ARTIFICIAL INTELLIGENCE

PNRR/SERICS - Improving the security of embedded systems running AI applications

Funded By	MINISTERO DELL'UNIVERSITA' E DELLA RICERCA [P.iva/CF:97429780584] Politecnico di TORINO [P.iva/CF:00518460019]
Supervisor	SANCHEZ SANCHEZ EDGAR ERNESTO - ernesto.sanchez@polito.it
Contact	SAVINO ALESSANDRO - alessandro.savino@polito.it SANCHEZ SANCHEZ EDGAR ERNESTO - ernesto.sanchez@polito.it DI CARLO STEFANO - stefano.dicarlo@polito.it
Context of the research activity	The main objective of this proposal consists on developing a strategy able to protect from security threats low cost embedded systems executing applications based on artificial intelligence algorithms with emphasis on RISC-V based systems. In this context, the solution will secure the different layers belonging to the full stack, including the architecture of the processor and the whole SoC, the available memories, the peripherals, the operative system and the applications running on it. PNRR M4C2, Investimento 1.3 - Avviso n. 341 del 15/03/2022 - PE0000014 Security and Rights in the CyberSpace (SERICS) - CUP E13C22001850001
Objectives	Computer systems security is one of the most important properties to be guaranteed in today's applications, and in particular, the system security becomes much more critical when the proposed solution involves AI-based algorithms, since in some cases, these algorithms may produce a wrong answer due to an initial system accuracy lower than 100%. Today, almost any computer-based system, from high-end computers to very simple embedded systems are susceptible to suffer security attacks, where the attacker tries for example, to steal private keys, valuable information or getting the control of the system; in other cases, the attacker may create a denial of service impairing the producer goodwill. Therefore, it is important to develop new techniques able to prevent software as well as hardware-based attacks in embedded systems running AI-based applications. The main goal of this proposal is to develop a methodology to protect an embedded system specially devised for running AI-based applications. The framework of the proposed strategy must cover security aspects that start at the system architectural level, going through the middleware, the operating

	system and covering also the AI-based application security aspects and the interaction of this applications with all the others needed in the system.

Skills and competencies for the development of the activity	The candidate must count with a good knowledge and familiarity with programming languages such as C and Python. In addition, she or he is required to have also good experience with the use of hardware description languages such as SystemVerilog, as well as a good knowledge on hardware simulation, validation and verification. Even if not explicitly required, the candidate may count with some experience with artificial intelligence applications based on Neural Networks.