World Academy of Science, Engineering and Technology
International Journal of Cognitive and Language Sciences
Vol:18, No:05, 2024

Lightweight Hardware Firewall for Embedded System Based on Bus Transactions

Authors : Ziyuan Wu, Yulong Jia, Xiang Zhang, Wanting Zhou, Lei Li

Abstract : The Internet of Things (IoT) is a rapidly evolving field involving a large number of interconnected embedded devices. In the design of embedded System-on-Chip (SoC), the key issues are power consumption, performance, and security. However, the easy-to-implement software and untrustworthy third-party IP cores may threaten the safety of hardware assets. Considering that illegal access and malicious attacks against SoC resources pass through the bus that integrates IPs, we propose a Lightweight Hardware Firewall (LHF) to protect SoC, which monitors and disallows the offending bus transactions based on physical addresses. Furthermore, under the LHF architecture, this paper refines two types of firewalls: Destination Hardware Firewall (DHF) and Source Hardware Firewall (SHF). The former is oriented to fine-grained detection and configuration, whose core technology is based on the method of dynamic grading units. In addition, we design the SHF based on static entries to achieve lightweight. Finally, we evaluate the hardware consumption of the proposed method by both Field-Programmable Gate Array (FPGA) and IC. Compared with the exciting efforts, LHF introduces a bus latency of zero clock cycles for every read or write transaction implemented on Xilinx Kintex-7 FPGAs. Meanwhile, the DC synthesis results based on TSMC 90nm show that the area is reduced by about 25% compared with the previous method.

Keywords : IoT, security, SoC, bus architecture, lightweight hardware firewall, FPGA
Conference Title : ICSLP 2024 : International Conference on Speech and Language Processing
Conference Location : New York, United States
Conference Dates : May 23-24, 2024