[For Short Presentation]

Securing the Edge AI: Rethinking AI in a Serverless World

Adil Bin Bhutto*[1] and Monowar Bhuyan†[1]

[1]Department of Computing Science, Umeå University, Sweden

May 15, 2025

Abstract

As Artificial Intelligence (AI) workloads move closer to users via edge computing and serverless platforms, the technology paradigm shift is entering a new era of intelligent, decentralized, and personalized systems. While this shift promises low-latency decision-making and scalable deployment, it also introduces complex and often under-explored security challenges. This presentation will facilitate the sharing of evolving risks and opportunities at the intersection of serverless infrastructure, edge AI, and security. Further, this presentation will enumerate the problems and potential solutions to secure systems and AI at the edge.

*adilbb@cs.umu.se

†monowar@cs.umu.se