## Project 2: Automatic Monitoring, Threat Detection, Alarm Generation

The project considers reactive closed-loop automation by implementing the observation, analysis, detection, and reactions in terms of alarm generation. To address the complexity and heterogeneity of the cloud-edge continuum, the project will investigate solutions for monitoring systems, with tailored monitoring agents, targeting far-edge and edge monitoring and selective distribution of monitoring data. The data usually are collected at the different layers of the 6G system (network, application, and physical) with the aim to correlate information related to typical network metrics (e.g., throughput, latency, etc.) and/or information metrics (e.g., age and value of information, semantics, etc.) with IoT platform and devices, e.g., traffic profiling information from specific network analysis applications. Furthermore, by allowing the utilization of semantics of information to allow for more accurate predictions and reducing energy consumption.

Perform a detailed literature study with recent works and describe their pros and cons. A detailed report will be the deliverable for this project.

Required background: Basic networking knowledge and understanding of ML concepts.

## Motivation:

Automatic monitoring is essential because it provides continuous, real-time oversight of systems, enabling the early detection of issues, minimizing downtime, and ensuring consistent performance and security. Manual monitoring is impractical and prone to errors in complex, large-scale environments, whereas automatic monitoring offers scalability, efficiency, and accuracy. It helps optimize resources, reduces the risk of costly failures, and supports compliance with regulatory standards. Additionally, automatic monitoring enhances user experience by maintaining service quality and supports modern practices like DevOps and continuous delivery, ensuring systems are reliable, secure, and responsive to issues as they arise.