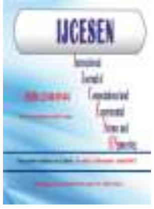
International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 10-No.4 (2024) pp. 827-834
http://www.ijcesen.com



ISSN: 2149-9144

Research Article

A Scalable, Secure, and Efficient Framework for Sharing Electronic Health Records Using Permissioned Blockchain Technology

P.Vinayasree[1]*, A. Mallikarjuna Reddy[2]

[1] Assistant Professor and Research Scholar, Department of Computer Science & Engineering Anurag University, Hyderabad, Telangana 500088, India
* **Corresponding Author Email:** vinayasreecse@anurag.edu.in **ORCID:** 0000-0002-3929-4988

[2] Associate Professor and Head, Department of Artificial Intelligence Anurag University, Hyderabad, Telangana 500088, India
Email: mallikarjunreddycse@cvsr.ac.in **ORCID:** 0000-0002-8665-9804

Article Info:

DOI: 10.22399/ijcesen.535
Received : 19 October 2024
Accepted : 23 October 2024

Keywords:

Distributed Hash Tables(DHTs)
Skip Lists
Delegated Proof of Stake
Attribute-Based Access Control
Adaptive filters

Abstract:

This paper presents a scalable, secure blockchain-based healthcare system architecture that efficiently manages large patient datasets. DHTs and Skip Lists enable efficient data access, while DPoS and PBFT facilitate parallel transaction processing. Adaptive filters, Radix Trees extended by Merkle Trees, and an immutable blockchain ledger secured by Tendermint consensus ensure data integrity and protection against evolving threats. Threshold Cryptography secures consensus participant selection, and Bulletproofs verify transactions, complying with healthcare regulations. ChaCha20, a symmetric stream cipher, encrypts sensitive data, enhancing performance across devices. ABAC manages access rights, ensuring fine-grained control over data accessibility. This architecture offers a comprehensive, efficient, and secure solution for healthcare data management in blockchain environments.

1. Introduction

Healthcare systems worldwide are grappling with the challenge of securely and efficiently managing vast amounts of patient data. Traditional centralized systems have proven inadequate in addressing these concerns, leading to a growing interest in blockchain technology as a potential solution [1], [2],[3], [6]. While public blockchain networks offer decentralization, they often fall short in terms of scalability, privacy, and regulatory compliance within the healthcare sector [4], [9]. In response to these limitations, permissioned blockchain solutions have emerged as a promising alternative for healthcare applications [5], [8].

These systems provide controlled access, allowing only authorized participants to join the network and validate transactions. This feature ensures enhanced privacy protection and compliance with stringent healthcare regulations [2], [7], [15]. Moreover, permissioned blockchains can achieve higher transaction throughput and lower latency compared to their public counterparts, making them more suitable for handling large volumes of patient data [6], [10].

Despite these advantages, existing blockchain implementations in healthcare still face challenges in scalability and security when dealing with extensive patient datasets [11], [14]. To address these issues, this paper proposes a novel, scalable, and secure blockchain-based architecture specifically designed for managing large patient datasets in healthcare settings [13], [18]. The proposed system leverages various advanced technologies to enhance performance, security, and compliance with healthcare regulations [19].

This paper is organized as follows: Section II provides a literature review of blockchain applications for healthcare [12], [17]. Section III presents the proposed system, outlining its key features and objectives [22]. Section IV describes the implementation methodology. Section V details the experimental setup. Section VI presents the results of the evaluation. Finally, Section VII concludes the paper and outlines future research directions.

2. Literature Review

The integration of blockchain technology in healthcare has emerged as a significant area of research and development, offering potential solutions to longstanding challenges in the sector. Blockchain's key features, including decentralized storage, authentication, distributed ledger, and immutability, make it well-suited to address strict healthcare legislative requirements, such as the 1996 HIPAA Act [10][21]. When integrated with healthcare cyber-physical systems (H-CPS), blockchain provides benefits such as device identification, authentication, integrity, and non-repudiation [14].

Blockchain is transforming healthcare delivery systems by enhancing operational efficiency and patient care [1]. However, implementation faces legal and regulatory challenges. Yaacob [2] highlights the complexities of regulating innovative technologies like distributed ledger technology (DLT) and blockchain in healthcare, emphasizing the need for robust legal frameworks. Min et al. [3] provide a comprehensive review of blockchain technology research and applications, identifying trends that suggest its potential for improving data integrity and security in healthcare.

Ali et al. [4] explore the integration of blockchain with hybrid deep learning to enhance security and scalability in healthcare systems. Ribitzky et al. [5] emphasize the importance of an interdisciplinary approach to blockchain implementation in healthcare, advocating for stakeholder collaboration. This collaborative approach is crucial for addressing multifaceted challenges, including supply chain management. Miah [19] offers insights into blockchain's role in enhancing transparency and traceability in the healthcare supply chain, particularly in pharmaceutical distribution.

Singh [15] proposes using blockchain technology to improve patient consent management, addressing critical ethical considerations in healthcare data management and enhancing patient autonomy. However, Ramzan et al. [9] identify significant barriers to blockchain adoption in healthcare, including technical hurdles and resistance to change. Llambias et al. [12] highlight the need for interoperability in blockchain systems, discussing gateway-based solutions for bridging various blockchain networks.

Scalability remains a challenge in blockchain-based healthcare systems due to the large volume of data generated by IoMT devices. To address this, innovative approaches like the combination of PUF, blockchain, and Tangle have been proposed, providing decentralized access control and security in H-CPS with minimal energy requirements, data storage, and response time [25]. Tandon et al. [16] present a framework for future research on blockchain in healthcare, calling for focused studies on user adoption, integration strategies, and long-term implications of blockchain technologies.

The literature review reveals that blockchain technology offers significant potential for addressing key challenges in healthcare data management, including security, privacy, and interoperability. However, several barriers to widespread adoption remain[25]. The proposed architecture in this paper aims to address these challenges by integrating advanced technologies like Distributed Hash Tables, Skip Lists, and hybrid consensus mechanisms to create a scalable and secure framework for managing electronic health records.

This novel approach combines the benefits of permissioned blockchain with innovative data structures and cryptographic techniques to enhance scalability, security, and efficiency. The use of ChaCha20 encryption, Bulletproofs for transaction verification, and Attribute-Based Access Control aligns with healthcare regulatory requirements while optimizing performance across diverse devices.

While the proposed system shows promise, further research is needed to evaluate its real-world performance, implementation costs, and integration challenges with existing healthcare IT infrastructure. Future studies should focus on practical adoption strategies and empirical assessment in diverse healthcare settings to fully realize the potential of blockchain technology in healthcare.

3. Proposed system

The proposed paper presents a comprehensive and innovative approach to managing electronic health records (EHRs) using permissioned blockchain technology[18]. The architecture combines advanced technologies to create a scalable, secure, and efficient framework for healthcare data management. Key features include scalability through Distributed Hash Tables (DHTs) and Skip Lists, multi-layered security measures using blockchain, Tendermint consensus, Threshold Cryptography, and Bulletproofs, and enhanced efficiency via Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT)[25]. Data integrity is ensured through adaptive filters, Radix Trees extended by Merkle Trees, and the immutable blockchain ledger. The system is designed for compliance with healthcare regulations, incorporating Bulletproofs for transaction verification and Attribute-Based Access Control (ABAC) for access management. Performance is optimized using ChaCha20 for encrypting sensitive data across various devices. This architecture addresses key challenges in healthcare data management, including scalability, security, regulatory compliance, and efficiency. It offers a promising solution for revolutionizing EHR management and sharing.

However, to fully assess the effectiveness of this proposed system, it would be important to see detailed performance metrics, real-world testing results, and comparisons with existing systems. Additionally, considerations such as implementation costs, training requirements for healthcare professionals, and potential integration challenges with existing healthcare IT infrastructure would need to be addressed for practical adoption.

4. Proposed Architecture

The proposed architecture for a scalable, secure, and efficient framework for sharing electronic health records using permissioned blockchain technology comprises the following components: Data acquisition and pre-processing involve IoT devices collecting patient data, which is then processed using adaptive filters. Data security is ensured through the ChaCha20 symmetric stream cipher, which encrypts the processed data.

For blockchain integration, the encrypted data is transformed into blockchain transactions and submitted to the permissioned blockchain network. Consensus and block creation are facilitated by Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT), allowing for parallel transaction processing. Consensus participants are selected using Threshold Cryptography, and a leader node chosen through PBFT collects valid transactions and creates a new block. Data integrity and verification are maintained using Bulletproofs for transaction verification and Radix Trees extended by Merkle Trees. The new block is then appended to the immutable blockchain ledger, secured by Tendermint consensus. Finally, data access and management are achieved through Distributed Hash Tables (DHTs) and Skip Lists for efficient data access, while Attribute-Based Access Control (ABAC) manages fine-grained access rights. This architecture combines various technologies to create a robust and secure system for electronic health record sharing.

4.1 Chacha20 Encryption

ChaCha20 is utilized as the symmetric stream cipher to encrypt sensitive patient data, ensuring confidentiality by encrypting processed information before its conversion into blockchain transactions. A 256-bit encryption key is employed for high security, while a 96-bit nonce prevents vulnerabilities from nonce reuse.

ChaCha20's efficiency across various devices is crucial in healthcare settings with diverse equipment. As a stream cipher, it encrypts data bit by bit, making it suitable for real-time encryption of continuous data from IoT healthcare devices.

The encryption is integrated into the data acquisition and pre-processing stage. ChaCha20's efficiency and security align with other advanced system technologies like Distributed Hash Tables and Attribute-Based Access Control.

It helps meet healthcare privacy and security regulations with robust encryption, enhancing security measures while maintaining efficiency—key requirements for managing sensitive patient data in electronic health records.

4.2 Consensus Mechanism

The consensus mechanism in the architecture for managing electronic health records with permissioned blockchain technology utilizes a hybrid approach combining Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT). This combination allows for parallel transaction processing, enhancing overall system efficiency. The approach incorporates stakeholder voting for delegates, ensures agreement among nodes even in the presence of malicious actors, and provides strong consistency and finality for transactions. Additionally, the system employs Tendermint consensus to secure the immutable blockchain ledger and uses threshold cryptography to enhance resistance to attacks. This hybrid consensus mechanism is designed to balance security, efficiency, and scalability in managing electronic health records on a permissioned blockchain network.This hybrid approach follows a structured process: Block proposal: A node proposes a new block containing electronic health record transactions. Delegate validation: Elected delegates vote to validate the proposed block, ensuring its accuracy and compliance with network rules. Network integrity check: The network verifies the integrity of participating nodes to detect any malicious activity. Block finalization: If no invalid block is detected, nodes send prepare and commit messages to finalize the block and add it to the blockchain. Malicious node handling: If an invalid block is detected, the responsible node is flagged as malicious, a new primary node is elected, and the consensus process restarts. This hybrid approach balances security, efficiency, and decentralization in managing electronic health records on a permissioned blockchain. It provides a robust framework for maintaining data integrity, ensuring consensus among network participants, and protecting sensitive health information. Data acquisition and pre-processing involve IoT devices collecting patient data, which is then processed using adaptive filters. Data security is ensured through the ChaCha20 symmetric stream cipher, which encrypts the processed data. For blockchain integration, the encrypted data is transformed into blockchain transactions and submitted to the permissioned blockchain network. Consensus and block creation are facilitated by Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT), allowing for parallel transaction processing. Consensus participants are selected using Threshold Cryptography, and a leader node chosen through PBFT collects valid transactions and creates a new block. Data integrity and verification are maintained using Bulletproofs for transaction verification and Radix Trees extended by Merkle Trees. The new block is then appended to the immutable blockchain ledger, secured by Tendermint consensus.

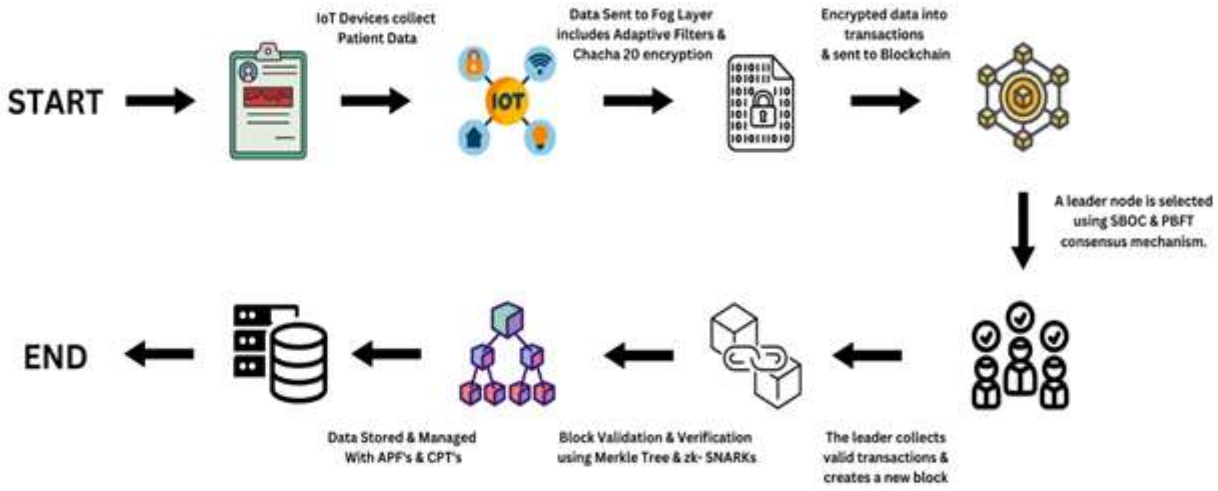

START
IoT Devices collect Patient Data
IOT
Data Sent to Fog Layer includes Adaptive Filters & Chacha 20 encryption
Encrypted data into transactions & sent to Blockchain
A leader node is selected using SBOC & PBFT consensus mechanism.
The leader collects valid transactions & creates a new block
Block Validation & Verification using Merkle Tree & zk- SNARKs
Data Stored & Managed With APF's & CPT's
END

Figure1: *Proposed Flow Diagram*

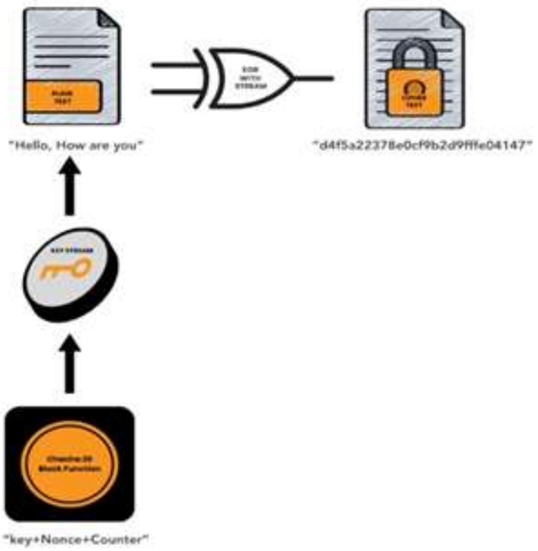


Figure 2: *Chacha 20 Flow diagram*

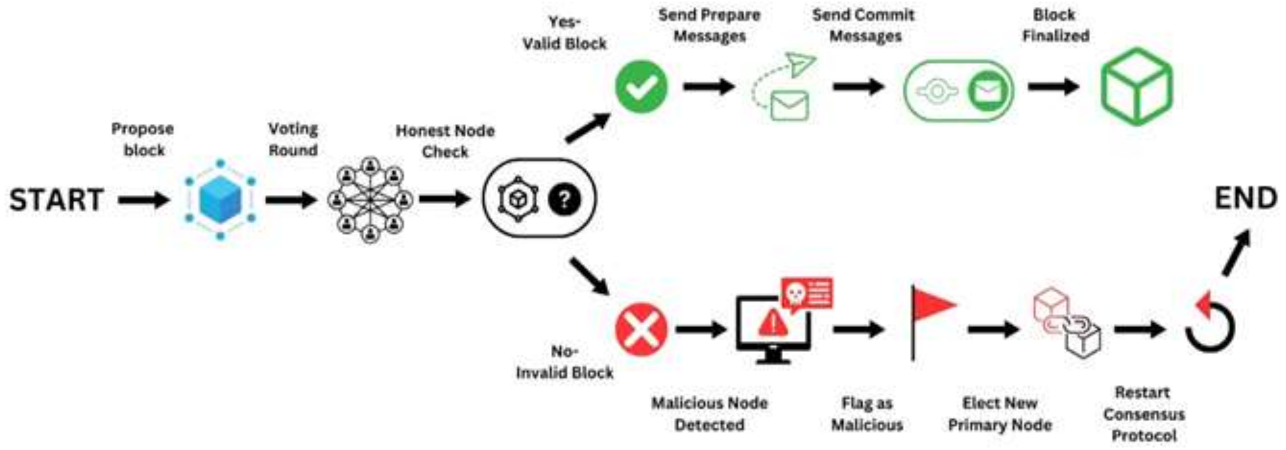


Figure. 3 *A -Isolate Malicious Node*

Implementation

The proposed blockchain healthcare system is implemented using the Go programming language to ensure high efficiency and concurrency.Here's an algorithm considering various variables for the described process:

Algorithm: Secure IoT Data Collection and Blockchain Integration

Input:

- IoT_Devices: Set of IoT devices collecting patient data
- Encryption_Key: 256-bit ChaCha20 encryption key
- Nonce: 96-bit nonce for ChaCha20
- ECDSA_PrivateKey: Private key for transaction signing
- Validator_Set: Set of network validators
- Stake_Scores: Stake scores for validators
- Reputation_Scores: Reputation scores for validators
- T: Threshold for t-of-n cryptography
- N: Total number of validators
- Block_Size: Maximum number of transactions per block
- State_Trie: Current state trie
- DHT: Distributed Hash Table
- ABAC_Policies: Attribute-Based Access Control policies

Output:

- Updated blockchain state
- Processed and stored patient data

Variables:

- raw_data: Raw data collected from IoT devices
- processed_data: Data after noise reduction and signal enhancement
- encrypted_data: Encrypted patient data
- transaction: Blockchain transaction containing encrypted data
- block: Proposed block of transactions
- validator_votes: Votes from validators on block acceptance
- access_request: Request for data access

Procedure:

```
1. For each device in IoT_Devices:
   raw_data = CollectData(device)
   processed_data = ProcessData(raw_data)
   encrypted_data = EncryptData(processed_data, Encryption_Key, Nonce)
   transaction = CreateTransaction(encrypted_data)
   SignTransaction(transaction, ECDSA_PrivateKey)
   BroadcastTransaction(transaction)
2. selected_validators = SelectValidators(Validator_Set, Stake_Scores, Reputation_Scores, T, N)
3. block_producer = SelectBlockProducer(selected_validators)
4. While True:
   transactions = CollectTransactions(Block_Size)
   block = CreateBlock(transactions, State_Trie)
   ProposedBlock(block, block_producer)
For each validator in selected_validators:
 validator_votes[validator] = VerifyAndVoteOnBlock(block, validator)
   If CountPositiveVotes(validator_votes) >= (2N + 1) / 3:
      FinalizeBlock(block)
      UpdateStateTrie(State_Trie, block)
      UpdateDHT(DHT, block)
5. For each access_request:
   If EvaluateABACPolicy(access_request, ABAC_Policies):
      GrantAccess(access_request)
   Else:
      DenyAccess(access_request)
```

```
6. ContinuouslyMonitor(SystemHealth, Performance, SecurityEvents)
7. PerformRollingUpgrades()
```

This algorithm outlines the main steps and variables involved in the process, from data collection to blockchain integration and access control. It includes considerations for encryption, consensus mechanisms, data storage, and system maintenance.

5. Experimental Setup

Blockchain Structure:	**Encryption**	**Data storage**
- Initial blocks: 1000 - Block generation rate: 1 block every 10 seconds - Experiment duration: 24 hours - Total blocks: Approximately 8600 - Transactions per block: Up to 100 - Total transactions: Approximately 864,000	- Algorithm: ChaCha20 symmetric stream cipher - Key size: 256-bit - Nonce: 96-bit, unique for each encryption operation	- Distributed Hash Tables (DHTs) - Skip Lists
	Consensus Mechanism	**Access control**
	- Validator selection: Delegated Proof of Stake (DPoS) - Consensus algorithm: Practical Byzantine Fault Tolerance (PBFT)	- Attribute-Based Access Control (ABAC)

6. Results

The cumulative number of healthcare transactions processed over a 24-hour period using a blockchain system is illustrated in Figure 1. The graph demonstrates a consistent upward trend, with an average processing rate of approximately 36,000 transactions per hour. At the 20-hour mark, the system had successfully processed around 720,000 transactions. This visualization underscores the blockchain's high-throughput capability and its ability to maintain consistent performance in managing healthcare transactions. Figure 2 illustrates the performance metrics of a blockchain-based healthcare system over a 24-hour period. The system demonstrates exceptional results (>99%) in four key areas: security, compliance, data integrity, and consensus efficiency. However, the remaining four metrics—scalability, efficiency, performance, and access control—show varying degrees of effectiveness, with percentages ranging from 0.5% to 50%, suggesting potential areas for system enhancement.

7. Conclusion

This paper presents a novel framework for managing electronic health records using permissioned blockchain technology. The proposed architecture addresses critical challenges in healthcare data management by integrating advanced technologies to create a scalable, secure, and efficient system. Key components of the framework include Distributed Hash Tables, Skip Lists, Delegated Proof of Stake, Practical Byzantine Fault Tolerance, adaptive filters, Radix Trees extended by Merkle Trees, Threshold Cryptography, Bulletproofs, ChaCha20 encryption, and Attribute-Based Access Control. The proposed system offers several significant advantages for healthcare data management, including improved scalability for handling large patient datasets, enhanced security measures tailored to sensitive healthcare data, regulatory compliance with healthcare privacy and security standards, and increased efficiency in data access and transaction processing. While the framework shows promise for revolutionizing EHR management, it is important to acknowledge the limitations of this study. Further research is needed to assess the system's real-world performance, implementation costs, and integration challenges with existing healthcare IT infrastructure. Future studies should focus on practical adoption strategies and empirical evaluation of the proposed architecture in diverse healthcare settings. The cumulative number of healthcare transactions processed over a 24-hour period using a blockchain system is illustrated in Figure 1. The graph demonstrates a consistent upward trend, with an average processing rate of approximately 36,000 transactions per hour. At the 20-hour mark, the system had successfully processed around 720,000 transactions. This visualization underscores the blockchain's high-throughput capability and its ability to maintain consistent performance in managing healthcare transactions. Figure 2 illustrates the performance metrics of a blockchain-based healthcare system over a 24-hour period. The system demonstrates exceptional results (>99%) in four key areas: security, compliance, data integrity, and consensus efficiency. However, the remaining four metrics—scalability, efficiency, performance, and access control—show varying degrees of effectiveness, with percentages ranging from 0.5%

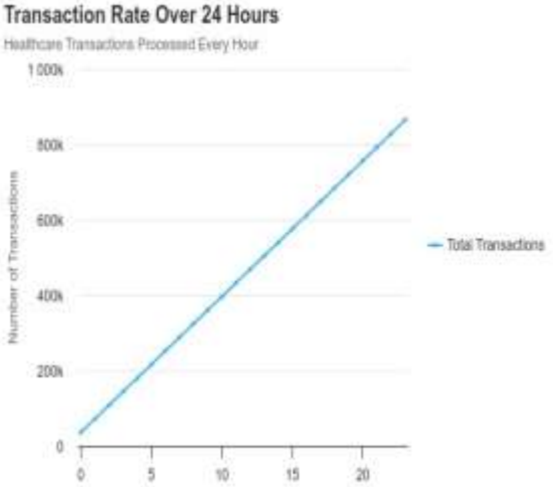


Figure 1. *The cumulative number of healthcare transactions processed over a 24-hour period.*

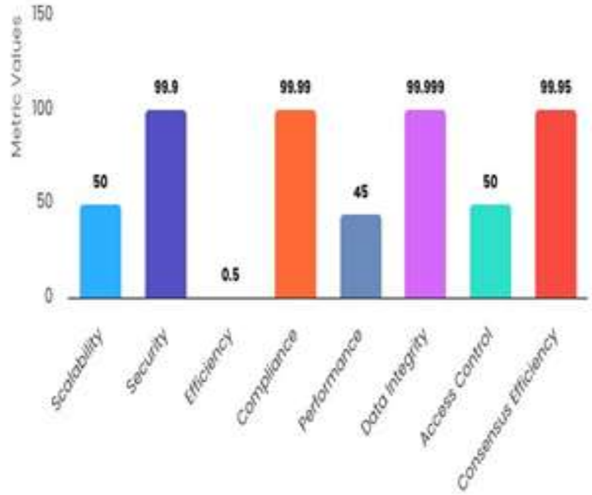


Figure 2 *illustrates the performance metrics of a blockchain-based healthcare system over a 24-hour period.*

to 50%, suggesting potential areas for system enhancement.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] A. Alhur, (2024). Impact of technological innovations on healthcare delivery: A literature review of efficiency, patient care, and operational challenges," *World Journal of Biology Pharmacy and Health Sciences*, 18(2):216–219, doi: 10.30574/wjbphs.2024.18.2.0273.

[2] H. Yaacob, (2021). Legal Issues In Distributed Ledger Technology (DLT) & Blockchain In Brunei Darussalam," *iEco | Islamic Economics Journal*, 1(1);1–24, doi: 10.59202/ieco.v1i1.390.

[3] A. Min *et al.*, (2023). Blockchain Technology Research and Application: A Literature Review and Future Trends. *Journal of Data Science and Intelligent Systems*, doi: 10.47852/bonviewjdsis32021403.

[4] A. Ali *et al.*, (2023). Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning.," *Sensors*, 23(18);7740, doi: 10.3390/s23187740.

[5] R. Ribitzky *et al.*, (2018).Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare, *Blockchain in Healthcare Today* doi: 10.30953/bhty.v1.24.

[6] *Blockchain Technology in Healthcare - Concepts, Methodologies, and Applications*. bentham science, 2023. doi: 10.2174/97898151651971230101.

[7] M. Ramachandran, Phd, (2023). S3EF-HBCAs: Secure and Sustainable Software Engineering Framework for Healthcare Blockchain Applications., *Blockchain in Healthcare Today*, 6(2);, doi: 10.30953/bhty.v6.286.

[8] S. Koul and T. Krishna, (2022). Introduction to Blockchain Technology and Its Role in the Healthcare Sector," crc, pp. 55–80. doi: 10.1201/9781003166511-4.

[9] S. Ramzan, A. Aqdus, R. Amin, D. Koundal, V. Ravi, and M. A. Al Ghamdi, (2023). Healthcare Applications Using Blockchain Technology: Motivations and Challenges," *IEEE Transactions on Engineering Management*, 70(8);2874–2890, doi: 10.1109/tem.2022.3189734.

[10] P. S. Aithal and E. Dias, (2021). Innovations in the Healthcare Industry Using Blockchain Technology, *igi global*,48–83. doi: 10.4018/978-1-7998-9606-7.ch003.

[11] S. M. N. Sakib, (2022). Adaption Of Blockchain Technology In Healthcare Supply Chain In Saudi Arabia. . doi: 10.33767/osf.io/g4wst.

[12] G. Llambias, R. Ruggia, L. González, J. Nogueira, and B. Bradach, (2023). Gateway-based Interoperability for Distributed Ledger Technology," *CLEI Electronic Journal*, 26(2), doi: 10.19153/cleiej.26.2.5.

[13] A. Shaikh, P. Ahire, K. Shewale, G. Shelke, M. Lokhande, and A. Sawalkar, (2023). Drug Tracing In Healthcare Supply Chain Using Distributed Ledger Technology, doi: 10.1109/icidca56705.2023.10100033.

[14] H. Yu, Q. Fan, M. An, and H. Zhao, (2023). Blockchain technology research and application: a systematic literature review and future trends. doi: 10.48550/arxiv.2306.14802.

[15] A. Singh, (2024). Enhancing Patient Consent Management through Blockchain Technology: A Promising Approach for Healthcare Data Security, *Interantional Journal Of Scientific Research In Engineering And Management*, vol. 08(3);1–5, doi: 10.55041/ijsrem29509.

[16] A. Tandon, A. Dhir, A. K. M. N. Islam, and M. Mäntymäki, (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda, *Computers in Industry* 122;103290, doi: 10.1016/j.compind.2020.103290.

[17] N. Kannengießer, A. Sunyaev, M. Pfister, M. Greulich, and S. Lins, (2020). Bridges Between Islands: Cross-Chain Technology for Distributed Ledger Technology, *Proceedings of the 53rd Hawaii International Conference on System Sciences*. DOI:10.24251/hicss.2020.652

[18] Y. Khan, A. Kashyap, L. Maini, V. Bajaj, S. Arora, and A. Yadav, (2022). Blockchain Technology in Healthcare, *MAMC Journal of Medical Sciences*, 8(3);187–192, doi: 10.4103/mamcjms.mamcjms_26_22.

[19] M. Miah, (2023). A Comprehensive Study on the Use of Blockchain Technology in Healthcare, *Information Technology and Management Science*, 26;1–9, doi: 10.7250/itms-2023-0001.

[20] H. Saeed *et al.*, (2022). Blockchain technology in healthcare: A systematic review. *PLOS ONE*, 17(4);e0266462, doi: 10.1371/journal.pone.0266462.

[21] M. A. Dwi Yuda and S. Watini, (2023). Implementation of Blockchain Technology as the Latest Solution to Improve Data Security and Integrity, *International Transactions on Education Technology (ITEE)*, 2(1);71–82, doi: 10.33050/itee.v2i1.418.

[22] Y. M. Alkhateeb, (2021). Blockchain Implications in the Management of Patient Complaints in Healthcare, *Journal of Information Security*, 12(3);212–223, doi: 10.4236/jis.2021.123011.

[23] N. Tyagi, S. Kumar, N. Sharma, S. Gautam, and B. Bhushan, (2022). An Integrated Approach of Blockchain & Big Data in Health Care Sector,” *river*, pp. 183–205. doi: 10.1201/9781003337218-9.

[24] A. J. M. Milne, A. Beckmann, and P. Kumar, (2020). Cyber-Physical Trust Systems Driven by Blockchain, *IEEE Access*, 8;66423–66437,doi: 10.1109/access.2020.2984675.

[25] V. K. V. V. Bathalapalli, E. Kougianos, S. P. Mohanty, B. Rout, and V. Iyer, (2024). PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in Healthcare Cyber-Physical Systems., *Sensors*, 24(3);938, doi: 10.3390/s24030938.

[26] Prasanth Rao, Adiraju & Reddy, K. & Velayutham, Sathiyamoorthi. (2021). *Automated Soil Residue Levels Detecting Device With IoT Interface*. 10.4018/978-1-7998-2566-1.ch007.

[27] K. Sudheer Reddy, G. P. S. Varma and S. S. S. Reddy, (2012). Understanding the scope of web usage mining & applications of web data usage patterns, *2012 International Conference on Computing, Communication and Applications, Dindigul, India*, pp. 1-5, doi: 10.1109/ICCCA.2012.6179230.

[28] C. N. S. Kumar et al., (2019). Similarity matching of pairs of text using CACT algorithm, *Int. J. Eng. Adv. Technol.*, 8(6);2296-2298, doi:10.35940/ijeat.F8685.088619.

[29] C. N. S. Kumar and K. S. Reddy, (2019). Effective data analytics on opinion mining, *IJITEE*, 8(10);2073-2080, doi:10.35940/ijitee.J9332.0881019.

[30] Nabi, S. A., Kalpana, P., Chandra, N. S., Smitha, L., Naresh, K., Ezugwu, A. E., & Abualigah, L. (2024). Distributed private preserving learning based chaotic encryption framework for cognitive healthcare IoT systems. *Informatics in Medicine Unlocked*, 49, 101547. https://doi.org/10.1016/j.imu.2024.101547

[31]A. Mallikarjuna Reddy, V. Venkata Krishna, L. Sumalatha,(2018). Face recognition based on stable uniform patterns. *International Journal of Engineering & Technology*, 7(2);626-634, 2018,doi: 10.14419/ijet.v7i2.9922

[32]Sudeepthi Govathoti, A Mallikarjuna Reddy, Deepthi Kamidi, G BalaKrishna, Sri Silpa Padmanabhuni and Pradeepini Gera, (2022). Data Augmentation Techniques on Chilly Plants to Classify Healthy and Bacterial Blight Disease Leaves. *International Journal of Advanced Computer Science and Applications(IJACSA)*, 13(6). http://dx.doi.org/10.14569/IJACSA.2022.0130618

[33]Swarajya Lakshmi V Papineni, Snigdha Yarlagadda, Harita Akkineni, A. Mallikarjuna Reddy. (2023). Big Data Analytics Applying the Fusion Approach of Multicriteria Decision Making with Deep Learning Algorithms. *International Journal of Engineering Trends and Technology*, 69(1), 24-28, doi: 10.14445/22315381/IJETT-V69I1P204

[34]A Mallikarjuna Reddy, Vakulabharanam Venkata Krishna, Lingamgunta Sumalatha and Avuku Obulesh, (2020). Age Classification Using Motif and Statistical Features Derived On Gradient Facial Images”, *Recent Advances in Computer Science and Communications* 13;965. https://doi.org/10.2174/2213275912666190417151247.

[35]A.Mallikarjuna, B. Karuna Sree, (2019). Security towards Flooding Attacks in Inter Domain Routing Object using Ad hoc Network. *International Journal of Engineering and Advanced Technology (IJEAT)*, 8(3).