The International Conference on Artificial Intelligence Security and Governance (ICAISG 2025)

ICAISG 2025

Hangzhou, China
December 12-14, 2025

We are pleased to announce that **2025 International Conference on Artificial Intelligence Security and Governance (ICAISG 2025)** will be held in **Hangzhou, China** during **December 12-14, 2025.** It is sponsored by **Hangzhou Dianzi University, China**, hosted by **School of Cyberspace, Hangzhou Dianzi University, China**, assisted by **Sino-France Joint Laboratory for Digital Media Forensics of Zhejiang Province**.

The International Conference on Artificial Intelligence Security and Governance aims to establish a global dialogue platform involving multiple stakeholders, promote the creation of an inclusive and balanced international governance framework, harmonize technical standards and regulatory policies, foster positive interactions between safety research and industrial innovation, and collectively guide AI technology toward trustworthy, reliable, and controllable development. It provides attendees with an opportunity to gain in-depth understanding of current hot issues and future trends.

KEYNOTE SPEAKERS

Prof. Shui Yu (IEEE Fellow)
University of Technology Sydney, Australia
Research Interest: Cybersecurity, Network Science, Big Data, and Mathematical Modelling

Prof. Chip Hong Chang (IEEE/IET/AAIA Fellow)
Nanyang Technological University, Singapore
Research Interest: Hardware security, AI security, biometric security, trustworthy sensing and hardware accelerators for post-quantum cryptography and edge computational intelligence

INVITED SPEAKER

Prof. Dimiter Velev
University of National and World Economy, Bulgaria
Research Interest: ICT, Information Systems for Disaster Management, AI, Cybersecurity, VR, Quantum Computing

TOPICS

Track 1: Content Generation and Tampering Content Detection
- Media Manipulation Detection and Localization
- Deepfake Forgery Detection and Mitigation
- Authenticity Assessment of AI-Generated Media (Images, Videos, Audio, Text)
- Approximate Reasoning

Track 2: Traceability and Provenance Analysis of Synthetic Content
- Source Device Attribution of Synthetic Media
- Generative Model Attribution (GANs, Diffusion Models)
- Identity Provenance in AI-Generated Content

Track 3: Security of Large Language Models
- Adversarial Attacks and Defense Strategies for LLMs
- Jailbreaking Attacks and Prompt Injection Mitigation
- Security Risks in Knowledge Distillation Pipelines
- Monitoring Malicious Adaptation of Open-Source LLMs
- Detection and Mitigation of Hallucinations in LLMs
- Content Integrity Assurance in Multimodal LLMs

Track 4: Data Privacy Protection
- Privacy Leakage in Federated Learning Systems
- Privacy-Preserving Data Anonymization Techniques
- Secure Multi-Party Computation Frameworks
- Ethical Implications of Synthetic Data Generation
- Countermeasures Against AI-Driven Data Reconstruction

Track 5: AI-Driven Cybersecurity
- AI-Powered Threat Detection and Incident Response
- Automated Vulnerability Discovery and Exploitation
- AI in Offensive and Defensive Network Operations
- Collaborative Threat Intelligence Sharing via AI
- Quantum Computing Threats to AI Security Protocols

More details please click https://www.icaisg.org/cfp.html

CONFERENCE PROCEEDINGS

Accepted papers of ICAISG 2025 (after proper registration and presentation) will be collected in the conference proceedings.

SUBMISSION GUIDELINES

- Language: All submissions should be written in English
- Submission Types: Abstract submission for presentation only without publication; Full paper submission for both presentation and publication.
- Paper Length: The submitted papers should be no less than 4 pages in double column, including all figures, tables, and references. When it exceeds 5 pages, extra page will be charged at 60 USD / 400 RMB per page.
- Submit your full paper or abstract directly to Online Submission System or icaisg_contact@yeah.net.

More details please click https://www.icaisg.org/submission.html

IMPORTANT DATES

- Submission deadline: July 5, 2025
- Notification Deadline: August 5, 2025
- Registration Deadline: August 20, 2025

Sponsored by:
杭州電子科技大学
HANGZHOU DIANZI UNIVERSITY

Hosted by:
杭州電子科技大学
网络空间安全学院
School of Cyberspace

Assisted by:
浙江-法国数字媒体取证联合实验室
Sino-France Joint Laboratory for Digital Media Forensics of Zhejiang Province

Patrons:
南京信息工程大学
Nanjing University of Information Science & Technology
江蘇海洋大學
JIANGSU OCEAN UNIVERSITY

Ms. Yolanda Dong   Emali: icaisg_contact@yeah.net   Tel:+86-18080013977   Website: https://www.icaisg.org