3rd International Conference on Emerging Trends in Cybersecurity (Hybrid)

University of Genoa, Italy

12-13 October 2026

Only Technical paper will be Published in the Proceeding

ICETCS 2026 Call for Paper

Aim of the Conference

The primary objective of the International Conference on Emerging Trends in Cybersecurity (ICETCS 2026) is to provide a global platform for researchers, academicians, industry professionals, and policymakers to converge, share insights, and explore the latest advancements and emerging trends in cyber and hardware security. This conference aims to facilitate discussions on cutting-edge research, innovative technologies, and practical solutions that address the evolving challenges posed by cyber threats in our interconnected world. By fostering interdisciplinary dialogue and knowledge exchange, the conference aims to contribute to the development of robust cyber and hardware security strategies, enhance collaboration between academia and industry, and ultimately strengthen collective resilience against cyber and hardware threats globally.

Please note: All accepted papers will be published in Lecture Notes in Electrical Engineering, which is a Scopus-indexed proceedings with Springer. Extended Paper will be invited to submit the following journals:
- IET Computers & Digital Techniques Journal.; International Journal of Information Privacy, Security and Integrity; EAI Endorsed Transactions on Internet of Things; Computers; Journal of Network and Computer Applications, Vehicular Communications; ACM Distributed Ledger Technologies

Organizing Committee

Patron:
Prof. Dr. Prashant Pillai, UoW, UK
Prof. Dr. Mohammed Atiquzzaman, UoO, USA
Prof. Mario Marchese, UoG, Italy

General Chair:
Prof. Dr. Arafatur Rahman, UoW, UK
Prof. Dr. Kim-Kwang Raymond, UoT, USA
Prof. Dr. Fabio Patrone, UoG, Italy

Executive General Chair:
Prof. Dr. Giovanni Gaggero, UoG, Italy
Dr. Shancang Li, Cardiff University, UK
Dr. Nazmul Hussain, UoN, UK

Technical Program Committee Chair:
Dr. Rashed Al Amin, UoS, Germany

Program Chair:
Prof. Dr. A. Taufiq Asyhari, MU, Australia

Publication Chair:
Prof. Dr. Zeeshan Ahmad, UoW, UK
Prof. Dr. Hai Tao, BUAS, China
Prof. Dr. Manimuthu Arunmozhi, AU, UK

Publicity Chair:
Prof. Dr. Zakirul Alam Bhuiyan, FU, USA
Prof. Dr. Ihsan Ullah, NUI, Ireland
Prof. Dr. Jasim Uddin, CMU, UK

Publicity Co-Chair:
Prof. Dr. Adeel Rafiq, UoW, UK
Prof. Dr. S M Nazmus Sadat, UU, Bangladesh
Prof. Dr. Muhammad Kamran Naeem, UN, UK

Scope of the Conference

Papers are solicited in, but not limited to, the following topics:

Cyber Security for Network Space Challenges
- Hacking & Phishing
- Supply Chain Risks
- Man-in-the-Middle Attack
- DNS Tunneling
- Malware and Ransomware
- DoS and DDoS
- Cloud and Insider Threats
- Cybersecurity Awareness
- Updating Systems and software
- Prevent Database Exposure
- Strategic Threat Intelligence
- Tactical Threat Intelligence
- Operational Threat Intelligence
- Structured Query Language Injection

Cyber Security for Mobility & Transport
- Ransomware & Scamming
- Exploitation of Devices or Networks
- Automatic License Plate Recognition
- Automatic Traffic Control Signals and System
- Digital Control System of networks in Tunnels
- Guideway Intrusion Detection System
- Autonomous Driving Assistant System Safety
- Access Control System
- Distributed Control System and Operations Zone
- Information Disclosure of Sensitive Personal and AI Data

Cyber Security for Internet of Things
- IoT Device Security
- Ensuring Cyber Resilience in IoT Agriculture Systems
- Crowdsourcing and Crowdsensing Security
- Securing Mobile Cellular Networks in IoT Landscapes
- Edge and Cloud Computing Security for IoT Infrastructure
- Next-Generation Communications and Networks Security in IoT
- Game Theory Applications for IoT Cybersecurity
- Industry 4.0 Security Challenges in IoT Implementations

Cyber Security for Connected Autonomous Vehicles
- Cyber-Physical Vehicular Health Monitoring Systems
- AI-ML-driven anomaly detection
- Automotive Ethernet and V2X networks
- Secure Over-the-Air (OTA) update mechanisms
- Digital twins for vehicle Security
- Resilient V2X communication protocols
- Cyber resilience modeling for autonomous and electric vehicles
- Integration of safety and security co-design (ISO 21434, UNECE WP.29)

Hardware Security
- Hardware Trojans and Supply Chain Trust
- Physically Unclonable Functions
- DNS Tunneling
- Hardware-Based Cryptography
- Reverse Engineering and Anti-Tampering
- Automotive and Industrial Hardware Security
- LLM for Hardware Security
- Embedded System Security & Test

Cloud Security
- LLM for Cloud Security
- State of Cloud Security
- Manual Configurations
- No Disaster Recovery Plan
- Domain Hijacking
- Inventory Management
- Bad Logging and Monitoring
- Misconfigured Networks
- Broken Access Control
- Improper Use of Default Configs
- Publicly Accessible Storage

Blockchain Security
- Theories of blockchain and distributed ledger technology
- Distributed consensus and fault tolerance mechanisms
- Decentralization, scalability, and security tradeoff
- Performance analysis and optimization
- Simulation and performance evaluation techniques
- Smart contract and chain code

Space Security
- Cyber resilience of satellite and ground-segment systems
- Secure architectures for LEO
- GEO satellite constellations
- AI for space cyber threat detection
- Zero-trust frameworks for space-ground integration
- Secure space-based IoT
- Quantum-resistant cryptography for satellite systems

Important Dates

Paper Submission Deadline: 31st July 2026
Notification of Acceptance: 31st August 2026
Final Paper Submission Deadline: 14th September 2026
Early Bird Registration Deadline: 20th September 2026
Final Registration Deadline: 4th October 2026

Details and Support

Prof. Rahman (arafatur.Rahman@wlv.ac.uk)
Prof. Gaggero (giovanni.gaggero@unige.it)
Dr. Amin (rashed.amin@uni-siegen.de)
Dr. Hussain (nhussain37@lancashire.ac.uk)

CYBER VEHICARE · Università di Genova · University of Wolverhampton · Cardiff University / Prifysgol Caerdydd · Springer