Call for Papers

Communications and Cyber Security Symposium (CCSS)

The 21st International Conference on Wireless Communications and Mobile Computing

Website: http://iwcmc.org/2025/

Submission Link: **https://edas.info/newPaper.php?c=32919**

Technically Sponsored by IEEE and IEEE UAE Section

May 12-16, 2025, Abu Dhabi, UAE

Chairs:

Yuli Yang, University of Essex, yuli.yang@essex.ac.uk

Peter Mueller, University of Basel & EPFL, peter.mueller@unibas.ch

Scope

With the advancement of mobile/computer applications and due to the proliferation of heterogeneous communication and computer networks, communications security and cyber security issues have become paramount. The development of a plethora of communication standards using different spectrum bands has refocused the research interests on mobile and wireless security. In particular, the importance of the addressed area has been dramatically highlighted by successful attacks against mobile/wireless platforms. New technologies such as cloud, fog computing, blockchain, federated learning, and physical-layer security have been developed very fast, which is calling for more creative and innovative designs for communications and cyber security.
The Communications and Cyber Security Symposium (CCSS) in IWCMC 2025 is soliciting original papers on research and development topics in the field of communications security, cyber security, and pervasive computing. Prospective authors are cordially invited to submit original technical papers.

Topics

Accepted papers will be published in the IEEE IWCMC 2025 proceedings and will be submitted to the IEEE digital library (IEEE Xplore). Authors are welcome to submit original papers (not published before and/or simultaneously to another venue) with topics that include but are not limited to:

- Application-Level Trust, Privacy and Security
- Artificial Intelligence for Security
- Attacks, Detection and Prevention
- Authentication Computer and Network Forensics
- Cryptanalysis, Lightweight Cryptographic Algorithms and Applications
- Federated Learning Based Security and Privacy
- Fog Computing Security and Privacy
- Formal Trust Models, Security Modelling and Protocol Design
- Identity Management and Key Management in Emerging Networks
- Identity Management and Key Management through Emerging Technologies
- Information Theoretical Security
- Intrusion Detection and Response in Wireless Networks
- Key Distribution and Management
- Mobile and Wireless Network Security
- Network Public Opinion Analysis and Monitoring
- Network Security Metrics and Their Performance Evaluation

- Physical Layer Security
- Privacy and Anonymity in Vehicular Networks
- Privacy and Security in Clouds and Contents Distribution Networks
- Privacy and Security in Location-based Services
- Quantum Communications for Security
- Quantum Key Distribution
- Quantum-Safe Public Key Infrastructure
- Reconfigurable Intelligent Surfaces for Security
- Security and Privacy for Artificial Intelligence
- Security and Privacy in the Internet of Things and Mesh Networks
- Security in Millimeter Wave Communications
- Security in Next-Generation Mobile Networks
- Security in Smart Grids
- Security in Virtual Machine Environments
- Security of Blockchain Technology
- Security of Cyber Physical Systems
- Security Risk Management
- Trustworthy Computing
- Web Security

Submitted papers are encouraged to address novel technical challenges or industrial and standard aspects of the key technologies related to the conference theme(s).

Important Dates

Deadlines will follow the main conference announced dates.

Note: Within this Symposium, there will be one Best Paper Award.