Developing Privacy-Enhancing Technologies for Edge Computing

With the rapid growth of IoT and the increasing need for real-time data processing, “edge computing” is becoming more prevalent across various industries such as healthcare, automotive, manufacturing, and smart cities.

Edge computing introduces several security and privacy challenges due to its decentralized nature, the diversity of parties (e.g., devices) involved, and the criticality of data being processed. The main challenges include (1) Increased Attack Surface: With more devices and nodes distributed across different locations, the number of potential entry points for attackers increases, (2) Device Vulnerabilities: Many edge devices have limited computational resources, making it difficult to implement robust security measures, and (3) Physical Security: Edge devices are often deployed in unsecured, remote, or public locations, making them vulnerable to physical tampering or theft.

By developing effective and customized privacy-enhancing technologies (such as Federated Learning, secure Multi-party Computation, or Private Set Intersection), this research aims to help enhance security and trust in edge computing systems, encouraging broader adoption while complying with strict data protection regulations, such as GDPR in Europe, that mandate strong privacy measures.

Enhancing Resilience of Cyber-Physical Systems through Robust Privacy-Preserving Distributed Systems

Cyber-Physical Systems (CPSs) are increasingly prevalent in critical infrastructure and services, integrating computing, networking, and physical processes. However, concerns about the resilience of CPSs against cyber threats or natural disasters are growing. The importance of enhancing the resilience of CPS to ensure these systems can withstand and recover from various types of disruptions (including cyber-attacks and natural disasters) has been underscored by the recent white paper published by America’s Cyber Defense Agency [1].

This PhD research aims to develop and implement innovative methods to improve the robustness and resilience of cyber-physical systems (CPS) against various disruptions while ensuring data privacy in distributed environments. This research addresses the critical need for CPS to maintain operational integrity and security during adverse events, such as cyber-attacks or natural disasters, by integrating advanced privacy-preserving technologies. The goal is to create CPS that are not only capable of quickly recovering from disruptions but also safeguarding sensitive information, aligning with contemporary technological advancements and regulatory requirements for data privacy.

[1]. America’s Cyber Defense Agency, Research, Development, and Innovation for Enhancing Resilience of Cyber-Physical Critical Infrastructure: Needs and Strategic Actions, 2023.