Project 3: Automated, Context-aware, Efficient and Robust Resource Control and Provisioning against Threats to Services and Applications

This project is related to the resource control and provisioning of applications and services under threats, real or potential. This involves corrective/mitigation actions, such as relocation of the application, tuning of network, cloud and storage resources dedicated to the service, based on the different threat scenarios. In this sense, we care to develop a robust risk-averse resource control solution with security and privacy considerations. We will leverage the semantic attributes of information, as well as potential contextual knowledge, to provide security guarantees subject to timing (and potential fairness/privacy) constraints.

Required background: Basic networking knowledge, programming skills.

Motivation:
Resource control and provisioning of applications refer to allocating, managing, and regulating the computing resources—such as CPU, memory, storage, and network bandwidth—required by applications to function effectively. Resource control involves setting limits and priorities on these resources to ensure that applications run efficiently without overconsumption or interference with other services. Conversely, provisioning is the process of configuring and deploying the necessary infrastructure and resources that applications need to operate, often dynamically, based on demand. Together, these practices ensure that applications have the right resources at the right time, optimizing performance and cost-efficiency.

These practices are crucial to security because poorly managed resource control and provisioning can lead to vulnerabilities. For instance, if an application is over-provisioned, it might waste resources, increasing the attack surface for potential threats. Under-provisioned applications, however, can lead to performance issues, making systems more susceptible to denial-of-service (DoS) attacks as they struggle to handle unexpected loads. Additionally, improper resource control can allow malicious applications to monopolize resources, disrupting service availability. By carefully managing resource control and provisioning, organizations can maintain a secure, resilient, and well-functioning application environment, reducing the risk of security breaches and ensuring critical services remain available and protected against threats.