Automatic Monitoring, Threat Detection, and Alarm Generation in Cloud-Edge 6G Systems

Project Overview

Modern distributed systems, especially those spanning the cloud–edge continuum in 6G networks, face unprecedented challenges in maintaining performance, reliability, and security.

The project aims to explore and prototype solutions for **intelligent monitoring**, with an emphasis on:

- **Heterogeneous system environments** (cloud, edge, and far-edge devices),
- **Tailored monitoring agents** adapted to resource constraints and communication limitations at various network layers,
- **Selective data distribution strategies** to balance monitoring overhead and system responsiveness,
- **Cross-layer data collection** (network, application, and physical layers), enabling correlation of diverse metrics such as network throughput/latency and information-centric measures (e.g., age and value of information, semantic relevance).

By integrating semantics-aware monitoring (where the importance and timing of information are considered), the project will investigate how advanced metrics and analysis techniques can improve predictive capabilities, threat detection accuracy, and energy efficiency in IoT-enabled platforms.

Motivation

Automatic, intelligent monitoring has become critical in large-scale, heterogeneous computing environments. Manual supervision is no longer feasible due to system complexity and scale. Automated solutions enable:

- **Real-time detection** of operational issues and security threats,
- **Reduced downtime** and improved reliability,
- **Efficient resource utilization** and energy savings,
- **Enhanced compliance** and regulatory oversight.

By exploring cutting-edge monitoring techniques and their deployment in the context of next-generation networks, this project offers students the opportunity to engage with both foundational and emerging research directions in cloud-edge computing, networking, and intelligent automation.

Key Objectives

- **Survey recent literature** (last 4 years) on cloud-edge monitoring, threat detection, and semantic-aware metrics.
- **Analyze state-of-the-art monitoring frameworks**: Compare their capabilities, limitations, and suitability for heterogeneous environments.
- **Implement designs** for adaptive, semantics-driven monitoring and alarm generation.
- **Discuss trade-offs** related to data fidelity, energy efficiency, latency, and scalability.
- **Prepare a report** summarizing findings, including a critical comparison of the latest approaches.

Expected Outcomes

1. **Literature Study:** Conduct a thorough review of recent research papers on:
    - Monitoring and anomaly/threat detection in cloud-edge/6G systems,
    - Semantic-aware metrics and their applications,
    - Alarm and response mechanisms in distributed systems.
2. **Comparative Analysis:** Compare and contrast different approaches, highlighting:
    - Strengths and weaknesses,
    - Applicability to various layers (cloud, edge, far-edge),
    - Implementation feasibility and performance trade-offs.
3. **Reporting:** Document all findings and analyses in a comprehensive, well-structured report.

Background Required

- Basic understanding of networking and programming
- Familiarity with machine learning concepts (supervised/unsupervised learning, anomaly detection)