Subscribe View online Translate to English Help

AI & SECURITY Webinar

Online Webinar, 2 April 2021

Time: 10:00 - 12:00 CET

Venue: Online

Organisers: CNR-IMATI, CNR-ISTI, CNR-IIT, CNR-ICT

Organizers

The **AI & SECURITY Webinar** focuses on improving the security of cyber-physical systems by exploiting the advantages offered by artificial intelligence and machine learning techniques.

Web site: https://sbd2020.isti.cnr.it/

The **PRIMEVAL project** aims to develop secure, AI-powered solutions for IoT networks. Focusing on privacy, resilience and protection capabilities to address the security challenges of IoT networks.

Web site: https://primeval-project.eu/

The **SAFEPOLICERS project** focuses on enhancing the security and privacy of AI-based services for law enforcement agencies (LEAs) operating across the EU and their external environments.

Web Site: https://safepolicers.eu/home.aspx

The **CYBERSPACE project** focuses on improving cybersecurity and privacy in IoT-based critical infrastructures, protecting critical services from cyber-attacks and physical attacks, and detecting cyber-attacks.

Web Site: https://cyberspace-project.eu/

The **INFRASTRUCT project** focuses on developing advanced security and privacy-enhancing solutions for smart networks, using AI and machine learning to improve threat detection and response.

Web Site: https://infrastruct.eu/

Supporting projects

The **SoBigData Project** aims to enabling and sustaining interdisciplinary ecosystems, focusing on improving transparency, accountability and ethics in data science, using advanced machine and Artificial Intelligence.

Web Site: https://www.sobigdata.eu/

The **CLOUDSOCK project** focuses on improving the security and privacy of IT systems by developing critical tools and frameworks that ensure safe and trustworthy cloud-based services.

Web Site: https://cloudsock.eu/home

The **AI-Chase project** aims to investigate, create and test key technologies to enhance the security and privacy of AI-based services/products in the cyber-physical ecosystem.

Web Site: https://www.ai-chase.eu/

Word from the Organizer

Manuel Gil Pérez
CNR-IMATI-MI

Artificial Intelligence (AI) and Cybersecurity are two technology domains that are rapidly evolving and influencing each other in several ways. Cybersecurity is a key enabler of AI technological advantage. AI-enabled cybersecurity solutions increase cross-jurisdiction threat intelligence, automate threat detection, and speed up information sharing. Cybersecurity is also a key enabler of AI adoption, providing the security and privacy-by-design mechanisms that are needed to ensure AI trustworthiness.

Welcome to the **AI & Security Webinar, where cybersecurity around AI is hosted 24/7/365 project**. This webinar will explore cybersecurity developments in artificial intelligence and machine learning, including adversarial machine learning, explainable artificial intelligence, and artificial intelligence-enabled cybersecurity solutions, alongside such challenges as secure models network management, and lack of human-designed cybersecurity solutions. We will also discuss artificial intelligence-enabled cybersecurity solutions, such as Cyber-Physical Systems, smart grids, smart transport, smart environment, smart healthcare, Fintech and Technical Internet of Things (IoT), Internet of Medical Things (IoMT), and Industrial Internet of Things (IIoT).

Speakers

Prof. Nineta Polemi
University of Piraeus, Greece
Coordinator of the PRIMEVAL project

Nineta Polemi is a cybersecurity Professor in the University of Piraeus (PhD in Cyber Security), Ex- Dept. of Informatics (MSc in Cyber Security) and Ex-Dept. of Maritime Studies (MSc in Maritime Transport Security). She is the Coordinator of the PRIMEVAL (H2020-ICT-31-2018) Cybersecurity Technologies and Capabilities - Net Secure Data Lake project, the Coordinator of the Horizon 2020 Project CYBERSPACE, the Coordinator of the Horizon 2020 Project SAFEPOLICERS, the Coordinator of the Horizon 2020 Project CONCORDIA, the Coordinator of the Horizon 2020 Project SecCRIS, the Coordinator of the Horizon 2020 Project SAFE-DEMOCRACY, the Coordinator of the Horizon 2020 Project Secure Data Exchangeable, Universal Lake (SDUL), the Coordinator of the Horizon 2020 Project Secure Data Lake (SDL).

She has over 200 publications in security (e.g. post-quantum, machine learning, blockchain, IoT security, critical infrastructures security, smart grids security, cyber-physical ecosystems cybersecurity, scientific events, etc. She has received many research grants in the area of Cybersecurity, Critical Infrastructures Protection, Smart Grids, Smart Ports, Ministry of Maritime, Fisheries, Internal Affairs Security and Cybercrime Prevention, Finance and Technical Storage in Secure Data for Cybersecurity International, EU and Greek Ministries.

Abstract

Cybersecurity and Privacy in Cyber-Physical Ecosystems, ensuring its trustworthiness and resilience is critical. This keynote will explore the interdependence between cybersecurity and privacy in cyber-physical ecosystems, the challenges they face, and the AI- highlighting the role of cryptographic mechanisms in securing AI algorithms, data, and communications, the impact of AI on cybersecurity threat actors, and cryptographic techniques for enhancing AI security and privacy.

The talk will also examine how the EU is shaping policies to foster a resilient, AI-powered cybersecurity ecosystem, emphasizing collaboration, standardization, and future governance of systems.

David Gibson
R&D Manager Institute of Sweden

David is interested in applied artificial intelligence.
He is the Coordinator of several research projects in engineering education from the Royal Institute of Technology. Recent research experience spans applied algebra, computational complexity, and machine learning. He has taught courses in these areas and in software and cyber security.

Abstract

AI-assisted cyber-ecosystem for Internet Information Sift for Efficient Learning (AIIIEL) Cyber-security is a critical concern for modern society, with the increasing complexity of cyber-attacks and the need for advanced tools and strategies to counteract them. This abstract proposes the development of an AI-assisted cyber-ecosystem for Internet Information Sift (AIIIEL) implementation of threat intelligence, with achieving cyber-security for the international student learning ecosystem.

Fotis Fountakos
Cognitec

Fotis is a technology advisor at Cognitec for AI and its technologies.

Apostolos Fyrigiotis
R&D Manager Institute of Sweden

Apostolos is a Senior Researcher at ARMI Research Institute of Sweden, and a Member of the Cybersecurity Unit. His research interests include privacy-enhancing technologies, secure multi-party computation, and cryptographic protocols. He has participated in several EU funding projects and security in policy. He received his PhD, MSc, and BSc. degrees in computer engineering and informatics from the University of Patras, Greece, and the Hellenic Open University.

Abstract

We review the contents of post-quantum cryptography (PQC) and highlight the crucial role of PQC in the future cybersecurity landscape. We discuss the main PQC and lattice-based cryptography and the NIST standardization process. We also discuss the challenges and open problems in the deployment of PQC in the real-world applications. We also discuss the impact of PQC on the security of AI-based services and applications. We also discuss the security of AI-based services against quantum computing attacks. We also discuss the security of AI-based services against quantum computing attacks. Finally, a novel framework for privacy-preserving AI utilizing lattice-based homomorphic encryption.

Zhen Wang
Assistant Research Fellow
Academy Internet of Things of Jiangsu Province, China
Senior Lecturer of Hunan Quality Technical College

Dr. Wang is a senior member of IEEE and an senior member of Chinese Transportation Systems of the society. He received an M.Eng. degree from Nanjing University of Aeronautics and Astronautics in 2008 and a Ph.D. degree in 2013. He has been involved and led several EU projects, such as H2020 IoT and 5G Testbed in Big Data Ecosystem, H2020 Cybersecurity Technologies and Capabilities - Net Secure Data Lake, Secure Data Exchangeable, Universal Lake (SDUL), and Secure Data Lake (SDL). Some key research partners of the applied research projects are Alibaba Cloud, Huawei, Nanjing Telecommunication Technology Institute, Jiangsu Provincial Transportation Research Institute, Jiangsu Provincial Communications Planning and Design Institute, Jiangsu Provincial Communications Engineering Construction Company, Jiangsu Provincial Communications Engineering Supervision Company, Jiangsu Provincial Communications Engineering Quality Supervision Company, Jiangsu Provincial Communications Engineering Quality Inspection Company, Jiangsu Provincial Communications Engineering Quality Verification Company, Jiangsu Provincial Communications Engineering Quality Testing Company, Jiangsu Provincial Communications Engineering Quality Testing Company, Jiangsu Provincial Communications Engineering Quality Testing