

# Special Track Proposal Format

## 2nd International Conference on Advances in Artificial Intelligence for Society (ICA2S-2026)

Organized by **Indian Institute of Information Technology Bhopal, India**  
In collaboration with **University of Vizja, Warsaw, Poland**

### 1. Title of the Special Track

*AI for Hardware Security, Trusted Computing, and Quantum-Resilient Systems*

### 2. Track Description

The proliferation of Artificial Intelligence (AI) across cloud, edge, and embedded platforms has significantly expanded the attack surface of modern computing systems, making hardware-level trust and security a critical concern. As AI workloads increasingly rely on specialized hardware accelerators, heterogeneous architectures, and distributed infrastructures, vulnerabilities such as hardware Trojans, counterfeiting, side-channel attacks, and supply-chain threats pose serious risks to system integrity and confidentiality. At the same time, the emergence of large-scale quantum computing threatens the security of widely deployed public-key cryptographic schemes, creating an urgent need for quantum-resilient security mechanisms.

This special track focuses on advancing AI-driven approaches for hardware security, trusted computing, and quantum-resilient system design. It aims to explore how machine learning and intelligent analytics can be leveraged for automated vulnerability detection, anomaly detection in hardware behavior, secure system verification, and adaptive defense mechanisms. The track also encourages research on trusted execution environments, confidential computing, and hardware roots of trust for AI-enabled infrastructures. In addition, contributions addressing post-quantum cryptography, secure hardware implementations of quantum-safe algorithms, and AI-assisted cryptanalysis are highly encouraged. The goal is to foster interdisciplinary research that integrates AI techniques with hardware and cryptographic security to build trustworthy and resilient computing systems for the emerging post-quantum and AI-driven era.

### 4. Topics of Interest

Topics include but are not limited to:

#### 1. *Topic 1: Artificial Intelligence for Hardware Security*

- *Machine Learning for Hardware Trojan Detection, Localization, and Classification*
- *AI-assisted Secure Hardware Design Validation and Formal Verification*
- *AI-based Behavioral Modeling for Hardware Anomaly Monitoring*
- *Intelligent Threat Detection and Attack Attribution in Hardware Platforms*
- *Learning-based Detection of Counterfeit and Tampered Integrated Circuits (ICs)*

**2nd International Conference on Advances in Artificial Intelligence for Society (ICA2S-2026)**

## 2. *Topic 2: Secure and Trusted Hardware Systems*

- *Trusted Execution Environments (TEE) and Hardware Root of Trust*
- *Secure Processor Architectures and Confidential Computing*
- *Secure Semiconductor Supply Chain and Hardware Provenance Verification*
- *Security Architectures for AI Accelerators and Edge Computing Devices*

## 3. *Topic 3: AI for Cybersecurity and Privacy*

- *AI-enabled Intrusion Detection and Threat Intelligence Systems*
- *Privacy-Preserving Machine Learning*
- *Adversarial Machine Learning and Robust AI System Design*
- *AI-based Risk Analysis and Security Analytics*

## 4. *Topic 4: AI for IoT and Edge Security*

- *Trustworthy AI Frameworks for IoT and Edge Computing*
- *Secure Edge Intelligence and Distributed AI Systems*
- *AI for Secure Device-to-Device and Machine-to-Machine Communication*
- *Intelligent Security Monitoring for Large-scale IoT Networks*
- *Resilient Edge Architectures for Latency-Critical Applications*

## 5. *Topic 5: Quantum-Resilient Security and Intelligent Cryptography*

- *Post-Quantum Cryptographic Algorithms and Protocols*
- *Secure Hardware Implementations of Quantum-safe Cryptography*
- *AI-assisted Cryptanalysis and Quantum Threat Modeling*
- *Quantum Machine Learning for Security Applications*
- *Hybrid Classical–Quantum Secure Computing Architectures*

## 6. *Topic 6: Emerging Intelligent Secure Systems*

- *Neuromorphic Computing and Secure Hardware Accelerators*
- *AI for Secure Smart Infrastructure and Smart Cities*
- *Trustworthy and Explainable AI for Security-critical Applications*
- *Next-generation Secure Computing Architectures for AI Workloads*

## **5. Special Track Organizers**

**Name: Dr. Rahul Chaurasia**

Designation: Asst. Professor

Department: Computer Science and Engineering

Institution: Indian Institute of Information Technology Bhopal

Country: India

Email: rahulchaurasia@iiitbhopal.ac.in

ORCID (optional): <https://orcid.org/0000-0001-5763-8601>

**2nd International Conference on Advances in Artificial Intelligence for Society (ICA2S-2026)**

## **6. Contact Information**

Primary Contact Person: Dr. Rahul Chaurasia, Asst. Prof. IIIT Bhopal

Email: rahulchaurasia@iiitbhopal.ac.in

Phone (optional): +91-9977487509