İTÜ
FACULTY OF MANAGEMENT
DATA SCIENCE AND ANALYTICS DEPARTMENT

DEPARTMENTAL SEMINARS

20 OCT 2025

13:00-14:00

ISB 210

Dr. Artrim Kjamilji

A Framework of Secure and Private Machine Learning Algorithms for the Post-Quantum Industry

SHORT BIO: Artrim Kjamilji received his BSc degree in Informatics and Computer Engineering from Ss. Cyril and Methodius University, Skopje, North Macedonia, in 2010; the MSc degree in Information-Communication Technologies from the American University of Europe-FON, Skopje in 2013; and the Ph.D. degree in Computer Science and Engineering from Sabanci University, Istanbul, Turkey, in 2021. He was a Lecturer at Sabanci University during 2021–2022. From 2022 he is an Assistant Professor at Istanbul Zaim University. His research interests include Post-Quantum Cryptography, Machine Learning, IoT, Network Security and Big Data Privacy.

ABSTRACT: Over the past decade, Machine Learning (ML) classifiers have found widespread application in industries such as health, cybersecurity, banking, etc. Despite their effectiveness, privacy, security, and regulatory concerns continue to limit their industrial deployment in practice. Existing laws and ethical requirements governing clients' and institutions' data impose strict constraints on the adoption of ML technologies in these areas.

In this talk, we address these challenges by presenting a framework for privacy-preserving ML classification utilizing advanced encryption techniques. Since many ML classifiers—including Deep Neural Networks (DNNs), Support Vector Machines (SVMs), Logistic Regression (LR), and variants of Naïve Bayes (NB)—can be formulated as matrix operations, we propose a secure toolkit of encrypted linear algebra primitives.

We demonstrate how the proposed toolkit enables secure and private ML inference under strict confidentiality guarantees while maintaining computational and communication efficiency. Furthermore, since the utilized cryptographic primitives are shown to be resilient to attacks from quantum computers, the presented schemes are applicable to the post-quantum industry.