AI & SECURITY Webinar

30th April 2025
01.00 PM - 17.00 PM CET

elacontic PREDICT-6G HARPOCRATES CONFIDENTIAL6G RIGOUROUS fAIth CUSTODES

What is it about

The AI & Security Webinar is a collaborative event co-organized by five EU-funded research projects: **ELASTIC, PREDICT-6G, HARPOCRATES, CONFIDENTIAL6G**, and **RIGOUROUS** - with the support of **FAITH** and **CUSTODES.**

The webinar will focus on the intersection of **artificial intelligence (AI)** and **cybersecurity** within the context of **next-generation networks**.

AI Security for Mobile Networks

As mobile networks grow and evolve, it becomes even more important to ensure they are secure and protect users' privacy. This webinar will bring together experts from various fields to discuss the **latest research, new technologies, and solutions** to address the **security challenges of AI and machine learning in mobile networks.**

Presentations will cover how these technologies can be used to **make networks safer, more reliable, and better at protecting data.**

Key Topics

Privacy-Preserving AI:
Exploring recent advancements in guaranteeing data privacy for distributed AI.

AI for Network Resilience:
Discussing how AI can predict network behavior, detect issues, and enhance security in 6G networks.

Blockchain and AI in Network Management:
Looking at how blockchain and AI can improve resource management and decision-making in 6G networks.

Projects

The **ELASTIC project** focuses on improving the security of cyber-physical systems, using technologies like WebAssembly to protect critical infrastructure from cyber threats.

More info: https://elasticproject.eu/

The **PREDICT-6G project** aims to develop secure, AI-powered solutions for 6G networks, focusing on privacy, resilience, and predictive capabilities to address the challenges of future mobile networks.

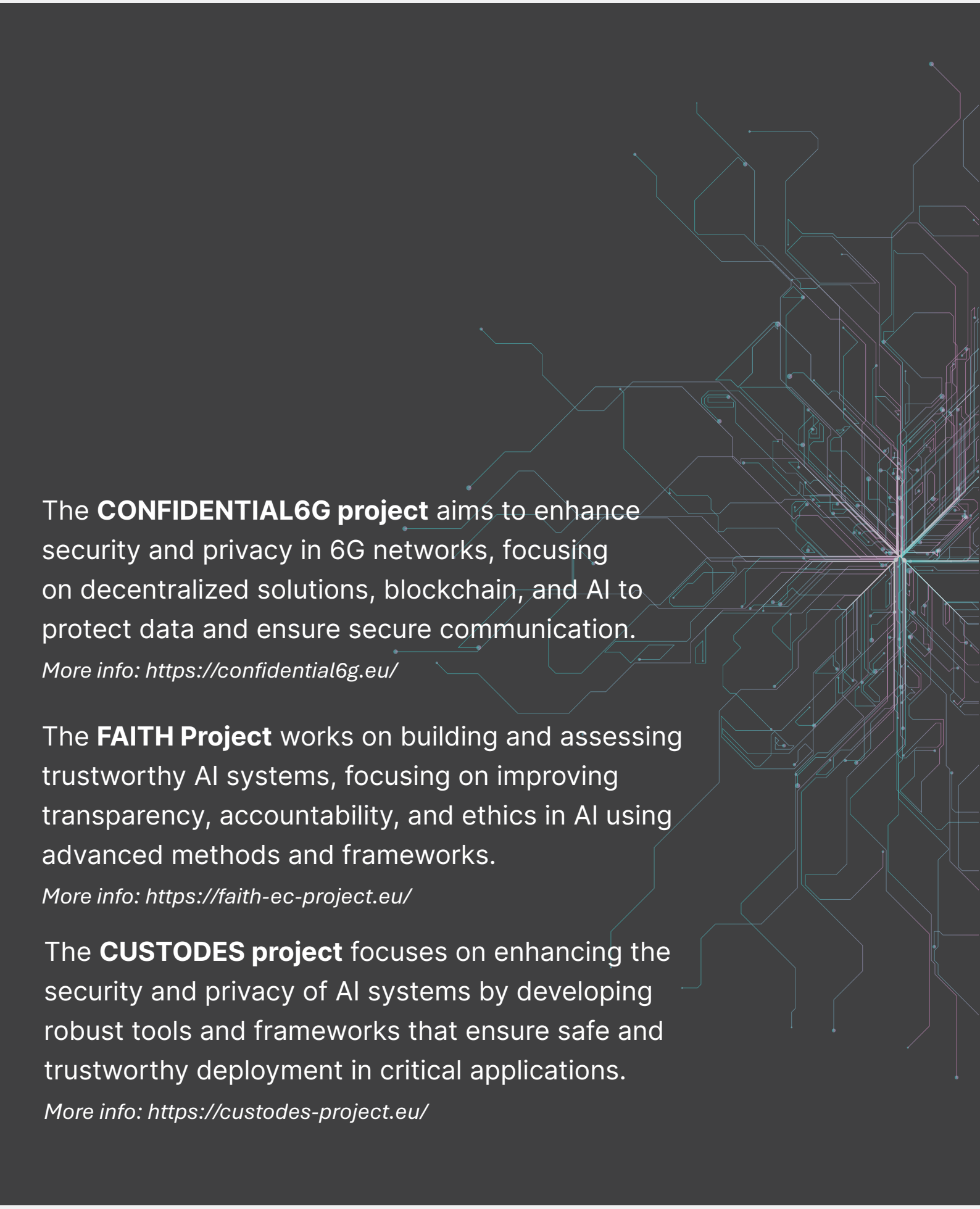
More info: https://predict-6g.eu/

The **HARPOCRATES project** focuses on enhancing the security and privacy of AI systems, developing solutions for secure machine learning and data protection in distributed environments.

More info: https://harpocrates-project.eu/

The **RIGOUROUS project** focuses on developing advanced security and privacy solutions for next-gen networks, using AI and machine learning to improve threat detection and incident response.

More info: https://rigourous.eu/



The **CONFIDENTIAL6G project** aims to enhance security and privacy in 6G networks, focusing on decentralized solutions, blockchain, and AI to protect data and ensure secure communication.

More info: https://confidential6g.eu/

The **FAITH Project** works on building and assessing trustworthy AI systems, focusing on improving transparency, accountability, and ethics in AI using advanced methods and frameworks.

More info: https://faith-ec-project.eu/

The **CUSTODES project** focuses on enhancing the security and privacy of AI systems by developing robust tools and frameworks that ensure safe and trustworthy deployment in critical applications.

More info: https://custodes-project.eu/

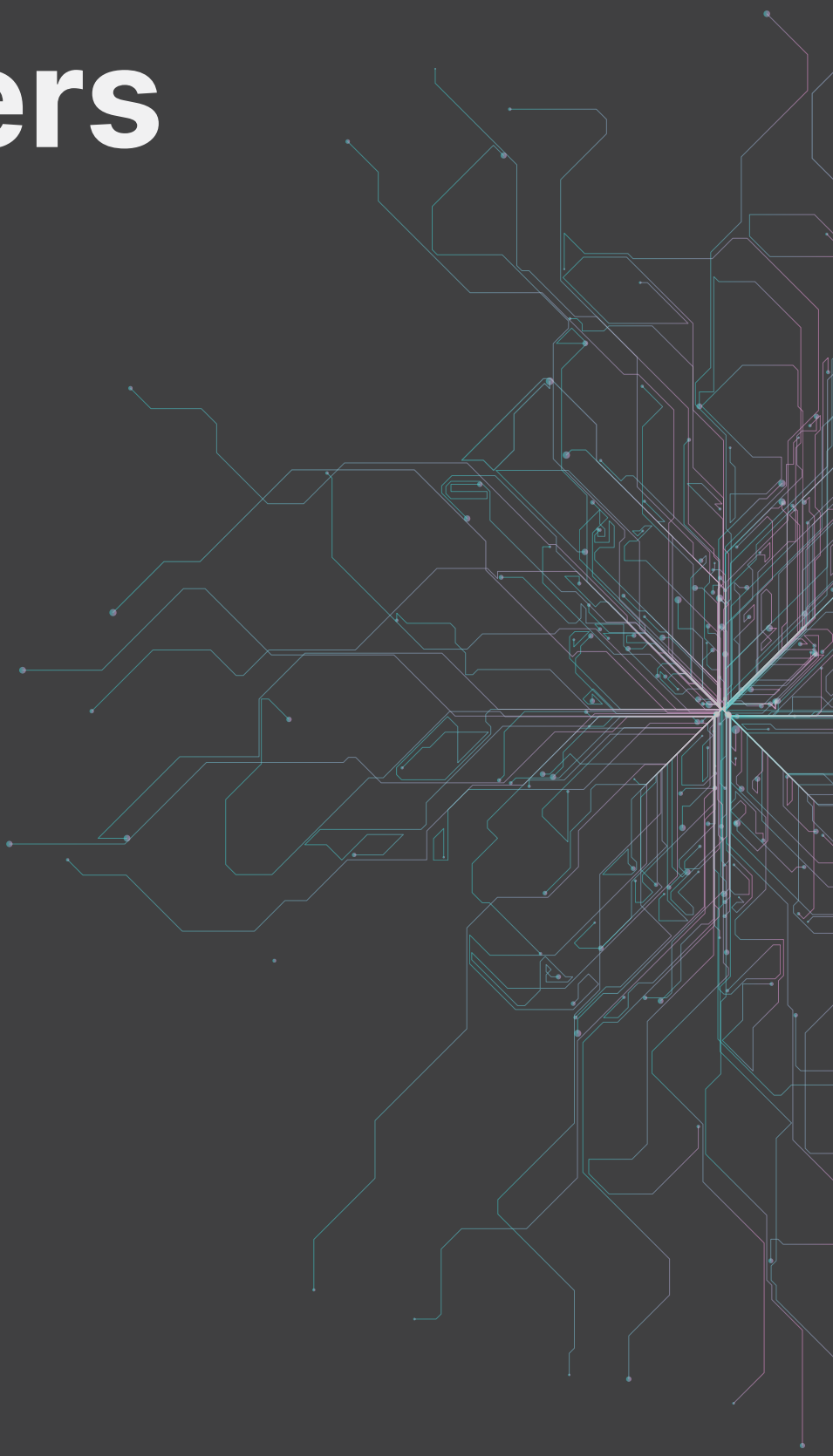
Dr. Nenad Gligoric

CEO of Zentrix Lab

Artificial Intelligence (AI) and cybersecurity are increasingly intertwined, forming the backbone of secure and resilient digital infrastructures in an evolving technological landscape. As mobile networks transition towards next-generation technologies, addressing security and privacy concerns becomes not only critical but also complex due to the innovative capabilities that AI brings to network management, threat detection, and user privacy.

Welcome to the AI & Security Webinar, jointly organized by several EU-funded projects. This webinar aims to explore essential developments in privacy-preserving AI methodologies, predictive network resilience mechanisms, and blockchain-enhanced solutions designed specifically to secure mobile network infrastructures. By gathering leading researchers, industry practitioners, and policymakers, we seek to foster dialogue, share insights, and promote collaborative efforts that ensure enhanced security, robust privacy protection, and sustained trustworthiness in Europe's AI-driven network ecosystems.

Speakers



Prof. Nineta Polemi

Cybersecurity Professor at University of Piraeus
CTO & Cofounder at trustilio B.V.

Nineta Polemi is a cybersecurity Professor in the University of Piraeus-UNIPI- (Cyber Security Lab, Dept. of Informatics) and CTO/ Co-Founder of Trustilio. She served (2017-2020) as Programme Manager and Policy Officer in the European Commission DG (CONNECT H1 Unit entitled 'Cybersecurity Technologies and Capabilities').

She has obtained her Ph.D. in Applied Mathematics (Coding Theory) from The City University of New York (Graduate Center). She held teaching and research positions in The City University of New York (Queens & Baruch Colleges), State University of New York (Farmingdale), Université Libre de Bruxelles (ULB)-Solvay Brussels School-. She has over 150 publications in security (e.g. port security, maritime security, maritime supply chain security) has organised numerous scientific and policy international cybersecurity scientific events. She has received many research grants (NATO, IEEE) and awards (NSA, MSI Army Research Office IEEE, CYNY, Hellenic Ministry of Maritime, Hellenic National Defense General) and has participated as Project and Technical Manager in more than 60 cybersecurity international, EU and national R&D and commercial projects.

Abstract:
As AI becomes a cornerstone of the European digital ecosystem, ensuring its security and trustworthiness is critical. This keynote will explore the intersection of cybersecurity certification for ICT systems and trustworthiness certification for AI, highlighting the role of cryptographic mechanisms in securing AI applications. It will cover emerging regulatory frameworks, standardization efforts, and cryptographic techniques that enhance AI security and privacy. The talk will also examine how the EU is shaping policies to foster a resilient, AI-driven digital landscape, ensuring compliance, transparency, and trust in next-generation AI systems.

David Eklund

RISE Research Institute of Sweden

David is a researcher in applied artificial intelligence.
David holds a PhD in mathematics and a Master's degree in engineering physics from the Royal Institute of Technology. Davids' research experience spans applied algebra, geometry and machine learning. He also has industry experience in the field of formal verification and railway signalling.

Abstract:
We introduce bounds on Mutual Information (MI) for efficient privacy-preserving feature selection with secure multi-party computation (MPC). The bounds are much cheaper to compute than common estimates of MI. Our experimental results show that we can achieve significant speed ups compared to a straightforward MPC implementation of Mutual Information, while achieving similar accuracy for the downstream machine learning model.

Fotis Foukalas

Cogninn

Fotis is a technology advisor at Cogninn for 6G and AI technologies.

Abstract:
Considering the predictive type of 6G networks, the security threats are numerous due to the deterministic and time sensitivity nature of the PREDICT-6G networks. In this talk, we will shed light in those threats and propose security enablers for future PREDICT-6G networks.

Apostolos Pyrgelis

RISE Research Institute of Sweden

Apostolos is a Senior Researcher at RISE Research Institutesof Sweden, and a Member of the Cybersecurity Unit. His research interests include privacy-enhancing technologies, appliedcryptography, and enjoys working on problems at the intersection of machine learning analytics and security or privacy. He received his B.Sc. and M.Sc. degrees in computer engineering and informatics from the University of Patras, Greece, and the Ph.D. degree from University College London (UCL), U.K.

Abstract:

We study the problem of privacy-preserving hyperparameter (HP) tuning for cross-silo federated learning (FL). We first perform a comprehensive measurement study and benchmark various single-shot HP tuning strategies compatible with privacy-preserving FL pipelines. We show that the optimal parameters of the FL server can be accurately tuned based on the HPs found by each client on its local data. We demonstrate that HP averaging is suitable for iid settings, while density-based clustering uncovers the optimal set of parameters in non-iid ones. To prevent information leakage from the exchange of the clients' local HPs, we design and implement PrivTuna, a novel framework for privacy-preserving HP tuning using multiparty homomorphic encryption.

Shen Wang

Assistant Professor (Tenured) |
Academic Director of NETSLAB research group,
School of Computer Science,
University College Dublin, Ireland

Dr. Wang is a senior member of IEEE and an active member of its Intelligent Transportation Systems (ITS) society. He received an M.Eng. degree from Wuhan University, China, and a Ph.D. degree from Dublin City University, Ireland. Dr. Wang has been involved with several EU projects as a co-PI, WP, and Task leader in big data streaming for air traffic control, and trustworthy AI for intelligent cybersecurity systems. Some key industry partners of his applied research projects are IBM Research Brazil, Boeing Research and Technology Europe, Telefónica Research and Fraunhofer FOKUS. His research interests include connected autonomous vehicles, explainable artificial intelligence, and security and privacy for mobile networks.

Abstract:
Federated learning (FL) is a promising distributed machine learning architecture that will play an important role for privacy-preserving AI-powered 6G networks. However, FL is still facing many security and privacy challenges such as back door attacks and membership inference attacks. This talk briefs the recent advances in UCD Netslab in advancing the robust and privacy enhanced FL under heterogeneous 6G networks utilising explainable AI (e.g., LIME, SHAP and LRP), especially for hierarchical FL and peer-to-peer FL.

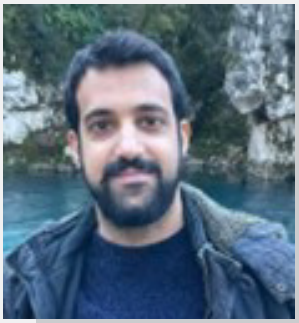
Madhusanka Liyanage

Associate Professor | Ad Astra Fellow
Director of NETSLAB research group
School of Computer Science,
University College Dublin, Ireland

Madhusanka Liyanage is an Associate Professor/Ad Astra Fellow at University College Dublin, Ireland. He is also a Docent/Adjunct Professor at the University of Oulu, Finland, the University of Ruhuna, Sri Lanka, and the University of Sri Jayewardenepura, Sri Lanka. He holds a Doctor of Technology degree from the University of Oulu, Finland (2016) and prestigious fellowships from 2018 to 2020. Madhusanka has been a Visiting Research Fellow at various renowned institutions globally.

He received the "2020 IEEE ComSoc Outstanding Young Researcher" award and was ranked among the World's Top 2% of Scientists in 2021, 2022, and 2023. He has over 200+ publications, authored books, edited books, and two patents. Additionally, he serves as an expert consultant at the European Union Agency for Cybersecurity (ENISA) and has secured over 5 Million euros in research funding. Currently, he leads four large EU Horizon Europe projects and is the director of the Netslab team at University College Dublin, Ireland.

Abstract:
The growing demand for spectrum, driven by mobile users, IoT devices, and data-intensive applications, has highlighted the limitations of static spectrum allocation. Dynamic Spectrum Access (DSA) offers a solution by allowing unlicensed users to opportunistically access idle licensed spectrum bands, improving spectral efficiency in beyond 5G (B5G) networks. However, effective DSA requires real-time coordination, security, and fair resource sharing. Blockchain, with its decentralized and immutable nature, provides a transparent and secure framework for spectrum allocation. Smart Contracts (SCs) automate DSA processes, enabling spectrum trading and AI-driven optimization, while Non-Fungible Tokens (NFTs) can be leveraged to tokenize and manage spectrum licenses dynamically. This talk explores blockchain-driven DSA frameworks, their advantages, and future research directions for efficient spectrum management.



Anastasios Giannopoulos

FDI

Anastasios E. Giannopoulos (Member, IEEE) (MEng, Ph.D) received the diploma of Electrical and Computer Engineering from the National Technical University of Athens (NTUA), where he also completed his Master Engineering (M.Eng) degree, in 2018 and his Ph.D. at the Wireless and Long Distance Communications Laboratory of NTUA. His research interests include advanced Optimization Techniques for Wireless Systems, ML-assisted Resource Allocation, Maritime Communications and Multi-dimensional Data Analysis.
He is currently working as a Researcher in the R&D department of FDI and as Research Associate at Department of Ports Management and Shipping, in the National and Kapodistrian University of Athens. He has authored more than 50 scientific publications in the fields of Wireless Network Optimization, Maritime Communications, Machine Learning and Multi-dimensional Analysis.

Abstract:
The increasing complexity of cloud-native 6G networks necessitates intelligent resource management to optimize scalability, energy efficiency, and service reliability. To this end, AI-driven self-healing mechanisms for dynamic server activation within a cloud-native system are required. In this work, we present a scheme integrating three key frameworks: the Management and Orchestration Framework for policy-based network service orchestration, the Cloud Continuum Framework for dynamic resource scaling, and the Artificial Intelligence and Machine Learning Framework for predictive analytics and anomaly detection. By leveraging AI models, the system continuously monitors workload variations,forecasts resource demand, and dynamically scales computing resources, ensuring optimal energy efficiency and SLA compliance. The proposed self-healing workflow enables proactive server activation and deactivation, addressing load bursts and underutilization scenarios.

Merlijn Sebrechts

Imec and Ghent University

Dr. ing. Merlijn Sebrechts is a senior researcher at imec and teaches at Ghent University in Belgium. He leads a number of research tracks focused on software deployment and trust in the cloud and on devices. He is currently serving on the Ubuntu Community Council and is standardizing WebAssembly System Interfaces for IoT devices as part of the W3C and the Bytecode Alliance. He teaches topics such as Distributed Systems Design, Open Source ecosystems and Computer Security. His work has been published in over 20 scientific publications and has received four awards.

Abstract:
Updating software on IoT devices is a pain, leading to an "internet of insecure things". Deployment speed has massively improved for cloud applications, but IoT development is still in the dark ages, where simple updates can take months or years. Moreover, existing workload isolation and sandboxing techniques are not adapted to low-resource devices and lack robust mechanisms to give applications limited access to external hardware. WebAssembly is great for cross-platform software distribution, and the WebAssembly System Interface (WASI) removes its dependency on browser technology. This turns WebAssembly into a highly performant virtualization and sandboxing platform for low-resource devices.

In this talk, we will discuss the challenges and opportunities for using WebAssembly to deploy software to cyber-physical systems. We'll highlight recent efforts to build cyber-physical WebAssembly interfaces, run device drivers in WebAssembly, and isolate individual embedded software components to limit the impact of supply-chain vulnerabilities.

Antonio Skarmeta

University of Murcia

Dr Antonio Skarmeta received the M.S. degree in Computer Science from the University of Granada and B.S. (Hons.) and the Ph.D. degrees in Computer Science from the University of Murcia Spain. Since 2009 he is Full Professor at the same department and University. Antonio F. Skarmeta has worked on different research projects in the national and international area in the networking, security and IoT and 5G area. His main interested is in the integration of 5G, security services, identity, IoT and Smart Cities,. He has been the head of the research group ANTS since its creation on 1995. Actually, coordinate an EU project RIGOUROUS and the spanish 6G project CERBERUS both on Security on B5G/6G. He has published over 200 international papers and is a member of several program committees.
He has also participated in several standardization fora like IETF, ISO and ETSI and being nominated as IPv6 Forum Fellow. He is also CTO of the spinoff company Odin Solution S.L. (OdinS) in the area of IoT and Smart Infrastructure.

Abstract:
Next generation networks and the strength of the distributed computing paradigm (edge/cloud) are transforming how services are provisioned, mainly when solutions focus on collaboration and aggregation of resources provided by different entities or organisations, that becomes essential to satisfy the most demanding computation and storage service requirements. However, it also entails challenges such as infrastructure and technologies heterogeneity, which directly impacts infrastructure management and especially security, that usually tends to be relegated to a second place. In this talk we will analyse some initial discussion in the context of EU project RIGOUROUS related to the security for future 6G networks and how the security and privacy requirements can be used to drive the enforcement of deployment of intelligent secure networks

Jorge Bernal

Associate Professor

Jorge Bernal Bernabe received the MSc, Master, and PhD in Computer Science as well as an MBA from the University of Murcia (Spain). he is an Associate professor (Profesor Titular) in the Department of Information and Communications Engineering of the University of Murcia. Jorge Bernal has been a visiting researcher in the Cloud and Security Lab of Hewlett-Packard Laboratories (Bristol UK) and in the University of the West of Scotland. Author of more than 45 papers published in JCR-indexed impact journals, plus numerous conference papers and book chapters.. During the last years, he has been working on several European research projects FP7 and H2020, such as ARIES, ANASTACIA, CyberSec4Europe, Inspire-5Gplus, Olympus, RIGOUROUS, ResilMesh. His scientific activity is mainly devoted to security, trust, and privacy management in distributed systems. He is also interested in the security and privacy aspects of the Internet of Things. Metrics: over 3600 citations in Google Scholar, h index : h33, i10 index: 61.

Abstract:

This talk introduces a Federated Network Intelligence Orchestration approach aimed at scalable and automated Federated Learning (FL)-based anomaly detection in B5G networks. By leveraging a horizontal Federated learning approach based on the FedAvg aggregation algorithm, which employs AI models like autoencoder trained on non-anomalous traffic samples to recognize normal behavior, the system orchestrates network intelligence to detect and prevent cyber-attacks. Integrated into a B5G Zero-touch Service Management (ZSM) aligned Security Framework, the proposal utilizes multi-domain and multi-tenant orchestration to automate and scale the deployment of FL-agents and AI-based anomaly detectors, enhancing reaction capabilities against cyber-attacks.

The proposed FL architecture can be dynamically deployed across the B5G Continuum, utilizing a hierarchy of Network Intelligence orchestrators for real-time anomaly and security threat handling.

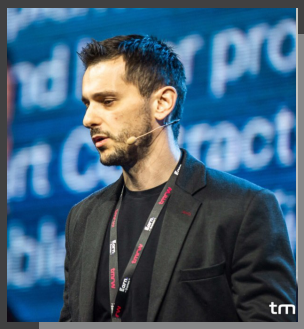
Sotirios Spantideas

FDI

Sotirios T. Spantideas (D.Eng, M.Sc, Ph.D) obtained the Diploma of Electrical & Computer Engineering from the Polytechnic School of the University of Patras in 2010. He then attended the Master Program ”Electrophysics” at the Royal Institute of Technology in Stockholm (KTH), from which he obtained the title MSc in 2013. In 2018 he obtained his PhD from the National Technical University of Athens (NTUA) with doctoral dissertation entitled “Development of Methods for obtaining DC and low frequency AC magnetic cleanliness in space missions”. His research interests include Electromagnetic Compatibility, Machine Learning for Wireless Networks, Magnetic Cleanliness for space missions and optimization algorithms for Computational Electromagnetics. He is working in the R&D department of FDI and as a Research Associate with National and Kapodistrian University of Athens (Department of Ports Management and Shipping - NKUA), participating in multiple Horizon projects. He has published over 50 papers in scientific journals and conferences in the fields of Electromagnetic Compatibility, Optimization Methods for Wireless Networks and Machine Learning for Resource Allocation problems.

Abstract:

The increasing complexity of cloud-native 6G networks necessitates intelligent resource management to optimize scalability, energy efficiency, and service reliability. To this end, AI-driven self-healing mechanisms for dynamic server activation within a cloud-native system are required. In this work, we present a scheme integrating three key frameworks: the Management and Orchestration Framework for policy-based network service orchestration, the Cloud Continuum Framework for dynamic resource scaling, and the Artificial Intelligence and Machine Learning Framework for predictive analytics and anomaly detection. By leveraging AI models, the system continuously monitors workload variations,forecasts resource demand, and dynamically scales computing resources, ensuring optimal energy efficiency and SLA compliance. The proposed self-healing workflow enables proactive server activation and deactivation, addressing load bursts and underutilization scenarios.



Dr. Nenad Gligoric

CEO of Zentrix Lab

Dr. Nenad Gligoric holds a PhD from the University of Belgrade and has extensive experience in research and application areas encompassing the Internet of Things (IoT), Artificial Intelligence (AI), and cybersecurity. As part of Zentrix, he currently coordinates innovation efforts across multiple European projects, including CONFIDENTIAL6G, ELASTIC, HARPOCRATES, and TITAN.

These projects primarily address key issues related to the integration of AI and cybersecurity within next-generation communication networks.
His career includes experience as an associate professor and positions within leading industry companies such as Ericsson.

Dr. Gligoric has actively collaborated with major technology companies, including Fujitsu, Huawei, Nokia, and Thales. He has published more than 30 peer-reviewed articles in journals and conferences, including those published by Elsevier, Springer, and Wiley.

13.00-13.20

Welcome and Opening Keynote

- Welcome by the organiser, Zentrix
- Cybersecurity Certification for ICT vs. Trustworthiness Certification for AI Systems - Prof. Nineta Polemi

13.20-14.20

Session 1: Privacy and Security in Federated and Distributed AI

HARPOCRATES: *Privacy and Security Preservation in Distributed AI*

- Efficient Privacy-Preserving Feature Selection - David Eklund
- Privacy-Preserving Hyperparameter Tuning for Federated Learning - Apostolos Pyrgelis

CONFIDENTIAL6G: *Advancing Robust and Privacy-Enhanced Federated Learning in 6G Networks - Shen Wang (UCD)*

14.30-15.30

Session 2: AI and Security for Predictive and Resilient Networking

RIGOUROUS: *AI/ML for Incident Detection and Mitigation in 6G Networks - Dr. Jorge Bernal*

PREDICT-6G: *Threats and Security Enablers for Predictive 6G Networks Speaker: Fotis Foukalas*

CONFIDENTIAL6G: *Enabling Decentralized Spectrum Access with Blockchain - Madhusanka Liyanage (UCD)*

15.40-16.40

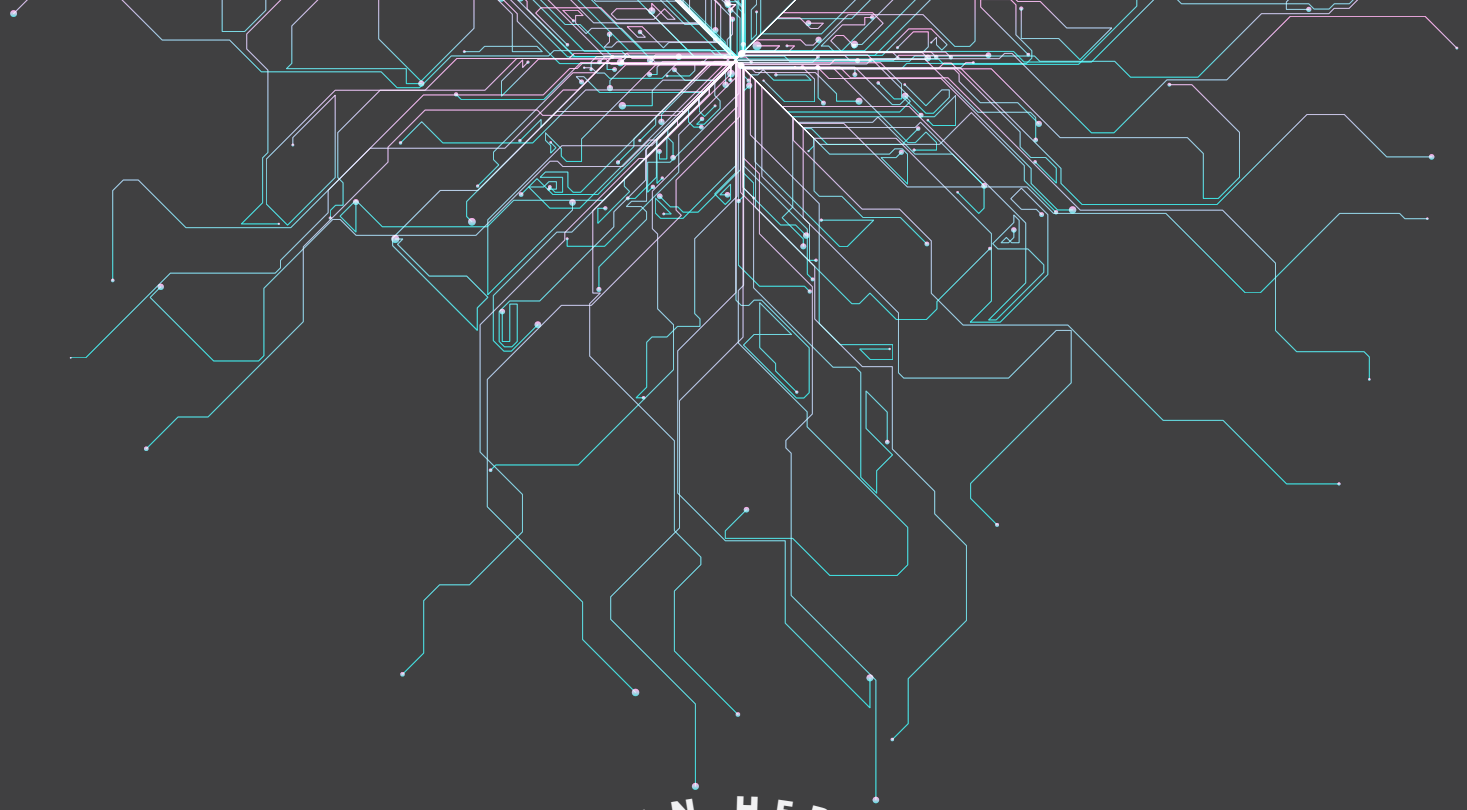
Session 3: Security and Privacy Management in Next-Generation Network Orchestration

RIGOUROUS: *DecSecOps Deployment of Security and Privacy in Multi-Segment Networks - Antonio Skarmeta*

FAITH/CUSTODES: *AI-Driven Self-Healing Edge/Cloud*

- Continuum Operations for Energy Saving in 6G Networks - Anastasios Giannopoulos, Sotirios Spantideas (FDI)

ELASTIC: *Resilient Cyber-Physical Devices with WebAssembly Sandboxing Speaker: Merlijn Sebrechts (IMEC)*



SCAN HERE • SCAN HERE • SCAN HERE • SCAN HERE • SCAN HERE •

Register now by scanning the QR code!

Co-funded by the European Union

6GSNS

UK Research and Innovation