Security-by-Design

Scope

Artificial Intelligence (AI) has been the focus of research in recent years. Internet of Things (IoT) devices powered by AI are proven to perform better than general purpose. Integrating AI in the edge devices and Internet of Things (IoT) devices improved the performance of resource constrained devices. But this has also given rise to a new set of challenges in privacy and security. Many vulnerabilities were discovered as a result. One of the potential solutions to improve security is through Hardware Assisted Security (HAS). Security integrated in the design of the hardware modules can significantly help with the robustness and performance of the devices. This special session acts as a platform to invite cutting edge research and solutions in the areas of security by design (SbD), HAS, AI for HAS, IoT, and Blockchain to address these problems. The topics for this special session of interests include, but are not limited to the following:

- Security by Design
- Security in IoT
- Smart Healthcare Security
- Cyber Physical Systems
- Hardware Assisted Security
- Blockchain Solutions
- Hardware Trojans
- Internet of Vehicles
- Physical Unclonable Functions
- Low Energy Design for Hardware Assisted Security
- Trojan Detection in IoT
- Improving Reliability of Circuits
- Security and privacy-preserving AI systems
- AI for threat detection and prevention

Tentative Presentations during the session

- Venkata P. Yanambaka, Jian Zhang, and Kahlan Edwards "PUF-ML: Machine Learning - Based Physical Unclonable Functions for Cost Effective Integration In Smart Healthcare".
- V. K. V. V. Bathalapalli, Venkata P. Yanambaka, Saraju P. Mohanty, and Elias Kougianos, "A Hardware-Assisted Approach for Deepfake Mitigation Using Puf-Based Facial Feature Attestation".
- Burra Subbarao, Chella Amala, Banee Bandana Das, Saswat Kumar Ram, and Saraju P. Mohanty, "Trojan Resilient Design for Securing SoCs from Adversaries".
- Chella Amala, Burra Subbarao, Tamoghna Ojha, Banee Bandana Das, Saswat Kumar Ram, and Saraju P Mohanty, "An Off-chip Based PUF design for FPGA Based IoT systems".
- Samir Ahmed, Shakil Mahmud, and Robert Karam, "A Modular Security Evaluation Platform for Physiological Closed-Loop Control Systems".
- Soumyashree Mangaraj, Jaganath P. Mohanty, Samit Ari, Ayaskanta Swain, and Kamalakanta Mahapatra, "PACAC: PYNQ Accelerated Cardiac Arrythmia Classifier with secure transmission – A Deep Learning based Approach".
- Pawan Oraon, Soumyashree Mangaraj, Ayas Kanta Swain, and Kamalakanta Mahapatra, "Hardware Accelerated Handwritten Digit Recognition with HLS Platform".