Cybersecurity at the critical edge

Jay Misra,

Professor in CS and ECE

Director and PI, NSF Distributed Resilient and Emergent-Intelligence Based Additive Manufacturing (DREAM) Center

BE BOLD. Shape the Future.®
New Mexico State University

Cybersecurity at the Critical Edge (infrastructure)

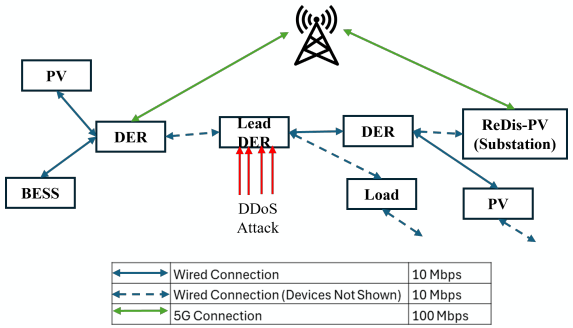
- Increasing number of devices (300K-500K)
  - Increased attack surface at the edge
  - Key exchange and freshness is a challenge
  - Trust assessment and management is a challenge
- Integration of OT == ICS+OT and IT + OT convergence
  - IT is moving into the OT space and there is a clash in principles
- More data moving up than down (volume increasing)
  - Challenges in addressing data provenance (devices, software, and data)
  - Data provenance becomes more complicated.
- Compliance vs technology tradeoff

Cybersecurity at the Critical Edge.

- Resilient Communications in the Smart Grid

Denial of Service (DoS) and Distributed Denial of Service (DDoS) are the most **common forms of cyber attack**, and they present a severe threat to smart grid communications.

The **use of 5G** for **backups/reliability** of communication has been discussed in the literature. However, there **hasn't been an evidence-based analysis**. We are working on that.



Selective activation of 5G or traffic rerouting in response to DDoS attacks.

- Secure and Resilient Distributed Manufacturing

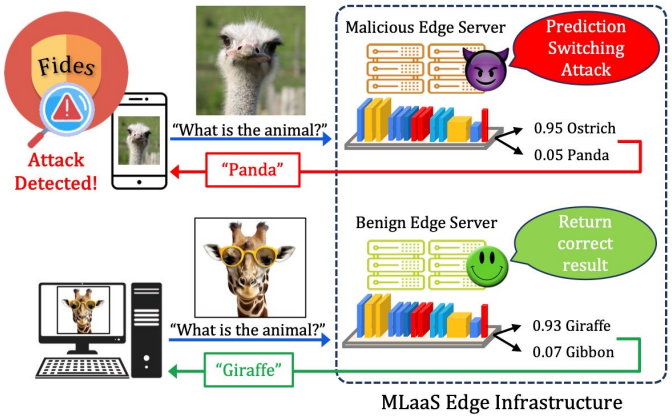
Through the **NSF DREAM Research Center**, we are building the foundational cyberinfrastructure that will bring **Distributed Intelligent Additive Manufacturing (DIAM)** to New Mexico and beyond.

Collaborating across **4 research institutions** with specialized skillsets in **cybersecurity**, **artificial intelligence**, **distributed networking systems**, **advanced manufacturing**, and **industrial engineering**, to build **future workforce**.

DREAM

- Resilient Machine Learning (ML) and AI

In augmented/virtual reality applications, **integrity verification of the outsourced ML tasks** is critical as the **edge device could be compromised**. Fides features a novel and efficient distillation technique–Greedy Distillation Transfer Learning–that **dynamically distills and fine-tunes** a space and compute-efficient verification model for verifying the corresponding service model while running inside a trusted execution environment.



MLaaS Edge Infrastructure

We consider the integrity verification of Machine Learning- as-a-Service inference, where clients send their data to the edge servers for ML inference tasks. In our proposed framework, Fides, we aim to detect any malicious misclassification caused by a malicious edge server when running the clients' inference tasks. ACM AsiaCCS'2024.

Machine Learning and the new frontier.

- Distributed and Federated Machine Learning
  - Efficient aggregation
  - Trustworthy operation
  - **Data is the Emperor**
    - Quality, Accuracy, Trust, Provenance Chain.
  - How to have trustworthy, dependable, robust models

NDN in Edge Centric Computing with Hierarchical ML Processing