Guiding Innovation
Fostering Partnerships

Technology Overview

LiteShield: On-Device Protection for Edge AI Systems

OTT1853

Applications

Autonomous and AI-enabled systems, industrial automation and smart-city systems, cybersecurity solutions for edge-based AI deployments

Target Problems

Edge AI systems are vulnerable to hidden backdoor attacks that can manipulate sensor inputs and alter AI behavior without detection. Existing security approaches may require retraining models, cloud connectivity, or high computational overhead, which are not suitable for real-time, on-device environments.

Solution

Building on the threat modeling approach presented in the video, UWM researchers have applied these concepts to edge AI systems, creating an on-device security solution that filters incoming data before it reaches the AI model. This device removes potential malicious triggers to prevent compromised or unsafe system behavior while maintaining normal operation.

Key Benefits

- Protects against backdoor and trigger-based attacks
- Operates directly on edge devices without cloud reliance
- Maintains normal AI model accuracy
- Does not require model retraining

About this Technology

LiteShield is a lightweight, on-device endpoint security software designed to protect edge AI systems by filtering sensor data before it is processed by AI models. It operates as a preprocessing layer that removes malicious or hidden "trigger" patterns embedded in input data, preventing compromised or unsafe outputs while preserving normal system behavior. The solution is specifically designed for real-time, resource-constrained environments, enabling deployment directly on edge devices without requiring cloud connectivity, model retraining, or significant computational overhead.

Stage of Development

This technology has been demonstrated on hardware with effective attack mitigation and preserved accuracy. It is advancing toward a product-ready prototype aligned with real-world deployment needs.

Partnering Opportunity

We seek partners in edge AI device manufacturing, cybersecurity and AI solution integration, pilot deployment programs, and startup or commercialization collaborations in AI, embedded systems, or edge computing.

Intellectual Property (IP)

Patent pending. Protected and managed by the UWM Research Foundation.

Lead Inventor

Zhen Zeng, UWM Assistant Professor, Computer Science