International Journal of Advances and Applications in Convergent Studies & Transdisciplinary (IJ-AACST)

Bridging Disciplines, Bridging Knowledge

Aligned with the Vision of NEP 2020 and UGC Guidelines

Website: https://aacstij.org || Email: journaleditor@aacstij.org

Performance Evaluation of a SHA256-Based Verification Mechanism for Secure Blockchain Transactions

DOI: https://doi.org/10.5281/zenodo.24104442

Miss. Sheetal R. Billore[1]*, Dr. Keshao D. Kalaskar[2]

*Corresponding Author: [1] Research Scholar, Sardar Patel Mahavidyalaya, Chandrapur, Maharashtra, India,

sheetalbillore123@gmail.com

[2] Professor, Dr. Ambedkar College of Arts, Commerce and Science, Chandrapur, Maharashtra, India,

keshao_kalaskar@yahoo.co.in

ABSTRACT

The security and integrity of digital records are critical requirements in distributed information systems, particularly where electronic healthcare records and administrative documents are exchanged across multi-organizational networks. This paper presents a performance evaluation of a Python-based blockchain architecture integrating SHA-256 hashing with a secret-key verification mechanism (SHA256-VK). The system incorporates core blockchain operational components: transaction creation, block generation, proof-of-work consensus, and transaction validation. Experimental evaluations were conducted on blockchain scales ranging from 50 to 500 blocks, assessing system memory utilization, execution runtime, and average block-generation latency. Experimental results demonstrate that memory utilization scales predictably from 0.28331 MB at 50 blocks to 0.28500 MB at 500 blocks, while total execution time increases from 58.897 seconds to 78.791 seconds. The measured mean block-generation time was approximately 5.486 seconds. The findings confirm predictable resource growth within the evaluated bounds and establish baseline performance metrics for lightweight verification mechanisms in distributed ledgers.

KEYWORDS: Blockchain, SHA-256, verification secret key, SHA256-VK, data integrity, execution time, memory utilization, healthcare information systems.

1. INTRODUCTION

Digital platforms increasingly handle data that demand strict assurances regarding authenticity, traceability, and immutability. Healthcare information systems represent a key application domain where electronic health records (EHRs)—encompassing medical histories, prescriptions, laboratory diagnostics, and personal identifiers—require robust protection against unauthorized alteration and data corruption. Traditional centralized database architectures present inherent vulnerabilities, including single points of failure, centralized attack vectors, non-transparent access control policies, and inadequate auditability.

Blockchain technology offers a decentralized, append-only distributed ledger where data records are

© 2026 The Author(s). This article is published by the AACST in the IJ-AACST under the Creative Commons Attribution 4.0 International (CC BY 4.0) License. The authors retain copyright and grant AACST a non-exclusive license to publish, distribute, and archive the work.