SECURITY CONSIDERATIONS FOR MOBILE EDGE COMPUTING

Rajeev Shorey (PhD)

Fellow INAE, Distinguished Scientist ACM
Distinguished Lecturer, IEEE Future Networks TC

CSE Department
Indian Institute of Technology, Delhi
India

LSU
16 November 2023

IEEE Future NETWORKS™

Enabling 5G and Beyond

IEEE

IEEE Future Networks – FutureNetworks.ieee.org

IEEE Future NETWORKS

Collaboration

IEEE Antennas and Propagation Society · CAS · IEEE ComSoc IEEE Communications Society · IEEE Electronics Packaging Society · ITSS IEEE Intelligent Transportation Systems Society · MTT-S · IEEE Reliability Society · SSCS · IEEE VTS Connecting the Mobile World

Content

IEEE Future Networks Tech Focus Issue 16, June 2023

+ technical newsletter, podcasts, videos, articles

Events

IEEE Future Networks World Forum • 2022 · IEEE Connecting the UNCONNECTED SUMMIT An IEEE Future Networks Program · 2022 5th IEEE 5G Workshop on First Responder and Tactical Networks, November 7, 2022, 8:30 AM–5:00 PM

+ more!

Research & Education

IEEE INGR International Network Generations Roadmap

+ eLearning, webinar series, white papers, tutorials

Join today! bit.ly/fntc-join

IEEE Future Networks

Be connected to IEEE Future Networks to shape future network requirements

Get monthly updates on technical workshops, summits, webinars, podcasts, and call for proposals, papers, and volunteer opportunities

Thousands are already members

Join today: bit.ly/fntc-join

Agenda of the Tutorial

- Introduction & Motivation
- Mobile Edge Security (MEC)
- MEC Architecture
- Security issues in Emerging Edge Paradigms
  - *Federated Learning*
  - *Reinforcement Learning*
- Summary and Future Directions

The Buzz on Edge Computing

Edge Computing

Edge Computing | News, how-tos, features, reviews, and videos

DATA CENTER EXPLORER By Andy Patrizio

Intel details FPGA roadmap

IBM, Bharti Airtel partner on edge cloud offerings in India

McLaren Racing relies on edge computing at Formula 1 tracks

McLaren's Formula 1 racing team securely delivers apps and data to track crews and guests via VMware Workspace ONE.

DATA CENTER EXPLORER By Andy Patrizio

HPE to ship a dedicated inference server for the edge

The small form factor HPE Edgeline EL8000 is designed for AI tasks such as computer vision and natural-language processing.

Akamai

Products & Solutions | Why Akamai | Resources

Solutions > Edge Compute

Edge Compute Solutions

Innovate in real time. With the world's largest serverless compute platform, Akamai puts your code closer to your users.

Edge Computing

Edge Computing | News, how-tos, features, reviews, and videos

CLOUD COMPUTING By David Linthicum

Cloud computing is reinventing cars and trucks

CLOUD COMPUTING By David Linthicum

The dirty little secret about edge computing

NEW TECH FORUM

Why edge computing matters for modern software development

The next stage of cloud computing brings computing power closer to users, paving the way to better user experiences and more intelligent applications.

Edge Computing Spend

- **Report by Market research firm IDC**

- **Edge computing spend is expected to surpass $300 billion by 2026, with a compound annual growth rate of 15% during the three year period**

- **Edge computing spend to be $208 billion in 2023, a 13.1% increase on 2022 spend !**

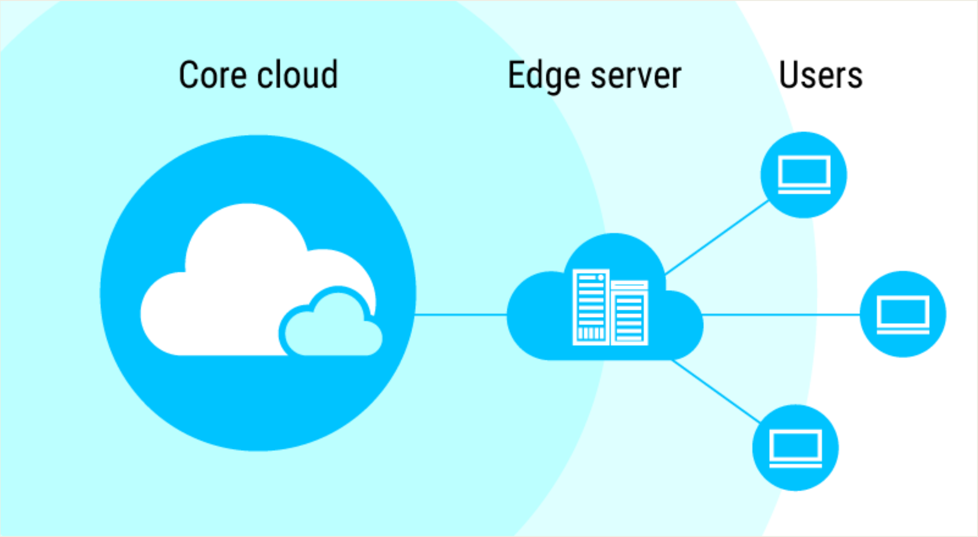
The 5G Vision: Three Broad Use Cases

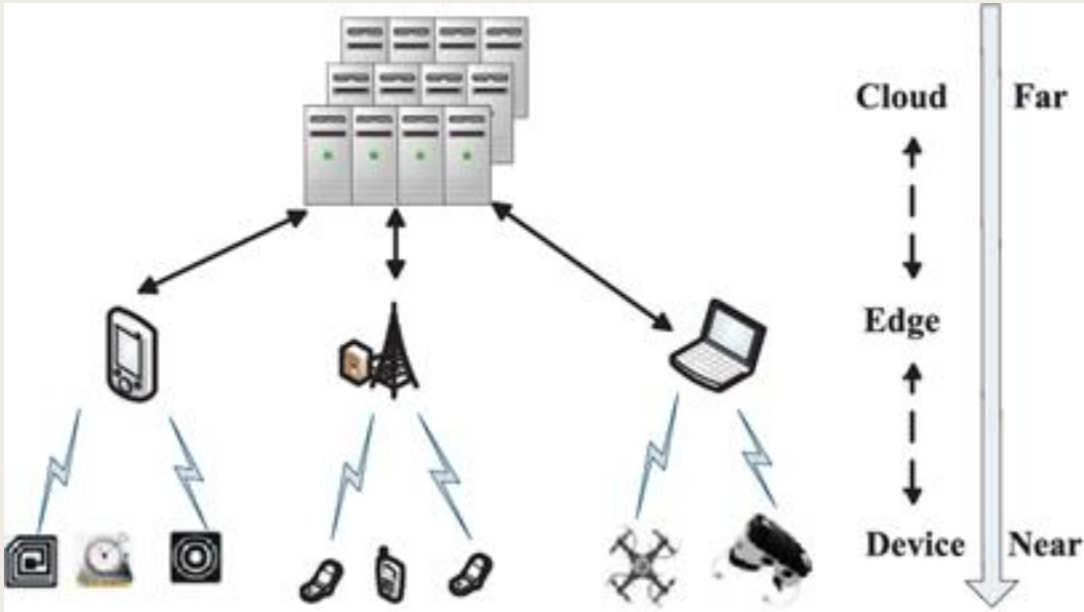
The three broad use cases include enhanced mobile broadband, mission-critical services and massive IoT

Ref: Leading the World to 5G, Qualcomm Technologies, Inc, 2016

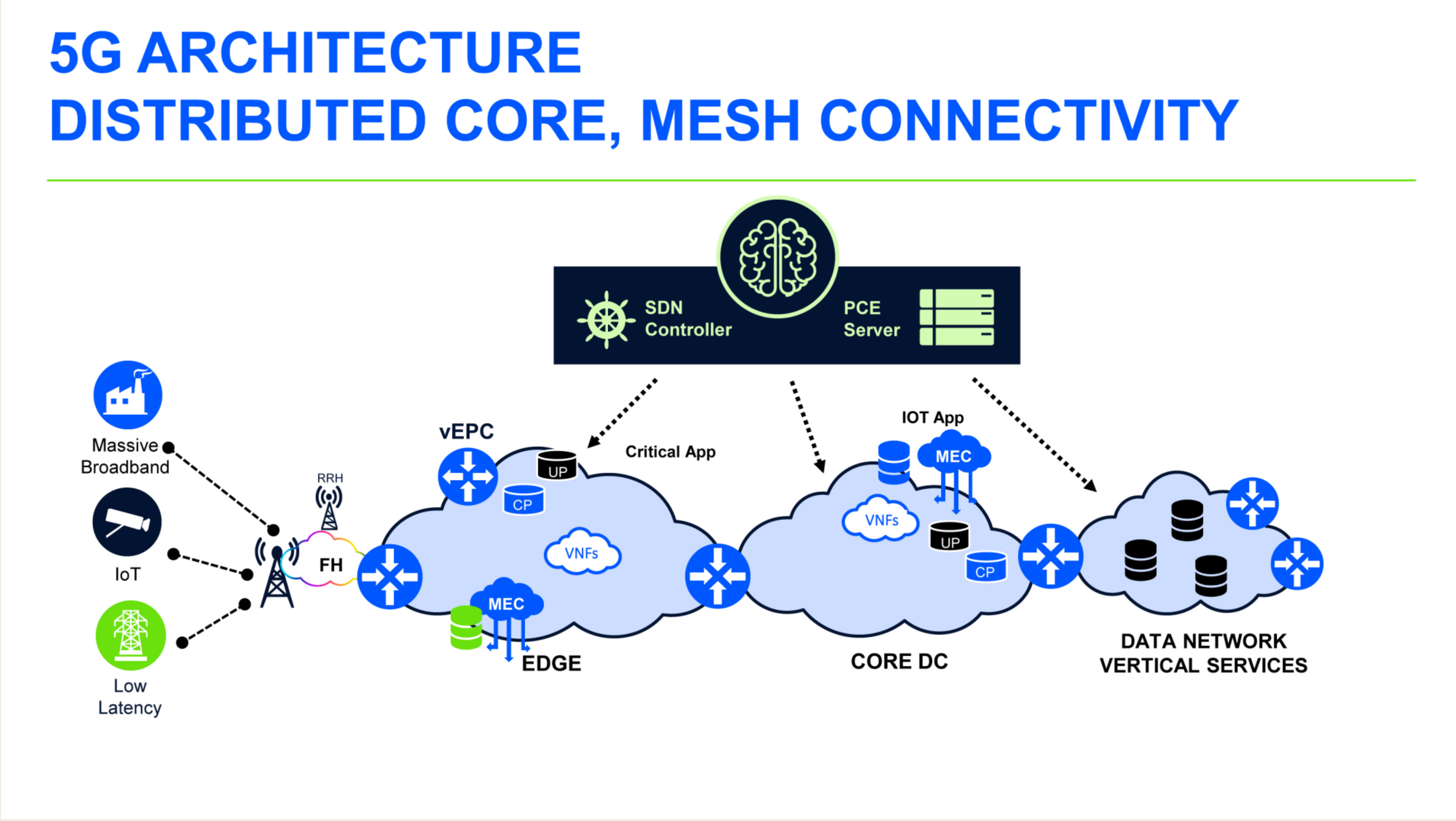
The three broad use cases are characterized by different metrics and parameters

The Edge Nodes Play a Key Role in Enabling 5G





The 5G Architecture



Edge Computing: Key Advantages

Low Latency

Backend Traffic Reduction

Efficient Data Management

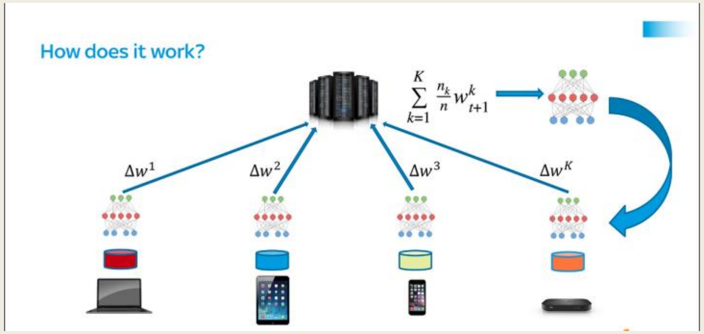
Rapid Access to Data Analytics

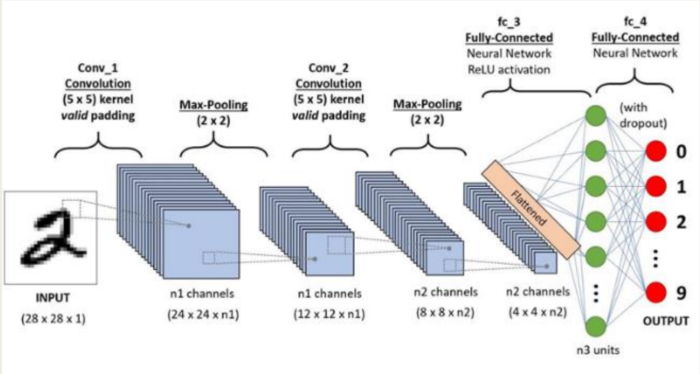
Network Load Reduction

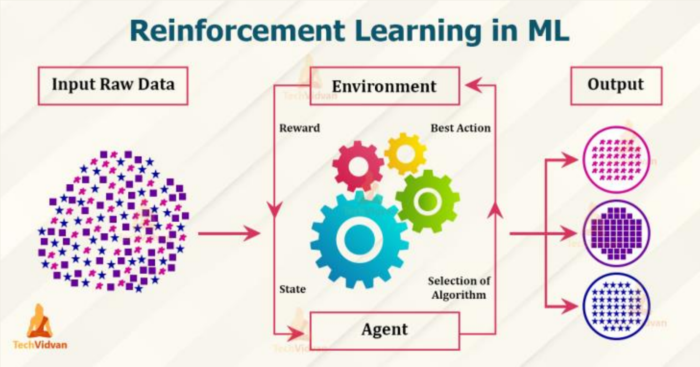
Cloud Cost Reduction

AI / ML / Deep Learning at the Edge Nodes

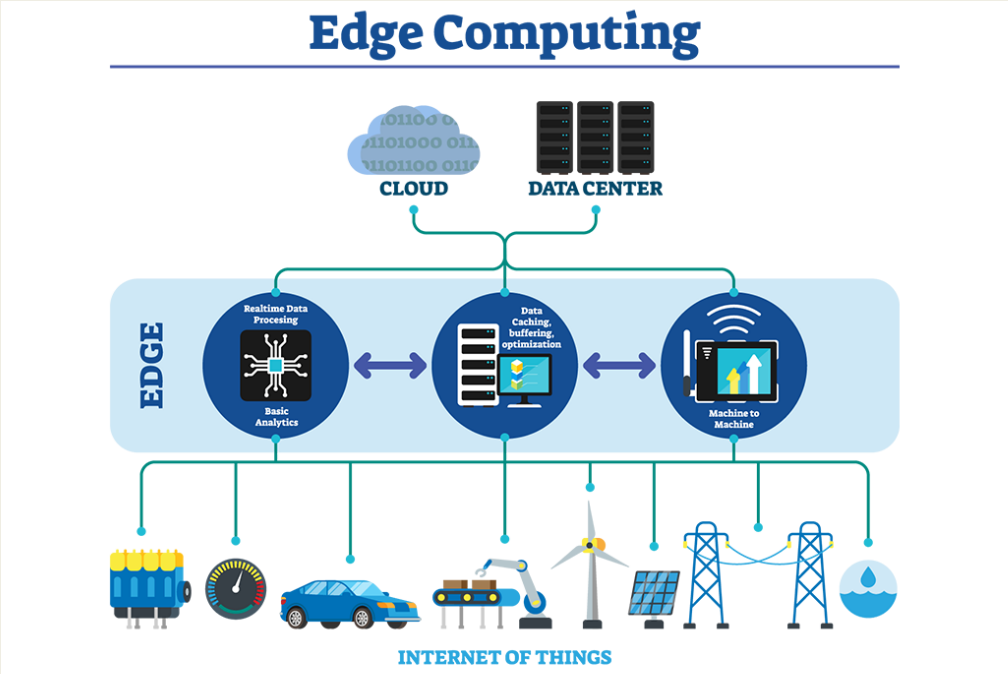
Learning at the Resource Constrained Edge Nodes





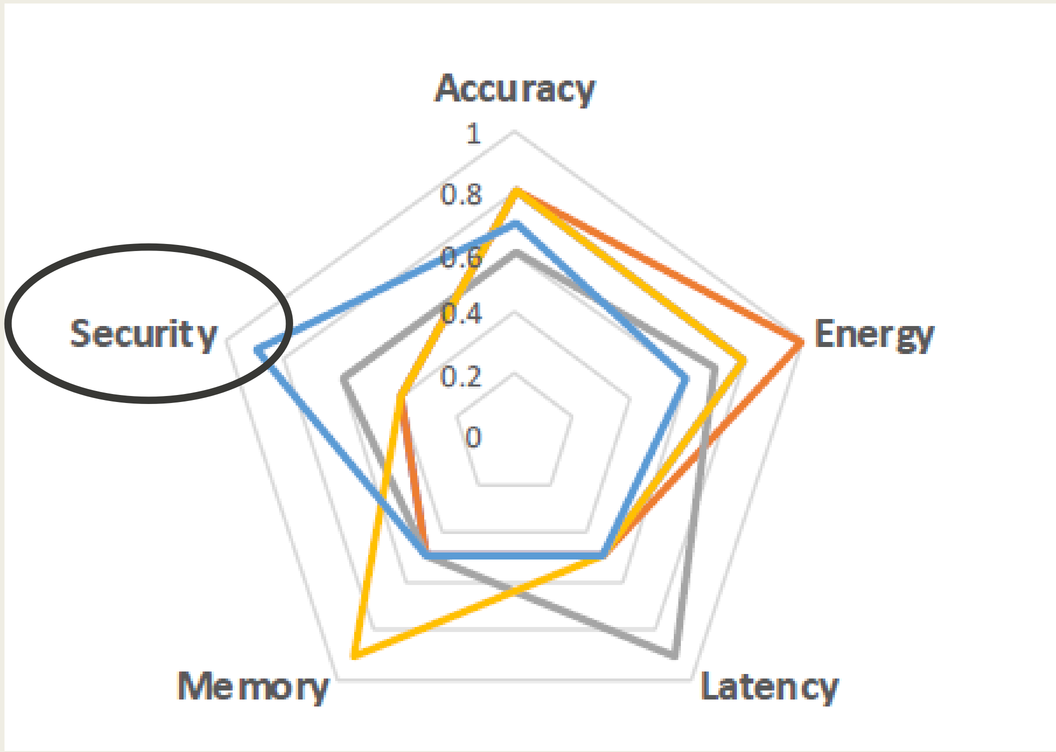


Resource Constrained Environment



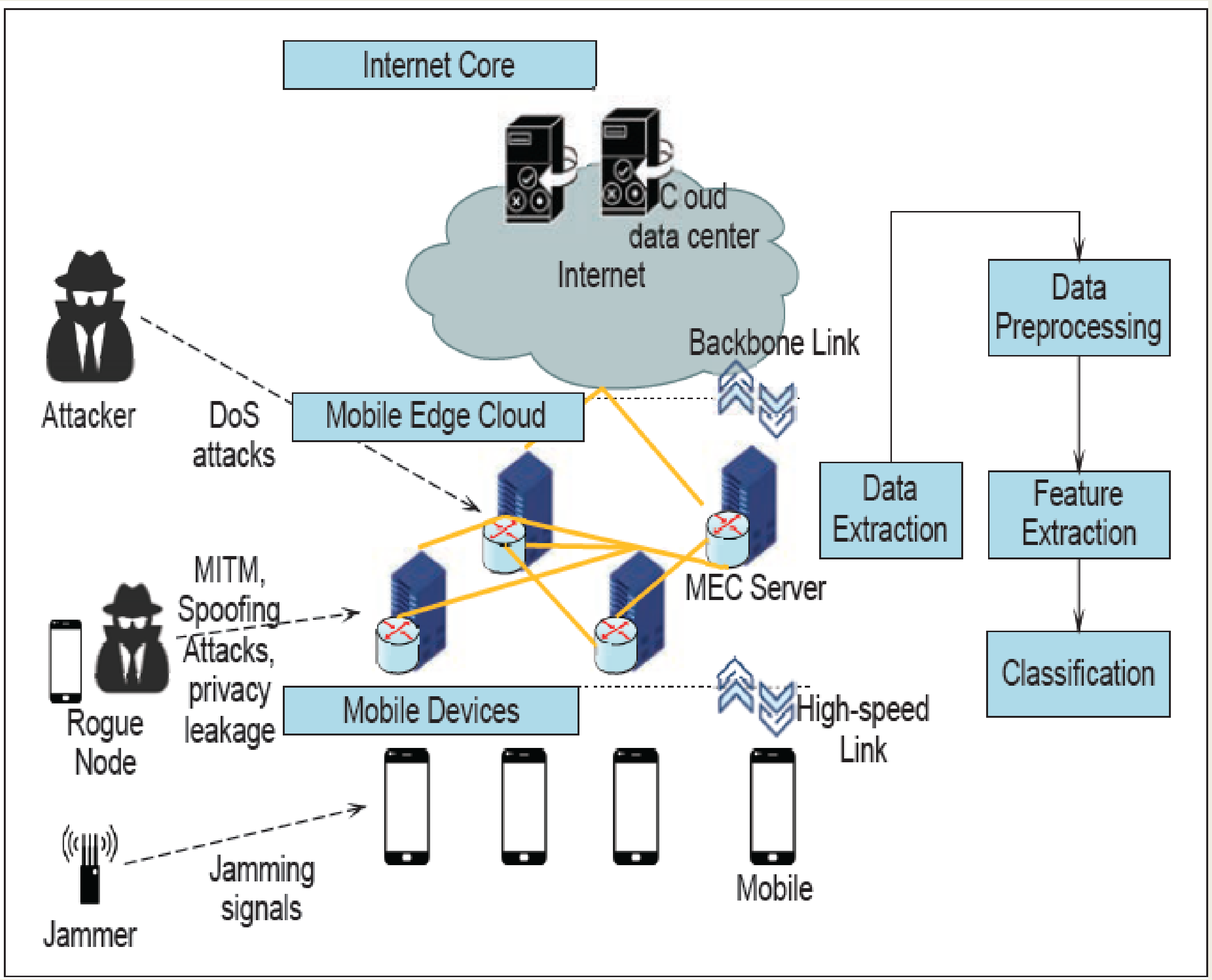
Security is critical when running ML / DL at the Edge

Design Space for Edge Intelligent Systems



MEC ARCHITECTURE

Secure Three Layer MEC Architecture



Reference: "Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities", S. Garg et al, IEEE Network, Sept/Oct 2021

CHALLENGES TO THE MEC PARADIGM

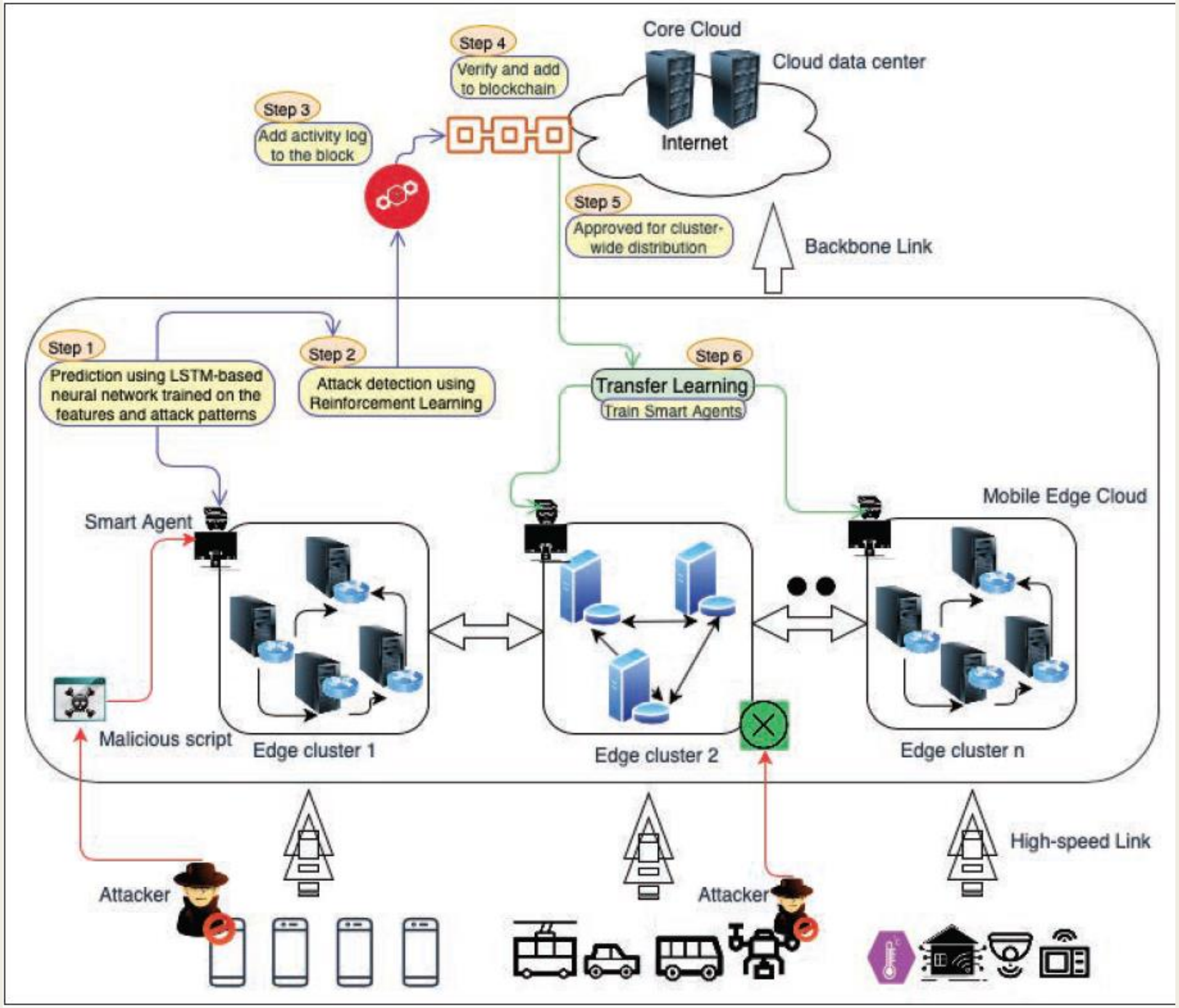
- Access control
- Heterogeneity of MEC systems
- Identity authentication
- Privacy preservation
- Secure data aggregation
- Mis-configurations
- Diversity of communication technologies
- Secure content distribution
- Resilience to attacks
- Lightweight protocol design
- Establishing trustworthy data sharing practices

CHALLENGES TO THE MEC PARADIGM

- The *lack of comprehensive security mechanisms* render the deployment of MEC a technically challenging problem

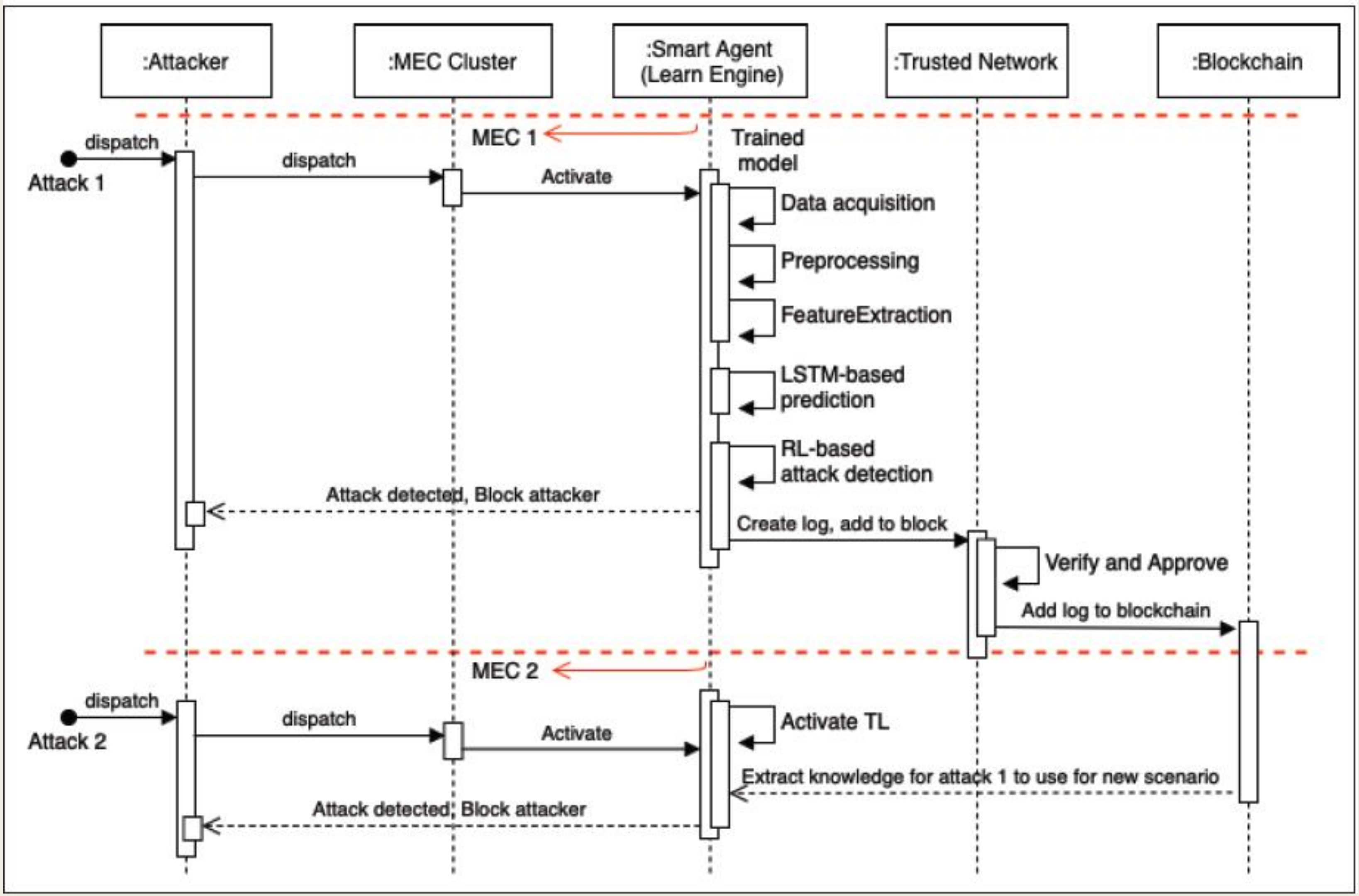
- The security goals of MEC should be grounded on a combined objective of securing the data and ensuring the safety and resiliency of systems and processes
  - Confidentiality
  - Integrity
  - Availability
  - Safety
  - Resiliency

Proposed SecEdge-Learn MEC Architecture



Reference: "Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities", S. Garg et al, IEEE Network, Sept/Oct 2021

Sequence of Activities in SecEdge-Learn



Reference: “Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities”, S. Garg et al, IEEE Network, Sept/Oct 2021

EMERGING PARADIGMS AT THE EDGE

FEDERATED LEARNING

A PRIVACY PRESERVING PARADIGM

The Buzz on Federated Learning

Google is using federated learning to improve Assistant's "Hey Google" accuracy

ReportLinker

The Global Federated Learning Market size is expected to reach $198.7 Million by 2028, rising at a market growth of 11.1% CAGR during the forecast period

MIT News

ON CAMPUS AND AROUND THE WORLD

Collaborative machine learning that preserves privacy

Researchers increase the accuracy and efficiency of a machine-learning method that safeguards user data.

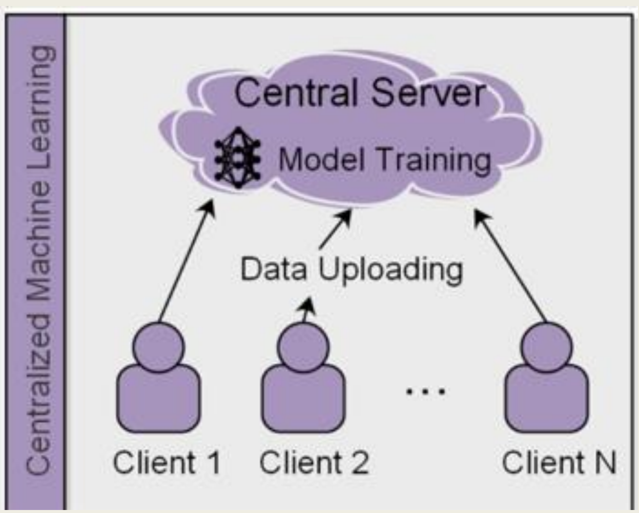
Adam Zewe | MIT News Office
September 7, 2022

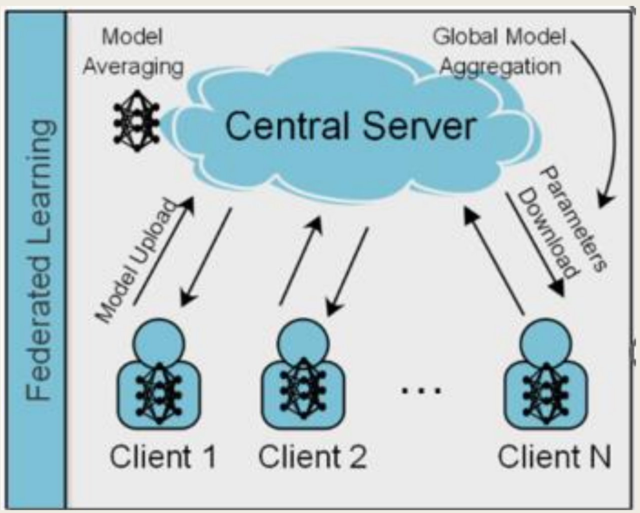
Applications of Federated Learning

- Application in the Healthcare Industry
- Applications for FinTech
- Applications in Insurance Sector
- Applications in IoT
- Application in other Industries and Technologies

CLASSICAL MACHINE LEARNING VERSUS FEDERATED LEARNING

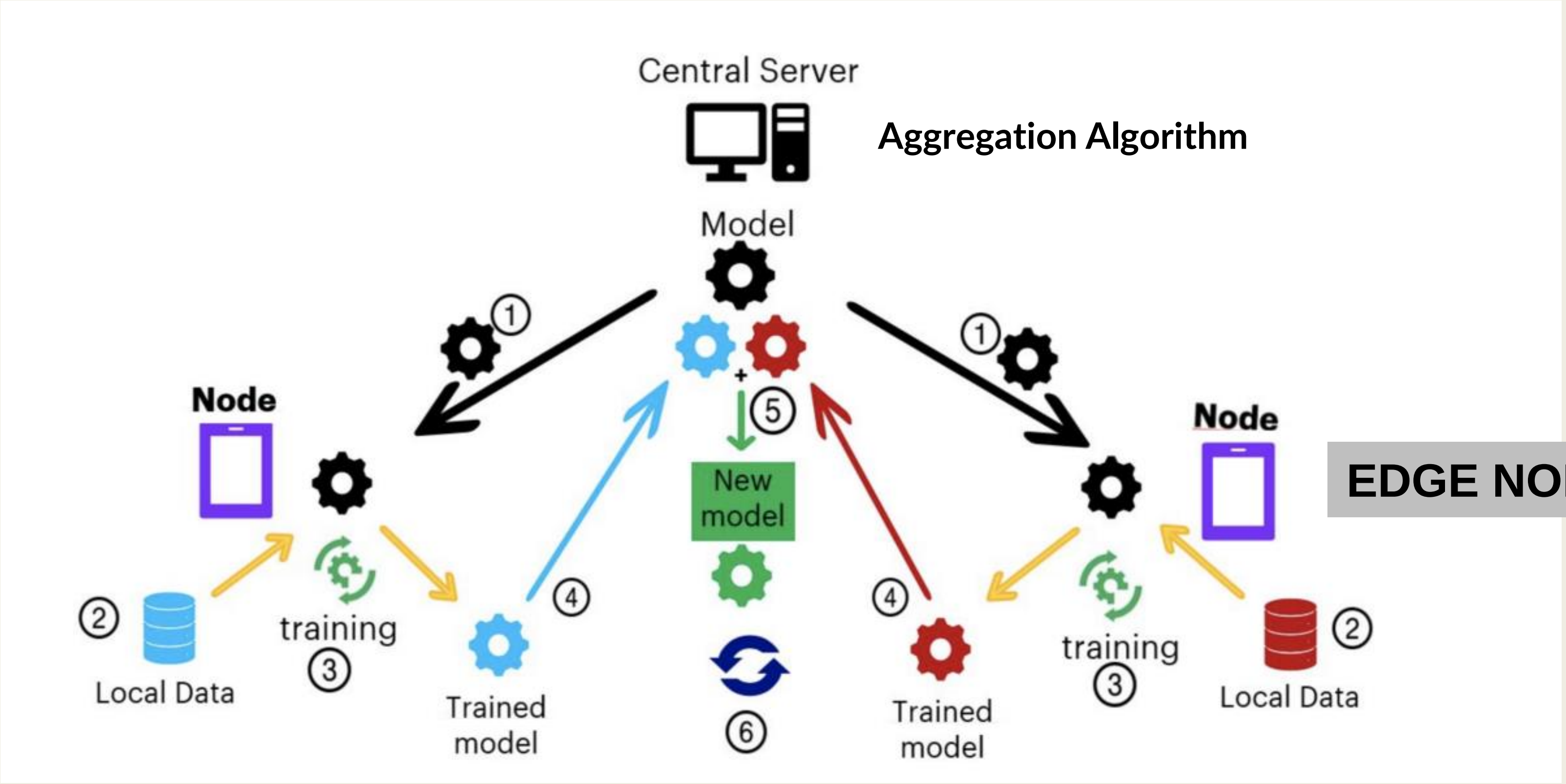
- Central machine learning
    - move the data to the computation
- Federated (machine) learning
    - move the computation to the data





Federated Learning

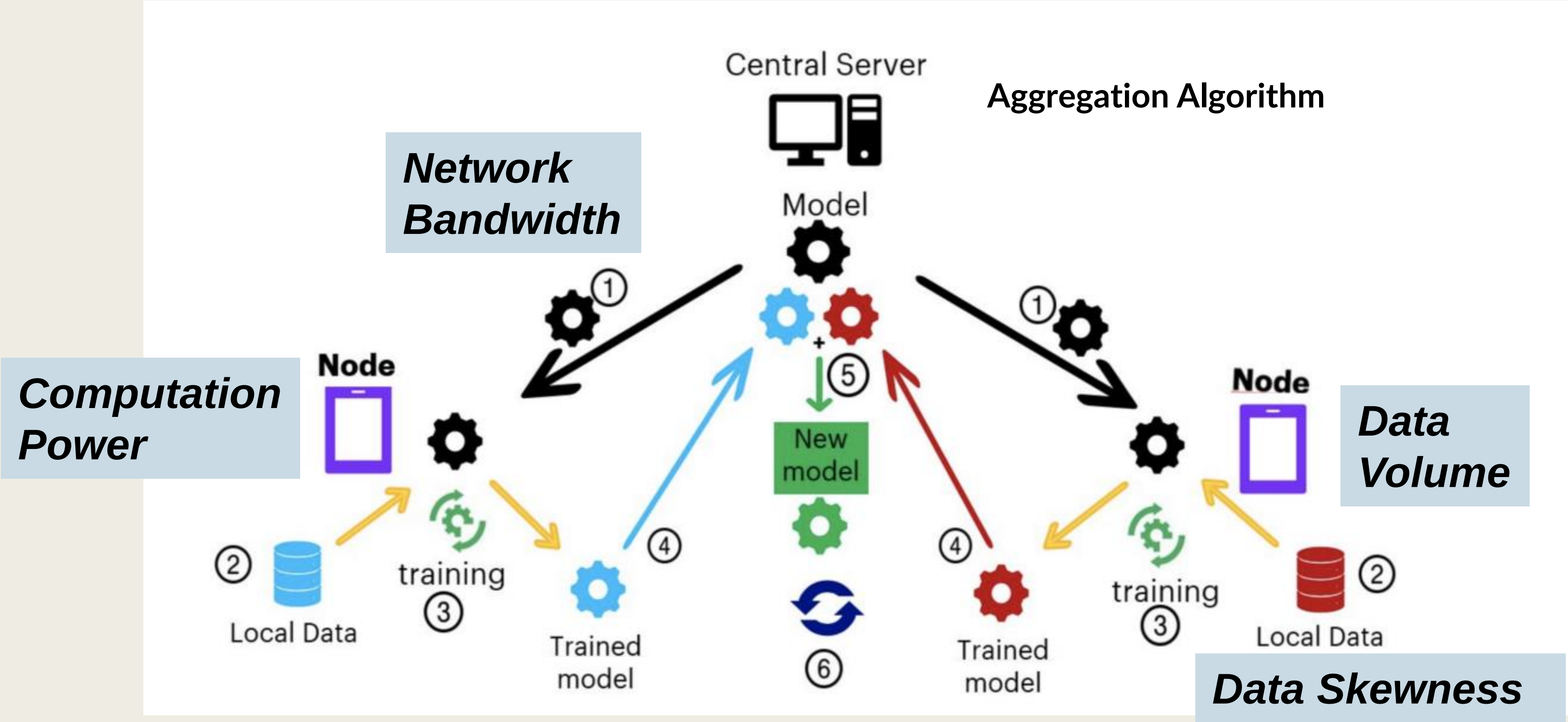
Distributed System with ML Model Exchange



EDGE NODES

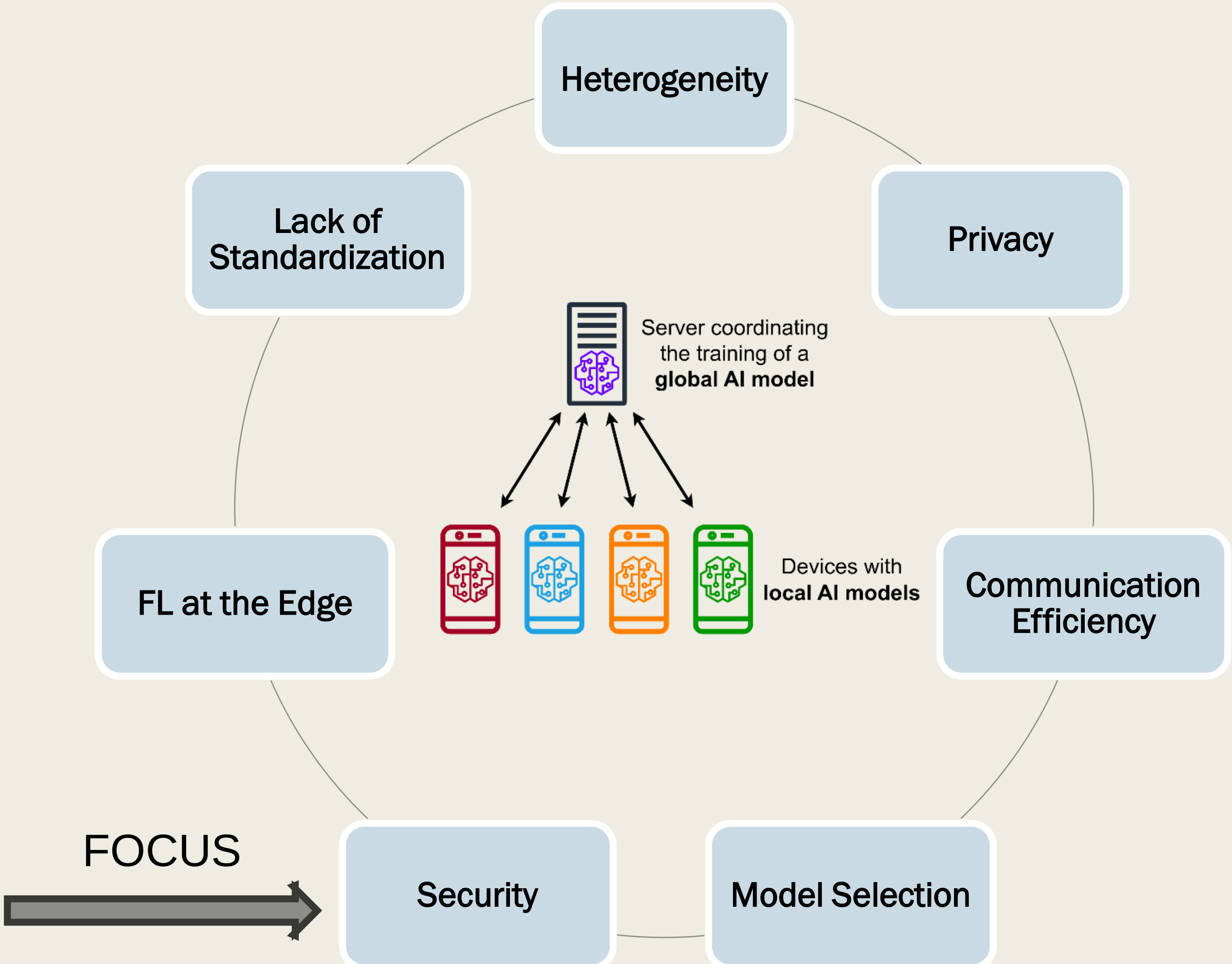
FL Key Objective: Privacy Preserving Paradigm !

Federated Learning & Network Parameters



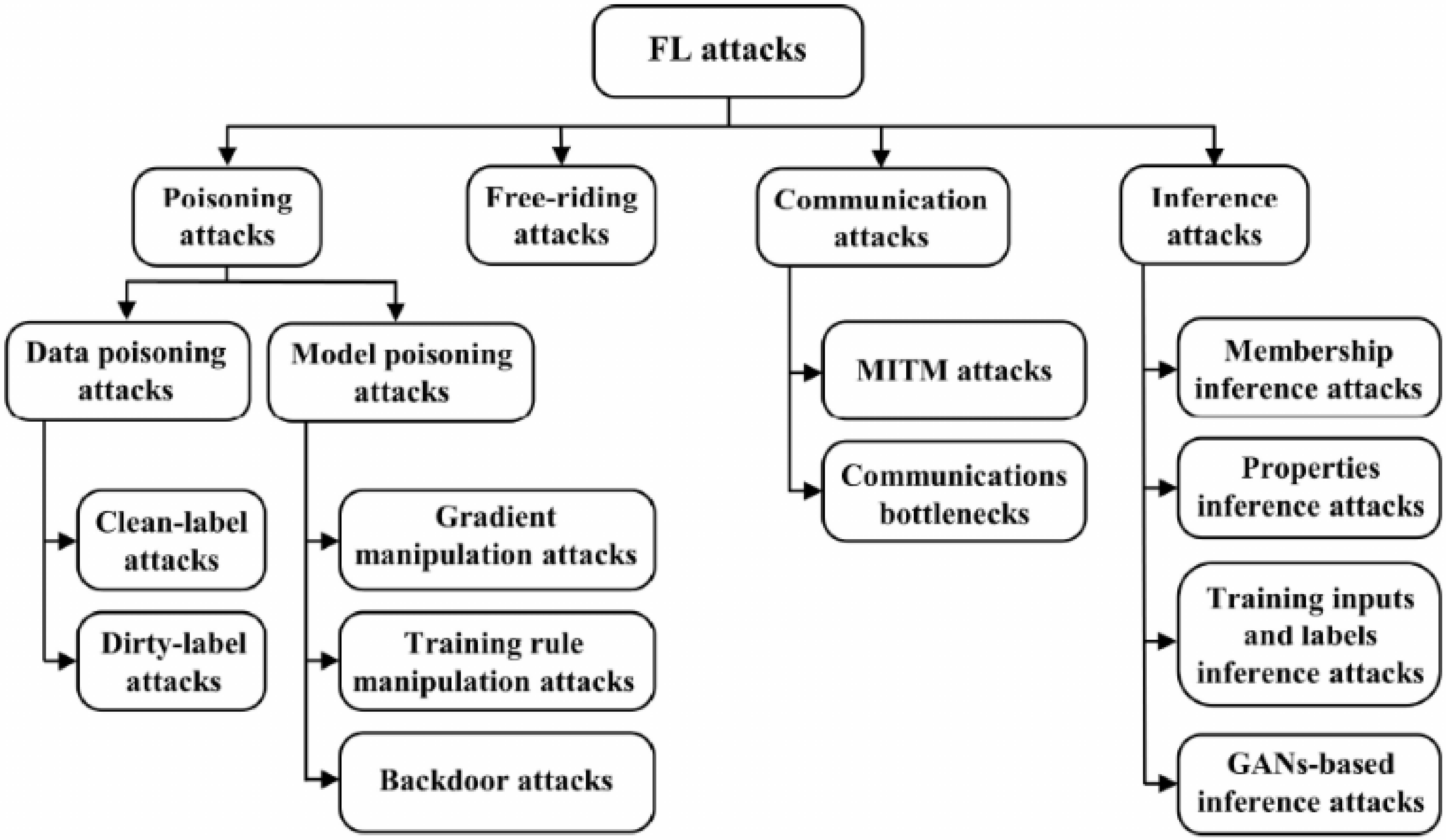
FL Performance is also a function of the System Parameters

Challenges of Federated Learning

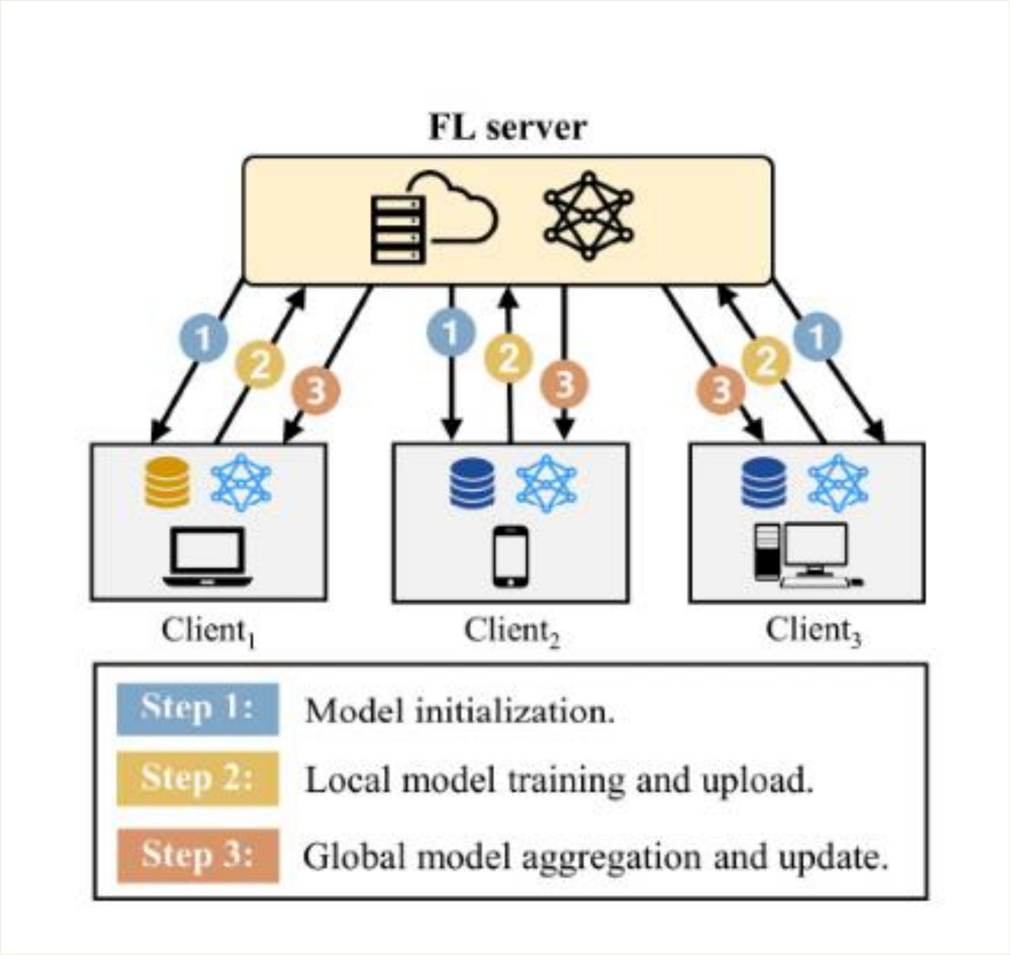


Threats, Attacks and Defences in Federated Learning

Taxonomy of Attacks on Federated Learning Systems



Attack Vectors in Federated Learning



Attack Vectors in Federated Learning

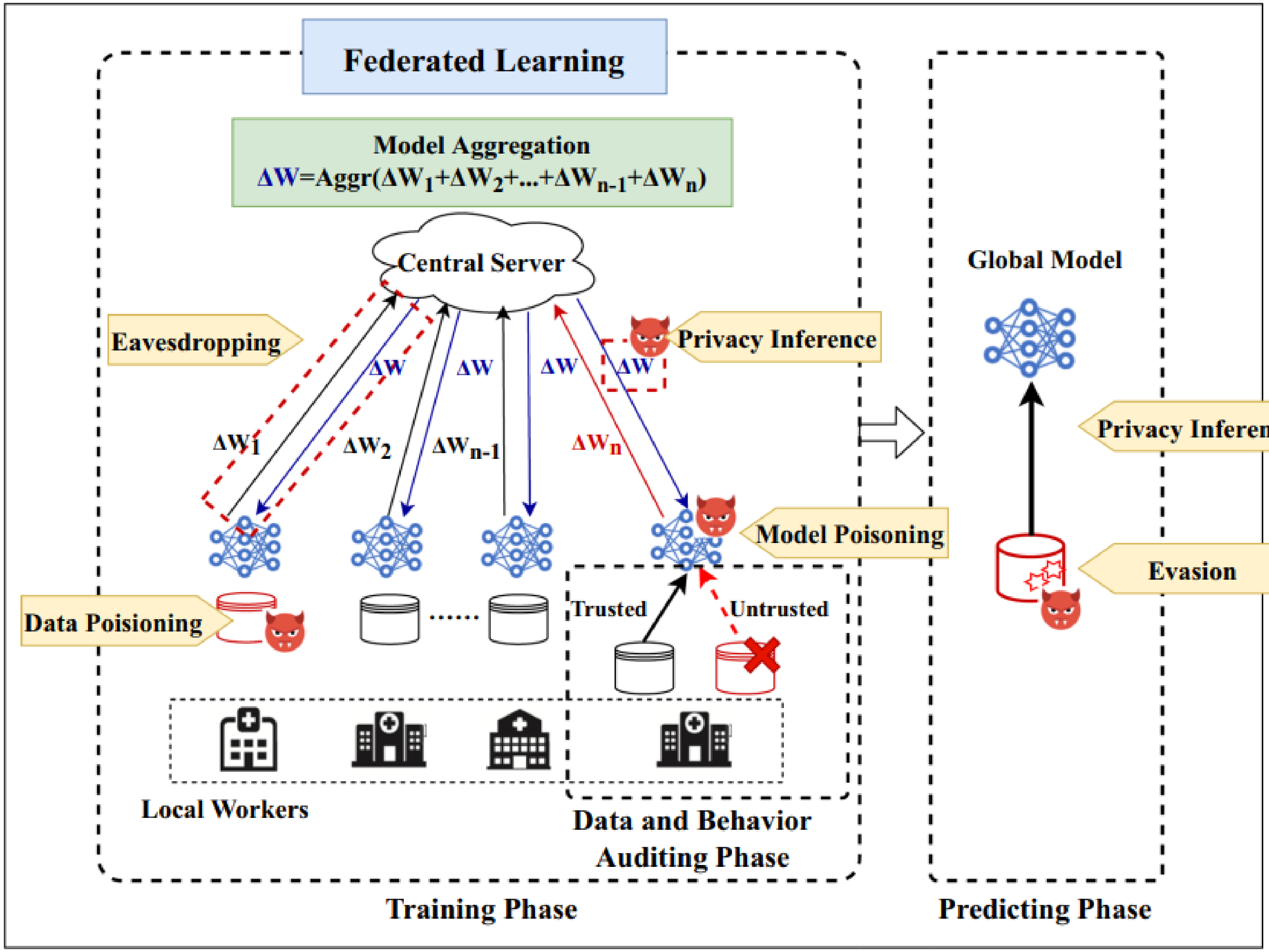
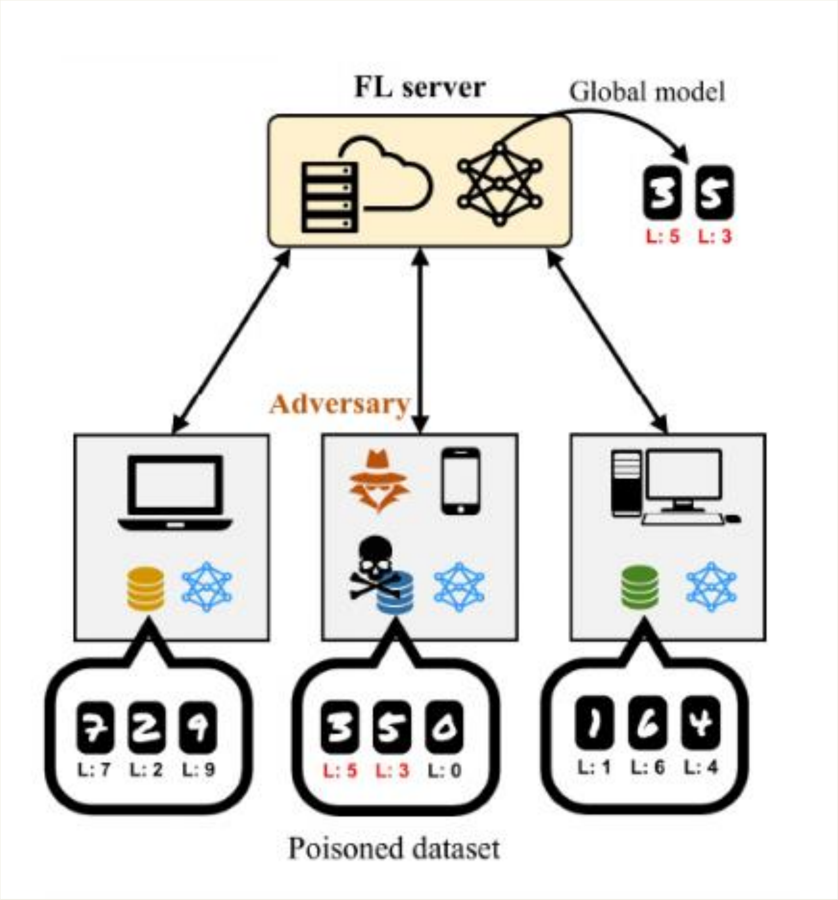
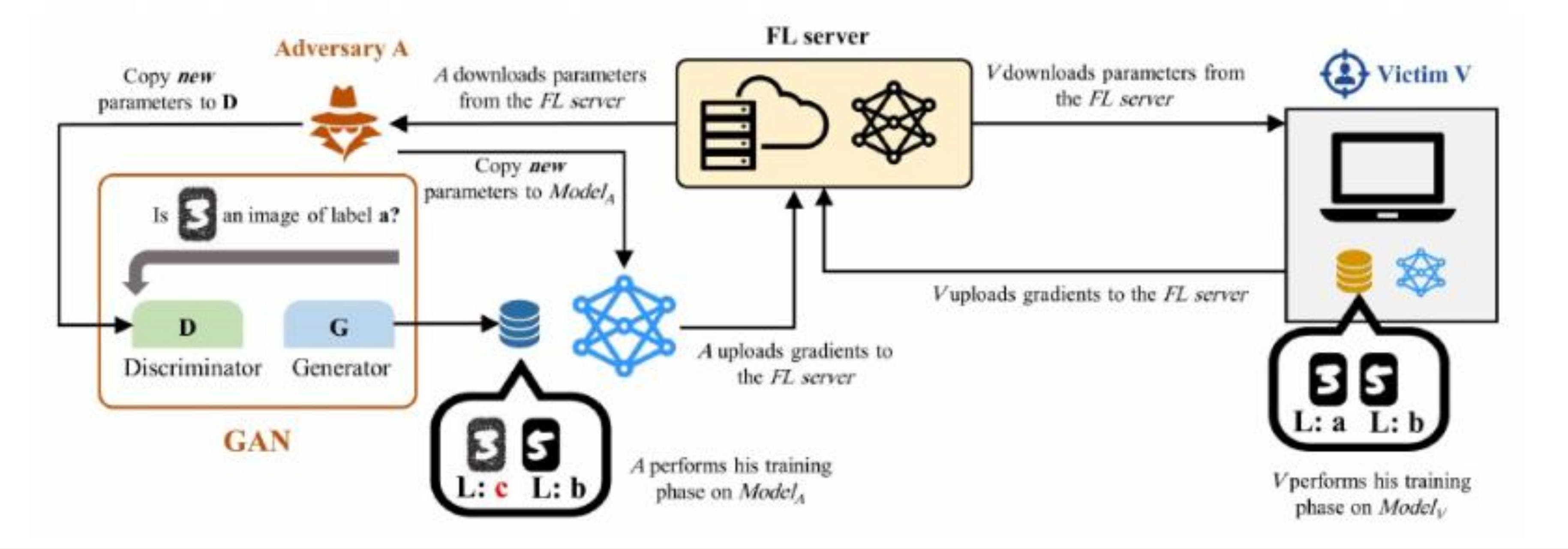


Fig. 1 The multi-phases framework of FL including data and behavior auditing, model training and model predicting

Data Poisoning Attack in Federated Learning Systems

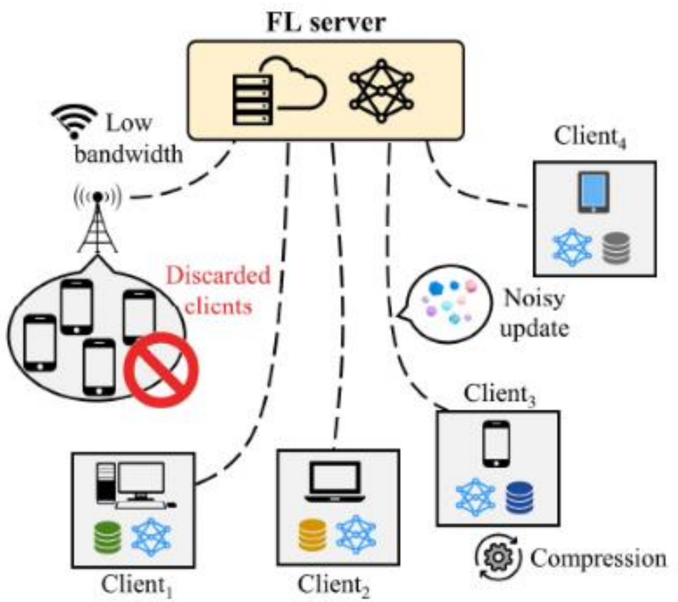


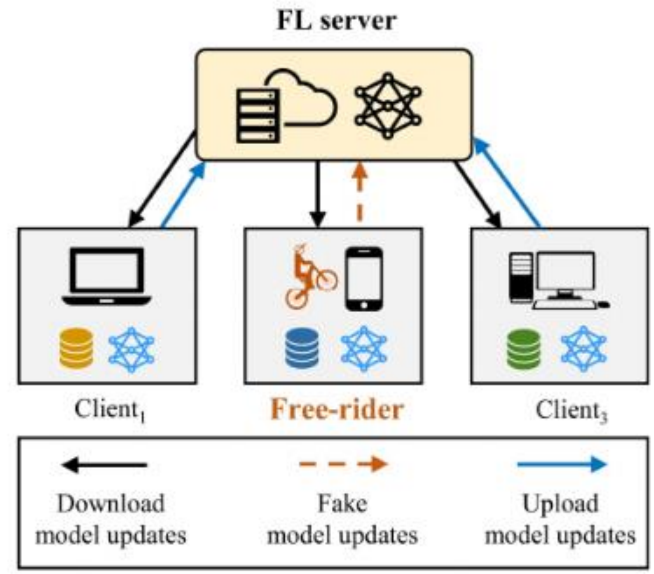
An Example of GANs-based Inference Attack in FL Systems



Federated Learning Systems: Challenges

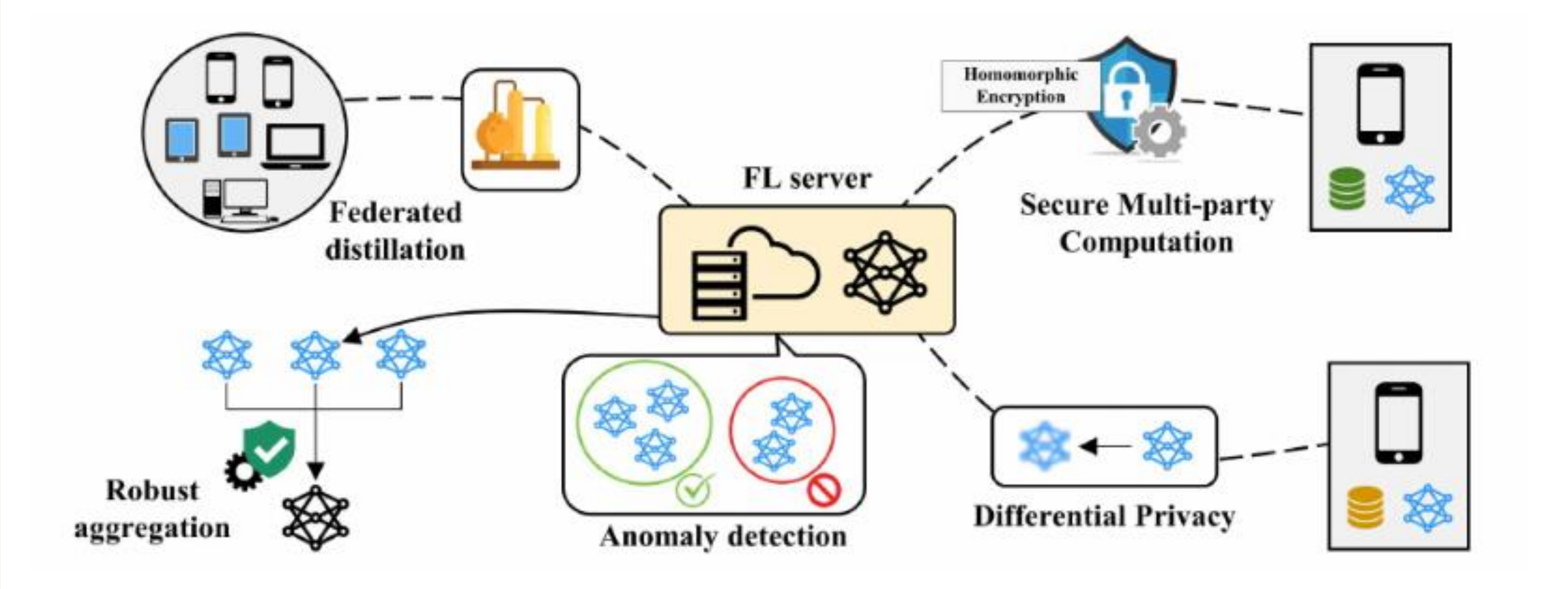
Communications bottlenecks in FL systems





An example of free-riding attack in FL systems

An Overview of Defensive Mechanisms in FL Systems

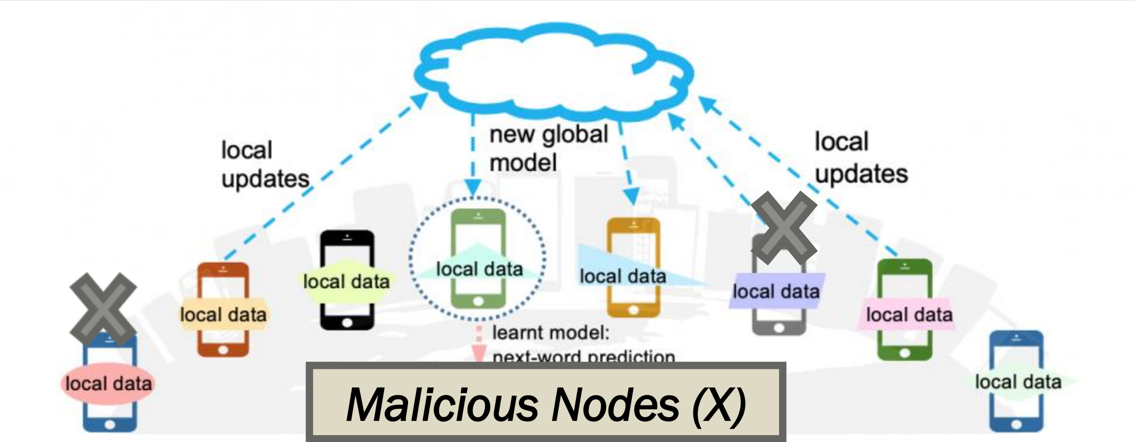


Federated Learning Defensive Mechanisms

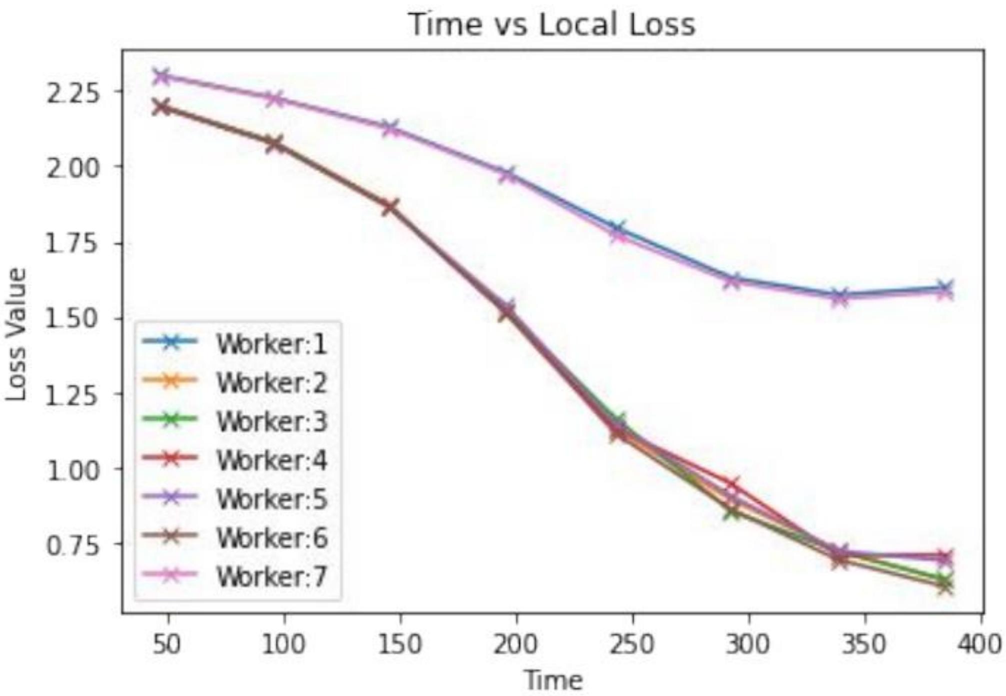
Defensive mechanisms	Key idea	Attacks
Differential Privacy	Introduce noise to the client's sensitive data before sharing individual updates with the FL server	• Data poisoning attacks • Backdoor attacks • Inference attacks
Secure Multi-party Computation	Encrypt clients' uploaded parameters	• Inference attacks • MITM attacks
Anomaly detection	Analyze clients' updates to identify misbehaving clients	• Free-riding attacks • Model poisoning attacks • Data poisoning attacks
Robust aggregation	Detect malicious individual updates during training process	• Inference attacks • Model poisoning attacks • Data poisoning attacks
Federated distillation	Transfer knowledge from afully trained model to another model	• Communications bottlenecks • MITM attacks • Inference attacks • GANs- based attacks

Maliciousness in Worker Nodes

- How do we detect Maliciousness in Worker Nodes and incorporate the same in selection criteria?
- Malicious Nodes Definition
  - *e.g.: Nodes with wrongly labelled data*
- The extent of the malicious nodes could be varied
- The number of malicious nodes and the total number of nodes could be varied
- We can also test in a dynamic setting where the nodes may be initially benign and may start turning malicious after some internal of time
- Ignoring such nodes becomes quite important for the selection algorithm



Incorporating Maliciousness in Worker Nodes: Swap the Labels

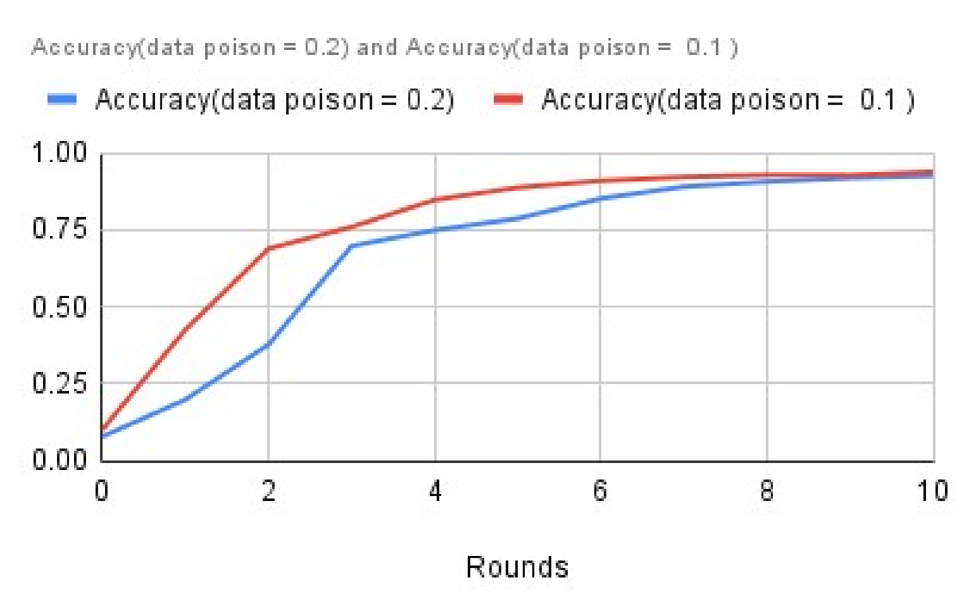


Local Model Loss for Malicious Node Detection

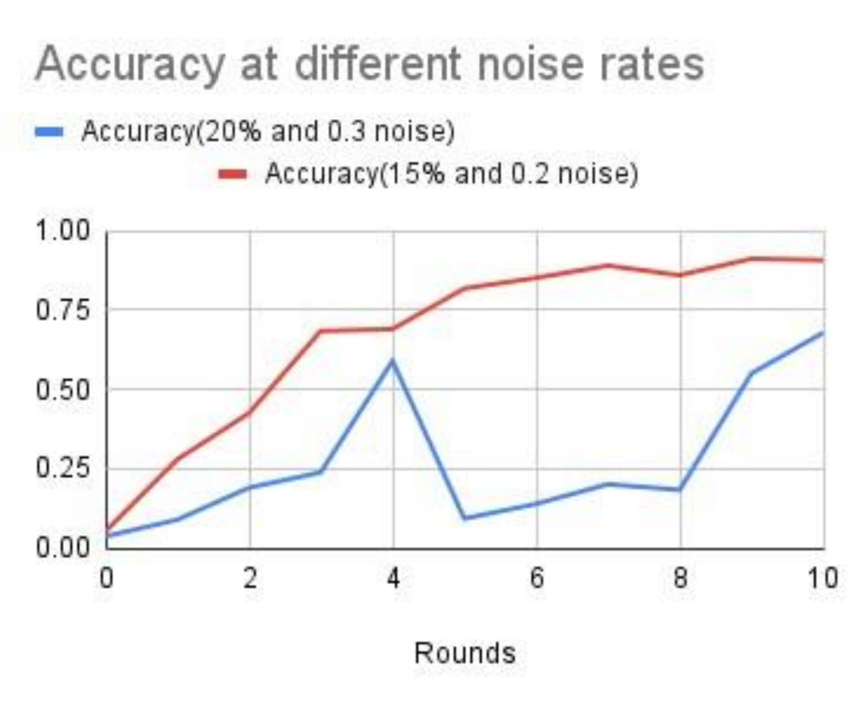
Total Worker Nodes: 20
Malicious Nodes: 4 (Labels swapped)
Data Distribution: Homogeneous
Dataset: MNIST

Considerably higher local model loss values for malicious nodes

Data Poisoning Attacks



Gradient Poisoning Attacks



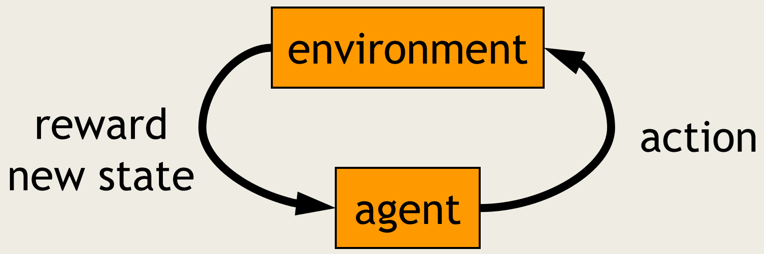
EMERGING PARADIGMS AT THE EDGE

REINFORCEMENT LEARNING

Work in Progress

Fundamentals

- Supervised learning
  - *classification, regression*
- Unsupervised learning
  - *clustering*
- Reinforcement learning
  - *more general than supervised/unsupervised learning*
  - *learn from interaction w/ environment to achieve a goal*



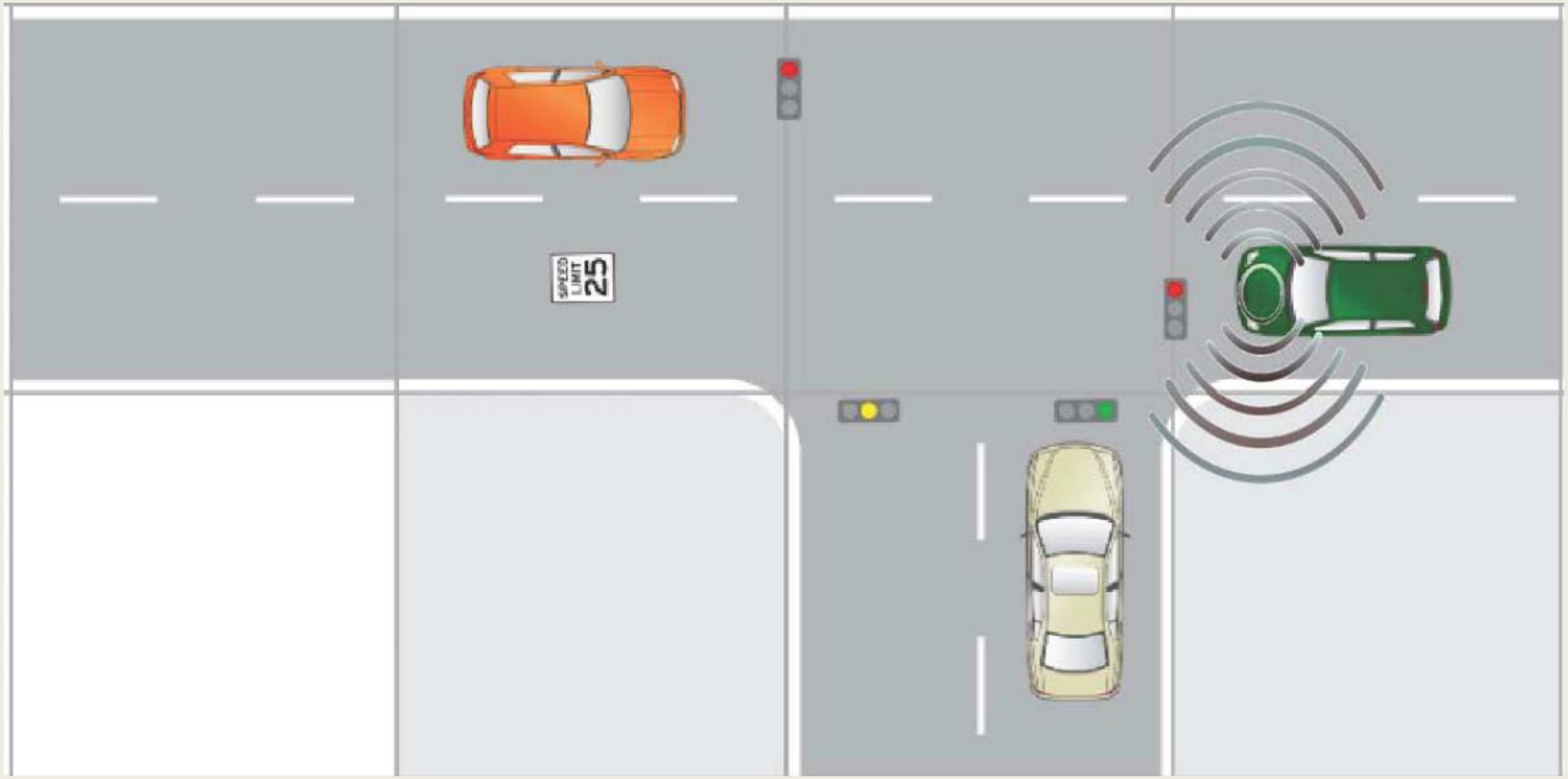
New Challenges in Reinforcement Learning: A Survey of Security and Privacy

Yunjiao Lei[1], Dayong Ye[1], Sheng Shen[1], Yulei Sui[1], Tianqing Zhu[1*] and Wanlei Zhou[2]

[1*]School of Computer Science, University of Technology Sydney, Broadway, Sydney, 2007, NSW, Australia.
[2*]School of Data Science, City University of Macau, Macau, China.

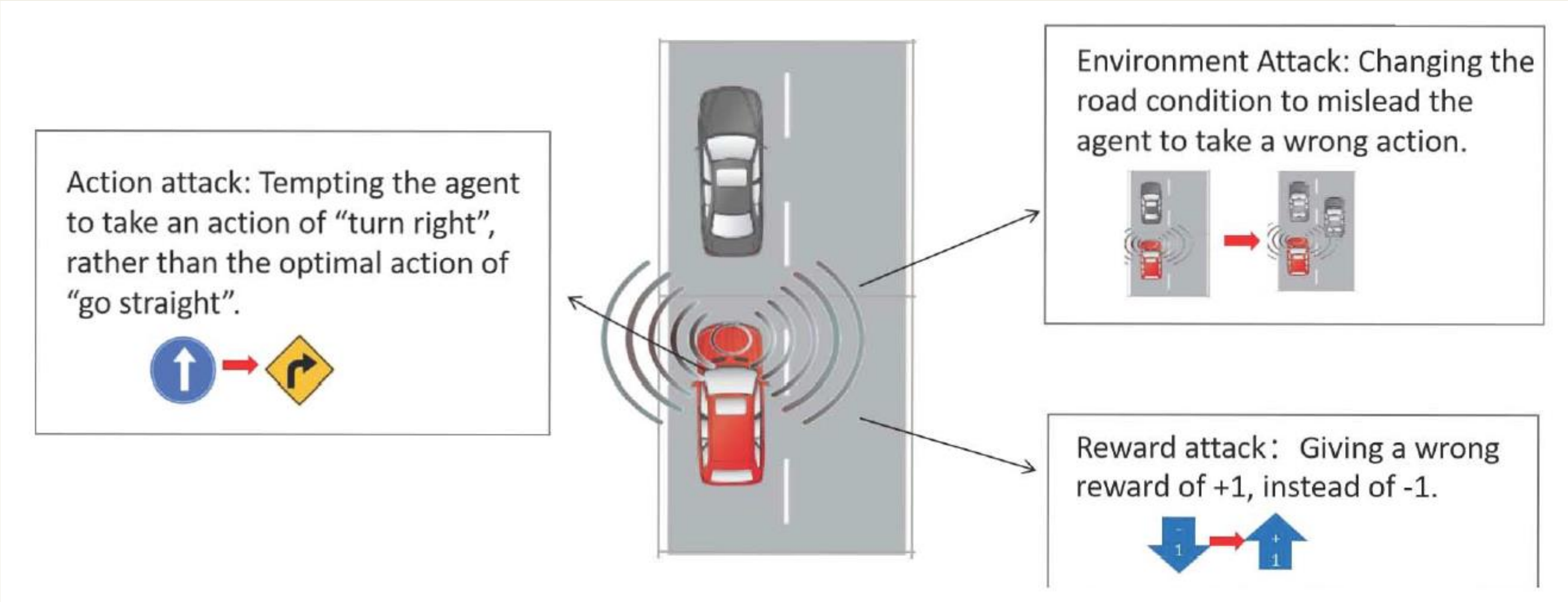
Springer Nature 2021

An Autonomous Driving Scenario



The green car is an agent. the environment comprises the road, the trac signs, other cars, etc.

A Simple Example of a Security Attack in Reinforcement Learning in the Context of Automatic Driving



Summary of Research Addressing Security in Reinforcement Learning

Subsection	Papers	Target	Impact	Strategies	Representative Methods
Security of state and action in MDP	Lee et al. [58]	Action	Reward	Perturbations	Optimization-based approaches Projected gradient descent
	Chen et al. [56]	Action	Policy	Action robustness	Zero-sum game Nash equilibriumt
	Zhao et al. [45]	State	Policy Action	Perturbations	Imitation learning
	Garrett et al. [64]	State	System destabilization	Perturbations	Z tables
	Sun et al. [40]	State	Reward, Action	Perturbations	Prediction model Neural network
	Ye et al. [57]	State	Action	Model learning	Deep neural network
	Dai et al. [65]	State-action	Policy	Safe exploration	Convolutional neural network Transfer learning
Security of environment in MDP	Rakhsha et al. [43]	Transition dynamics / rewards	Policy	Data poisoning	Optimization problems having constraints
	Chan et al. [59]	Features	Reward	Adversarial sample	Sliding-window method Gradient function
	Wang et al. [22]	Environment conditions	Robust policy	Robust adversarial learning	Cross-entropy method Actor-critic architecture
	Li et al. [46]	Non-stationary environment	Robust policies	Robust adversarial learning	Minimax optimization End-to-end learning approach
	Lin et al. [44]	Features	Action	Adversarial sample	Gradient-based methods
	Li et al. [66]	Environment	Policy	Two-player zero-sum game	Nash equilibrium
	Zhai et al. [67]	Environment	Policy	Two-player zero-sum game	Nash equilibrium Lyapunov network
Security of reward function in MDP	Zhang et al. [54]	Reward	Policy	Poisoning attack	Optimal control problems
	Li et al. [68]	Reward	Policy	Adversarial inverse reinforcement learning	Imitation learning Entropy regularization term

Key Findings of the Edge Security Report

- Edge deployments are increasing in scale across investments, projects, use cases, endpoints and types of endpoints
- Security is the top challenge cited by enterprises with edge deployments
- Risks to edge systems such as cyberattacks and from edge systems due to vulnerabilities and misconfigurations are on the rise

Reference:
https://www.redhat.com/en/resources/state-of-edge-security-report-overview

Summary and Future Directions

- MEC Security is a critical area that needs a lot more attention considering the huge growth of the Edge
- New paradigms at the Edge such as Federated Learning, Reinforcement Learning, etc are likely to spawn additional attack surfaces and attack vectors
- Need robust mitigation of the attacks since Edge nodes will become more complex with each passing year

THANK YOU

rajeevshorey@gmail.com