UNIVERSITAS
GADJAH MADA
Verifikasi Integritas Firmware ESP32 Secara Terdesentralisasi Berbasis Smart Contract DChain
Brian Ilham Hermatristan, Triyogatama Wahyu Widodo, M.Kom
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

VERIFIKASI INTEGRITAS FIRMWARE ESP32 SECARA TERDESENTRALISASI BERBASIS SMART CONTRACT DCHAIN

Oleh

Brian Ilham Hermatristan 22/496068/PA/21295

Proliferasi perangkat IoT seperti ESP32 telah memperluas permukaan serangan terhadap manipulasi firmware, sementara server verifikasi terpusat konvensional menimbulkan Single Point of Failure (SPOF) yang kritis. Penelitian ini merancang, mengimplementasikan, dan mengevaluasi secara empiris sebuah sistem verifikasi integritas firmware yang terdesentralisasi menggunakan arsitektur tiga tingkat: perangkat akhir ESP32, Gateway Server berbasis Node.js, dan smart contract FirmwareIntegrity yang di-deploy pada jaringan dChain. ESP32 menghitung hash SHA-256 dari firmware yang sedang berjalan saat boot dan memeriksa hash master yang tidak dapat diubah di blockchain melalui pemanggilan verifyHash tanpa biaya gas, sementara transaksi logVerification mencatat log audit permanen yang dapat diverifikasi publik untuk setiap upaya verifikasi. Pengujian fungsional mencapai False Acceptance Rate dan False Rejection Rate sebesar 0% pada 40 percobaan, mengonfirmasi deteksi manipulasi yang andal melalui efek avalanche SHA-256. Latensi verifikasi rata-rata adalah 358,0 ms pada kondisi jaringan ideal dan 388,8 ms pada kondisi terdegradasi, peningkatan hanya 8,6%, meskipun outlier latensi parah terjadi lima kali lebih sering pada kondisi sinyal yang lemah. Hasil penelitian menunjukkan bahwa SPOF integritas berhasil dieliminasi dengan latensi yang tetap layak untuk siklus boot IoT di dunia nyata.

Kata kunci*—integritas firmware, ESP32, blockchain, smart contract, dChain*

UNIVERSITAS
GADJAH MADA
Verifikasi Integritas Firmware ESP32 Secara Terdesentralisasi Berbasis Smart Contract DChain
Brian Ilham Hermatristan, Triyogatama Wahyu Widodo, M.Kom
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

DECENTRALIZED INTEGRITY VERIFICATION FOR ESP32 FIRMWARE USING DCHAIN SMART CONTRACTS

By

Brian Ilham Hermatristan 22/496068/PA/21295

The proliferation of IoT devices such as the ESP32 has expanded the attack surface for firmware tampering, while conventional centralized verification servers introduce a critical Single Point of Failure (SPOF). This research designs, implements, and empirically evaluates a decentralized firmware integrity verification system using a three-tier architecture: an ESP32 end-device, a Node.js Gateway Server, and a FirmwareIntegrity smart contract deployed on the dChain Network. The ESP32 calculates a SHA-256 hash of its running firmware at boot and queries the immutable on-chain master hash through a gasless verifyHash call, while a logVerification transaction records a permanent, publicly auditable log of each attempt. Functional testing achieved a 0% False Acceptance Rate and 0% False Rejection Rate across 40 trials, confirming reliable tamper detection via the SHA-256 avalanche effect. Verification latency averaged 358.0 ms under ideal network conditions and 388.8 ms under degraded conditions, an increase of only 8.6%, though severe latency outliers occurred exactly five times more frequently under degraded signal strength. The results demonstrate that the integrity Single Point of Failure is eliminated while maintaining latency suitable for real-world IoT boot sequences.

Keywords— *firmware integrity, ESP32, blockchain, smart contract, dChain*