DOI: https://doi.org/10.29070/ew4hyt02

Impact of Blockchain-Based Automation on Healthcare EHR Systems: Efficiency, Scalability, and Patient Outcomes

Basavaraj Halabhavi [1] * , Dr. Neha Surana [2]

1. Research Scholar, Department of Computer Application, University of Technology, Jaipur, Rajasthan, India
b06071984@gmail.com ,
2. Assistant Professor, Department of Computer Application, University of Technology, Jaipur, Rajasthan, India

Abstract: The integration of A revolutionary approach to healthcare systems that use Integrating blockchain technology with hybrid deep learning approaches may improve security, scalability, and patient care. When it comes to storing, distributing, and controlling access to data, blockchain offers a decentralised, transparent architecture that guarantees data integrity, privacy, and interoperability. Hybrid deep learning allows for the efficient and accurate analysis of complicated healthcare data by integrating standard machine learning techniques with deep learning algorithms. This research recommends a permissions-based blockchain design for secure and scalable healthcare systems to guarantee that only permitted individuals may access and modify vital health records. In addition to allowing for the prediction of diseases, treatment suggestions, and prompt diagnoses, the framework allows for the real-time study of massive amounts of healthcare data. Better scalability, security, interoperability, and decision-making are just a few of the many advantages that may be gained by merging hybrid deep learning with blockchain technologies. Complicating factors that must be addressed for implementation to be successful include computational complexity, compliance with regulations, and ethical considerations. With the use of blockchain technology and hybrid deep learning, healthcare institutions can streamline data administration, provide patients with more individualized treatment, and advance medical research. This will allow them to surpass previous limits.

Keywords: Blockchain, Automation, Healthcare , Healthcare Systems, Efficiency, Scalability, Patient

---------------------------X---------------------------

INTRODUCTION

Demands for data security have never been higher due to the fast digitisation of healthcare, which has resulted in the creation of enormous electronic records on patients. Blockchain, a decentralised database that facilitates digital data transactions between the use of P2P networks by users is bringing forth novel opportunities to enhance the confidentiality, authenticity, and security of healthcare data.

Blockchain technology's use has several advantages, one of which is the elimination of middlemen and the promotion of transparency. To ensure that transactions in a trustless and unpredictable environment are legitimate, it employs cryptography and consensus procedures. The receiving node in a blockchain distributed P2P network verifies the message and adds it to a block. Each block's contents are verified using a consensus process called Proof-of-work (PoW).

Addressing issues with data storage, sharing, privacy, and security is a prominent example of a healthcare sector use of blockchain technology. Medical treatment business cannot function without interoperability, which allows for the seamless flow of health-related information, such as electronic health records (EHR), among healthcare providers and patients. This enables providers to securely share patient medical records, regardless of the provider's location and trust relationships between them.

Blockchain technology has shown opportunity for healthcare communities to securely store, monitor, and exchange electronic health records. Healthcare infrastructure and software cost increases have also put a significant strain on global economies. By streamlining operations, boosting compliance, decreasing costs, and facilitating greater utilisation of healthcare-related data, blockchain technology is having a beneficial impact on healthcare outcomes in the healthcare industry.

Several healthcare applications are now investigating blockchain technology, including IoMT security, data management and storage, device connection, and the internet of medical things (IoMT). Everyone from patients and carers to researchers and pharmaceutical and insurance corporations has benefited from the QoE enhancements brought forth by blockchain technology in these domains. To make healthcare smarter, enhance healthcare services, and improve users' experience, it is vital to be able to exchange healthcare data without compromising users' privacy and data security.

LITERATURE REVIEW

Ait Bennacer, Sara et.al. (2022). Many problems with data management, data sharing, data immutability, trust, transparency, information security, and patient privacy are plaguing today's healthcare systems. Furthermore, there are a number of issues brought about by the centralization of the many current healthcare systems, which makes data management for those receiving healthcare as well as those giving it. A decentralized peer-to-peer network, blockchain technology might radically alter several industries, including healthcare. with the ability to digitalize and revolutionise data management. A better overview of current efforts on healthcare applications based on Blockchain is the goal of this study.

Panigrahi, Amrutanshu et.al. (2022). Financial services, supply chain management (SCM) across industries, a network of interconnected physical devices and medical records are just a few of the many areas where blockchain technology is already making a big splash by offering a safe and efficient way to communicate data. Thanks to the HCS app's security features and interoperability, suppliers and patients may exchange data without any hitches. If a patient lacks these characteristics, it shows that they have trouble understanding their own health condition. Therefore, the HCS may become more efficient and effective by integrating blockchain technology, which will address this drawback. The potential advantages of blockchain technology provide the groundwork for its use in several areas of healthcare information systems (HCS), including but not limited to many systems, including electronic health records (EHRs), billing, telemedicine, and EMRs.

Adeghe, Ehizogie et.al. (2024). An innovative paradigm shift is taking place with the blockchain technology has the ability to enhance patient privacy, security, and results when used to healthcare data management. The article starts off by delving into the basics of blockchain technology and how it is currently being used in healthcare. To provide the groundwork for a thorough examination, we focus on the possible advantages and disadvantages of using blockchain technology. Using decentralised architecture and smart contracts for strong access control, the article analyses how blockchain guarantees data integrity and immutability from a security perspective. Discussed further are blockchain's potential effects on patient privacy, particularly its ability to let people keep their health records private and in control. To provide a comprehensive study of the privacy environment, the research also explores regulatory compliance and legal implications. Examining how blockchain improves interoperability, simplifies healthcare operations, and may revolutionise the patient experience is key to understanding the effect on patient outcomes. The beneficial benefits seen in healthcare settings may be better understood via the use of real-world case studies. Nevertheless, in order to fully grasp the revolutionary possibilities, one must first investigate the obstacles and constraints. For a well-rounded look at the challenges to broad blockchain adoption, we cover topics including technical issues, ethical concerns, and the need of seamless connection with current healthcare systems. The article provides advice to organisations thinking about using blockchain technology by outlining potential developments in healthcare and blockchain. Finally, it presents blockchain as a driving force behind a sea change in healthcare data management by reviewing important results and highlighting the need of further study.

Chelladurai, Usharani et.al. (2022). For medical professionals, EHRs are a product of the extensive digitization of medical data made possible by technological advancements. The current situation calls for patients to have access to their medical records at several local hospitals. Patients in critical condition have an even greater obstacle when trying to integrate disparate health information from different sources into a unified whole: the timely the sharing of pertinent medical records between different doctors. In this article, we outline how blockchain smart contracts might meet the regulatory needs of healthcare providers, patients, and doctors. In order to construct an intelligent e-health system, the suggested solution intends to use a blockchain platform for the sharing of health information. Launching health models, the suggested method enables for the safe storing and quick access of medical information by using an updated Merkle tree database design to provide immutable medical records on the decentralized blockchain system. Additionally, the ability to update medical data, permit the exchange of health information between different physicians, and set up viewership contracts are all advantages. This system stores clinical data using blockchain technology. Patients and doctors alike may take advantage of the system's streamlined access to EHRs and robust record of all events, thanks to a distributed ledger. An important part of this system is that it uses cryptographic hash functions to provide a high degree of secrecy and integrity. To guarantee its effectiveness, the proposed technique has been tested on many trials. The recommended setup's performance has been evaluated using both quantitative and qualitative indicators. These metrics include latency, transactions per second, and resource utilisation.

Mazlan, Ahmad et.al. (2020). The decentralised ledger known as "blockchain" allows for an encrypted, private, trustworthy, and transparent transfer of data. Because there is no difference between the two databases and the records are planned to update periodically, Activities related to validation and coordination are made easier in this case. Blockchain technology's potential use in the medical and how it solves scalability issues are the main topics of this study. Consequently, sixteen options were classified into two primary categories: optimisation of storage and redesign of blockchain. Problems with protocols, large amounts of data and transactions, a lack of nodes, and block size are still there. Research question formulation, research methodology, article screening, abstract-based keywording, data extraction, and mapping are the six steps that make up this review. We utilised the given keywords to search for relevant articles using the Atlas.ti programme. Consequently, forty-three quotes and forty-eight codes were generated. The quotes were categorised using manual coding. The next step was to map the codes onto the network. Two primary categories, storage optimisation and blockchain redesign, accounted for sixteen solutions. There are a total of thirteen suggestions for blockchain redesign, including three for storage optimisation and twelve for blockchain models, read/write mechanisms, and bidirectional networks.

METHODOLOGY

The proposed methodology involves collecting IoT information gathered from sensors and sent to a central hub. Next, the data is validated and processed using blockchain technology from a multitude of IoT edge devices. Outsourcing the data encryption process to the cloud enables statistical and deep learning operations on the encrypted data. Next, characteristics such as age, sex, weight, height, and heart rate are extracted by feature extraction. For feature-and interaction-based data and user classification, the platform employs Support Vector Machine (SVM). A validation model is used to confirm and verify the result. Improved efficiency and effectiveness are the goals of the technique IoT devices.

Proposed Algorithms

The proposed framework uses a novel algorithm to govern it, which outlines the process of updating, creating, and revoking policies. The algorithm first creates a Patient Health Record (PHR) upon user request, revises the current PHR and removes it in case the user acts in an unauthorized manner. Data collection also includes information gathered from patients, medical devices, and the surrounding environment., it also assigns qualities to physicians and patients via a network of sensors. Devices for monitoring, wearable sensors, and implanted sensors are all part of this category of medical equipment.

Algorithm 1 Create, Update, and Revoke Medical Records

```
procedure CreateRecord(patientID, data) record ← new MedicalRecord
record.patientID ← patientID record.data ← data save record    ▷ Save the record in the database
end procedure
procedure UpdateRecord(recordID, newData) record ←
fetch MedicalRecord with recordID
    if record ≠ null then record.data ← newData save record  ▷ Update the record in the database
    end if
end procedure
procedure RevokeRecord(recordID) record ← fetch MedicalRecord with recordID
    if record ≠ null then delete record    ▷ Delete the record from the database
    end if
end procedure
```

Sensing Layer in IOMT

In IoMT, the sensing layer records and sends data on biometric, behavioural, and environmental data for analysis and decision-making in a centralized or distributed system. This data can include vital signs, medication adherence, patient activity, and environmental conditions. The term "Distributed QEMR algorithm" related to IoMT is not widely recognized, so it may refer to a specific algorithm or approach not commonly known.

Mathematical Model

Here is one way to depict the mathematical model:

$$\begin{aligned} \text{Objective Function:} \quad & \max_{x_1,x_2} 3x_1 + 5x_2 \\ \text{Subject to:} \quad & 2x_1 + 4x_2 \leq 10 \\ & x_1 + 3x_2 \leq 7 \\ & x_1, x_2 \geq 0 \end{aligned}$$

The proposed model uses Secure electronic medical record data using homomorphic encryption (HE) so that users or AI models may execute complicated mathematical or statistical operations without requiring decryption. To verify characteristics, Algorithm 2 uses a bi-linear pair group, signature count, and master keyBeginning with a group of bilinear pairs, such G1 and G2, the user chooses a value at random. Part of the algorithm's operation, as detailed in Algorithm 3, is choosing cluster heads according to battery life. Users may protect their data and privacy by encrypting it locally and then uploading it to the cloud via HE. One may speak about HE in three different ways: totally, partly, and hybridly. The constraints of the suggested technique and the integration with various IoMT devices necessitated the usage of completely HE in this study. The main benefit of HE is its ability to perform operations over encrypted data without decryption.

RESULTS

This section presents a detailed simulation and results of a proposed model for private information retrieval. The model's performance was assessed by comparing it to a benchmark model. In comparison with appointment allocation techniques and the B+-Tree indexing data structure, the proposed framework achieves reduced communication overhead, which is applicable to SHealth, MedRec, and ECC-Smart systems. Hyperledger fabric, a blockchain technology, was used to run the simulation and provide the findings. and validated on the Ethereum test net. The publicly available data set was used in the research paper. The results show demonstrating the suggested system is more efficient at transferring transactions than both permissionless and private blockchains, indicating its superior performance. The data set used in the simulation is publicly available from UNSW. The framework's lightweight authentication system also contributes to its superior performance.

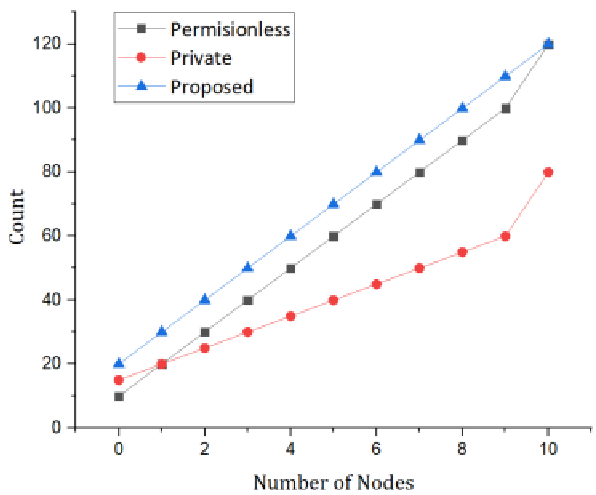

Figure 1. Findings from simulations where the ratio of nodes to counts is the driving factor.

The study presents outcomes of the simulation for user classification using LSTM deep learning and the

SVM algorithm. The system keeps track of what users have done in the past and keeps a record of their behaviour so that they might be granted access depending on their actions. Also included are simulation findings for IoT-connected moving sensors, with a particular emphasis on round count vs latency. The research evaluates the suggested architecture by contrasting it with reference models, looking at metrics like encryption time on the quantity of nodes. These findings are presented in Figure 2.

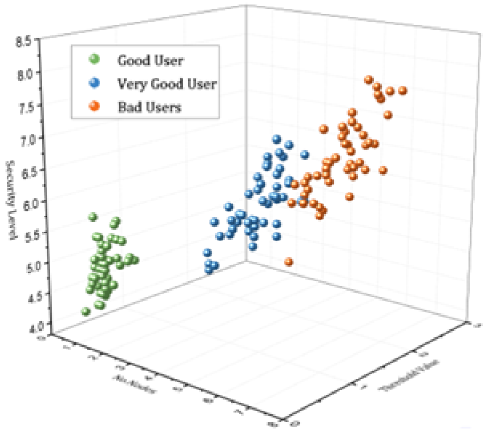

Figure 2. Classification of users based on the behaviour and interaction with the system model.

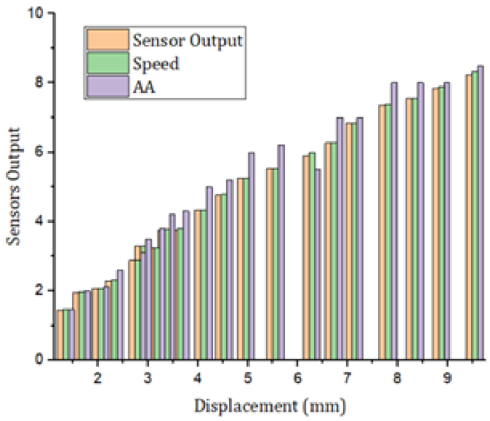

Figure 3. Findings from the models developed using the sensor ratio output to node count.

The suggested system is efficient and resilient, since it has minimal latency when compared to benchmark models. We provide a comparative study using d2d distance and transaction volume as our primary foci. Also compared are the network latency, ideal power distribution, and key distribution, all of which point to the suggested method having less delay. The number of transactions and the distance between two nodes are used to measure the framework's performance. For the same set of features, the suggested method outperforms the benchmark models when it comes to execution time while utilising lightweight HE. By comparing it to the benchmark models, Table 1 assesses the proposed framework's resilience to attacks. Proving the effectiveness of the suggested framework in reducing network latency, optimal power distribution, and transaction performance.

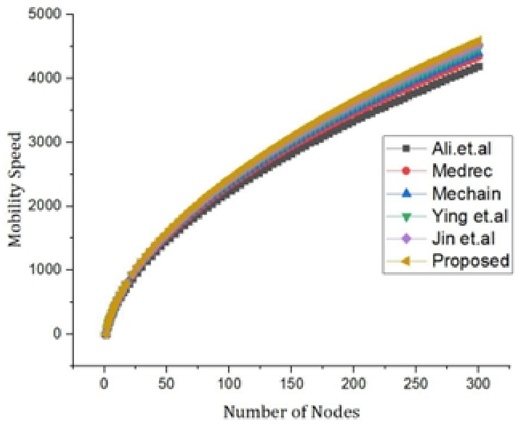

Figure 4. Comparative analysis of the proposed framework versus benchmark model based on the speed and number of nodes.

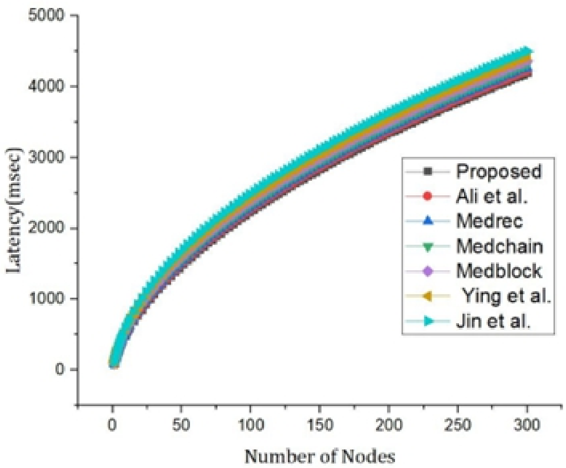

Figure 5. Using latency and node count as metrics, compare the proposed framework to a benchmark model.

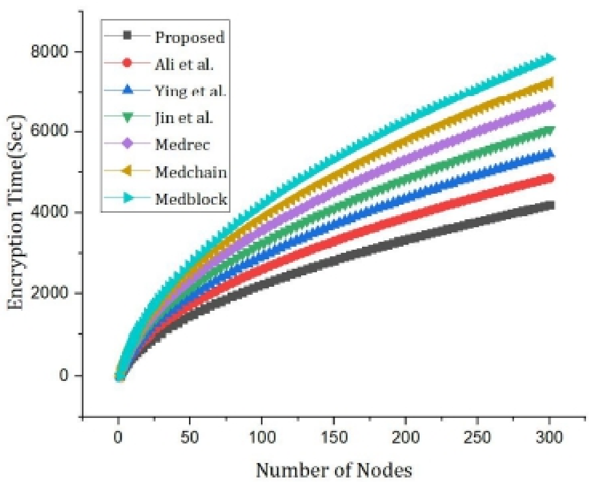

Figure 6. Analysis comparing the total number of nodes and the amount of time needed for encryption.

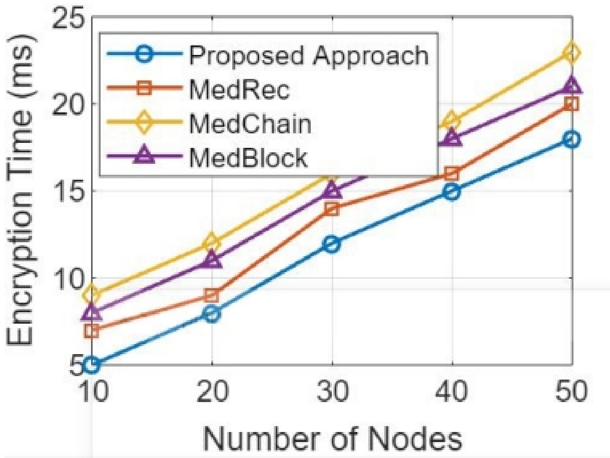

Figure 7. Analysis comparing the total number of nodes and the amount of time needed for encryption.

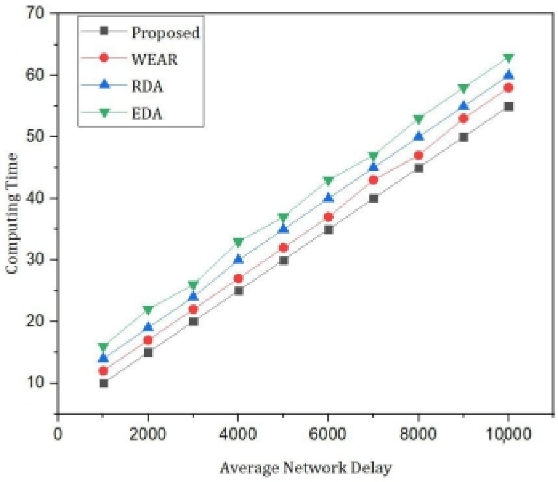

Figure 7. Search index and number of characteristics used for comparison.

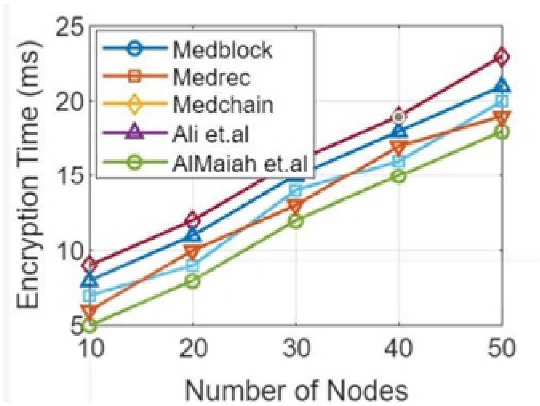

Figure 7 offers a comparison study using secret key rate and traditional optical power.

Figure 8. Classical optical power vs. secret key rate comparison analysis

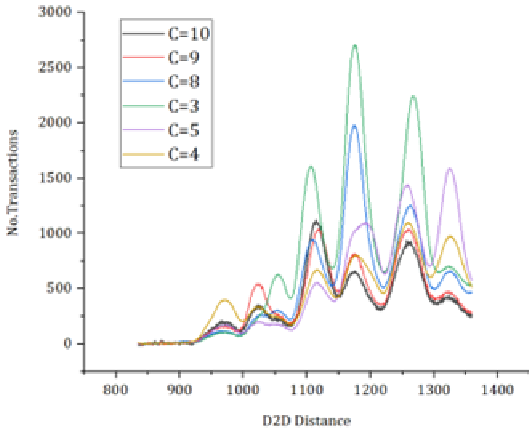

Figure 9. Evaluation of the relationship between d2d distance and transaction volume.

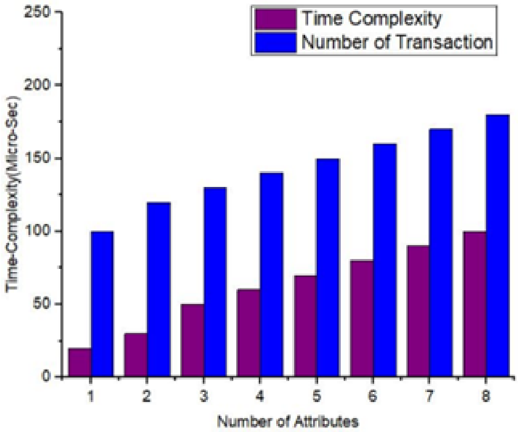

Figure 10. Graphical representation of the simulation outcomes as a function of complexity and number of characteristics.

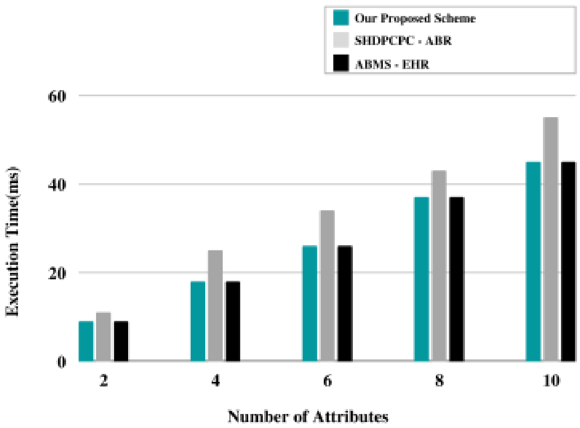

Figure 11. The suggested method is compared to existing model standards.

Table 1 analyses the suggested and benchmark models' attack resistance and compares it.

Table 1. Evaluation of attack resistance against different threats.

Models	Collusion Attacks	DoS	DDoS
Medblock [25]	No	No	Yes
Ali et al. [5]	Yes	No	No
Medchain [50]	Yes	No	No
Medrec. [54]	Yes	No	No
Proposed	Yes	Yes	Yes

CONCLUSIONS

The Blockchain-Powered Healthcare Systems This framework is designed to enhance healthcare data management and analytics by making it more scalable, secure, interoperable, and privacy-friendly. This system integrates hybrid deep learning with blockchain technology to guarantee the confidentiality, privacy, and immutability of medical records. Through the use of smart contracts, patients are given more control over their data by automating data access, exchange, and consent management. Utilize hybrid deep learning methods that ensure data privacy to enhance healthcare analytics and decision-making. Among these methods are federated learning, transfer learning, and deep neural networks. Medical treatment systems, patient outcomes, and data security and privacy might all be significantly enhanced by using this paradigm. To fully progress this unique method and realise its promise in the healthcare area, ongoing research, cooperation, and practical implementations are necessary.

References

1. Ait Bennacer, Sara & Khadija, Sabiri & Abdessadek, Aaroud & Khalid, Akodadi & Cherradi, Bouchaib. (2022). Impact of Blockchain technology in Healthcare. ITM Web of Conferences. 43. 01007. 10.1051/itmconf/20224301007.

2. Panigrahi, Amrutanshu & Nayak, Ajit Kumar & Paul, Rourab. (2022). HealthCare EHR: A Blockchain-Based Decentralized Application. International Journal of Information Systems and Supply Chain Management. 15. 1-15. 10.4018/IJISSCM.290017.

3. Adeghe, Ehizogie & Okolo, Chioma & Ojeyinka, Olumuyiwa. (2024). Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes. 13-020. 10.53022/oarjst.2024.10.2.0044.

4. Chelladurai, Usharani & Pandian, Seethalakshmi. (2022). A novel blockchain based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing. 13. 10.1007/s12652-021-03163-3.

5. Mazlan, Ahmad & Mohd Daud, Salwani & mohd sam, Suriani & Abas, Hafiza & Rasid, Siti & Yusof, Fathi. (2020). Scalability Challenges in Healthcare Blockchain System - A Systematic Review. IEEE Access. 8. 1-1. 10.1109/ACCESS.2020.2969230.

6. Adavoudi Jolfaei, Amirhosein & Aghili, Farhad & Singelee, Dave. (2021). A Survey on Blockchain-Based IoMT Systems: Towards Scalability. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3117662.

7. Aldalabeeh, Ahmad. (2024). Utilizing Blockchain to Measure Privacy and Security in a Healthcare

System Jordan Healthcare System as a Case Study.

8. Zghaibeh, Manaf & Farooq, Umer & Ul Hasan, Najam & Baig, I. (2020). SHealth: A Blockchain-Based Health System with Smart Contracts Capabilities. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2986789.

9. Elghoul, Mohammed & Bahgat, Sayed & Hussein, Ashraf & Hamad, Safwat. (2023). Securing Patient Medical Records with Blockchain Technology in Cloud-based Healthcare Systems. International Journal of Advanced Computer Science and Applications. 14. 10.14569/IJACSA.2023.0141133.

10. Upadhyay, Saumya & Agarwal, Shikha & Chaudhary, Aarti & Singh, Pulomja & Sharma, Dr. Rashmi. (2024). Blockchain in Healthcare Systems: A Systematic Review. 140-147. 10.1109/ICDT61202.2024.10489533.

11. Rawas, Soha & Samala, Agariadne. (2024). Transforming Healthcare Data Management: A Blockchain-Based Cloud EHR System for Enhanced Security and Interoperability. International Journal of Online and Biomedical Engineering (iJOE). Vol. 20 No. 02 (2024). 10.3991/ijoe.v20i02.45693.

12. Roehrs, Alex & André da Costa, Cristiano & Righi, Rodrigo & Silva, Valter & Goldim, Jose & Schmidt, Douglas. (2019). Analyzing the Performance of a Blockchain-based Personal Health Record Implementation. Journal of Biomedical Informatics. 92. 103140. 10.1016/j.jbi.2019.103140.

13. Haddad, Alaa & Habaebi, Mohamed & Islam, Mohd & Hasbullah, Nurul & Ahmad Zabidi, Suriza. (2022). Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems. IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3201878.

14. Singh, Yuvraj & Jabbar, M. & Shandilya, Shishir K & Vovk, Olena & Hnatiuk, Yaroslav. (2023). Exploring applications of blockchain in healthcare: road map and future directions. Frontiers in Public Health. 11. 1229386. 10.3389/fpubh.2023.1229386.

15. Rai, Bipin Kumar & Tyagi, Akanksha & Arora, Bhawana & Sharma, Shivani. (2022). Blockchain Based Electronic Healthcare Record (EHR). 185-193. 10.1007/978-981-16-7985-8_19.