



Hangzhou, China  
November 20-22, 2026

# 2026 The 2nd International Conference on Artificial Intelligence Security and Governance

Submission Deadline: **June 15, 2026**

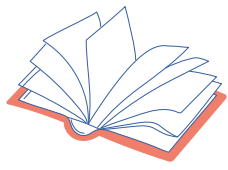
## ABOUT ICAISG



We are pleased to announce that 2026 The 2nd International Conference on Artificial Intelligence Security and Governance (ICAISG 2026) will be held in **Hangzhou, China** during **November 20-22, 2026**. 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, China.

It 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.

## Conference Proceedings



Submitted papers will be peer reviewed by program committees and technical committee, and accepted papers will be published into conference proceedings.

## Conference Program

**Day 1 - Friday - November 20, 2026**  
10:00-17:00 | Registration & Materials Collection

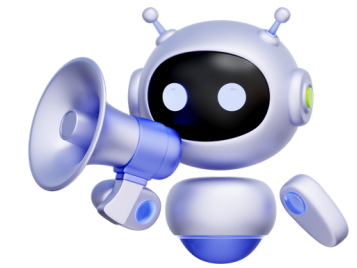
**Day 2 - Saturday - November 21, 2026**  
09:00 - 09:05 | Opening Remark  
09:05 - 11:50 | Keynote Speeches  
12:00 - 13:30 | Lunch  
13:30 - 18:00 | Parallel Sessions  
18:00 - 20:30 | Dinner Banquet and Award Ceremony

**Day 3 - Sunday - November 22, 2026**  
08:30 - 12:00 | Invited Speeches & Parallel Sessions  
13:30 - 18:00 | City Tour in Hangzhou

## Conference Awards

- Young Researchers Awards
- Best Reviewer Award
- Best Student Paper Award
- Best Paper Award
- Best Oral Presentation Award

## 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

### Track 4: Data Privacy Protection

- Privacy Leakage in Federated Learning Systems
- Privacy-Preserving Data Anonymization Techniques
- Secure Multi-Party Computation Frameworks

### Track 5: AI-Driven Cybersecurity

- AI-Powered Threat Detection and Incident Response
- Automated Vulnerability Discovery and Exploitation
- AI in Offensive and Defensive Network Operations

### Track 6: Automated Adversarial Testing and Validation

- Generation and Application of Adversarial Examples
- AI-Based Attack Simulation and Penetration Testing

For more topics, please click [HERE](#).

## Submission Guidelines

- ◇ [Template Download](#)
- ◇ English is the official language. Paper should be prepared in English.
- ◇ Abstract submission is for presentation only without publication.
- ◇ Full paper submission is for both presentation and publication. (No less than 5 pages)
- ◇ Submission Methods:
  - By online submission system: <http://www.easychair.org/conferences/?conf=icaisg2026>
  - Or Submit to [icaisg\\_contact@yeah.net](mailto:icaisg_contact@yeah.net) as attachment

Co-sponsored by:



Hosted by:



Assisted by:



Patrons:



Ms. Yolanda Dong

Email: [icaisg\\_contact@yeah.net](mailto:icaisg_contact@yeah.net)

Tel.: +86-18080013977

9:30-18:00, Monday to Friday (GMT+8 Time Zone)



<https://www.icaisg.org/index.html>