Secure Zero-Trust Collaboration for Edge Anomaly Detection

Shanshan Zhao
Lecturer in Manufacturing
Shanshan.Zhao@uwe.ac.uk

Research Overview

The Industrial Internet of Things (IIoT), which manages critical control systems, is increasingly vulnerable to threats like ransomware and data poisoning. This risk comes from three areas: we can't share sensitive operational data; existing monitoring misses complex, system-wide attacks; and our field devices are too limited to run proper security measures. To solve this, we introduce FedSLAD, a novel framework that secures your operations. FedSLAD revolutionizes industrial anomaly detection by integrating Blockchain for system trust, Lightweight Cryptography to ensure data privacy during collaboration, and optimized processing for highly efficient, scalable security across all your edge devices in a Zero-Trust environment.

Industry Relevance

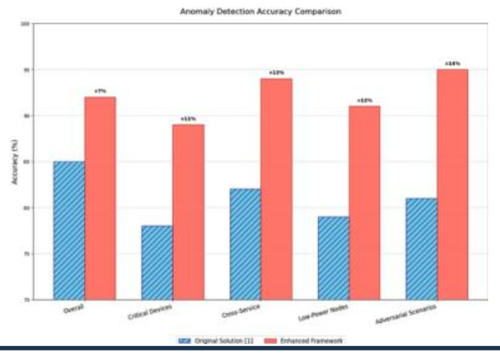
- **Potential applications:** Critical infrastructure monitoring; Cross-facility collaboration; Asset fleet management
- **Benefits:** Risk mitigation and resilience; Cost-effective security and data integrity and trust..
- **Alignment with sector priorities:** Zero-trust mandates; Industry 4.0 compliance; Cybersecurity defense.

Methods & Technologies

The FedSLAD system operates in three simple steps to secure your network. First, during **Setup**, we use **Blockchain trust scores** to vet and form monitoring groups, ensuring only trusted sensors participate. Second, in the **Training Phase**, we use **Lightweight Cryptography** to protect sensitive operational data, allowing different facilities to securely improve the detection model without sharing their raw data. Finally, the **Detection Phase** monitors threats in real-time, utilizing a special **ContextGuard** feature to spot complex attacks. If a threat is found, the system instantly updates the **Blockchain trust scores** to block the compromised sensor, securing your network and isolating the risk.

Innovations

- **Private, collaborative intelligence**: we use lightweight cryptography that allows the system to train a powerful security model across multiple facilities or partners without ever decrypting or exposing the raw data from any location.
- **Smart, context-aware threat hunting:** we developed a feature called ContextGuard that sets security alert levels dynamically based on what's happening across the entire network, not just one sensor.



Opportunities

- We seek access to an operational IIoT network or critical assets for installing our nodes to perform final validation and performance testing.
- Opportunities to integrate our Micro-NN anomaly models directly into existing industrial control systems, such as SCADA, CMMS, or specific edge gateways.

RISE WITH US
UWE Bristol