

THE 16TH INTERNATIONAL CONFERENCE ON COMMUNICATION AND NETWORK SECURITY



Communication and Network Security

December 19–21, 2026 Harbin, China



Chair

Paulo Batista

University of Évora, Portugal

Track 3 Data Security

Introduction: Modern digital systems generate, process and share massive volumes of heterogeneous data across networks, IoT devices and edge infrastructures, bringing severe challenges to data confidentiality, integrity and traceability. Advanced cryptographic primitives, post-quantum cryptography, homomorphic encryption and secure multi-party computation lay critical foundations for trustworthy data processing, while threats including data leakage, tampering, illegal access and system breaches keep evolving rapidly. This track welcomes high-quality original submissions addressing theories, algorithms, implementations and practical case studies of data security. Topics cover cryptography and encryption, data integrity and authenticity, network security protocols, AI-driven threat detection, IoT and edge data security, database auditing, data loss prevention, digital forensics, secure data erasure, risk assessment, as well as regulatory compliance. This track aims to bring together researchers and industry practitioners to exchange cutting-edge findings, discuss open challenges, and promote innovative solutions for securing data throughout its full lifecycle.

SUBMISSION

→Submission System: <https://www.zmeeting.org/submission/iccns2026>
→Email Submission Address: iccns_secretary@young.ac.cn
*Full Paper Template: https://iccns.org/acm_template.docx;
<https://iccns.org/LaTeX-Templates.zip>
*Abstract Template: https://iccns.org/abstract_template.docx

For more details about submission, please visit <https://iccns.org/sub.html>

CONTACT

Ms. Lesley Lei (Conference Secretary)
E-mail: iccns_secretary@young.ac.cn
Tel: +86-18010667294
WeChat: Add iconf-cs-2 and send the keyword ICCNS 2026

TOPICS

Topics of interest include, but are not limited to:

Cryptography and Encryption Techniques
Data Integrity and Authenticity
Network Security Protocols
Machine Learning for Threat Detection
Application Security
Incident Response and Management
Security in IoT Devices
Data Backup and Recovery Solutions
Regulatory Compliance
Homomorphic Encryption for Data Processing
Zero-Knowledge Proofs and Applications
Post-Quantum Cryptography and Migration
Secure Multi-Party Computation
Data Security in Edge Computing
Data Loss Prevention (DLP) Technologies
Database Security and Auditing
Secure Data Deletion and Sanitization
Digital Forensics and Data Recovery
Security Metrics and Risk Assessment

IMPORTANT DATE

Submission Deadline: October 25, 2026
Notification Deadline: November 20, 2026
Registration Deadline: December 01, 2026

Sponsored by



Organized by



Co-organized by

