

# 2nd IEEE Conference on Secure and Trustworthy CyberInfrastructure for IoT and Microelectronics

March 24–26, 2026  
Houston, Texas

## CALL FOR PAPERS

### IMPORTANT DATES

**JANUARY 10, 2024**  
**Paper Submission**  
**Deadline**

**JANUARY 30, 2025**  
**Acceptance**  
**Notification**

**FEBRUARY 15, 2025**  
**Registration**  
**Deadline**

**FEBRUARY 25, 2025**  
**Camera-ready**  
**Submission Deadline**

#### GENERAL CHAIRS

- Dr. Fathi Amsaad, Wright State University, USA
- Dr. Ahmed Abdelgawad, Central Michigan University, USA
- Dr. Alaa Ali Hameed, Istinye University, Turkey

#### PROGRAM CHAIRS

- Dr. Tara Salman, Texas Tech University, USA
- Dr. Akshay (AK)Raghavendra Kulkarni, Prairie View A&M University, USA
- Dr. Akhtar Jamil, National University of Computer and Emerging Sciences, Pakistan

#### SCIENTIFIC COMMITTEE

- Dr. Abdul Razaque, Visiting Assistant Professor, Ohio Northern University
- Dr. Ahmad Javaid, Associate Chair & Undergrad Program Director, University of Toledo
- Dr. Ahmed Abdelgawad, Professor, Central Michigan University, USA
- Dr. Ahmed Aleroud, Augusta University
- Dr. Ahmed Ammar, Assistant Professor, Ohio Northern University
- 

#### Welcome to SATC-2025

We are pleased to invite you to the 2nd IEEE Conference on Secure and Trustworthy CyberInfrastructure for IoT and Microelectronics (SaTC 2026), scheduled to take place from March 24–26, 2026. The second edition of SaTC is organized at Sheraton North Houston at George Bush Intercontinental, Houston Texas, USA. It provides a unique platform to discuss the recent advancements in security and assurance challenges in IoT/Edge computing, communication systems, and embedded computing. We plan to submit the conference proceedings for publication to IEEE Xplore.

#### Topics of Interest

Topics of interest include but not limited to the following:

- AI for Smart City Infrastructure Management
- Blockchain for IoT Device Authentication
- Autonomous Vehicles and AI-powered Navigation
- Secure Embedded AI Systems
- AI-driven Threat Detection for IoT
- Quantum-Safe Cryptography for IoT
- Zero Trust Architecture in IoT Networks
- Trusted Computing for IoT Applications
- IoT Privacy Enhancing Technologies
- Generative AI for Predictive Modeling and other applications
- Edge Computing Security Techniques
- AI-based Fraud Detection Systems
- Heterogeneous System Security Integration
- Deep Learning for IoT Anomaly Detection
- Smart Contract Security in IoT
- 5G and IoT Security
- Advanced IoT Security Frameworks
- Secure IoT Communication Protocols
- AI in Healthcare for Diagnosis and Treatment
- IoT-Based Distributed Systems Security
- Assured Additive Manufacturing for IoT Hardware
- Trustworthy Machine Learning for IoT
- Digital Twin Security for IoT Systems

#### FINANCIAL AND TECHNICAL SPONSORS

