LM-Driven TSP 2025

The International Workshop on Large Model-Driven Trust, Security and Privacy in Distributed Computing Systems (LM-Driven TSP in DCS)

In conjunction with IEEE TrustCom 2025

14-17 November，2025, Guiyang, China

Call for paper

The rapid advancement of distributed computing systems and the widespread deployment of large-scale models, such as foundation models and generative AI, have introduced new dimensions and complexities in ensuring trust, security, and privacy. As large models become integral components in intelligent systems, there is a pressing need to address the novel threats, vulnerabilities, and ethical concerns they bring. In response to this emerging landscape, the International Workshop on Large Model-Driven Trust, Security and Privacy in Distributed Computing Systems (LM-TSP 2025) will be held in conjunction with the 24th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2025) in November 2025, Guiyang,Guizhou , China.

Topics of interest include, but are not limited to:

1. Blockchain-based secure communication for large models
2. Trust management with large models in distributed systems
3. Security frameworks for deploying foundation models
4. Privacy-preserving training and inference with large models
5. Adversarial attacks and defenses in large model systems
6. Secure federated and decentralized large model learning
7. Data integrity and confidentiality in AI pipelines
8. Robustness of large models in critical infrastructures
9. Authentication and access control using large models
10. Detection of hallucination and misuse in AI agents
11. Auditing and explainability of large model decisions
12. Ethics and governance in large model-based security

Important Dates:

Paper submission deadline: before 1 August, 2025
Author notification: 1 October, 2025
Final manuscript due: 15 October, 2025
Registration Due: 21 0ctober, 2025

Submission Instructions

Papers submitted to LM-Driven TSP in DCS 2025 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/N34130). The length of the papers should not exceed 6 pages + 2 pages for over length charges. Accepted and presented papers will be included into the IEEE Conference Proceedings published by IEEE CS CPS and submitted to IEEE Xplore. Authors of accepted papers, or at least one of them, are requested to register and present their work at the conference, otherwise their papers will be removed from the digital libraries of IEEE CS after the conference. Distinguished papers presented at the conference, after further revision, will be recommended to special issues of reputable SCI/EI-indexed journals. Submitting a paper to the workshop means that, if the paper is accepted, at least one author should attend the Symposium and present the paper.

Chairs

Yongxin Tong，Beihang University, China
Yifan Sun，Renmin University of China, China
Qinnan Zhang，Beihang University, China
Wang Gang, Northeastern University, China
Chen Yao，National University of Singapore, Singapore
Misha Xu，University of the Arts London，United Kingdom
Qiu Wangjie，Beihang University, China
Qing Xia，Institute of Software, Chinese Academy of Sciences, China
Sheng Gao, Central University of Finance and Economics, China
Wu Tong，University of Science and Technology Beijing，China
Wanting Yang，Singapore University of Technology and Design, Singapore
Xiangyun Tang, Minzu University of China, China
Yuan Yanli, Beijing Institute of Technology, China
Zhang Hainan，Beihang University, China
Zhang Yuntao，Beijing University of Posts and Telecommunications，China

Contact

Please email inquiries concerning the workshop to: zhangqn@buaa.edu.cn