ARTIFICIAL INTELLIGENCE

PNRR/SERICS - Enhancing Hardware Security in RISC-V Architecture through Artificial Intelligence

Funded By	MINISTERO DELL'UNIVERSITA' E DELLA RICERCA [P.iva/CF:97429780584] Politecnico di TORINO [P.iva/CF:00518460019] Dipartimento di Automatica Informatica [P.iva/CF:00518460019]
Supervisor	DI CARLO STEFANO - stefano.dicarlo@polito.it
Contact	SAVINO ALESSANDRO - alessandro.savino@polito.it DI CARLO STEFANO - stefano.dicarlo@polito.it
Context of the research activity	This Ph.D. proposal aims to explore the integration of artificial intelligence (AI) techniques into RISC-V computer architecture to enhance hardware security. By leveraging the flexibility and openness of the RISC-V instruction set architecture (ISA), this research seeks to develop novel AI-based solutions that can detect and mitigate various hardware security vulnerabilities, including side-channel attacks, hardware Trojans, and fault injections. "Progetto finanziato nell'ambito del PNRR - M4C2, Investimento 1.3 - Avviso n. 341 del 15/03/2022 - PE0000014 Security and Rights in the CyberSpace (SERICS) - CUP E13C22001850001"
	The increasing complexity and interconnectedness of modern computer systems have raised significant concerns about their vulnerability to security threats. As these systems become more intricate, the potential attack surfaces expand, making them more susceptible to a variety of hardware security issues. Addressing these challenges requires innovative approaches that can effectively identify and mitigate potential vulnerabilities. This Ph.D. proposal aims to explore the integration of artificial intelligence (AI) techniques into RISC-V computer architecture to enhance hardware security. The RISC-V instruction set architecture (ISA), known for its flexibility and openness, provides an ideal platform for developing and implementing advanced security solutions. This research will leverage these attributes to create novel AI-based methods for detecting and mitigating hardware security vulnerabilities. The proposed study will focus on several key areas of hardware security, including side-channel attacks, hardware Trojans, and fault injections. Side-channel attacks exploit unintended information leakage from hardware

Objectives	implementations to extract sensitive data. Hardware Trojans, and malicious alterations to hardware components, can compromise the integrity and functionality of a system. Fault injections, and deliberate manipulations of a system's operational environment, can cause incorrect computations and system failures. To address these threats, the research will develop AI-driven techniques capable of identifying anomalies and potential security breaches in real-time. Machine learning algorithms, particularly those designed for pattern recognition and anomaly detection, will be employed to analyze hardware behavior and detect deviations indicative of security threats. Deep learning models may be used to enhance the accuracy and efficiency of these detections by learning complex patterns associated with various types of attacks. Moreover, this research will investigate the implementation of these AI techniques directly within the RISC-V architecture. By integrating AI at the hardware level, the system can perform security monitoring and threat mitigation with minimal performance overhead. This integration will involve designing custom AI accelerators and security modules that can operate seamlessly within the RISC-V framework. The expected outcomes of this research include the development of robust AI-based hardware security solutions that can be readily adapted to different implementations of the RISC-V architecture. These solutions will aim to provide comprehensive protection against a wide range of hardware security threats, thereby enhancing the overall security posture of modern computer systems. In summary, this Ph.D. proposal seeks to harness the power of AI to bolster the security of RISC-V computer systems. By developing advanced AI-based techniques for detecting and mitigating hardware vulnerabilities, this research aims to address the pressing security challenges posed by the increasing complexity of modern computer architectures.

Skills and competencies for the development of the activity	Candidate must possess a combination of technical skills, knowledge, and research capabilities: - Strong understanding of computer architecture, particularly the RISC-V ISA - Proficiency in hardware security concepts - Solid knowledge of AI and machine learning techniques - Proficiency in HDL such as Verilog, VHDL, or SystemVerilog, and experience with C/C++, Rust and Python is required. - Ability to read and understand the literature. - Effective English communication skills, both written and verbal