The International Workshop on **Communication-efficient Edge Intelligence Networks with Secure and Privacy-preserving Distributed Generative AI (EIN-GAI)**

To be held in conjunction with The 24th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (Trustcom2025: https://ieee-aiplus- 2025.org/trustcom.html), 14-17 November, 2025, Guiyang China.

Call for paper

Generative artificial intelligence (GAI) has emerged as a prominent AI paradigm that fundamentally depends on extensive training datasets to achieve state-of-the-art performance. However, current training datasets are primarily sourced from the online public domain, whose data supplies are being rapidly exhausted and approaching depleted. To address this issue, distributed AI, such as federated learning (FL) and mixture of experts (MoE), offers a promising alternative by enabling collaborative model training across decentralized private data sources. While these distributed paradigms address data scarcity concerns, they inevitably introduce significant communication, privacy, and security vulnerabilities such as data reconstruction, membership inference, backdoor attacks, and poisoning attacks. In addition to these classic risks, specific vulnerabilities in GAI, including Jailbreak, Personally Identifiable Information (PII) detection, and Hallucination, exacerbate new threats in these distributed paradigms. In this context, the development of defensive strategies against these threats is both critically urgent and technically non-trivial.

This workshop brings together scholars and professionals to tackle evolving communication-efficiency, security, and privacy challenges in distributed AI. Our goal is to identify cutting-edge topics, promote interdisciplinary collaboration, and stimulate research towards communication-efficient, secure, and privacy-preserving edge intelligence networks with GAI. We warmly invite researchers and experts to contribute to advancing this field by submitting their latest work.

Topics of interest include, but are not limited to:

1. Dynamic resource optimization for distributed GAI

2. Privacy-preserving techniques for distributed GAI

3. Adversarial attacks and defenses of distributed GAI

4. Communication-efficient techniques for edge GAI

5. Robust aggregation mechanisms for distributed GAI

6. Decentralized trust management for distributed GAI

7. Trustworthy and efficient MoE/FL based GAI frameworks

8. Communication-efficientprivacy-preserving, and security-enhanced end-edge-cloud based GAI

9. Trustworthy and dynamic data management for edge GAI

Important Dates

- **Paper submission deadline:** 1 August, 2025
- **Author notification:** 5 October, 2025
- **Final manuscript due:** 20 October, 2025
- **Registration due: in accordance with TrustCom 2025**

Submission Instructions

All papers need to be submitted electronically through the conference submission website https://edas.info/N34128 with PDF format. The length of the papers should not exceed 6 pages + 2 pages for over length charges. Manuscript Templates for Conference Proceedings can be found at: https://www.ieee.org/conferences_events/conferences/publishing/templates.html. Once accepted, at least one of the authors of any accepted paper is requested to register the paper at the conference.

Workshop Co-Chairs

Long Shi, Nanjing University of Science and Technology, China (longshi@njust.edu.cn)
Kang Wei, Southeast University, China (kang.wei@seu.edu.cn)
Taotao Wang, Shenzhen University, China (ylshao@hku.hk)
Jiaheng Wang, Southeast University, China (jhwang@seu.edu.cn)
Tao Huang, James Cook University, Australia (Tao.huang1@jcu.edu.au)
Ming Ding, DATA61, CSIRO, Australia (Ming.Ding@data61.csiro.au)
Yulin Shao, The University of Hong Kong, Hong Kong SAR, China (ylshao@hku.hk)
Zhou Su, Xi’an Jiaotong University, China (zhousu@ieee.org)