

Lecture Title: AI-powered evolution towards open and secure edge architectures

Lecture Abstract (250 words):

The talk will discuss how to tackle the challenges of edge computing evolution described around the following three main pillars: i) “edge for AI”, namely a flexible, modular and converged edge platform design, unifying the lifecycle management and closed-loop automation for cloud-native applications, MEC and network services across a multi-domain edge-cloud continuum, while fully exploiting the capabilities of cutting-edge multi-core and multi-accelerator platforms for ultra-high computational performance, ii) “AI for edge” namely an AI-powered portfolio of solutions that will leverage the multitude of information and metrics provided by the VERGE platform monitoring mechanisms to manage and orchestrate the VERGE platform computing and network resources, and iii) security, privacy and trustworthiness of AI for Edge, through a suite of methods and tools that will ensure a) security of the AI-based models against adversarial attacks, b) privacy of data and models, and c) training and execution that does not lead to unsafe states by providing explanations for model decisions, improving trust in models.