Dr .D. Kumutha, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Hardware Root of Trust Based Secure Boot System for Embedded IoT Devices

Dr .D. Kumutha , Punith Raj R, Chinmayi TS, P. Sai Sushant, and Ritesh Majjagi.

Abstract- More and more IoT devices are turning up in factories, hospitals, homes and important systems. This raises serious security concerns for the hardware inside them. Things like firmware changes or malware can hit right at startup and that causes real trouble. Traditional software protections do not cover the early startup stage all that well. The idea here is to use a hardware root of trust to build a safer boot process for these embedded systems. Trust starts from something that cannot be changed in hardware and then moves up to the main firmware. It seems this chain helps prevent unauthorised access and rollback issues before they get underway. Cryptographic checks using SHA-256 and ECDSA help verify that the code is intact and comes from the right source. They built it around STM32 microcontrollers with a fairly light bootloader that fits limited hardware. I think this keeps things practical for smaller devices. Tests showed better resistance to tampering and more reliable checks overall. Protection against attacks improved in the results but there could be other angles to consider in real deployments.

Keywords- Secure Boot, Hardware Root of Trust (HRoT), IoT Security, Embedded Systems, Firmware Protection, SHA-256, ECDSA, STM32 Microcontroller, Lightweight Bootloader, Firmware Integrity, Authentication, Tamper Resistance, Rollback Protection, Cryptographic Verification, Trusted Execution Chain.

I. INTRODUCTION

The Internet of Things (IoT) has rapidly transformed modern technology by connecting billions of smart devices across healthcare, industrial automation, transportation, smart cities, and consumer electronics.

Embedded IoT devices continuously exchange sensitive data and operate in environments exposed to cyber threats. Firmware-level attacks have emerged as one of the most critical security concerns because attackers can modify firmware, inject malicious code, or gain unauthorized access during system startup.

The boot process is the foundation of embedded system security. If the startup firmware is compromised, the entire device can become vulnerable. Traditional software-based security techniques fail to secure the initial boot stage because the verification mechanism itself may be compromised.

Secure boot mechanisms address this challenge by ensuring that only authenticated and trusted firmware executes on the device.

A Hardware Root of Trust provides a secure and tamper-resistant foundation for cryptographic operations and secure key storage.

The proposed system uses SHA-256 hashing and ECDSA digital signatures to validate firmware integrity and authenticity. This architecture establishes a secure chain of trust from hardware to firmware execution.

II. LITERATURE SURVEY

Several researchers have proposed secure boot mechanisms for embedded systems and IoT platforms.

TPM-based architectures provide strong hardware security but increase system cost and power consumption.

Lightweight software-only approaches reduce computational overhead but lack secure hardware key storage.

Recent research on low-power secure booting demonstrates the importance of lightweight cryptographic algorithms such as SHA-256, ECC, and ECDSA for IoT environments.

Low-power secure boot systems optimize energy consumption and memory utilization while maintaining firmware integrity verification.

However, many existing solutions lack strong hardware root of trust mechanisms and remain vulnerable to physical attacks and key extraction.

The proposed work improves security by integrating hardware-based root of trust with secure bootloader implementation and cryptographic verification.

III. PROPOSED METHODOLOGY

The proposed methodology follows a multi-stage secure boot architecture.

The process begins from a hardware-based Root of Trust stored in immutable memory.

The bootloader verifies firmware integrity using SHA-256 hashing and validates firmware authenticity using ECDSA digital signature verification.
The secure boot process follows these stages:

1. Power-on initialization.
2. Execution of Root of Trust.
3. Bootloader integrity verification.
4. Firmware hash generation.
5. Signature authentication.
6. Conditional execution of application firmware.

If verification fails, firmware execution is blocked immediately.

This ensures that unauthorized or modified firmware cannot execute on the embedded device.

IV. IMPLEMENTATION

The implementation uses STM32 microcontrollers with separated flash memory regions for bootloader and application firmware.

The bootloader resides at the initial flash memory location, while the application firmware is stored at a separate address offset.

SHA-256 generates a unique hash for firmware verification.

ECDSA signatures are validated using public keys stored in secure hardware memory. The bootloader verifies firmware before transferring control to the application.

The system also supports rollback protection, firmware authentication, and controlled application execution.

This architecture improves system reliability and prevents malicious firmware injection.

V. RESULTS AND DISCUSSION

Experimental analysis demonstrates that the proposed architecture successfully detects firmware tampering and unauthorized firmware modifications.

The secure bootloader prevents execution of

invalid firmware and maintains secure startup operation.

Compared to software-only secure boot approaches, the proposed HRoT architecture provides stronger tamper resistance and secure key protection.

The implementation also achieves lightweight operation suitable for low-power IoT devices.

Memory utilization and boot overhead remain within acceptable limits for embedded platforms.

The architecture significantly improves security reliability and firmware trustworthiness in IoT systems.

VI. CONCLUSION

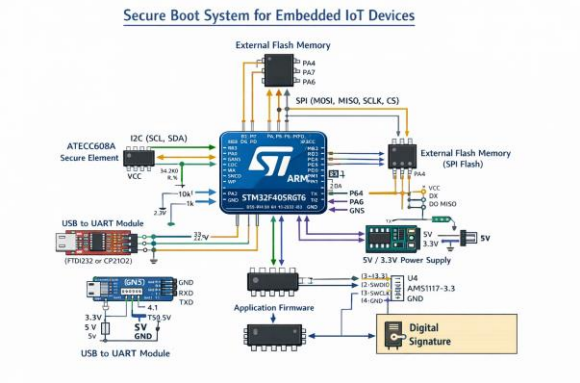
This paper presented a Hardware Root of Trust based secure boot architecture for embedded IoT devices.

The proposed system establishes a secure chain of trust from immutable hardware to application firmware using SHA-256 and ECDSA cryptographic verification.

The implementation demonstrates secure firmware validation, improved tamper resistance, and reliable startup protection suitable for resource-constrained IoT environments.

Future work includes secure OTA updates, remote attestation, and integration of advanced cryptographic mechanisms.

Fig.1 Proposed Hardware Root of Trust Secure Boot Architecture



VII. COMPARISON WITH EXISTING SYSTEMS

Feature	Existing System	Proposed System
Security	Software Based	Hardware Root of Trust
Verification	Basic Validation	SHA-256 + ECDSA
Key Storage	Normal Memory	Secure Hardware
Tamper Resistance	Limited	Strong
IoT Suitability	Moderate	Highly Suitable

REFERENCES

1. Wang, R., and Yan, Y., "A Survey of Secure Boot Schemes for Embedded Devices," IEEE ICACT, 2022.
2. Harrison Blake, "Low-Power Secure Booting for IoT Edge Devices," 2025.
3. Trusted Computing Group, "Trusted Platform Module Overview," TCG Publications.
4. STMicroelectronics, "STM32 Secure Boot and Secure Firmware Update," Application Note, 2023.
5. ARM Ltd., "ARM Trusted Firmware

tation. Documentation," ARM Security Documen.