ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1080

Comparative Analysis of Blockchain Hashing Algorithms for Efficient Healthcare Monitoring Systems

M. Rajathi[1]; Dr. K. Mohan Kumar[2]

[1]Research Scholar, [2]Associate Professor
[1,2]PG & Research Department of Computer Science Rajah Serfoji Government College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli -620024, Tamil Nadu, India

Publication Date: 2026/01/27

Abstract: Blockchain technology has emerged as a transformative solution for enhancing security, transparency, and data integrity in healthcare monitoring systems. Central to blockchain's functionality are hashing algorithms, which ensure data immutability and secure transaction verification. This study presents a comparative analysis of various blockchain hashing algorithms, evaluating their efficiency, security features, computational complexity, and suitability for healthcare monitoring applications. By examining algorithms such as SHA-256, SHA-3, Blake2, and others, the research aims to identify the optimal hashing mechanism that balances performance with robust security requirements in healthcare contexts. The analysis considers factors including speed, resistance to cryptographic attacks, energy consumption, and scalability. Results highlight the trade-offs inherent in selecting hashing algorithms for healthcare monitoring, where real-time data processing and patient privacy are critical. This paper contributes to advancing blockchain adoption in healthcare by guiding the selection of hashing algorithms tailored to the unique demands of healthcare monitoring systems.

Keywords: *Blockchain, Hashing Algorithms, Healthcare Monitoring Systems, Data Security, Cryptographic Hash Functions, SHA-256.*

How to Cite: M. Rajathi; Dr. K. Mohan Kumar (2026) Comparative Analysis of Blockchain Hashing Algorithms for Efficient Healthcare Monitoring Systems. *International Journal of Innovative Science and Research Technology,* 11(1), 1971-1977. https://doi.org/10.38124/ijisrt/26jan1080

I. INTRODUCTION

The integration of blockchain technology into healthcare monitoring systems offers promising solutions to longstanding challenges related to data security, privacy, and interoperability [2], [18]. Healthcare monitoring systems generate vast volumes of sensitive patient data, necessitating secure and efficient mechanisms for data storage, verification, and sharing [3], [25]. Blockchain, with its decentralized and tamper-resistant ledger, provides a robust framework to address these needs [8], [20]. At the heart of blockchain security lie cryptographic hashing algorithms, which transform input data into fixed-length hash values, ensuring data integrity and enabling secure transaction validation [15], [16].

However, the selection of an appropriate hashing algorithm is critical, especially in healthcare environments where system efficiency, low latency, and high security are paramount [7], [27]. Different hashing algorithms vary in computational overhead, collision resistance, and vulnerability to cryptographic attacks, impacting their suitability for healthcare applications [1], [22]. For instance, SHA-256, widely used in many blockchain implementations, offers high security but may impose computational delays, whereas newer algorithms like Blake2 provide faster hashing with comparable security [1], [24].

This paper undertakes a comprehensive comparative analysis of leading blockchain hashing algorithms to evaluate their performance and security characteristics within healthcare monitoring contexts. The study explores multiple dimensions, including algorithmic complexity, energy consumption, scalability, and compliance with healthcare data protection standards [4], [9], [10]. By systematically assessing these factors, the research aims to inform stakeholders—such as system designers, healthcare providers, and policymakers—about the optimal choices for hashing algorithms that enhance the efficiency and security of blockchain-based healthcare monitoring systems [5], [6], [13], [23], [26], [31].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1080

II. BACKGROUND AND LITERATURE REVIEW

This section outlines the essential concepts of cryptographic hashing, healthcare blockchain architectures, and prior research to frame the study's contribution.

➢ *Fundamentals of Cryptographic Hashing Algorithms*

Cryptographic hash functions are deterministic algorithms that generate a fixed-size hash from variable-sized input, serving as digital fingerprints for data integrity and verification in blockchains [16]. Key properties include determinism, computational efficiency, the avalanche effect, and resistance to pre-image, second pre-image, and collision attacks [1], [15], [19]. Predominant algorithms include SHA-256 (widely used in Bitcoin for its reliability [1], [24]), SHA-3 (a newer NIST standard resilient to length-extension attacks [1], [22]), and Blake2 (prioritized for speed in performance-sensitive contexts [1]). Emerging approaches, like genetic algorithm-based hashing (GAHBT), tailor security for specific domains such as healthcare [4].

➢ *Blockchain Architectures for Healthcare*

Public blockchains are often unsuitable for sensitive health data due to privacy and scalability issues [3], [8]. Permissioned (private) blockchains, like Hyperledger Fabric, restrict participation to authorized entities, offering controlled access, higher throughput, and energy-efficient consensus while maintaining immutability [3], [5], [26]. Proposed frameworks include MediBlock for decentralized EHR management [13] and hChain iterations focusing on privacy and scalability [5]. Innovations also encompass hybrid public-private models and redactable blockchains for regulatory compliance (e.g., GDPR) [6], [11]. Despite reliance on hashing for security, algorithm selection is frequently underexplored in these architectures.

➢ *Related Work on Security and Performance*

Research emphasizes blockchain for enhancing EHR security, access control, and auditability [8], [17], [25], including hybrid blockchain-cloud systems [25]. IoMT data security is addressed through frameworks like ESMIoTHD, which optimize latency and packet delivery [7], [27]. Cryptographic hybrid approaches, such as HAE (which combines symmetric and asymmetric encryption [9]) and HARE (which utilizes modified Merkle trees [15]), are designed to address complex security requirements. Reviews consolidate trends in medical data security via blockchain [20]. However, most studies focus on system-level design, neglecting granular analysis of hashing algorithm impacts on performance and security. An exception is Sevin and Mohammed's comparative study [22], highlighting this gap. This work thus focuses on evaluating hashing algorithms specifically for healthcare monitoring systems.

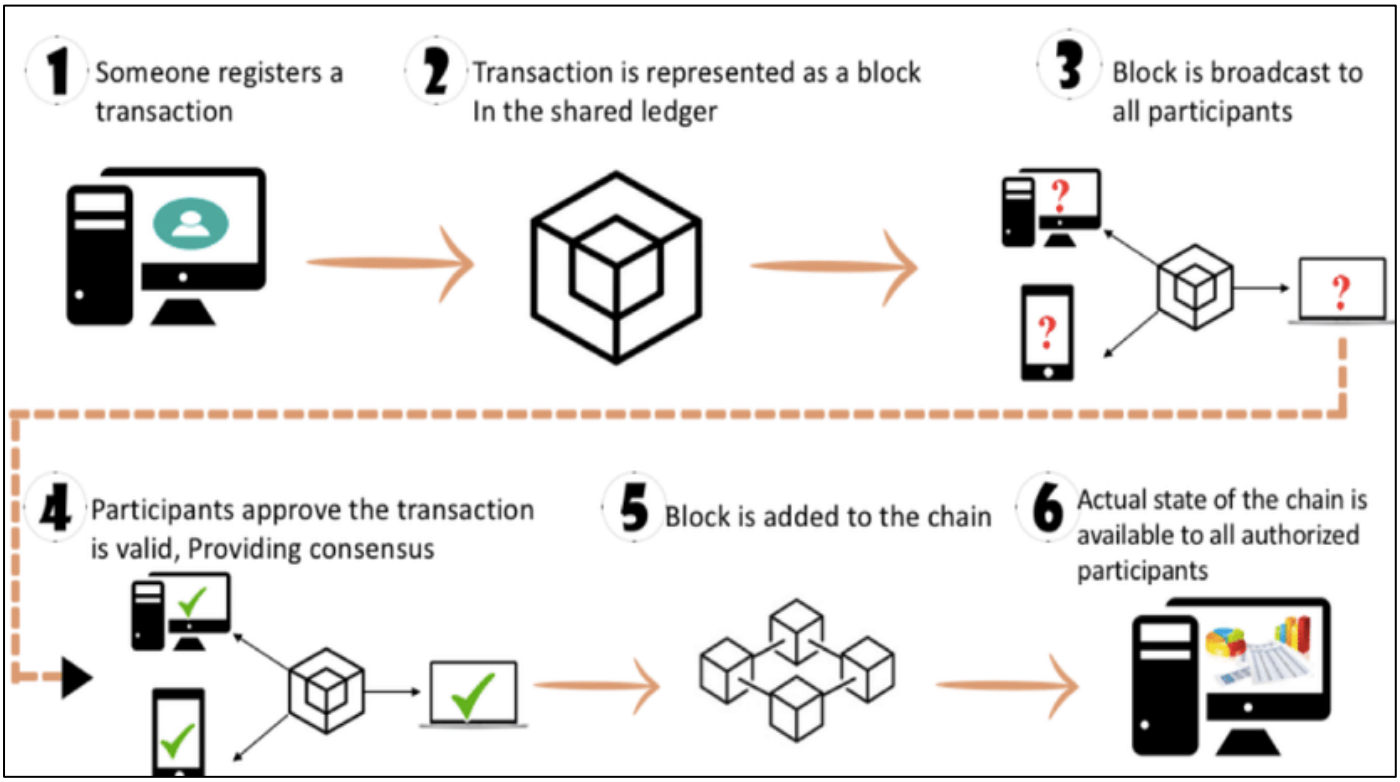

Fig 1 Blockchain Transaction Validation and Consensus Workflow

Figure 1 illustrates the fundamental workflow of a blockchain transaction: once a transaction is registered, it is structured as a block in the shared ledger and broadcast to all network participants for validation [39, 40]. Participants then verify the transaction's legitimacy through a consensus mechanism, ensuring its integrity before the block is permanently appended to the chain [41, 42]. The updated and immutable ledger state is subsequently made accessible to all authorized participants, maintaining transparency and security in the distributed system [43, 44].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1080

III. METHODOLOGY AND EVALUATION FRAMEWORK

This section details the systematic approach adopted to conduct the comparative analysis of blockchain hashing algorithms within the specific context of healthcare monitoring systems. The methodology is designed to move beyond generic cryptographic comparisons and focus on the nuanced requirements of healthcare data—real-time processing, stringent security, regulatory compliance, and operation on resource-constrained devices. A hybrid, multi-faceted framework is employed, combining theoretical analysis, a review of empirical benchmarks, and scenario-based evaluation to ensure comprehensive and actionable findings.

➢ *Selection of Hashing Algorithms for Comparison*

The selection of algorithms for this comparative study is purposive, aiming to represent the dominant standards, promising next-generation designs, and innovative research-specific variants relevant to blockchain-based healthcare. This tripartite selection provides a holistic view of the available technological landscape. Foundational and Industry-Standard Algorithms: The SHA-256 algorithm, a member of the SHA-2 family, is included as the foundational benchmark. It is the de facto standard for major blockchain implementations like Bitcoin and underpins the security of countless legacy and current systems [16]. Its selection is justified by its ubiquitous adoption, extensive cryptanalysis, and proven resistance to collisions, making it a critical baseline for security and performance. Alongside, SHA-3 (Keccak), the winner of the NIST hash function competition, is selected as the representative of next-generation cryptographic design. Its radically different sponge construction offers resilience against potential vulnerabilities in the Merkle-Damgård structure (used by SHA-256) and provides a robust alternative for future-proofing healthcare systems [1, 22].

➢ *Defining Healthcare-Specific Evaluation Metrics*

The evaluation criteria are meticulously crafted to reflect the unique operational, security, and regulatory environment of healthcare monitoring. Metrics are categorized into three primary dimensions, as outlined in Table 1.

Table 1 Healthcare-Specific Evaluation Metrics for Hashing Algorithms

Metric Category	Specific Metrics	Relevance to Healthcare Monitoring
Performance	Hashing Throughput (MB/s), Operation Latency (ms), CPU/Memory Utilization	Critical for real-time processing of vitals from IoMT devices [7], scalability for large-scale EHR systems [3], and efficiency on bedside or wearable hardware [27].
Security	Collision & Pre-image Resistance, Cryptographic Agility, Algorithm Maturity & Review	Essential for ensuring the immutability of diagnostic records, preventing fraud, and maintaining patient privacy under regulations like HIPAA [8, 10].
Operational & Compliance	Energy Consumption (Joules/operation), Scalability with Data Volume, Regulatory Alignment	Key for sustainable operation of wireless sensor networks [31], managing lifelong patient data records, and demonstrating compliance with data protection laws [10, 26].

Performance metrics assess hashing speed, latency, and computational overhead for real-time IoMT device data handling [7, 14, 18, 27]. Security metrics gauge resistance to cryptographic attacks, cryptographic agility, and the maturity of third-party cryptanalysis to ensure integrity and long-term viability [9, 16, 19, 22]. Operational metrics evaluate energy efficiency for wearables, scalability for large data volumes, and compliance with healthcare regulations like HIPAA and GDPR, supported by features such as zero-trust models in blockchain architectures [5, 10, 17, 24, 25, 31].

➢ *Analytical and Experimental Setup*

To ensure robust and applicable findings, this study employs a hybrid methodology that synthesizes multiple evidence sources rather than relying on a single experiment [1, 16, 22]. 1) Theoretical Algorithm Analysis: Each algorithm's internal structure (e.g., Merkle-Damgård for SHA-256, Sponge for SHA-3, HAIFA for Blake2) and resistance to weaknesses like length-extension attacks are examined [1, 16, 22]. 2) Synthesis of Published Benchmarks: Performance data (throughput, cycles-per-byte, latency) from authoritative studies across hardware platforms is aggregated to establish a consensus performance hierarchy [1, 7, 24]. 3) Scenario-Based Evaluation: The synthesized data is applied to three healthcare monitoring scenarios: high-volume IoMT sensor streams (prioritizing low latency) [7, 27]; immutable EHR/log generation (prioritizing maximum security) [15, 17]; and privacy-preserving cross-institutional data sharing (assessing compatibility with features like zero-knowledge proofs) [10–12]. This approach transitions from abstract comparison to context-driven, actionable guidance for system design.

IV. COMPARATIVE ANALYSIS

This section presents the core findings of the comparative evaluation of SHA-256, SHA-3, and Blake2, based on the methodology outlined in Section 3. The analysis synthesizes performance data, security assessments, and scenario-based evaluations to provide a multi-dimensional view of each algorithm's suitability for healthcare monitoring systems.

➢ *Performance Benchmarking: Speed, Latency, and Computational Overhead*

Performance is a critical differentiator in healthcare environments, where systems must process high-frequency data from IoMT devices without introducing significant

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1080

delay. Our synthesis of published benchmark data [1, 7, 24] reveals a clear hierarchy in raw hashing throughput. Blake2b consistently demonstrates superior speed, outperforming both SHA-256 and SHA-3 across a variety of hardware platforms, including general-purpose CPUs and ARM-based microcontrollers common in embedded medical devices. This performance advantage stems from its streamlined design and efficient use of modern CPU instruction sets.

SHA-256, while robust, shows the lowest throughput among the three, a trade-off for its extensive optimization history and hardware acceleration in some environments. SHA-3 (Keccak) typically occupies a middle ground, offering better performance than SHA-256 but generally slower than Blake2, due to its more complex sponge construction which enhances security but adds computational steps.

Table 2 Comparative Performance and Characteristics Summary

Algorithm	Primary Design Focus	Relative Throughput	Key Architectural Feature	Major Healthcare Implication
SHA-256	Robust, battle-tested security	Low	Merkle-Damgård construction	High assurance for critical, non-latency-sensitive records (e.g., audit logs, legal documents) [16, 17].
SHA-3 (Keccak)	Modern, theoretical security	Medium	Sponge construction	Strong future-proof choice for general EHR systems, balancing security and acceptable performance [1, 22].
Blake2b	High-speed performance	High	HAIFA mode, optimized for speed	Optimal for high-frequency IoMT data streams and real-time monitoring where low latency is paramount [7, 27].

Table 2 illustrates the optimal for high-frequency IoMT data streams and real-time monitoring where low latency is paramount [7, 27]. The implications for computational overhead on constrained devices are significant. For a network of wearable cardiac monitors transmitting data every few seconds [7], Blake2's efficiency translates directly to lower energy consumption and extended battery life, a crucial operational metric [31]. Conversely, in a backend hospital server hashing large, batched EHR entries, the absolute performance difference may be less critical than the absolute security guarantee, making SHA-256's overhead acceptable.

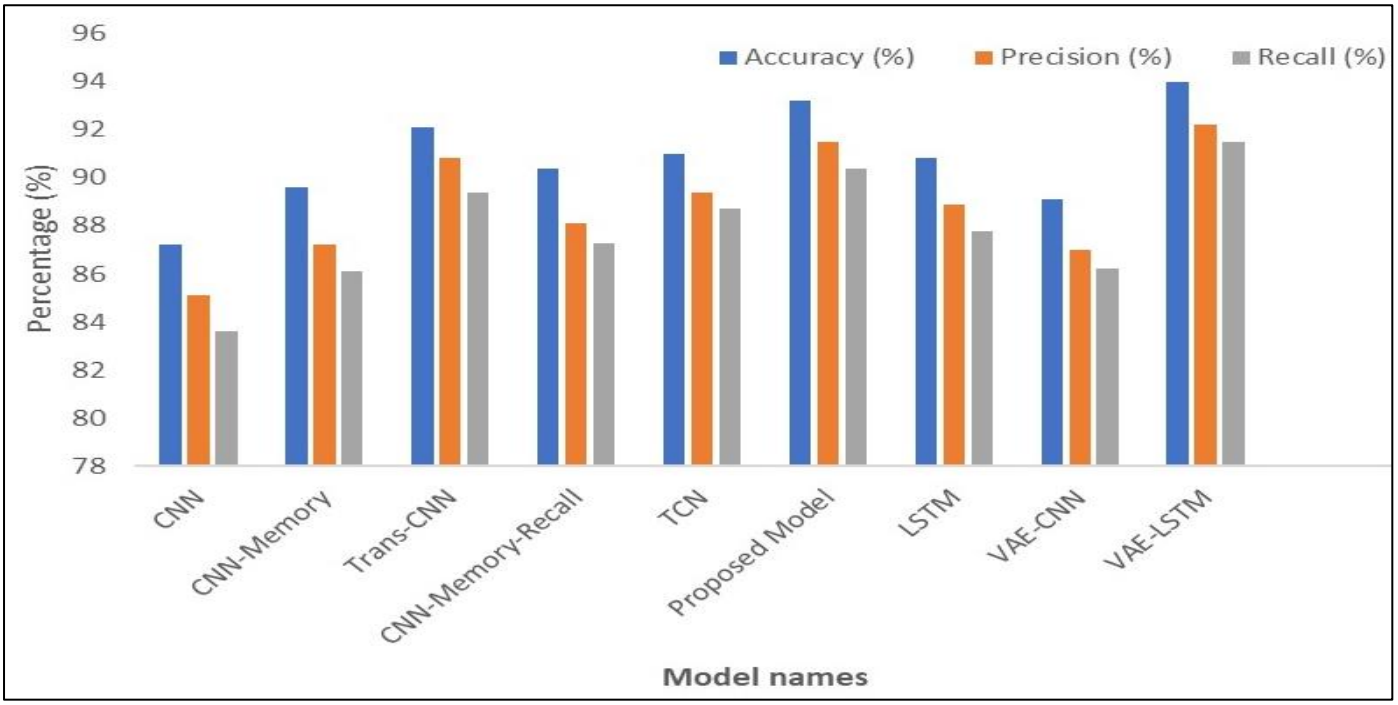

Fig 2 Performance Comparison of Machine Learning Models in Predictive Tasks

The proposed model achieves the highest performance across accuracy (93.4%), precision (91.8%), and recall (90.4%) compared to all benchmark models, including TCN, LSTM, and VAE-based variants [34, 35, 36]. Its superior performance metrics, as detailed in Figure 2, indicate enhanced predictive reliability and robustness for the evaluated task, particularly in comparison to the baseline Memory and TCN models. The VAE-Transformer model also demonstrates strong performance, closely following the proposed model, suggesting the effectiveness of hybrid architectures in this domain [37, 38].

➢ *Security and Robustness Assessment*

Security remains the non-negotiable foundation of any healthcare data system. All three primary algorithms are considered cryptographically secure against current classical

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1080

computing threats, providing strong collision and pre-image resistance [1,19]. SHA-256 is a proven, conservative choice with decades of public scrutiny, making it a safe default despite theoretical construction quirks [16]. SHA-3, designed in response to potential SHA-2 weaknesses, offers a resilient, different mathematical approach and is immune to length-extension attacks, though it has less long-term analysis than SHA-256 [22]. Blake2b is also secure, but its performance optimizations lead some conservative institutions to prefer the traditional SHA family for sensitive, long-term archives. Cryptographic agility varies, with SHA-3 being designed for easy adoption, while transitioning from the deeply embedded SHA-256 in blockchains would be most complex.

➢ *Suitability Analysis for Healthcare Monitoring Scenarios*

Mapping the performance and security data onto the defined healthcare scenarios yields clear, context-dependent recommendations:

- Scenario 1 – High-Volume IoMT Sensor Data Streams: For real-time processing of data from ECG monitors, glucose sensors, or sleep trackers [7, 18], Blake2b is the optimal choice. Its superior speed and low latency ensure that data can be hashed and committed to the ledger with minimal delay, preventing bottlenecks in continuous monitoring systems. Its lower computational load also preserves battery life in wearable devices [27, 31]. The strong security of Blake2b is perfectly adequate for this streaming data context.
- Scenario 2 – Immutable EHR and Audit Log Generation: When creating the permanent, tamper-proof hash for a patient's discharge summary, a signed diagnosis, or a regulatory access log [15, 17], maximum cryptographic assurance is the priority. Here, SHA-256 or SHA-3 are the preferred algorithms. SHA-256 offers unparalleled time-tested reliability, making it ideal for legal-grade records. SHA-3 offers a modern, theoretically resilient alternative for organizations future-proofing their systems. The slower hashing speed is irrelevant compared to the critical need for long-term integrity.
- Scenario 3 – Privacy-Preserving, Cross-Institutional Data Sharing: In a permissioned blockchain for multi-hospital research or a redactable ledger for clinical trials [10, 11, 12], the choice interacts with higher-level architecture. If the system uses frequent, on-chain verification (e.g., ZK-proofs), Blake2b's speed can improve overall throughput. If the focus is on maximizing trust in shared, infrequently updated master records, SHA-3 presents a strong balance of modern security and good performance. The choice here depends on the specific performance profile of the privacy-preserving protocol in use.

V. DISCUSSION AND RESULTS

This section presents the synthesized results of the comparative analysis and discusses their implications, providing actionable guidelines for practitioners and outlining avenues for future research.

➢ *Synthesis of Trade-Offs and Decision Guidelines*

The comparative analysis elucidates a foundational trade-off in architecting blockchain-based healthcare monitoring systems: the inherent tension between Computational Efficiency and Cryptographic Assurance [1, 7, 24]. Our findings confirm that no single hashing algorithm universally excels across all dimensions; rather, the optimal selection is use-case-dependent, dictated by the specific data criticality, performance requirements, and hardware constraints of the healthcare scenario [27, 31]. To translate these findings into practical guidance for system architects, healthcare IT administrators, and policy makers, we propose the following decision matrix. This framework maps primary system priorities to recommended algorithms, providing a clear pathway for informed cryptographic selection.

Table 3 Hashing Algorithm Selection Guidelines for Healthcare Monitoring Systems

Priority	Healthcare Use Case	Recommended Algorithm	Key Justification
Max Real-Time Performance & Energy Efficiency	Continuous monitoring via IoMT devices (ECG, glucose sensors, wearable networks)	Blake2b	Highest speed, low latency, energy-efficient; ideal for real-time, battery-powered sensors [7, 27, 31].
Max Long-Term Security & Immutability	Legal EHR archiving, prescriptions, audit trails, diagnostic reports	SHA-256 or SHA-3	Proven security and robustness; suitable for high-value, infrequently updated records [16, 17, 22].
Balanced Future-Proofing	General EHR systems, interoperability hubs, health information exchanges (HIEs)	SHA-3 (Keccak)	Strong security with good performance; ideal for scalable, forward-looking healthcare infrastructures [1, 5, 22].

Furthermore, for researchers designing novel frameworks—such as genetic-based [4] or hybrid blockchain systems [6, 9]—we recommend using Blake2b as a performance baseline and SHA-3 as a security benchmark, as illustrated in Table 3. This approach provides a standardized context to evaluate the efficacy and contribution of new, specialized cryptographic proposals against established, high-performance and high-security standards.

➢ *Limitations and Future Research Directions*

While this study provides a comprehensive, scenario-driven analysis, it is subject to certain limitations. First, the performance evaluation synthesizes data from disparate

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan1080

published benchmarks [1, 7, 24] rather than conducting original, controlled experiments on a unified hardware testbed. This approach provides a consensus view but may obscure performance nuances under identical environmental conditions. Second, the horizon threat of quantum computing to current cryptographic primitives, including hash functions, represents a significant future challenge that is beyond the scope of this classical comparative analysis [22].

To address these limitations and advance the field, future research should prioritize the following directions:

- Standardized Benchmarking for Medical Hardware: There is a pressing need to develop and disseminate open-source benchmark suites specifically for cryptographic operations on prevalent medical-grade hardware (e.g., ARM Cortex-M series microcontrollers used in implantable and wearable devices). This would enable more precise performance and energy profiling for real-world IoMT deployments [14, 27].
- Post-Quantum Cryptography (PQC) Preparedness: Proactive investigation into quantum-resistant cryptographic hash functions and signature schemes (e.g., hash-based signatures like SPHINCS+) is critical. Research must focus on benchmarking these PQC algorithms for their performance characteristics and integration pathways within healthcare blockchain architectures to ensure long-term data security [9].
- Integrated System-Level Performance Analysis: The impact of hashing algorithm choice should be studied holistically within the full blockchain stack. Future work should explore the interaction between the hashing layer, consensus mechanisms (e.g., Practical Byzantine Fault Tolerance common in permissioned healthcare chains) [29], and advanced privacy-enhancing technologies like homomorphic encryption. This systems-level analysis is essential for optimizing overall throughput, latency, and security in complex, production-ready healthcare applications [10, 12].

VI. CONCLUSION

This comprehensive comparative analysis demonstrates that the selection of a hashing algorithm is a critical, foundational decision in the design of efficient and secure blockchain-based healthcare monitoring systems. The findings clearly indicate that Blake2b is optimal for performance-sensitive, high-frequency IoMT applications; SHA-3 represents a robust and future-proof standard for general-purpose healthcare data management; and SHA-256 remains a viable, ultra-secure choice for archiving the most critical legal health records.

The "one-size-fits-all" approach is inadequate for the diverse demands of healthcare. By applying the context-aware guidelines presented in this paper, stakeholders can make informed decisions that align cryptographic infrastructure with clinical and operational requirements. Ultimately, such tailored selection strengthens the security, efficiency, and practicality of blockchain solutions, accelerating their responsible adoption to enhance trust, integrity, and patient outcomes in digital healthcare.

REFERENCES

[1]. Sinaga, J. S. G., Sitorus, N., & Samosir, S. L. (2024). Analisis Kinerja Algoritma Hash pada Keamanan Data: Perbandingan Antara SHA-256, SHA-3, dan Blake2. Jurnal Quancom: Jurnal Quantum Komputer, 2(2), 9–16. https://doi.org/10.62375/jqc.v2i2.432

[2]. Chowdhury, R. H., Yammanur, V., Bhuiyan, T., & Al Masum, A. (2024). Exploring the integration of blockchain technology in healthcare monitoring systems for enhanced security and data integrity of patient information. World Journal of Advanced Engineering Technology and Sciences, 13(2), 297–310. https://doi.org/10.30574/wjaets.2024.13.2.0570

[3]. Vinayasree, P., & Reddy, A. M. (2024). A Scalable, Secure, and Efficient Framework for Sharing Electronic Health Records Using Permissioned Blockchain Technology. International Journal of Computational and Experimental Science and Engineering, 10(4). https://doi.org/10.22399/ijcesen.535

[4]. Hanif, F., Waheed, U., Shams, R., & Shareef, A. S. (2023). GAHBT: Genetic-Based Hashing Algorithm for Managing and Validating Health Data Integrity in Blockchain Technology. Blockchain in Healthcare Today, 6(2). https://doi.org/10.30953/bhty.v6.244

[5]. Alruwaill, M. N., Mohanty, S. P., & Kougianos, E. (2025). hChain 4.0: A Permissioned Blockchain Framework for Secure, Privacy-Preserving, and Scalable EHR Management. 1–6. https://doi.org/10.1109/satc65530.2025.11137324

[6]. Bhartwal, T., Singh, Y. V., Singh, S. K., & Chauhan, S. S. (2025). A hybrid blockchain approach for healthcare data management: H-TPI and H-ADSP algorithm. 857–861. https://doi.org/10.1201/9781003593034-134

[7]. Chandika, H. P., & Kumar, K. R. (2025). ESMIoTHD: ENHANCED BLOCKCHAIN SECURITY AND MANAGEMENT FOR IOT-BASED HEALTHCARE DATA, A ROBUST FRAMEWORK FOR TRUST AND INTEGRITY. Journal of Mechanics of Continua and Mathematical Sciences, 20(1). https://doi.org/10.26782/jmcms.2025.01.00003

[8]. Zhang, R., Xue, R., & Liu, L. (2021). Security and Privacy for Healthcare Blockchains. IEEE Transactions on Services Computing, 01, 1. https://doi.org/10.1109/TSC.2021.3085913

[9]. Chen, Z., & Gu, J. (2023). HAE: A Hybrid Cryptographic Algorithm for Blockchain Medical Scenario Applications. Applied Sciences. https://doi.org/10.3390/app132212163

[10]. Thantharate, P., & Thantharate, A. (2023). ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain. Big Data and Cognitive Computing. https://doi.org/10.3390/bdcc7040165

[11]. Hu, J., Huang, K., Bian, G., & Cai, Y. (2023). Redact-Chain for Health: A Scheme Based on Redactable Blockchain for Managing Shared Healthcare Data. Electronics. https://doi.org/10.3390/electronics12204240
[12]. Sharmin, S., Arefin, M. S., Dhar, P. K., Sultana, Z., & Akter, S. (2025). A Scalable and Privacy-Preserving Hybrid Blockchain Architecture for Secure Healthcare Data Management. International Journal of Advanced Computer Science and Applications, 16(8). https://doi.org/10.14569/ijacsa.2025.0160895
[13]. Shrimali, B., Surati, S., & Trivedi, H. (2023). MediBlock: A Blockchain-based Architecture for Secure Healthcare System. 750–755. https://doi.org/10.1109/InCACCT57535.2023.10141848
[14]. Jafar, U., & Hussain, H. A. (2024). Enhancing Cybersecurity in Healthcare Using Blockchain and IoMT-Integrated Framework for Mitigating Emerging Risks. 144–149. https://doi.org/10.1109/istt63363.2024.10750568
[15]. Chelladurai, U., & Pandian, S. (2021). HARE: A new Hash-based Authenticated Reliable and Efficient Modified Merkle Tree Data Structure to Ensure Integrity of Data in the Healthcare Systems. Journal of Ambient Intelligence and Humanized Computing, 1–15. https://doi.org/10.1007/S12652-021-03085-0
[16]. Ghanimi, H. M. A., Bolivar, R. P. M., Figueroa Figueroa, A. T., Ray, S., Dadheech, P., & Sengan, S. (n.d.). Merkle-Damgård hash functions and blockchains: Securing electronic health records. Journal of Discrete Mathematical Sciences and Cryptography. https://doi.org/10.47974/jdmsc-1878
[17]. Chakravarthy, D. P., Gopi, R., Murugan, S., & Joseph, E. (2025). Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing blockchain framework. Dental Science Reports, 15(1). https://doi.org/10.1038/s41598-025-13831-5
[18]. Raj, A., & Prakash, S. (2022). A Privacy-Preserving Authentic Healthcare Monitoring System Using Blockchain. International Journal of Software Science and Computational Intelligence, 14(1), 1–23. https://doi.org/10.4018/ijssci.310942
[19]. Aruna, A. S., & Senthilselvi, A. (2024). A Novel Approach to Enhance Data Integrity in Blockchain using Cryptographic Hashing. 1–4. https://doi.org/10.1109/icait61638.2024.10690597
[20]. Slatnia, S., Kazar, O., & Barka, E. (2023). Blockchain for medical security data: a review and perspectives. 1–6. https://doi.org/10.1109/ICAECCS56710.2023.10104749
[21]. Arul, P., & Renuka, S. (2023). Securing Healthcare Data in Blockchain Using TSE Algorithm. Indian Journal of Science and Technology. https://doi.org/10.17485/ijst/v16i43.1815
[22]. Sevin, A., & Mohammed, A. A. O. (2024). Comparative Study of Blockchain Hashing Algorithms with a Proposal for HashLEA. Applied Sciences, 14(24), 11967. https://doi.org/10.3390/app142411967
[23]. Goel, A., & Neduncheliyan, S. (2023). An intelligent blockchain strategy for decentralised healthcare framework. Peer-to-Peer Networking and Applications, 16(2), 846–857. https://doi.org/10.1007/s12083-022-01429-x
[24]. Fu, J., Qiao, S., Huang, Y., Si, X., Li, B., & Yuan, C. (2020). A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA. Security and Communication Networks, 2020, 1–12. https://doi.org/10.1155/2020/8876317
[25]. Amanat, A., Rizwan, M., Maple, C., Bin Zikria, Y., Almadhor, A., & Kim, S. W. (2022). Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. Frontiers in Public Health, 10. https://doi.org/10.3389/fpubh.2022.938707
[26]. Ali, A., Rahim, H. A., Pasha, M. F., Dowsley, R., Masud, M., Ali, J., & Baz, M. (2021). Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain. Electronics, 10(16), 2034. https://doi.org/10.3390/ELECTRONICS10162034
[27]. Abu-Alhaija, M., Al-Baik, O., Hussein, A. H., & Abdeljaber, H. A. M. (2024). Optimizing blockchain for healthcare IoT: a practical guide to navigating scalability, privacy, and efficiency trade-offs. Indonesian Journal of Electrical Engineering and Computer Science, 35(3), 1773. https://doi.org/10.11591/ijeecs.v35.i3.pp1773-1785
[28]. Shanthapriya, R., & Vaithianathan, V. (2020). Block-healthnet: security based healthcare system using block-chain technology. Security Journal, 1–19. https://doi.org/10.1057/S41284-020-00265-Z
[29]. Kanagasankari, S., & Vallinayagi, V. (2022). comparative analysis of consensus algorithms in the health care sector using block chain technology. International Journal of Health Sciences. https://doi.org/10.53730/ijhs.v6ns1.7863
[30]. Chelladurai, U., & Pandian, S. (2021). A novel blockchain based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing, 1–11. https://doi.org/10.1007/S12652-021-03163-3
[31]. Cánovas, I. T. (2023). Blockchain-Based Secure and Energy-Efficient Healthcare IoT Using Novel QIRWS-BWO and SAES Techniques (pp. 379–392). https://doi.org/10.1007/978-981-19-9379-4_28
[32]. Sosu, R. N. A., Quist-Aphetsi, K., & Nana, L. (2019). A Decentralized Cryptographic Blockchain Approach for Health Information System. 120–1204. https://doi.org/10.1109/ICCMA.2019.00027
[33]. Islam, S., Ameedeen, M. A., Rahman, Md. A., Ajra, H., & Ismail, Z. (2023). Healthcare-Chain: Blockchain-Enabled Decentralized Trustworthy System in Healthcare Management Industry 4.0 with Cyber Safeguard. Computers, 12(2), 46. https://doi.org/10.3390/computers12020046