2027 ACM International Conference on Trustworthy and Responsible AI and Computing Systems (TRUST 2027)
March 7-9, 2027 · Washington DC
https://eigtrust.acm.org/trust2027/

Call for Papers

EA Track 7: Trustworthy AI for Integrated Communications and Computing (TAI-ICC)

Track Chairs:

- Weiwei Jiang, Beijing University of Posts and Telecommunications (jww@bupt.edu.cn)
- Momina Shaheen, *University of Roehampton, United Kingdom*. (Momina.Shaheen@roehampton.ac.uk)
- Umar M. Khokhar, Georgia Gwinnett College, Georgia, Unites States (ukhokhar@ggc.edu)

Description

Future societal infrastructures rely heavily on the seamless integration of network communications and computing resources, entirely optimized by AI. However, the black-box nature of AI, coupled with unique hardware limitations and dynamic network topologies, poses massive trust and security challenges. This Emerging Area Track invites researchers from academia and industry to submit high-quality papers defining the future of secure, private, accountable, and resilient AI deployments in integrated communication and computing architectures. **Track Topics**

- **Privacy-Preserving AI in Networking:** Federated learning, split learning, and differential privacy tailored for distributed edge computing and wireless nodes.
- **Adversarial Robustness at the Edge:** Defense against adversarial attacks, model inversion, and data poisoning targeting communication-focused AI models.
- **Explainable AI (XAI) for Network Operations:** Interpretable AI models for automated network configuration, fault diagnosis, and Zero-Touch Network Management (ZSM).
- **Safe and Resilient Reinforcement Learning:** Safe RL and Deep RL frameworks for dynamic spectrum access, beamforming, and ultra-reliable low-latency communications (URLLC).
- **Trust Modeling and Certification:** Quantitative metrics, benchmarks, and continuous auditing frameworks to evaluate the "trust score" of multi-vendor AI agents in network slices.
- **Hardware-Assisted Trust for Network AI:** Leveraging Trusted Execution Environments (TEEs) and cryptographic accelerators to secure AI execution at the network edge.

Paper Submission and Publication

Manuscripts should be in PDF format, using the 2-column ACM sigconf template, see https://www.acm.org/publications/proceedings-template. Full papers cannot exceed 9 pages, including an appendix, plus unlimited pages for the GenAI Usage Disclosure section and references. Reviewing will be double-blind. Submissions must not reveal the authors' names and their affiliations and avoid obvious self-references. Accepted papers will be in the ACM Digital Library and indexed in EI Compendex and Scopus.
Submission Link: https://cmt3.research.microsoft.com/TRUST2027/Submission/Index

Important Dates

Abstract Registration: October 24, 2026
Paper Submission: October 31, 2026
Notification of Acceptance: December 31, 2026
Final Manuscript (Camera Ready): February 28, 2027