Automated, Context-Aware, and Robust Resource Control for Securing Services Against Emerging Threats

Project Overview

This project addresses the dynamic control and provisioning of computational resources (CPU, memory, storage, and network bandwidth) for critical services and applications in the presence of real or potential security threats. The objective is to investigate and implement **automated and context-aware resource management methods** that adapt to evolving threat scenarios by dynamically reallocating or tuning resources across cloud, network, and storage infrastructure.

Students will implement and evaluate strategies for:

- Detecting threat conditions and contextual changes affecting services,
- Triggering mitigation and corrective actions (e.g., migrating applications, adjusting resource allocations, enforcing security and privacy constraints),
- Leveraging semantic and contextual information to improve the timeliness and effectiveness of resource management decisions.

Motivation and Significance

Efficient resource control and provisioning are foundational for the secure and resilient operation of modern applications and services. In cloud and distributed environments, improper resource allocation can create severe vulnerabilities:

- **Over-provisioning** can waste resources and increase the attack surface.
- **Under-provisioning** can cause performance degradation and leave systems vulnerable to denial-of-service (DoS) and resource starvation attacks.
- **Lack of context-awareness** can result in generic, suboptimal responses that fail to address the root causes of security incidents.

With the increasing sophistication of cyber threats and the complexity of service delivery environments, there is a critical need for **intelligent, adaptive, and context-sensitive mechanisms** that anticipate, detect, and respond to risks in real time. This project will enable students to investigate advanced techniques at the intersection of resource management, security, and contextual intelligence, with direct relevance to both industry and research.

Key Objectives

- Analyze and classify typical threat scenarios affecting resource availability and service continuity.
- Implement an automated framework for monitoring, decision-making, and resource adjustment in response to threats and context changes.
- Integrate semantic and contextual information (e.g., user behavior, application criticality, system state) into the resource control logic.

- Ensure that the solution provides guarantees regarding security, privacy, performance, and fairness.

Expected Outcomes

- A simulation demonstrating automated, context-aware resource control and provisioning in the presence of threats.
- Documentation of design decisions, algorithms, and evaluation results.
- A final report and presentation discussing challenges, experimental findings, and directions for future research.

Background Required

- Knowledge of networking systems
- Programming (Python or similar languages)