Autonomic Trust Architecture for Secure Edge Intelligence in Cyber-Physical Systems

A. Research Area / Keywords

Edge AI, AIoT Security, Trusted Hardware, Cyber-Physical Systems, Distributed Attestation, Edge Intelligence Governance

B. Proposed Start Date

(Select date according to PGRS schedule)

C. Abstract (≤1000 characters)

Edge intelligence systems are increasingly deployed in real-world environments, including smart manufacturing, healthcare monitoring, and autonomous infrastructure. These systems rely on distributed AI models running directly on edge devices, but ensuring trustworthy execution across heterogeneous, resource-constrained environments remains a major challenge. Existing security mechanisms typically address hardware isolation, distributed verification, or AI-based monitoring separately, leaving gaps in end-to-end system trust.

This project proposes an integrated trust architecture for secure edge intelligence in cyber-physical systems. The research will combine hardware-enforced isolation mechanisms, distributed integrity verification, and adaptive AI-based anomaly detection into a unified autonomic trust framework. The objective is to enable continuous verification and trustworthy operation of edge intelligence systems deployed in real-world environments. The outcomes of this research will contribute to the development of secure and resilient AIoT infrastructures for next-generation intelligent systems.

D. Research Background (≤2500 characters)

Edge intelligence has become a key architectural paradigm for modern cyber-physical systems. In many applications—including smart manufacturing, intelligent transportation, digital healthcare, and autonomous infrastructure—AI models are increasingly deployed directly on

edge devices to support real-time decision making. This shift reduces latency, improves scalability, and enables local autonomy in distributed environments.

However, the security and trustworthiness of edge intelligence systems remain significant challenges. Edge environments are typically composed of heterogeneous devices with varying computational capabilities, operating under resource constraints and exposed to potentially hostile networks. These characteristics make it difficult to guarantee that AI models execute securely and that system behavior remains trustworthy over time.

Recent advances in trusted hardware architectures provide mechanisms such as secure boot chains and hardware-based isolation that help establish device-level trust. At the same time, distributed verification mechanisms have been proposed to record and verify the integrity state of edge devices in decentralized networks. In parallel, machine learning techniques are increasingly used for anomaly detection and monitoring in distributed systems.

Despite these advances, most existing solutions address these challenges in isolation. Hardware-based protection mechanisms often focus only on CPU execution environments and may not adequately protect peripheral access or system interactions. Distributed verification approaches can provide tamper-resistant records of device states but may introduce latency and scalability constraints. AI-based monitoring methods can detect anomalies but typically operate independently from system-level trust frameworks.

As a result, a significant gap remains in integrating these mechanisms into a unified architecture capable of providing continuous trust assurance for edge intelligence systems. Addressing this gap is critical for enabling the secure deployment of AI-enabled cyber-physical infrastructures that operate in safety-critical and mission-critical environments.

E. Objectives and Research Questions (≤2500 characters)

The objective of this research is to design and evaluate an integrated trust architecture that enables secure and verifiable execution of edge intelligence systems in cyber-physical environments.

The project aims to develop a unified framework that combines hardware-based trust anchors, distributed integrity verification, and adaptive intelligence monitoring to ensure trustworthy operation of distributed AI systems.

The research will address the following key questions:

First, how can hardware-enforced isolation mechanisms be extended to protect not only CPU execution environments but also peripheral interfaces and communication pathways in edge

devices? Ensuring comprehensive hardware trust is essential for protecting AI workloads from low-level attacks.

Second, how can distributed verification mechanisms be designed to provide scalable and efficient attestation of edge device integrity while minimizing latency and computational overhead in resource-constrained environments?

Third, how can intelligent monitoring mechanisms be integrated with hardware and distributed trust infrastructures to enable adaptive detection of anomalous behaviors in edge intelligence systems?

Fourth, how can these components be combined into a unified autonomic trust architecture that continuously evaluates system integrity and dynamically responds to security threats?

By addressing these questions, the research seeks to develop a holistic approach to trust management for edge intelligence systems deployed in real-world cyber-physical environments.

F. Research Methods and Approach (≤3500 characters)

The research will follow a system-driven design methodology that integrates hardware security mechanisms, distributed verification infrastructures, and intelligent monitoring techniques into a unified trust architecture for edge intelligence systems.

The first phase of the project will focus on analyzing existing edge intelligence architectures and identifying key vulnerabilities across device, network, and system layers. This analysis will examine the attack surfaces of edge computing platforms, including hardware interfaces, communication channels, and distributed coordination mechanisms.

In the second phase, the research will design a hardware-anchored trust layer for edge devices. This layer will extend trusted execution environments to support stronger isolation across both computational and input/output pathways. The goal is to ensure that AI workloads executed on edge devices remain protected from unauthorized access or manipulation.

The third phase will develop a distributed attestation framework that enables secure verification of device states across a network of edge nodes. This framework will explore lightweight consensus and verification mechanisms that allow devices to report and validate their integrity states while maintaining scalability and low latency.

The fourth phase will incorporate adaptive monitoring mechanisms based on machine learning techniques to detect anomalous system behavior. These mechanisms will analyze system telemetry, execution patterns, and network interactions to identify potential security threats or deviations from expected behavior.

In the final phase, the research will integrate these components into a unified autonomic trust architecture that continuously evaluates the security and reliability of edge intelligence systems. The architecture will be implemented and evaluated through prototype deployments in representative AIoT environments.

Experimental evaluation will examine system performance, security resilience, scalability, and real-time responsiveness under different deployment conditions. Through this approach, the research aims to demonstrate how integrated trust architectures can support the secure operation of next-generation cyber-physical intelligence infrastructures.