Journal of Information Technology and Digital World (ISSN: 2582-418X)
www.irojournals.com/itdw/

Enhanced Blockchain Framework for Secure and Scalable Personal Health Record Management in Telemedicine

Malini A.S.[1], **Ayesha S.**[2], **Karpagavalli K.**[3]

Department of Computer Science and Engineering, P.S.R.R. College of Engineering, Sivakasi, India.

E-mail: [1]malini@psrr.edu.in, [2]ayeshaayesha4799@gmail.com, [3]karpagavallik222004@gmail.com

Abstract

The key features of blockchain technology, such as transparency, security, and trust in sharing data, have attracted much attention in terms of utilizing this technology in the healthcare industry. Telemedicine's Personal Health Records have major challenges in terms of privacy, ownership of information, data integrity, and safe sharing. To solve these challenges, a solution based on a blockchain architecture, such as a permissioned blockchain system based on Hyperledger Fabric and Byzantine Fault Tolerance (BFT), is recommended as a model for safe management of Personal Health Records. However, a permissioned blockchain system has limitations in terms of scalability and latency. A hybrid solution based on Ethereum, which uses Ganache as a tool to implement a solution based on a Proof of Authority algorithm, which works as a private blockchain, is recommended. IPFS and Filecoin are two examples of decentralized storage technologies, which can be very helpful in storing information, particularly in healthcare, which tends to be too large to store in one place. IPFS provides access to manage files in a decentralized manner, and Filecoin offers a reward system for storing information, thus making it more accessible. There is also the use of Layer 2 scaling solutions such as Polygon to improve transaction speed and reduce end-to-end latency. To test the performance of the proposed system, a simulated scenario is created to demonstrate the improvements in end-to-end latency, throughput, and utilization compared to the existing Hyperledger Fabric environment. From the simulation, it is clear that the proposed system is a safe, scalable, and efficient solution for managing PHRs in telemedicine.

DOI: https://doi.org/10.36548/jitdw.2026.1.004
Received: 29.01.2026, received in revised form: 27.02.2026, accepted: 15.03.2026, published: 24.03.2026

Keywords: Hyperledger Fabric, Ganache, Ethereum, Proof of Authority (PoA), Blockchain Technology, Telemedicine, Personal Health Records (PHR), Decentralized Storage, and Smart Contracts.

1. Introduction

Personal Health Records (PHR) are an important part of the gradual shift of the healthcare system towards computerized patient information management systems in the present digital age. PHR is a system that allows an individual to store their health information in a digital format, enabling patients as well as medical practitioners to access their health information. PHRs contain a number of health information elements, including medical history, diagnosis, prescription medication, immunizations, and test results. PHRs allow patients to manage their health information, as opposed to Electronic Health Records (EHR), which are managed by medical practitioners.

Managing Personal Health Records (PHRs) is an important part of a healthcare system because it helps doctors make better decisions and gives patients better care. But there are now big problems with data privacy, data security, and data interoperability because medical data is now digital. Data privacy and integrity are in doubt because of cases of unauthorized access, data breaches, and the lack of data standards. Using blockchain technology could be a good way to solve the problems mentioned above. This technology is an important tool for PHRs because it is decentralized and unchangeable, which makes it more secure and open. Healthcare providers can use blockchain technology to make sure that patient data is safely shared and stored, and maintain a record of that data for each patient. This technology also helps find problems with illegal access and data manipulation. This plan will make people trust digital health records. Several studies have looked into different blockchain technologies for managing healthcare data. A systematic review underscored the potential of blockchain technology to tackle social determinants of health to enhance health outcomes, along with the advantages and disadvantages of employing blockchain to bolster the security of medical records [2].

One of the most important things in the healthcare field maintains medical records safe. The privacy, accuracy, and availability of healthcare information are important for building trust in a system that is very sensitive. There is a growing number of breaches, cyberattacks, and unauthorized access to patient information, which shows that personal health records

(PHRs) need better security right away. Recent studies show that fraudsters are going after healthcare organizations because they have a lot of private health information that is easy to steal.

A major concern in the healthcare industry is privacy-related issues. Many patients are concerned about the possibility that their health-related information could be misused for illegal purposes. In addition, maintaining health-related data while transmitting it is another concern because the amount of data being transmitted is increasing. In most cases, traditional data security methods, which are based on access control and traditional data storage systems, are unable to meet the needs and complexities of the healthcare environment. This paper proposes a scalable PHR management system based on a blockchain environment, which can switch from a permissioned Hyperledger Fabric architecture to an Ethereum-based PoA network.

1.1 Major Challenges of Healthcare Data Management

Personal Health Records (PHRs) bring a range of serious challenges to healthcare organizations, primarily security, privacy, and reliability. The most important challenges are:

- **Illicit Access and Data Leakage:** Cybercriminals highly value health information. Patients risk losing money, their identities can be stolen, and they can also be swindled, as the information is often sold on the dark web.
- **Lack of Data Control and Ownership:** Since medical practitioners are in charge of patient records, patients have no control over their records. This has led to a lack of patient willingness to use EHRs, as they fear the misuse of their information, their rights to access it, and concerns about confidentiality.
- **Data Integrity and Reliability:** Health information must be accessible and reliable, and it needs to be updated in order to enable informed medical decisions. The necessity for authentic and verified information is emphasized by the fact that corruption of information can lead to misdiagnosis, improper treatment, or even death.
- **Lack of Interoperability:** The providers' ability to access the entire patient history is impaired by the siloed nature of the patient information stored across different healthcare systems that are not compatible with each other.

1.2 Blockchain Technology in Healthcare

Blockchain technology, initially designed for virtual currencies such as Bitcoin, is seen as a solution to PHR-related healthcare challenges. The decentralized nature of blockchain prevents information from being changed without the consent of the network. This technology provides privacy and security through encryption and consensus mechanisms that give patients control over their information.

Moreover, PHRs offer healthcare practitioners precise information, which reduces healthcare errors, improves healthcare coordination, and enables telemedicine. However, despite the need to go digital, there are various challenges associated with the process. There are several uses of blockchain technology in healthcare management, such as in the management of medical records via soulbound tokens (SBTs), which can uniquely identify healthcare providers and patients, helping to solve some of the challenges facing the management of personal health records (PHRs).

A solution was developed in this study to improve healthcare management via a blockchain solution based on Ethereum and Ganache. This solution helps in incorporating blockchain technology in telemedicine to solve some of the challenges facing telemedicine, such as privacy issues, data intrusion, and compatibility.

2. Literature Survey

Recent advancements in blockchain technology have been significantly influential in providing secure healthcare data management and sharing platforms. For example, Murthy et al. in reference [1] developed a secure personal healthcare data sharing architecture based on a private permissioned blockchain network, which provides confidentiality in telemedicine services. On another note, Babu and Jothi in reference [5] developed a privacy-preserving analytics framework based on zero-knowledge proofs and blockchain technology in a multi-tenant cloud environment.

Some studies have also focused on enhancing the performance and interoperability of blockchain. Touloupou et al. [2] validated a benchmarking framework for blockchain platforms such as XRPL and Ethereum. Alhussayen et al. [3] also addressed the interoperability challenges faced by blockchain by presenting a blockchain oracle technique for permissioned blockchain platforms.

In the field of secure communication in healthcare and trust management, Patel et al. [4] proposed a fuzzy-enhanced secure messaging framework in smart healthcare systems. Al Qathrady et al. [7] proposed a dynamic blockchain trust management model that enhances the reliability and security of smart healthcare systems. Geetha et al. [8] also contributed to the field by proposing a secure paradigm of data sharing using blockchain technology, which improves cybersecurity in smart healthcare systems.

Several researchers have worked on blockchain technology in the field of access control and data sharing. Singh et al. [9] proposed a blockchain-based architecture for secure e-healthcare data sharing in Industry 5.0. Vernekar et al. [11] and Quasim et al. [12] proposed blockchain-based record management systems.

In addition to this, there have been various studies on decentralized electronic health record systems. Mulchandani et al. [13] and Singh and Gupta [15] presented blockchain-based medical record systems. Deshpande et al. [14] presented MedNcrypt, a decentralized system for storing health records using blockchain and IPFS.

Various studies on the emerging applications of blockchain in healthcare ecosystems have also been presented. Musamih et al. [6] presented a study on the application of NFTs in healthcare supply chain management. Guo et al. [10] presented a security-oriented system based on blockchain and federated learning.

Overall, these studies demonstrate that blockchain technology offers strong solutions for data sharing security, decentralized data storage, and data privacy preservation in healthcare systems. Nevertheless, challenges such as scalability, interoperability, and computational costs remain major issues of concern for future research.

3. Proposed Work

The proposed system utilizes a decentralized multi-layered structure to provide secure and efficient PHR management in telemedicine systems. In this system, blockchain technology, decentralized storage, and smart contracts are integrated to provide security and privacy to the PHRs. Figure 1 illustrates the architecture of the proposed blockchain technology-based PHR system.

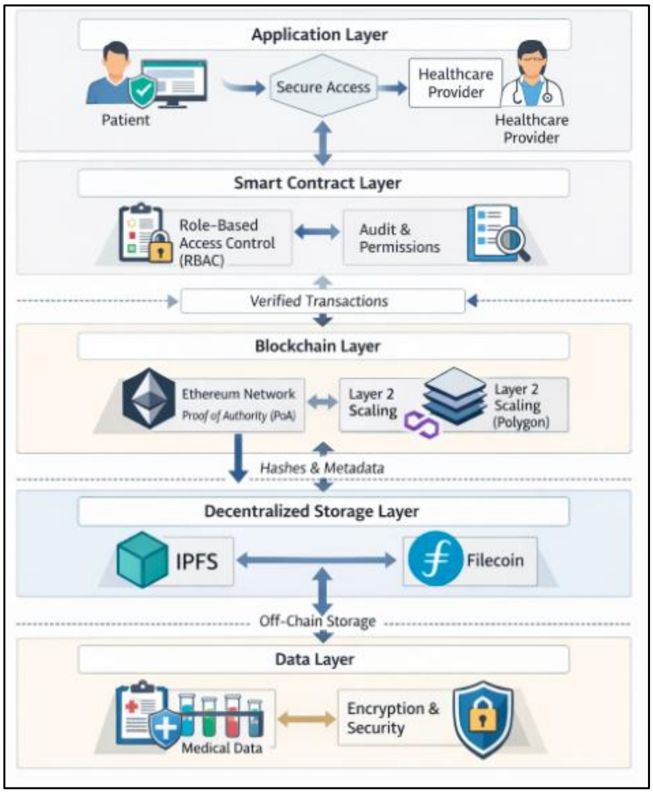

Figure 1. Proposed System Architecture

At the data layer, the PHRs of the patients, including their medical history, prescription records, diagnosis reports, etc., are created and collected from the healthcare providers. In the proposed system, for handling the large files of medical records, off-chain decentralized storage using IPFS and Filecoin technologies is implemented. In this system, the actual files of the medical records are stored using IPFS and Filecoin technologies. However, the corresponding hash values of the files are stored in the blockchain to maintain their integrity and save space in the blockchain.

At the blockchain layer, the proposed system utilizes a private Ethereum blockchain with Ganache and Proof of Authority consensus algorithms. In this system, the Proof of Authority consensus algorithm is chosen due to its lower latency and reduced computational complexity. In this system, all transactions, including access, update, and sharing of medical records, are recorded in the blockchain.

The smart contract layer is responsible for access control and data governance. Smart contracts are used for Role-Based Access Control (RBAC) for the management of access permissions by the patient for the healthcare providers. Smart contracts also keep a record of all the activities performed on the data managed by the PHR.

The application layer includes users such as the patient and the healthcare providers who interact with the system via a web interface. The patient can upload and manage their health records, and the healthcare providers can request access to the patient's health records for diagnostic and treatment purposes.

The system applies smart contracts in the verification of access permission before any access is granted to the data. The system architecture has included Layer 2 scaling technologies such as Polygon to enhance scalability and improve system performance by processing transactions off the main blockchain network. This improves the efficiency of the system in transaction processing by reducing latency. The Hyperledger Fabric architecture has been used as a reference in comparing the proposed architecture with the existing one, while the proposed system's architecture is based on the Ethereum architecture.

Lastly, the security layer provides end-to-end security for critical healthcare data using encryption and the immutability of the blockchain technology. The use of decentralized storage systems, blockchain technology, and smart contracts provides a secure environment for personal health records in telemedicine services.

4. Simulation

To assess the effectiveness of the proposed blockchain-based PHR system, a scenario-based simulation model has been developed to mimic real-world telemedicine workloads. The simulation model has been implemented with varying transaction rates, ranging from 50 to 250 transactions per second (tx/s).

The simulation model is developed by using Python-based data generation and visualization tools. This ensures the performance evaluation process is consistent and reproducible. The performance metrics such as latency, throughput, and CPU utilization are modeled based on system characteristics observed in blockchain networks. Latency is modeled to increase non-linearly with the transaction rate due to congestion in the network. The system’s throughput increases with the transaction rate and then remains constant when the system is fully utilized. CPU utilization is modeled based on transaction load; it increases proportionally with the transaction rate.

The baseline system (Hyperledger Fabric) is considered to have higher computational overheads due to the complexity of consensus algorithms, whereas the proposed system using

Ethereum with Proof of Authority (PoA) is considered to have reduced processing complexity and increased efficiency.

The simulated values are created using varying parameters to represent realistic performance trends. The values are varied slightly to represent realistic scenarios that may occur in real-world scenarios. The values are then used to generate the performance graphs shown in Figures 2-4. Simulation is a method of evaluating the proposed system that provides a comparative analysis of the system performance under varying workloads.

5. Result and Discussion

Performance evaluation is conducted by simulating scenarios to mimic real-world telemedicine workloads with different transaction rates. The performance evaluation of the proposed blockchain-based Personal Health Record (PHR) system is conducted by simulating scenarios to mimic real-world telemedicine workloads with different transaction rates. The key performance indicators considered in the assessment are latency, throughput, and CPU utilization, which enable the evaluation of the scalability and efficiency of the system. The proposed Ethereum-based architecture with Proof of Authority (PoA) is compared with the existing Hyperledger Fabric architecture.

5.1 Latency Analysis

The performance latency for varying transaction rates is shown in Figure 2. The system is tested at transaction rates ranging from 50 to 250 transactions per second.

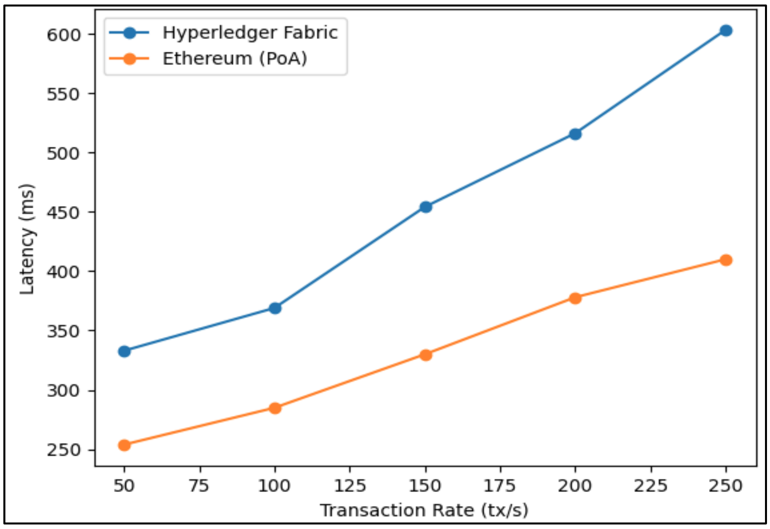

Figure 2. Latency Variation Under Different Transaction Rates

4.2 Throughput Analysis

The performance of the throughput is shown in Figure 3. The figure represents the varying transaction rates of the system.

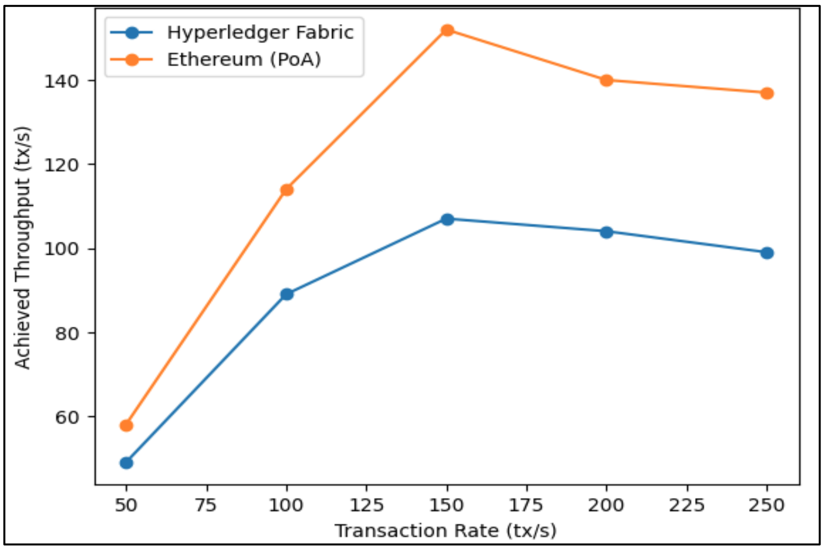

Figure 3. Throughput Performance Under Varying Transaction Rates

The result obtained indicates that throughput increases with the rate of transactions up to a certain limit, after which it remains constant. This is because it has reached saturation at that limit. From the result, it is clear that the system based on Ethereum reaches a maximum throughput of 150-165 tx/s, while the system based on Hyperledger Fabric reaches a maximum of 110-120 tx/s.

The result obtained confirms that the proposed system can handle a large number of transactions, hence making it scalable for use in the healthcare system. In addition, the proposed system can increase its throughput using Layer 2 scaling, which reduces the load on the blockchain.

4.3 CPU Utilization Analysis

The CPU utilization of both systems under different transaction rates is shown in Figure 4. As expected, CPU usage increases with the transaction rate due to the higher computational demand.

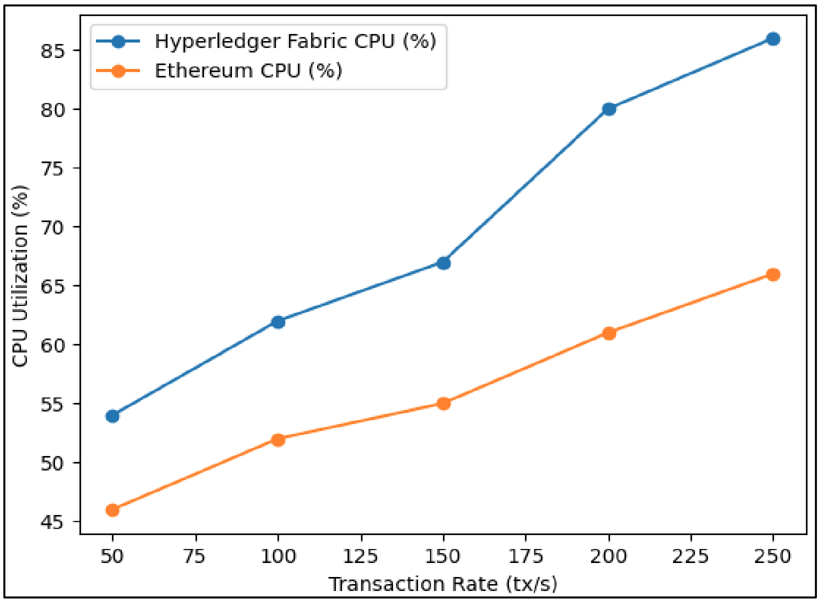

Figure 4. CPU Utilization Under Increasing Transaction Load

The CPU usage of Hyperledger Fabric is high, reaching up to 85%, while in the proposed system, based on Ethereum technology, CPU usage is less, about 65-70%.

4.4 Overall Performance Evaluation

From the above comparative analysis, it is clear that the proposed system is performing better in all parameters compared to the baseline system. Some of the key differences are:

- Reduced latency under high transaction loads
- Higher throughput enabling better scalability
- Lower CPU utilization indicating improved efficiency

The use of decentralized storage mechanisms such as IPFS and Filecoin further reduces the burden on the blockchain by storing large medical data off-chain while maintaining secure hash references on-chain.

4.5 Discussion

The results show the effectiveness of integrating the Ethereum blockchain with PoA consensus in the context of telemedicine applications. The suggested system guarantees the safe, scalable, and efficient handling of personal health information, while patient data privacy and integrity are assured. The results, though obtained via simulation, show realistic scenarios with varying workloads and thus provide valuable insights into the real-world effectiveness of the suggested solution. In the future, real-time testing and benchmarking with the help of tools like Hyperledger Caliper will be conducted to validate the results.

Table 1. Comparison of Blockchain-Based Healthcare Systems

Method	Consensus Mechanism	Storage Approach	Access Control	Scalability Strategy	Performance Limitation
Murthy et al. [1]	BFT (Hyperledger Fabric)	IPFS (off-chain)	Permissioned access	Limited by network size	Higher latency due to consensus overhead
Babu & Jothi [5]	PoW-based blockchain	Cloud storage	Encryption-based access	Not optimized for scalability	High computational cost of PoW
Singh et al. [9]	PoW-based system	Centralized database	Role-based access	Limited decentralization	Single point of failure
Deshpande et al. [14]	PoW (Ethereum)	IPFS	Smart contract-based	Moderate scalability	Gas cost and latency issues
Proposed System	PoA (Ethereum - Ganache)	IPFS and Filecoin	RBAC and Smart Contracts	Layer 2 (Polygon) integration	Simulation-based evaluation (real deployment future work)

The comparison of the proposed blockchain-based healthcare system with existing systems is presented in Table 1. The architectural benefits of the proposed system are presented in the table. The existing systems are based on Proof of Work (PoW) or Byzantine Fault Tolerance (BFT), which are associated with high computational overhead and latency. However, in the proposed system, Proof of Authority (PoA) is used to achieve high efficiency. In addition, data availability is increased by using IPFS with Filecoin. Furthermore, scalability is achieved using Layer 2 scaling with Polygon to solve the problems associated with telemedicine systems.

6. Conclusion

The proposed system will have considerable improvements over the existing system, such as low latency, increased throughput, and low resource utilization. This paper proposes an end-to-end blockchain-based system for implementing Personal Health Records (PHR) under telemedicine, which will address issues such as ownership, accuracy, security, and reliability of transactions. To make the sharing of PHR effective, this paper has proposed Hyperledger as part of the proof of concept, which shows the advantages of using Byzantine Fault Tolerance (BFT) along with IPFS. Scalability, operational efficiency of transactions, and interoperability are greatly improved by implementing enhancements such as using Ganache and Ethereum with Proof of Authority, decentralized storage using Swarm and Filecoin, and using Layer 2 solutions such as Polygon. Security and governance are improved by adding audit trails using smart contracts and Role-Based Access Control. The system facilitates an open and decentralized healthcare environment with patient autonomy. The system is a step towards the secure transfer of patient records. To facilitate the wider adoption of blockchain technology in healthcare services, future work will extend the system's functionality to accommodate wider-scale networks, including the integration of AI technology for analytics in personal healthcare services and user interface improvements to enhance patient accessibility.

References

[1] Murthy, Ch VNU Bharathi, and M. Lawanya Shri. "Secure Sharing Architecture of Personal Healthcare Data Using Private Permissioned Blockchain for Telemedicine." IEEE Access 12 (2024): 106645-106657.

[2] Touloupou, Marios, Klitos Christodoulou, and Marinos Themistocleous. "Validating the Blockchain Benchmarking Framework Through Controlled Deployments of XRPL and Ethereum." IEEE Access 12 (2024): 22264-22277.

[3] Alhussayen, Asma A., Kamal Jambi, Maher Khemakhem, and Fathy E. Eassa. "A Blockchain Oracle Interoperability Technique for Permissioned Blockchain." Ieee Access 12 (2024): 68130-68148.

[4] Patel, Nishi, Dhyan Patel, Nilesh Kumar Jadav, Tejal Rathod, Sudeep Tanwar, Giovanni Pau, Gulshan Sharma, Fayez Alqahtani, and Amr Tolba. "Fuzzy-Enhanced Secure

Messaging Framework for Smart Healthcare System." IEEE Access 12 (2024): 102977-102993.

[5] Babu, S. Bharath, and K. R. Jothi. "A Secure Framework for Privacy-Preserving Analytics in Healthcare Records Using Zero-Knowledge Proofs and Blockchain in Multi-Tenant Cloud Environments." IEEE Access 13 (2024): 8439-8455.

[6] Musamih, Ahmad, Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Mohammed Omar, and Samer Ellahham. "Using NFTs for Product Management, Digital Certification, Trading, And Delivery in the Healthcare Supply Chain." IEEE Transactions on Engineering Management 71 (2022): 4480-4501.

[7] Al Qathrady, Mimonah, Muhammad Saeed, Rashid Amin, Mohammed S. Alshehri, Asma Alshehri, and Samar M. Alqhtani. "Smart Healthcare: A Dynamic Blockchain-Based Trust Management Model Using Subarray Algorithm." IEEE Access 12 (2024): 49449-49463.

[8] Geetha, R., T. Vijayanandh, X. Mercilin Raajini, VS Divya Sundar, and P. Kumari Deepika. "Enhanced Cybersecurity: Development and Evaluation of a Secure Data Sharing Paradigm Based on Blockchain Technology." In 2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP), IEEE, 2024, 1-7.

[9] Singh, Gyaneshwar, Saurabh Rana, Dheerendra Mishra, and Muhammad Khurram Khan. "Blockchain-Based Access Control Architecture for Enhancing Authorized E-Healthcare Data Sharing Services in Industry 5.0." IEEE Transactions on Consumer Electronics (2024).

[10] Guo, Zhengxin, Shizhan Chen, Chao Wang, Hongyue Wu, Kai Ma, and Zhiyong Feng. "Security-Oriented Architecture for Blockchain-Based Federated Learning in the Financial Industry." In 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, 2024, 465-470.

[11] Vernekar, Adarsh, Akash Sakhare, Prashant Bhapkar, Saurabh Jadhav, and Rahul B. Adhao. "Blockchain Based Record Management System in Hospitals." In 2023 4th International Conference on Innovative Trends in Information Technology (ICITIIT), IEEE, 2023, 1-4.

[12] Quasim, Mohammad Tabrez, Mohammad Mufareh Mobarak, Khair Ul Nisa, Mohammad Meraj, and Mohammad Zunnun Khan. "Blockchain-Based Secure Health Records in the Healthcare Industry." In 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, 2023, 545-549.

[13] Mulchandani, Mona, Priti Samrit, Srusti Wakode, Palak Tahlyani, Iqra Ansari, and Muskan Sheikh. "A System for Medical Record Using Blockchain." In 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), IEEE, 2023, 1-4.

[14] Deshpande, K. V., Tejas Patil, Shubham Nagare, Rushikesh Sarode, and Abhishek Dhanke. "MedNcrypt: A Blockchain Based Decentralised Health Record Storage System Using IPFS." In 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), IEEE, 2023, 1579-1587.

[15] Singh, Shreya, and Siddhi Gupta. "Medehr-Electronic Health Record Using Blockchain." In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), IEEE, 2023, 58-62.