

Enhancing Security in IoT Devices through Hardware Cryptography

Quinn Perez

PhD

University of São Paulo

Av. Prof. Luciano Gualberto, 380 - Butantã, São Paulo - SP, 05508-010, Brazil

Chris Lopez

Dr.

Norwegian University of Science and Technology

Høgskoleringen 1, 7491 Trondheim, Norway

Sam Brown

Prof.

Technion – Israel Institute of Technology

Technion City, Haifa 3200003, Israel

Abstract. This article addresses the growing concern of security in IoT devices by exploring hardware-based cryptographic solutions. Focusing on the design of secure processors and encryption modules, the study presents methods to safeguard data integrity and confidentiality. The implementation of these techniques is crucial for protecting sensitive information in connected devices.

Keywords: IoT Security, Hardware Cryptography, Secure Processors, Encryption Modules, Data Integrity

Introduction

The proliferation of Internet of Things (IoT) devices has raised significant security concerns, necessitating robust cryptographic solutions. This paper investigates hardware-based approaches to enhance security in IoT devices. By designing secure processors and dedicated encryption modules, the study aims to protect data integrity and confidentiality. These hardware cryptographic techniques offer a promising solution to the vulnerabilities inherent in software-based security measures. The research underscores the importance of integrating these solutions into IoT devices to safeguard sensitive information.

This is a preliminary version. To read the full version of the article, please purchase a subscription.

References

1. Kumar, N., & Kataria, V. Enhanced Sentiment Classification using a Multi-layered Stacked Ensemble Architecture.
2. Рагимов, Э. (2011). КВАЛИМЕТРИЧЕСКИЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ ПРОГРАММНЫХ КОМПЛЕКСОВ, РЕАЛИЗУЮЩИХ СИСТЕМУ УПРАВЛЕНИЯ КОРПОРАТИВНЫМИ СЕТЯМИ. Problems of information technology, 2(1), 18-23.

3. Рагимов, Э. Р. О. (2010). Механизм верификации безопасности программных средств, функционирующих в системе защиты информации корпоративных сетей. Вопросы защиты информации, (4), 37-40.