Title: Privacy and security for AI/ML including Privacy enhancing technologies

Professor/PhD Heung Youl Youm

Soonchunhyang University, Korea (Republic of)

Abstract

Nowadays, there are many use cases based on AI/ML technologies. There are many risks for applications and services based on AI/ML. Privacy-enhancing technologies (PET) refers to technologies that respect fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individual. There are several use cases for privacy enhancing technologies: Cryptographic algorithms, Data masking techniques, technologies based on AI/ML such as Federated learning and synthetic data. They can be applicable for various use cases: Test data management, Financial transactions, Healthcare services, Facilitating data transfer between multiple parties including intermediaries.

This keynote will identify privacy principles for services based on AI/ML. In addition, some privacy guidelines will be presented for the service providers, considering the lifecycle of services and applications based on AI/ML. It also identifies various types of privacy enhancing technologies and provide how they could be designed to improve the privacy while keeping the usage of personal data. It also provides privacy risks and their countermeasures to mitigate threats for the services and applications using ICTs including AI/ML technologies.