TDDE63 Advanced Project Course: Information Security

Nikolaos Pappas

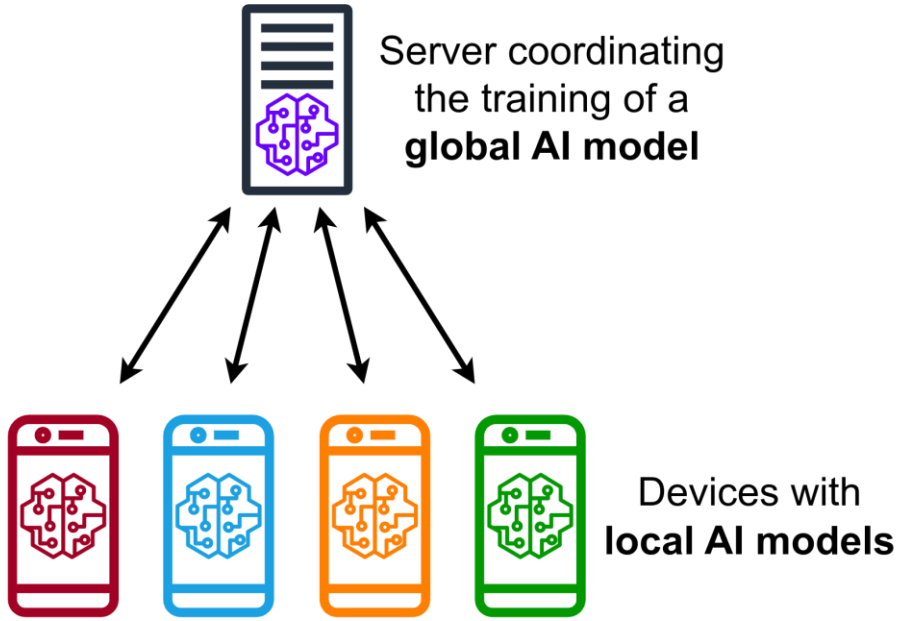
Associate Professor, Docent

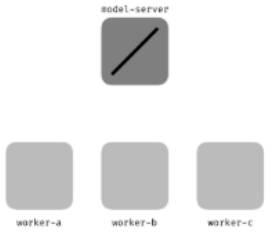
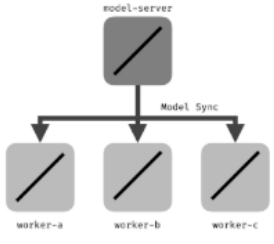
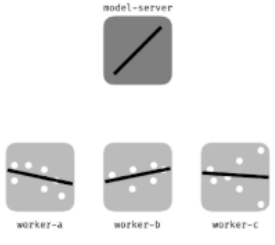
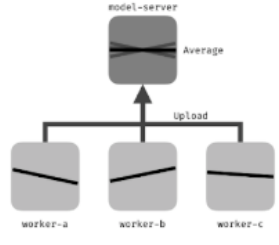
LINKÖPING UNIVERSITY

Project 1: Scalable and Sustainable Methodologies for ML Driven Security Operations, Energy-aware scheduling for secure model training at the edge.

Project overview

- Focus: Reducing **carbon footprint** and **energy consumption** in distributed AI/ML training at the edge
- Approach: Leverage **federated learning** and distributed paradigms
- Challenges:
  - Resource-constrained edge devices
  - Privacy and security requirements
  - Balancing scalability with sustainability



Step 1	Step 2	Step 3	Step 4
			
Central server chooses a statistical model to be trained	Central server transmits the initial model to several nodes	Nodes train the model locally with their own data	Central server pools model results and generate one global mode without accessing any data

Project goals

- **Intelligent Client Selection**: Energy- and security-aware participation
- **Energy-Aware Scheduling**: Optimize communication protocols to minimize usage
- **Systematic Trade-Offs**: Evaluate performance vs. security vs. energy
- **Scalability Analysis**: Assess methods in large heterogeneous edge networks
- **Aim**: Practical, secure, and environmentally sustainable ML training

Motivation

- **Why Important?**
  - Privacy & security → Data stays local
  - Resource optimization → Bandwidth & latency improvements
  - Energy efficiency → AI's growing environmental impact
- **Challenge**: Current frameworks ignore:
  - Energy profiles & availability of devices
  - Real-time security risks
- **Task**: Develop adaptive algorithms & protocols for sustainable, secure training

Learning Outcomes & Background

➢ **Learning Outcomes**

- Experience with **federated learning & edge computing**
- Understand interplay: **security, energy, ML system design**
- Skills in **design, simulation, evaluation** of scheduling protocols
- Exposure to **real-world AI–sustainability challenges**

➢ **Background Required**

- Computer networks
- Programming (Python or equivalent)
- (Optional) Machine learning

Expected outcomes

- **Simulation**: Energy-aware scheduling for federated learning

- **Comparative Study**: Baseline vs. energy-aware protocols
  - Metrics: Energy savings, accuracy, security robustness
- **Submission**:
  - Simulation results
  - Analytical report
  - Final presentation with findings & future directions

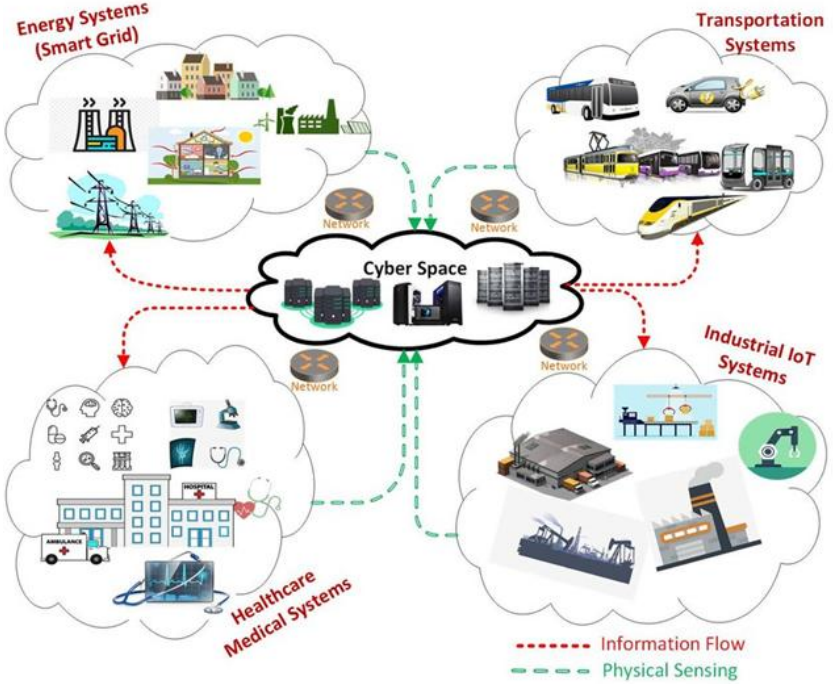
Project 2: Automatic Monitoring, Threat Detection, Alarm Generation

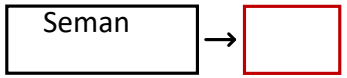
Project overview

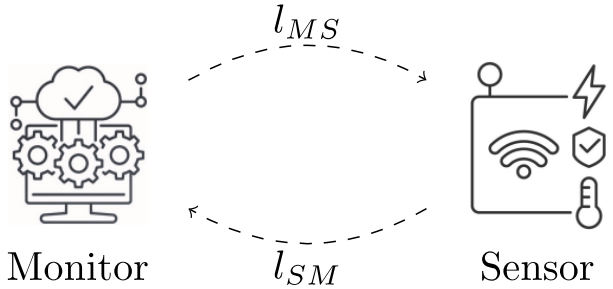
- Challenge: Ensuring **performance, reliability, and security** in 6G cloud–edge systems.
- Focus Areas:
  - Heterogeneous system environments (cloud, edge, far-edge)
  - Resource-aware monitoring agents
  - Selective data distribution strategies

Cross-layer data collection (network, application, physical layers)

- *Approach: **Semantics-aware monitoring** → improves prediction, threat detection, and efficiency.*

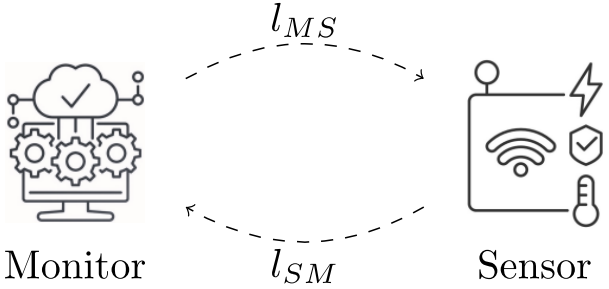






Motivation

- Manual supervision infeasible due to **scale and complexity**.
- Automated monitoring enables:
  - Real-time **threat detection** & operational insights
  - Reduced downtime → improved **reliability**
  - Efficient **resource & energy utilization**
  - Support for **compliance & regulation**
- Significance: N**ext-gen intelligent cloud-edge systems**.



Background required

- **Networking & Programming** basics
- Familiarity with **machine learning concepts**:
  - Supervised/unsupervised learning
  - Anomaly detection
- (Optional but useful) Prior knowledge in **distributed systems**

Key objectives

- **Literature Survey**: Recent (last 4 years) monitoring & threat detection research.
- **Framework Analysis**: Compare state-of-the-art systems.
- **Implementation**: Adaptive, semantics-driven monitoring + alarm generation.
- **Trade-Off Study**: Data fidelity vs. latency, scalability, energy efficiency.
- **Critical Report**: Summarize findings and comparisons.

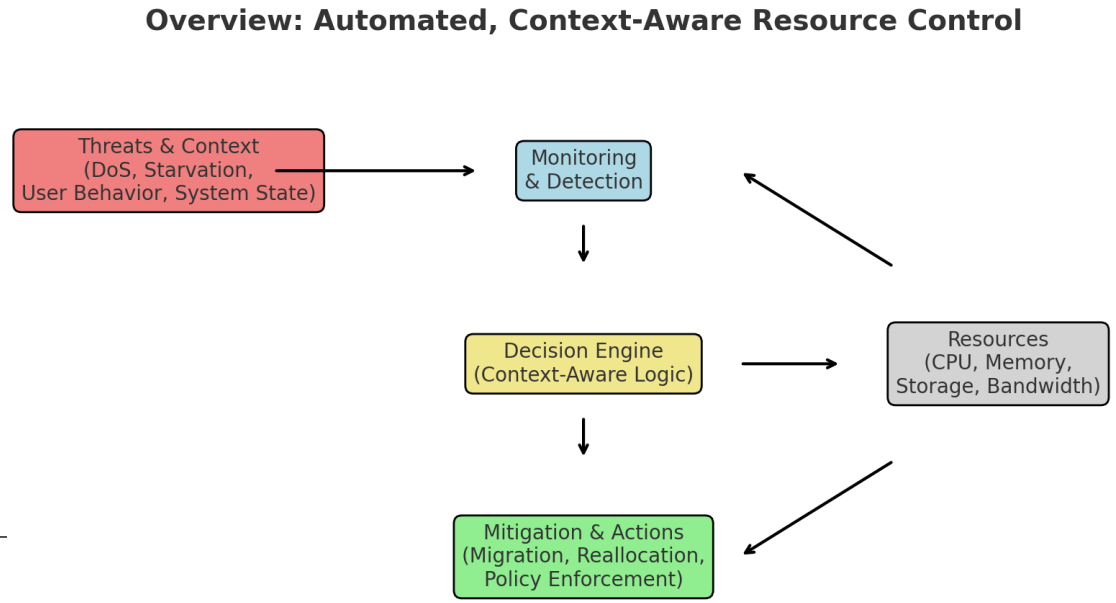
Expected outcomes

- **Literature Study:** Cloud-edge monitoring, threat detection, semantic-aware metrics.
- **Comparative Analysis**
  - Strengths/weaknesses, applicability across cloud–edge–far edge.
  - Performance and feasibility trade-offs.
- **Reporting:** Comprehensive, well-structured report summarizing results.

Project 3: Automated, Context-aware, Efficient and Robust Resource Control and Provisioning against Threats to Services and Applications

Project overview

- Focus: **Dynamic resource control & provisioning** under threat conditions
- Resources: CPU, memory, storage, network bandwidth
- Goals:
  - Detect threats & contextual changes
  - Trigger mitigation (migration, reallocation, enforcement)
  - Use **semantic/contextual information** for better decisions
- Scope: Cloud, network, and storage infrastructure



Motivation

- Resource mismanagement risks:
  - **Over-provisioning** → wasted resources, larger attack surface
  - **Under-provisioning** → DoS, starvation, performance loss
  - **No context-awareness** → generic, ineffective responses
- Why needed?
  - Threat sophistication is rising
  - Complex service delivery → higher risk of vulnerabilities
- Value: Adaptive, real-time, context-sensitive solutions for **security + resilience**

Background Required

•Networking systems knowledge
•Programming (Python or similar)
•Basic ML knowledge

Key objectives

- **Threat Analysis**: Classify attack scenarios affecting availability & continuity
- **Automated Framework**: Monitoring → decision-making → resource adjustment
- **Contextual Intelligence**: Integrate semantics (user behavior, criticality, state)
- **Assurances**: Security, privacy, performance, fairness

Expected outcomes

- Simulation of context-aware, threat-resilient resource control
- Documentation of algorithms, design decisions, evaluations
- Final report & presentation: findings, challenges, research directions