International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Improving Blockchain Security: Integrating Encryption and Hashing Techniques

Ankita Srivastava[1*], Shish Ahamad[2]

Submitted: 03/05/2024 **Revised**: 16/06/2024 **Accepted**: 23/06/2024

Abstract: In real-time systems, the maintenance of patient records and identity management has become increasingly crucial for efficient record-keeping. This study delves into the potential of blockchain technology to bolster data protection. The primary goal is to suggest enhancements through the utilization of hashing and encryption approaches. Under this methodology, each record functions as an operation, with all blockchain transactions securely recorded in a public ledger. The inclusion of data encryption before blockchain storage offers an additional layer of security, currently under scrutiny. The hashing algorithm is employed to further fortify blockchain security. Hashing & encryption are fundamental modules of blockchain, ensuring data confidentiality, legitimacy, and permanence within the distributed ledger. Encryption converts sensitive data into ciphertext, accessible solely with the appropriate cryptographic key, thereby thwarting unauthorized entry. The security of blockchain technology relies on the collaboration between hashing and encryption, providing robust protection against data manipulation and unauthorized entry while upholding the distributed ledger's integrity. This research assesses security and performance enhancements by examining error rates, efficiency, precision, and security protocols. Performance is gauged in terms of time, security is analyzed by identifying external attacks on blocks, and accuracy is evaluated using metrics like recall, precision, and F1-score.

Keywords: *Data protection, Encryption methods, Hashing algorithms, EHR (Electronic Health Record), Performance enhancements*

1. Introduction

The rising demand for healthcare apps underscores the need for secure patient data storage [1]. Outdated methods of safeguarding records are being replaced by blockchain technology, offering a modern and robust solution for protecting medical information [2]. Academic institutions and businesses have increasingly explored blockchain over the last decade. This distributed and immutable ledger Blockchain 3.0, currently in development, is gaining traction among early adopters across sectors such as public services, energy, and healthcare. This new generation of blockchain technology aims to eliminate the need for a trusted third party to verify and record transactions [6, 7]. The decentralized nature and inherent privacy and security features of blockchain make it particularly attractive for healthcare providers aiming to enhance patient care [8, 9]. Its design ensures that only authorized individuals can access sensitive medical data [10]. Originally introduced as part of the Bitcoin protocol, the blockchain acts as a distributed ledger where all network transactions are securely recorded and verified [11, 12]. Each block consists of a header and a body, with the header containing the previous block's hash, forming a connected chain [12]. Tools like Merkle trees, timestamps, and nonce in block headers facilitate efficient transaction analysis and processing [13].

Miners can adjust the nonce to solve mathematical challenges. A blockchain transaction, a basic work unit, is stored in a block and involves two participants [14]. System users' majority approval is required for validation. Once a transaction is recorded, it becomes immutable, ensuring its integrity [15]. This immutability results in each participant having a single ledger copy. Smart contracts embedded in the blockchain enable seamless transaction execution, self-verification, and enforcement when all conditions are met [16, 17]. Block chain's decentralized, permanent, accessible, and anonymous attributes make it highly resistant to manipulation [18, 19].

1.1. Role of Data Compression in Streamlining Blockchain Operations

Data compression plays a vital role in minimizing size within blockchain technology. Given that every node in the network holds a copy of the entire distributed ledger, reducing data size is key to improving efficiency and scalability. Employing data compression methods can greatly decrease the storage space needed for transactions, smart contracts, and other blockchain-related data. This size reduction offers multiple advantages, such as quicker data transfer across the network, lower storage demands for each node, and enhanced overall performance [21-24]. As the blockchain expands, effective data compression becomes essential in tackling bandwidth and storage capacity issues [22]. Ultimately, data compression optimizes resource use within the blockchain and enhances

[1*]*Research scholar, Department of CSE Integral University, Lucknow, India. Orcid:0000-0003-4218-287X. Email: ankita@iul.ac.in*
[2]*Professor, Department of CSE Integral University, Lucknow, India, 0000-0002-3347-7724. Email: shish@iul.ac.in*
***Corresponding author:** Ankita Srivastava*
**Email: ankita@iul.ac.in*

its capacity to scale effectively in various practical applications. [23]

1.2. Hashing in Security of Blockchain Data

1. Deterministic and Secure

Data in blockchain undergoes hashing to produce a fixed-size hash value. This deterministic process ensures identical inputs generate identical outputs, crucial for data consistency and verification. The algorithm is irreversible, enhancing security by making it nearly impossible to reverse-engineer the original data from its hash. Additionally, it's designed to be collision-resistant, ensuring each piece of data has a unique hash, minimizing fraud risks

2. Immutability and Consensus

Blockchain blocks are linked via hashed references, creating an immutable chain where altering any block affects all subsequent ones, reinforcing data integrity. Hash values also underpin consensus mechanisms like Proof of Work, securing transactions by validating them across the network through computationally intensive hashing.

3. Digital Signatures

Hash values are integral to digital signatures in blockchain transactions. Senders sign transaction hashes with private keys, and recipients verify these signatures with corresponding public keys, ensuring transaction authenticity and integrity. Hashing is pivotal in blockchain, providing robust security and integrity mechanisms that safeguard decentralized systems against tampering and fraud, ensuring trust and reliability.

1.3. Factors Affecting Transaction Performance on Blockchain

When transactions happen on a blockchain, a few things really impact how well they work. Making these factors work smoothly is key to keeping the network running efficiently and able to handle more activity. Let's explore what really affects how transactions perform:

1. **Blockchain Consensus Mechanism:** The choice of how we agree on transactions makes a big difference in how fast they go. For instance, Proof of Work (PoW) involves solving complex puzzles, which can slow down transaction confirmations. In contrast, Proof of Stake (PoS) and other methods can make confirmations happen quicker.
2. **Block Size and Block Time:** The size of blocks and how long it takes to create a new one are really important. Bigger blocks can fit more transactions but need more resources to check and share. On the other hand, shorter times between blocks mean faster confirmations, though it might lead to more chances for problems like forks.
3. **Transaction Throughput:** This tells us how many transactions a blockchain can handle at once. More throughput is crucial for growing smoothly, as blockchain networks must handle more users and transactions over time.
4. **Node Scalability:** The number of computers (nodes) in a blockchain affects how well it grows. Adding more nodes can spread out the work and make things more fair, but it can also slow things down. Ways to handle this, like sharding or layer 2 ideas, help make sure everything runs smoothly even with more nodes.
5. **Security Measures:** The security level within the blockchain network, including the robustness of cryptographic algorithms, influences the time taken for transaction validation and confirmation. It is crucial to balance security and performance; as high fees may deter users.

2. Literature Review:

Blockchain has gained significant attention over the past decade as a revolutionary technology, extensively studied across academic and industrial sectors including government, energy, and healthcare. It functions as a decentralized and immutable ledger, eliminating the need for intermediaries to verify and record transactions. This advancement, sometimes referred to as Blockchain 3.0, is currently in development by multiple organizations with the promise of significantly improving patient care. Its decentralized architecture, bolstered by robust privacy and security features, makes it particularly attractive for healthcare applications by ensuring that only authorized personnel have access to sensitive medical information.

The concept of blockchain originated in 2008 through the Bitcoin protocol, designed as a chain of blocks where each transaction is securely recorded and validated. Techniques like Merkle trees, timestamps, and nonces within block headers streamline transaction processing and reduce manual oversight. The immutable nature of blockchain ensures that once a transaction is recorded, it cannot be altered, thereby ensuring trustworthiness. Smart contracts embedded in blockchain automate business logic execution, enabling self-verification and enforcement of predefined conditions. Blockchain technology is valued for its decentralization, durability, accessibility, and anonymity, offering robust resistance against tampering and unauthorized manipulation.

Recent research underscores blockchain's relevance in healthcare, focusing on its ability to address challenges in data transmission and privacy. Griggs et al. [1] propose blockchain-based smart contracts for secure management of Protected Health Information (PHI) from medical

sensors. Radanović and Likić [2] demonstrate blockchain's utility in recording transactions across decentralized networks, while Calvaresi et al. [3] explore its application in enhancing transparency within MAS-based distributed systems handling sensitive data. Zhang and Lin [4] highlight blockchain's role in improving diagnostic accuracy through secure online medical data collaboration. Liang et al. [5] discuss blockchain's use in safeguarding privacy in wearable technology, and Miraz and Ali [6] explore its integration into IoT environments. Firdaus et al. [7] address security issues related to blockchain and Android mobile devices, while Li et al. [8] showcase advancements in medical record management using blockchain-based Distributed Ledger Systems (DPS). Epiphaniou et al. [9] predict widespread benefits of distributed ledger technology across various sectors, including ongoing healthcare pilot projects. Zhou et al. [10] propose a closed-loop approach to managing chronic diseases with blockchain-enabled electronic health records, while Iram et al. [11] analyze the environmental impact of energy consumption. Rathee et al. [12] investigate multimedia methods for enhancing data exchange and analysis in healthcare across diverse mobile platforms. Collectively, these studies illustrate blockchain's potential to revolutionize healthcare and other sectors by improving security, efficiency, and transparency. Ongoing advancements and future applications underscore the transformative impact of blockchain technology.

3. Problem Statement

Ensuring the security of healthcare data is paramount, prompting numerous projects within the industry to explore blockchain technology for storing patient information [13-18]. While traditional methods address healthcare data security, they often fall short in terms of performance. Current research on blockchain in healthcare remains relatively nascent, leaving much untapped potential.

4. Proposed Work

The proposed study focuses on researching blockchain security and its applications in healthcare, emphasizing security and performance issues. The investigation aims to safeguard patient information from unauthorized access. Recent advancements offer promising methods to enhance both blockchain security and operational efficiency in healthcare applications. A comparative analysis between recommended and traditional models will assess the performance and security levels of the proposed blockchain model within healthcare settings. Initial steps involve compressing healthcare datasets to optimize storage efficiency and data security.

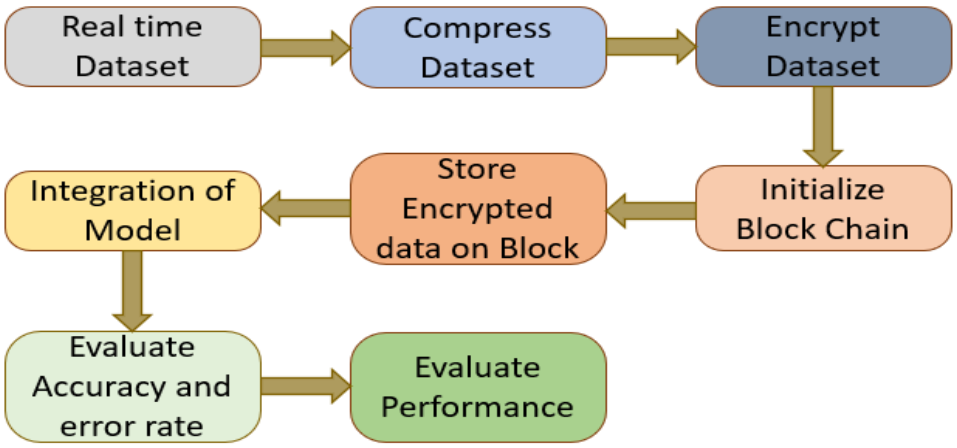

Fig 1. Security Model Proposed

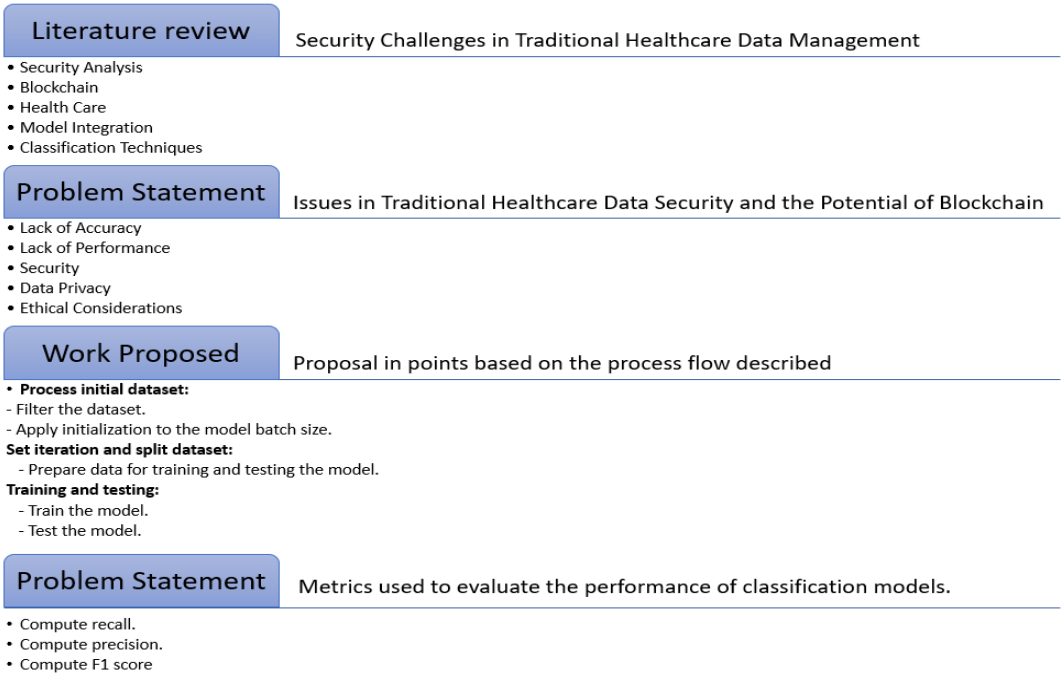

Fig 2. Research Methodology of the Proposed Work

5. OUTCOMES AND INTERPRETATION:

In this study, we compared several different deep learning models to see which one predicts the best. For the conventional approach, Table 1 shows how well each model did with measures like precision, recall, F1 score, and support. The traditional deep learning model achieved an accuracy of 96.33%, which is great for healthcare security. In Table 2, we see the results of our proposed approach, which also achieved an accuracy of 97.5%. This shows that our new method is providing even better accuracy compared to the conventional model.

Table 1. Performance Metrics of Traditional Method

	Precision	**Recall**	**F1-Score**	**Support**
Redesign	0.92	0.91	0.91	**311**
Successful	0.97	0.96	0.97	**1850**
Accuracy	-	-	0.96	**2158**
Macro avg.	0.93	0.94	0.94	**2158**
Weighted avg.	**0.94**	**0.94**	**0.94**	**2158**

Confusion Matrix:

	Predicted Redesign	**Predicted Successful**
Actual Redesign	TP=283.01	FN = 27.99
Actual Successful	FP = 148.00	TP = 1794.50

Overall Accuracy: 96.33%

Table 2. Performance Metrics of the Proposed Method

	Precision	**Recall**	**F1-Score**	**Support**
Redesign	0.91	0.92	0.92	320

Successful	0.98	0.98	0.98	1859
Accuracy	-	-	0.975	2175
Macro avg.	0.945	0.95	0.95	2175
Weighted avg.	**0.965**	**0.975**	**0.965**	**2175**

Confusion Matrix:

	Predicted Redesign	**Predicted Successful**
Actual Redesign	TP=293	FN = 25
Actual Successful	FP = 37	TP = 1820

Overall Accuracy: 97.5%

5.1. Comparison of Overall Accuracy

Table 3 presents the overall accuracy metrics between traditional and proposed method works

Conventionalwork	***Proposed work***
96.33	**97.5**

According to Table 3, the overall accuracy for both conventional and proposed works is as follows:

- Conventional Work: 97.95%
- Proposed Work: 99.06%

This table illustrates the comparative accuracy performance between the two approaches.

Comparison of Performance

This section presents a simulation depicting the time required for block processing, offering a detailed analysis. Studies indicate that block processing requires significantly less time compared to traditional methods. Table 4 presents a comparison of processing times between the proposed and traditional approaches.

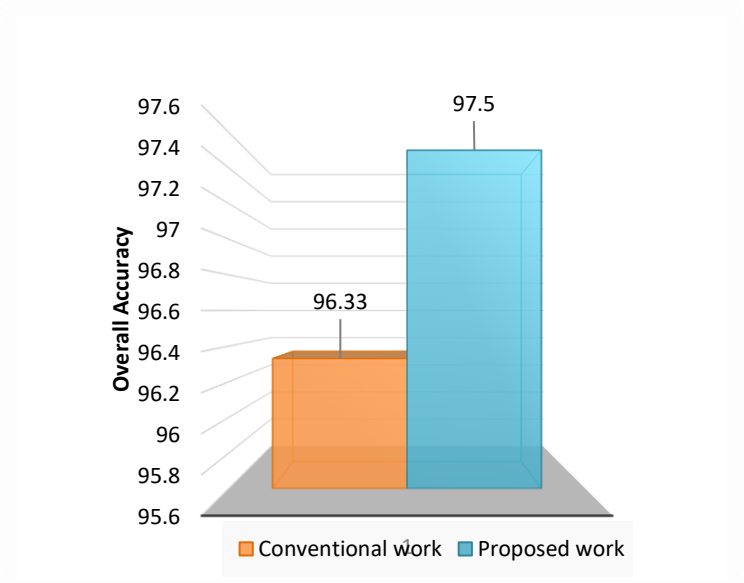

Fig 1: Comparison of accuracy

Table 4: Performance Comparison: Traditional/Conventional vs Proposed Time Taken

No of blocks	Time Taken by Traditional Approach	Time Taken by Proposed Approach
1	0.385	0.281
2	0.52	0.34
d	0.72	0.41
4	0.86	0.53
5	0.99	0.62
6	1.19	1.02
7	1.33	1.19
8	1.44	1.29
9	1.75	1.45
10	1.89	1.66

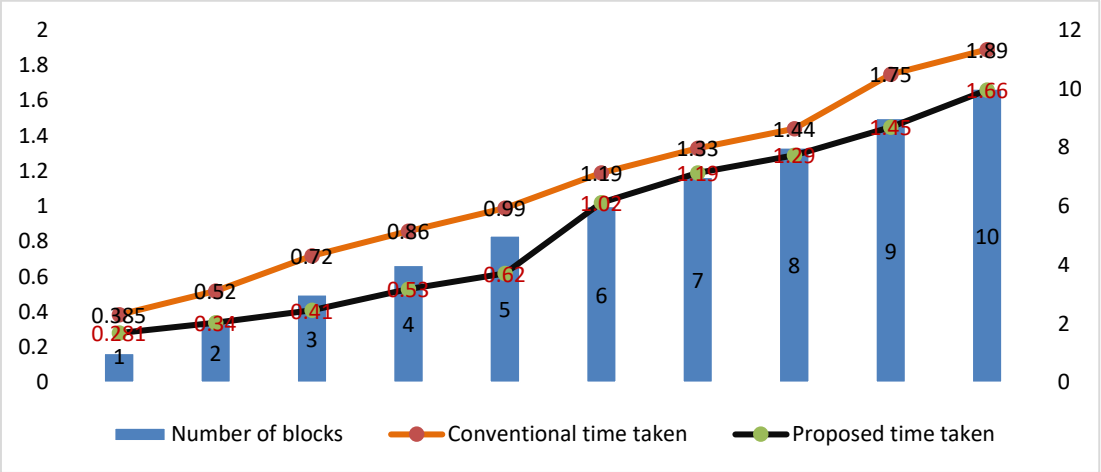

Figure 2: Performance Comparison Traditional / Conventional Vs Proposed

4.2. Comparison of Security

This section examines the impact of external attacks on blocks, specifically comparing the compromised blocks between traditional and proposed methods at regular intervals of 5 blocks. The findings, depicted in Table 5, reveal significantly fewer compromised blocks under the proposed method compared to traditional approaches. This comparative analysis highlights the effectiveness of the proposed method in mitigating external attacks. The study aims to evaluate and compare the processing times between standard and suggested labor methods.

Table 5: Security comparison: Traditional vs Proposed Method

Block	Traditional	Proposed
1	0	0
5	1	0
10	2	1
15	4	2
20	6	3
25	9	4
30	11	7
35	17	9
40	21	12
45	28	15
50	35	18

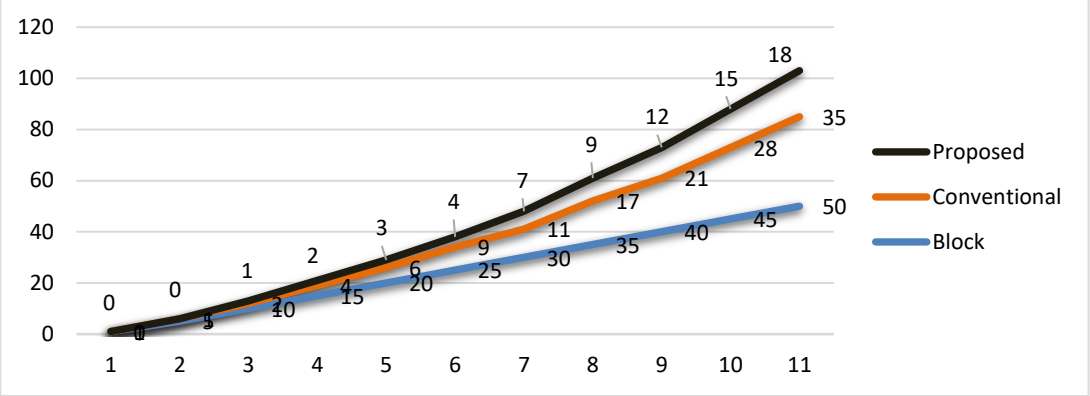

Fig 3: Security comparison Conventional/ Traditional Vs Proposed

5. Conclusion

Researchers are aggressively addressing security challenges in blockchain applications for healthcare, with a focus on protecting personal patient data from theft. Concurrently, they are looking at the performance and security issues that come with blockchain technology. The proposed approach aims to significantly improve the security and speed of blockchain systems. Improving the efficiency of healthcare systems and safeguarding industry applications are critical to assuring reliability. The study compares the suggested model's performance to the safety of traditional models in healthcare situations. Ongoing study continues to investigate security and performance challenges associated with blockchain technology, notably its potential to improve healthcare delivery.

5.1. Research Focus

This study aims to advance blockchain applications' accuracy, performance, and security in real-world scenarios. It focuses on identifying and addressing security vulnerabilities, including external attacks that impact blockchain blocks. Future research will further explore optimization strategies for transactions to enhance accuracy and security.

ACKNOWLEDGMENTS

In accordance with the standards set by university doctoral studies and research, we are pleased to declare the assignment of Manuscript Communication Number [IU/R&D/2024-MCN0002875] to this article. This unique identifier is essential for facilitating effective communication and tracking of our research progress throughout the publication journey. We express our sincere gratitude to Mohd Usman Khan for his invaluable contributions in preparing the original research article and overseeing the analysis. His input has been pivotal in the advancement of this project. We sincerely thank all individuals who have contributed to the development of this work.

References:

[1] K. N. Griggs et al., "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, pp. 1-7, 2018. doi: 10.1007/s10916-018-0982-x.

[2] I. Radanović and R. Likić, "Opportunities for use of blockchain technology in medicine," *Appl. Health Econ. Health Policy*, vol. 16, pp. 583-590, 2018. doi: 10.1007/s40258-018-0412-8.

[3] D. Calvaresi et al., "Multi-agent systems and blockchain: Results from a systematic literature review," in *Adv. Pract. Appl. Agents Multi-Agent Syst. Complex.: PAAMS Collect.*, vol. 16, 2018, pp. 110-126. doi: 10.1007/978-3-319-94580-4_9.

[4] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 140, 2018. doi: 10.1007/s10916-018-0995-5.

[5] X. Liang et al., "Towards decentralized accountability and self-sovereignty in healthcare systems," in *Inf. Commun. Secur.: 19th Int. Conf.*, Beijing, China, 2018, pp. 387-398. doi: 10.1007/978-3-319-89500-0_34.

[6] M. H. Miraz and M. Ali, "Blockchain enabled enhanced IoT ecosystem security," in *Emerg. Technol. Comput.: First Int. Conf.*, London, UK, 2018, pp. 38-46. doi: 10.1007/978-3-319-95450-9_3.

[7] A. Firdaus et al., "Root exploit detection and features optimization: Mobile device and blockchain based medical data management," *J. Med. Syst.*, vol. 42, pp. 1-23, 2018. doi: 10.1007/s10916-018-0966-x.

[8] H. Li et al., "Blockchain-based data preservation system for medical data," *J. Med. Syst.*, vol. 42, pp. 1-13, 2018. doi: 10.1007/s10916-018-0997-3.

[9] G. Epiphaniou et al., "Blockchain and healthcare," in *Blockchain Clin. Trial*, Springer International Publishing, 2019, pp. 1-29. doi: 10.1007/978-3-030-11289-9_1.

[10] T. Zhou et al., "Med-PPPHIS: Blockchain-based personal healthcare information system for national physique monitoring and scientific exercise guiding," *J. Med. Syst.*, vol. 43, pp. 1-23, 2019. doi: 10.1007/s10916-019-1430-2.

[11] S. Iram et al., "Connecting to smart cities: Analyzing energy times series to visualize monthly electricity peak load in residential buildings," in *Proc. Future Technol. Conf. (FTC)*, Springer International Publishing, 2019, pp. 333-342. doi: 10.1007/978-3-030-02686-8_26.

[12] G. Rathee et al., "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimed. Tools Appl.*, vol. 79, no. 15-16, pp. 9711-9733, 2020. doi: 10.1007/s11042-019-07835-3.

[13] I. Abu-Elezz et al., "The benefits and threats of blockchain technology in healthcare: A scoping review," *Int. J. Med. Inform.*, vol. 142, article 104246, 2020. doi: 10.1016/j.ijmedinf.2020.104246.

[14] D. J. Munoz et al., "Clinicappchain: A low-cost blockchain hyperledger solution for healthcare," in *Blockchain Appl.: Int. Congr.*, Springer International Publishing, 2020, pp. 36-44. doi: 10.1007/978-3-030-23813-1_5.

[15] R. M. Amir Latif et al., "A remix IDE: Smart contract-based framework for the healthcare sector by using blockchain technology," *Multimed. Tools Appl.*, pp. 1-24, 2020. doi: 10.1007/s11042-020-10087-1.

[16] A. Mubarakali, "Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach," *Mobile Netw. Appl.*, vol. 25, pp. 1330-1337, 2020. doi: 10.1007/s11036-020-01551-1.

[17] G. Nagasubramanian et al., "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Comput. Appl.*, vol. 32, pp. 639-647, 2020. doi: 10.1007/s00521-018-3915-1.

[18] A. Hasselgren et al., "Blockchain in healthcare and health sciences-A scoping review," *Int. J. Med. Inform.*, vol. 134, article 104040, 2020. doi: 10.1016/j.ijmedinf.2019.104040.

[19] R. Casado-Vara et al., "Cooperative algorithm to improve temperature control in recovery unit of healthcare facilities," in *Int. Symp. Distrib. Comput. Artif. Intell.*, Springer International Publishing, 2018, pp. 49-62. doi: 10.1007/978-3-030-00524-5_8.

[20] M. P. McBee and C. Wilcox, "Blockchain technology: Principles and applications in medical imaging," *J. Digit. Imaging*, vol. 33, pp. 726-734, 2020. doi: 10.1007/s10278-019-00310-3.

[21] M. U. Khan and F. Ahamad, "An Affective Framework for Multimodal Sentiment Analysis to Navigate Emotional Terrains," *Telematique*, vol. 23, no. 01, pp. 70-83, 2024.

[22] A. Srivastava and S. Ahmad, "Bio-Computing Based Algorithms for Cloud Security: A Critical Review," in *2022 IEEE World Conf. Appl. Intell. Comput. (AIC)*, Sonbhadra, India, 2022, pp. 894-900. doi: 10.1109/AIC55036.2022.9848965.

[23] F. Ahmad and M. M. Tripathi, "Approaches of big data in healthcare: a critical review," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 2, pp. 122-127, 2018.

[24] M. U. Khan and F. Ahamad, "Multimodal Data Analysis and Machine Learning Techniques: A Comparison and Review," *NeuroQuantology*, vol. 20, no. 22, pp. 4196-4208, Dec. 2022.