The International Workshop on Security, Privacy, and Trust in Artificial Intelligence (SPTAI 2024)

Artificial Intelligence (AI) has been widely used in all areas of human life, providing people with convenient, efficient and intelligent services and experiences, greatly improving the quality of life and promoting social innovation and change. However, alongside the immense potential for social and economic benefits, AI also introduces substantial privacy, data assurance, and security concerns. Therefore, safeguarding the security, privacy and reliability of AI is an important prerequisite for realizing its maximum value and effectiveness. This workshop focuses on the security, reliability and privacy protection issues brought by AI and big models, and discusses how to ensure the safety and reliability of AI technologies for wide applications.

Topics of interest include, but are not limited to:

- Adversarial Machine Learning Techniques
- Federated Learning Security and Privacy
- Privacy-Preserving Data Mining
- Trustworthy AI and Explainability
- Secure Machine Learning Infrastructure
- Robustness in Machine Learning
- Secure Data Sharing and Collaboration
- Anomaly Detection and Prevention in AI Systems
- Convergence of Artificial Intelligence and quantum computing
- Security in Cross-modal Learning and Integration
- Collaborative Security and Privacy in Multi-Intelligent Systems
- A Study of Fairness and Social Ethics in Artificial Intelligence
- Security in Machine Unlearning
- Machine Learning for Security in Smart Cities

Important Dates

- Paper submission deadline: before **September 1st, 2024**
- Author notification: **October 15th, 2024**
- Final manuscript due: **November 10th, 2024**

Submission Instructions

Papers submitted to IEEE SPTAI 2024 should be written in English conforming to the IEEE Conference Proceedings Format (8.5" x 11", Two-Column). The paper should be submitted through the EDAS (https://edas.info/newPaper.php?c=32834). The length of the papers should not exceed 6 pages + 2 pages for over length charges.

Accepted and presented papers will be submitted for possible inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. If accepted, at least one of the authors must attend the workshop to present the work. Accepted papers without presentations will be removed from the digital libraries of IEEE CS after the conference.

Program Chair

Yinghui Zhang, Xi'an University of Posts and Telecommunications, China

Program Committee

Yangguang Tian, University of Surrey, UK
Guowen Xu, University of Electronic Science and Technology of China
Wei Liu, Xi'an University of Posts and Telecommunications, China
Axin Wu, State Key Laboratory of Cryptology, China
Muhammad Baqer Mollah, University of Massachusetts Dartmouth MA, USA

Contact

Please email inquiries concerning the workshop to: weiliuxupt@163.com