The 31st International Conference on Parallel and Distributed Systems
Hefei, China December 14 - 18, 2025
Ubiquitous Computing for Global Communities

Call for Papers

Information Security

Track Co-Chairs

- **Jing Chen, Wuhan University, China,** chenjing@whu.edu.cn
- **Cong Wu, The University of Hong Kong, Hong Kong,** congwu@hku.hk
- **Yang Liu, Nanyang Technological University, Singapore,** yangliu@ntu.edu.sg

Scope and Motivation

The rapid expansion of digital technologies has led to an increased need for robust information security measures in today's interconnected world. As cyber threats evolve, information systems are facing unprecedented risks, including data breaches, ransomware attacks, privacy violation, malware infections, phishing, etc. This track aims to address these growing concerns by exploring advanced strategies, tools, and methodologies to safeguard sensitive data. The track will bring together researchers, practitioners, and industry experts to discuss the latest developments in securing digital infrastructures. By fostering collaboration and knowledge exchange, we aim to strengthen the global cybersecurity landscape. The challenges posed by emerging technologies, such as artificial intelligence, the Internet of Things (IoT), and cloud computing, will be key focal points. This track will explore both theoretical and practical aspects of securing digital assets, promoting a safer digital environment for all. The ultimate goal is to inspire innovative solutions that will help mitigate the evolving security risks of our increasingly digital world.

Topics of Interest

Our track seeks original contributions in the following topical areas, plus others that are not explicitly listed but are closely related:

- Cybersecurity and cyberattack detection
- Cryptography and encryption techniques
- Blockchain and distributed ledger technologies for security
- Artificial intelligence in cybersecurity
- Security in cloud computing
- Internet of things (IoT) security
- Privacy-preserving technologies and techniques
- Risk management and cybersecurity governance
- Cybersecurity in smart cities and critical infrastructure
- Secure software development lifecycle

- Security in 6G and next-generation network
- Malware analysis and forensics
- Digital identity management and authentication
- Network security and intrusion detection systems
- Penetration testing and ethical hacking
- Cybersecurity for autonomous systems
- Security in big data and analytics
- Security in DevOps and continuous integration
- Secure mobile computing and applications
- Advanced persistent threats (APT) detection and mitigation
- Human factors and social engineering in cybersecurity
- Security in artificial intelligence and machine learning systems
- Cybersecurity incident response and recovery
- Security and safety for GenAI

Important Dates

Paper Submission: 2025-08-15
Notification: 2025-10-01
Camera Ready and Registration: 2025-10-15

How to Submit a Paper

Each submission should include the authors' names, affiliations, an abstract, and 5–10 keywords. Papers are limited to 8 pages, including figures and references. Up to two additional pages may be included with an overlength charge. Full instructions on how to submit papers are provided on the IEEE ICPADS 2025 website: http://ieee-icpads.org.cn/CFP-research-paper.html