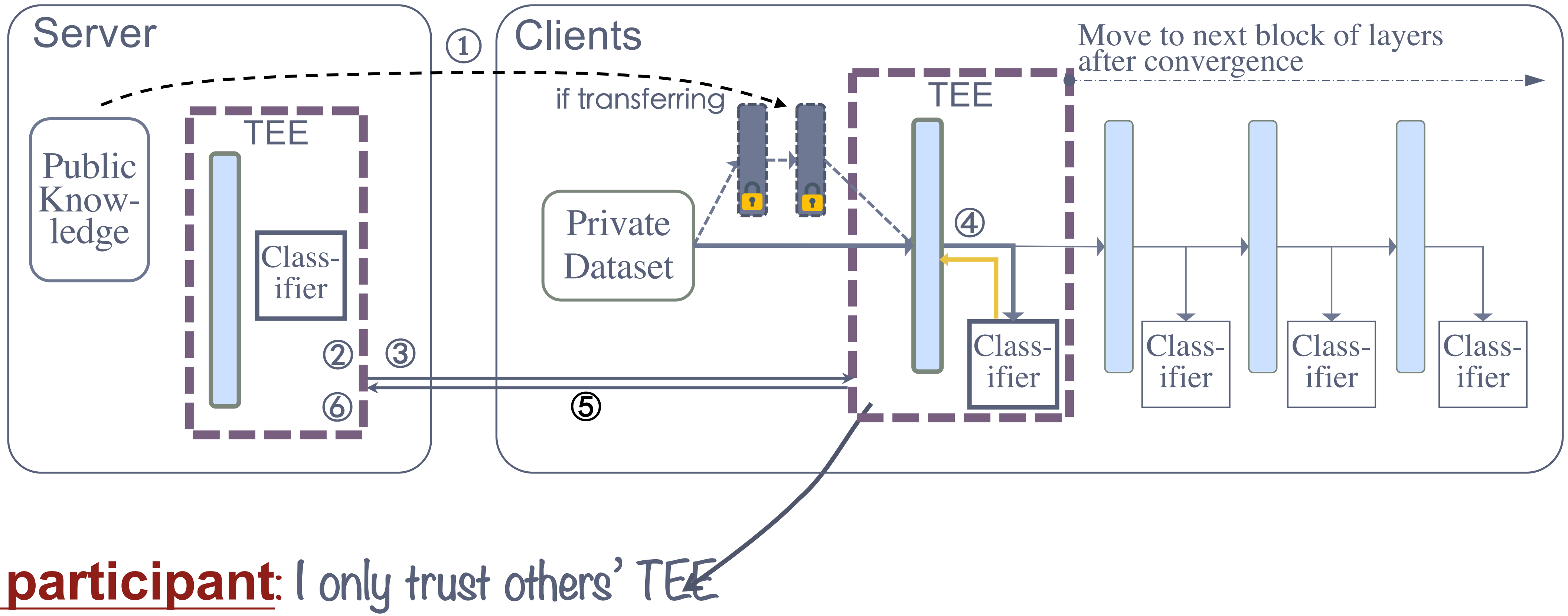
- DL with TEEs
  - Intel SGX ***vs*** Arm TrustZone
  - Inference ***vs*** Training
- Limited computational resources
  Secure memory
  - 128MB for Intel SGX
  - 16MiB for Arm TrustZone

Can we leverage TEEs for Federated Learning?



PPFL: Privacy-preserving Federated Learning with Trusted Execution Environments

Leveraging Greedy Layer-wise Learning



Any participant: I only trust others' TEE

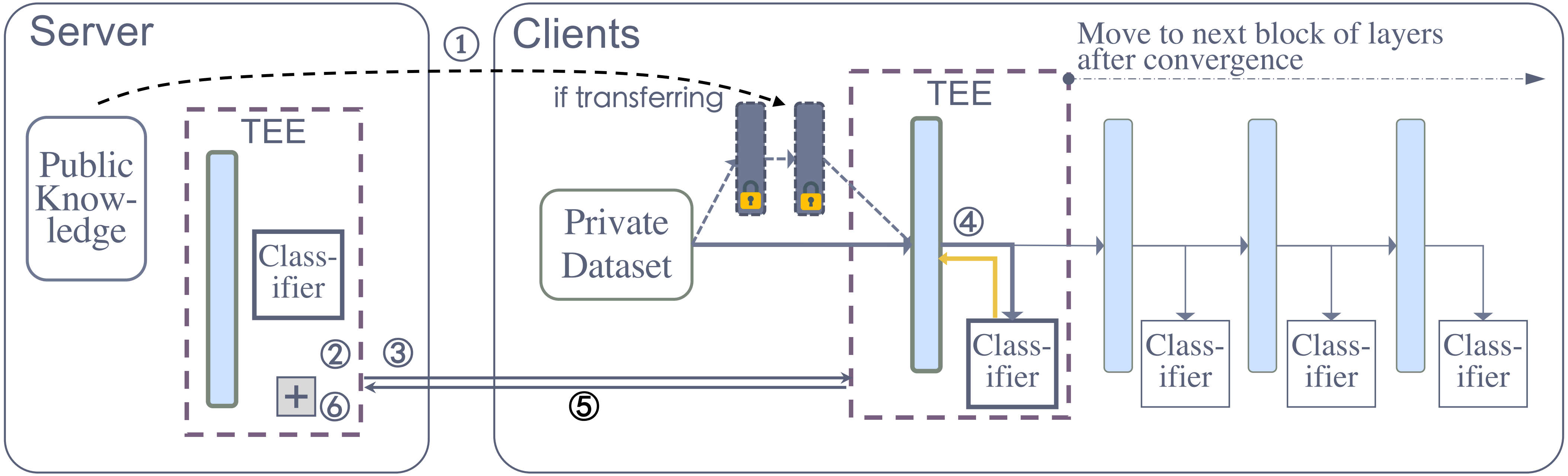
PPFL: Privacy-preserving Federated Learning with Trusted Execution Environments

Configuration

Device selection & secure channel
Transferring knowledge if any ①
Model initialization ②
model broadcasting ③

Reporting

Layer-wise local training ④
model reporting ⑤
Secure aggregation ⑥



Performance Evaluation and Summary

Privacy

- Protecting training layers to defend against privacy-related attacks

Model performance

- Comparable ML utility with even less communication cost

System cost

- ~15% CPU time, ~18% memory usage, ~21% energy consumption

Layer wise training

- Multi-layer block for heterogeneous environments

Code -> https://github.com/mofanv/PPFL

Fan (Vincent) Mo, Hamed Haddadi, Kleomenis Katevas, Eduard Marin, Diego Perino and Nicolas Kourtellis, PPFL: Privacy Preserving Federaded Learning with Trusted Executed environment, ACM Mobisys 2021 Best paper award
https://arxiv.org/pdf/2104.14380.pdf

Takeaways

- **AI can help networks for a better reliability, quality and security/privacy**
- **Networks can also help AI-based applications**
- **Challenges ahead but many promising solutions and directions**

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

SPATIAL

CHARITY
Cloud for Holography and Augmented RealITY

DAEMON

ACCORDION

PIMcity

Diego Perino, Kleomenis Katevas, Andra Lutu, Eduard Marin, and Nicolas Kourtellis, Privacy-Preserving AI for Future Networks
https://dl.acm.org/doi/pdf/10.1145/3512343