National Institute of Technology Rourkela

Registration Seminar

| | |
|---|---|
| Seminar Title | : Secure RISC-V SoC: Vulnerabilities Detection and Mitigation |
| Speaker | : Bharat Patidar ( Rollno : 523ec6010) |
| Supervisor | : Kamalakanta Mahapatra |
| Venue | : EC Seminar Hall |
| Date and Time | : 25 Aug 2025 (5.00 P. M.) |

Abstract : The rapid adoption of open-source RISC-V processors in edge IoT systems offers flexibility and cost benefits but exposes them to significant hardware security threats, particularly Hardware Trojans (HTs). These malicious modifications, introduced at various stages of the design and manufacturing process, can cause data leakage, system disruption, and critical infrastructure compromise. This research focuses on foundational work in developing a secure RISC-V System-on-Chip (SoC) by detecting and mitigating HTs with minimal performance and resource overhead. A comprehensive literature review reveals limitations in existing methods, such as coarse-grained protections, high complexity, and limited runtime coverage. The proposed approach combines lightweight runtime detection, formal verification, and error correction code (ECC) mechanisms to identify and neutralize HTs, including software-exploitable and silent data corruption attacks. Experimental work involved FPGA-based implementations of CDAC AT1051 and PicoRV32 SoCs, insertion of trigger-based and parametric Trojans, and integration of ECC modules for real-time integrity monitoring. Results demonstrate successful HT effects in simulation on pico-rv 32, forming a robust foundation for a hardware root of trust in RISC-V SoCs. Future work targets development of efficient light weight HT detection approaches, expanding detection coverage, and refining countermeasures to enhance resilience against emerging hardware threats.

**Keywords**&mdash ***RISC-V, Hardware Trojan, ISA (Instruction Set Architecture), Hardware Security, Execution, Pipelining, Address, Memory.***