The Double Nature of Machine *Learning (ML)/ Artificial Intelligence (AI) in Cybersecurity*

Training School

4 - 6 June 2025

Polytechnic University of Tirana

FTI – Faculty of Information Technology

Polytechnic University of Tirana, Faculty Information Technology

Venue: Universiteti Politeknik i Tiranes, Bulevardi Dëshmorët e Kombit Nr. 4, Tiranë 1000, Albania

Google Maps: *https://g.co/kgs/cqG3tNQ*

*Room: (**Aula Magna –** Amphitheater of Polytechnic University of Tirana)*

AGENDA

DAY 1 (04.06.2025)

08.30 - 9.00	*Arrival and registration of the participants*
09.00 - 9.30	***Welcoming remarks by organizers***
09.30 - 11.00	***Güzin Ulutaş***
	Exploring AI Technologies for Cybersecurity: From Deepfake Detection to Anomaly - Based IDS
	She is a Computer Engineering professor at Karadeniz Technical University, specializing in cybersecurity, multimedia security, network security and deepfake detection. She chairs the Cybersecurity Branch of the department and she is also an advisory board member of TUBITAK EEEAG sub branch. She also contributes to BEING-WISE and has supervised many MSc and PhD students.
11.00 -11.30	*Coffee break*
11.30 -13.00	***Güzin Ulutaş***
	Exploring AI Technologies for Cybersecurity: From Deepfake Detection to Anomaly - Based IDS (Continued)
13.00 - 14.30	*Lunch break*
14.30 -16.00	***Ali Hassan Sodhro***
	Adaptive IoT-5G Physical Layer Authentication Mechanism for Healthcare Applications: From Developments to Implementing Recommendations
	He is a Senior Lecturer at Kristianstad University, Sweden, with prior roles at Mid-Sweden and Gothenburg Universities. He holds a PhD from the Chinese Academy of Sciences and has completed prestigious postdoctoral fellowships across Europe.
16.00 - 16.30	*Coffee break*
16.30 - 17.30	***Ali Hassan Sodhro***

Adaptive IoT-5G Physical Layer Authentication Mechanism for Healthcare Applications: From Developments to Implementing Recommendations - Continued

17.30 - 18.00 ***Panel Discussion and Concluding remarks***

DAY 2 (05.06.2025)

09.00 - 10.30 ***Davide Andreoletti***

Privacy-Enhancing Technologies for ML Inference: Models, Methods, and Trade-Offs

He is a researcher at the University of Applied Sciences and Arts of Southern Switzerland (SUPSI), within the Institute of Information Systems and Networking (ISIN), where he leads the research sector on privacy and trust. He received his Ph.D. in Information Technology from Politecnico di Milano, Italy, in 2020, focusing on privacy-preserving technologies (PETs) applied to telecommunication networks. His current research interests lie at the intersection of machine learning and privacy preservation, with particular emphasis on protecting privacy in generative AI systems, especially Large Language Models.

10.30 - 11.00 *Coffee break*

11.00 -12.30 ***Davide Andreoletti***

Privacy-Enhancing Technologies for ML Inference: Models, Methods, and Trade-Offs (Continued)

12.30 - 14.00 *Lunch break*

14.00 - 15.30 ***Edlira Martiri***

Synthetic data for AI-driven cybersecurity in Next-Generation Networks (6G and beyond)

She is a cybersecurity expert with Ph.D.s from the University of Tirana and NTNU, Norway. She specializes in data protection, information security, and risk management. As co-founder of Cyber Morfosis, she advances secure systems, ethical tech, and cybersecurity innovation.

15.30 -16.00 *Coffee Break*

16.00 - 17.30 ***Ivan Chorbev***

AI strengthening Cybersecurity, AI abused for Cyberattacks, and AI threatened by Cyberattacks

Ivan Chorbev is a Full Professor and Head of the Software Engineering Department at the Faculty of Computer Science and Engineering at the Ss Cyril and Methodius University in Skopje (UKIM). His main interests and activities include Software engineering, Machine learning, Data Science. He is part of the ongoing projects CyberMACS, MKSafeNet, EuroCC2.

17.30 - 18.00 ***Panel Discussion and Concluding remarks***

DAY 3(06.06.2025)

09.00 -10.30 Omran Ayoub

Explainable Artificial Intelligence to Enhance the Transparency and the Reliability of Machine Learning-based Network Intrusion Detection Systems – First Part

He is a lecturer-researcher at the University of Applied Sciences and Arts of Southern Switzerland, where he also co-leads the research area on trustworthy and secure information networks and society. His research interests lie in machine learning applications for networks and explainable artificial intelligence.

10.30 -11.00 Coffee break

11.00 - 12.30 Omran Ayoub

Explainable Artificial Intelligence to Enhance the Transparency and the Reliability of Machine Learning-based Network Intrusion Detection Systems – ***(continued)***

12.30 - 14.00 Lunch break

14.00 - 15.00 Trainees Presentation Session and Discussion

Hussein Fawaz

Explainable and Uncertainty-Aware Intrusion Detection for Trustworthy Cybersecurity

Rashmi Erandika Ratnayake

Machine Learning-Driven Data Trust Evaluation for Blockchain-Enabled IoT Systems

Selina CHEGGOUR

Machine Learning Vulnerabilities in 6G: Adversarial Attacks and Their Impact on Channel Gain

Jiali XU

Advancements in Scalable and Robust 5G Jamming Detection: From On-Device Machine Learning to Collaborative Intelligence

15.00 - 15.30 Coffee Break

15.30 - 16.30 Trainees Presentation Session and Discussion(continued)

Sonay Caner-Yıldırım

Who Clicks the Link? Exploring Diversity-Aware XAI for Phishing Susceptibility Prediction

Aymen Bouferroum

Accelerating Trust Convergence in IIoT: A ML Approach for Dynamic Network Conditions

Sahana Sridhar

Integration of LLMs and AGI into next-generation 6G communications with a special focus on Information Security

16.30 - 17.00 Distribution of certificates and Concluding Remarks