ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(4)

REVIEW ARTICLE

A Detailed Survey of Blockchain Applications in Medical Record Storage: Technical Issues and Scalability Constraints

Dr. Prithviraj Singh Rathore*

Assistant Professor, Mandsaur University, Mandsaur

Department of Computer Sciences and Applications
Email-prathviraj.rathore@meu.edu.in

Received on: 01-10-2025; Revised on: 05-11-2025; Accepted on: 09-12-2025

Abstract*— The high-speed digitalization of medical care has exacerbated the requirement to have safe, transparent, and interoperable systems in order to handle the sensitive medical data. The use of blockchain technology has become a potential solution that can help solve the old problems of integrity and access to medical data. This in-depth survey will discuss the application of blockchain in the medical record storage with emphasis on technical challenges and scalability problems. The architecture of blockchain is decentralized and immutable, which improves the data security, patient privacy, cross-platform interoperability, allowing trusted exchange of the electronic medical records (EMRs). The paper identifies the main advantages, including enhanced accuracy, confidential sharing, decrease in administrative expenses, and the access to medical data all over the world. It also examines significant threats as an organization, societal and technological which influence implementation. The critical technical issues, such as challenges to consensus mechanisms, energy usage, and security concerns outside the encryption, and on-chain/off-chain storage considerations are assessed in detail. Scalability issues related to increasing volumes of medical data, network overload, and throughput bottlenecks are also addressed as well as new architectural resolutions of effective blockchain-based healthcare systems.

Keywords*– Blockchain Technology, Medical Record Storage, Energy Efficiency, Scalability, Electronic Health Records (EHRs), Healthcare Blockchain, Consensus Mechanisms.

I. INTRODUCTION

The fast-paced digital transformation of the healthcare sector has resulted in an enormous rise in the generation, sharing, and use of electronic medical records (EMRs)[1][2]. The information in these records is often very sensitive and crucial for the patients, thus they require secure, tamper-proof, and interoperable data management solutions [3] [4]. Although conventional governed EMR systems are the ones being used the most, they still have a number of drawbacks, such as security compromise, one point of failure, data being closed off from view and patients having very little or no say over their own health data[5][6]. At the same time, the cyber threats are going up, and one of the major challenges for healthcare companies all over the world has now become to keep medical records secure, intact and accessible at all times.

The use of Blockchain technology has come to the fore as a potential choice because of its decentralized structure, incorruptibility, distributed agreement, and capability to securely share data among untrusted parties[7]. The use of blockchain for cryptographically verifiable transactions has the potential to change entirely the storage, access, and management of medical records[8][9]. Different blockchain frameworks that include public, private, and consortium-based architectures have been researched recently with the aim of protecting patient data privacy, easing interoperability among healthcare providers, and increasing traceability within the healthcare ecosystem[10]. What's more, the use of smart contracts not only allows controlling access automatically but also enables finely-grained authorization and auditability, thereby making it even more difficult for unauthorized users to penetrate EMR systems.

Blockchain adoption for medical record storage is a very promising technology but it entails yet technical and operational challenges[11]. Scalability problems, slow transactions, high computational resources needed, increasing storage, the drawback of the consensus mechanism, and inter-systems communication difficulties are still in the way of broad implementation[12][13]. Moreover, the use of blockchain technology in healthcare entails that the compliance of standards, like HL7 and FHIR for the technical side, and the regulations such as HIPAA and GDPR for the data privacy side, should be met[14]. These difficulties are a reminder of the importance of being fully aware of the pros and cons of blockchain in healthcare settings.

A. Structure of the Paper

The paper is structured as follows: Section I introduces the topic and highlights the challenges of using blockchain in medical record storage. Section II covers the basics of

blockchain technology in healthcare. Section III explores blockchain applications in Medical Record Management, while Section IV addresses scalability issues. Section V highlights the literature review, concludes the paper and suggests future research directions in Section VI.

II. BLOCKCHAIN TECHNOLOGY IN HEALTHCARE SYSTEM

The rise of blockchain technology as a responsible, transparent mechanism for storing and distributing data is paving the way for new opportunities to address serious data privacy, security, and integrity issues in healthcare. Blockchain technology has attracted considerable attention from industry and academia over the past few years. Indeed, new blockchain applications and research studies surface every day [15]. Blockchain technology is a distributed ledger for peer-to-peer (P2P) networks for digital data transactions that may be publicly or privately distributed to all users, allowing any type of data to be stored in a reliable and verifiable way [16].

A. Blockchain-Based Healthcare Applications

The medical industry is undergoing a change via blockchain technology as it provides the means for safe, clear, and fast handling of medical information in various clinical settings. The technology's flexibility permits the easy scattering, safeguarding, and sharing of confidential health information among the parties that are allowed access. A visual representation of the general process that blockchain-based healthcare applications follow is depicted in Figure 1. It shows the connection between different medical data sources, the blockchain infrastructure, the application layers, and the main healthcare players.

Figure 1. A workflow of blockchain-based healthcare applications

1. Blockchain technology is redefining data modelling and governance in many healthcare applications.
2. This is mainly due to its adaptability and ability to segment, secure, and share medical data and services in an unprecedented way.
3. Blockchain technology is at the centre of many current developments in the healthcare industry.
4. Emerging blockchain-based healthcare technologies are conceptually organized into four layers, including data sources, blockchain technology, healthcare applications, and stakeholders.

B. Enhances Healthcare Security using Blockchain

Blockchain technology strengthens healthcare security through data immutability, cryptographic verification, and decentralized control.

Data Immutability and Integrity: Blockchain's distributed ledger ensures that once medical records are recorded, they cannot be altered or deleted, preventing data tampering by malicious insiders or external attackers. Each medical record is hashed and stored as a cryptographic digest, ensuring integrity and non-repudiation. Any modification in patient data creates a new version while maintaining a full historical audit trail, ensuring transparency and regulatory compliance (e.g., HIPAA, GDPR).

Cryptographic Verification: Elliptic Curve Cryptography (ECC) and SHA-256 hashing provide strong encryption to secure patient records against unauthorized access. Decentralized Identity (DID) mechanisms enable secure authentication, reducing risks associated with stolen credentials or identity fraud[17]. Multi-signature (multi-sig) verification ensures that critical actions (such as modifying access permissions) require approval from multiple authorized entities (e.g., the patient and the healthcare provider). By leveraging these features, blockchain provides a secure, tamper-proof, and transparent system for managing healthcare data.

C. Threats of Blockchain Technology in Medical Records

Blockchain technology offers a myriad of benefits; however, it also comes with considerable risks. These risks can be broadly categorized into three main areas [18] organizational, societal, and technological threats. Each category presents unique challenges that must be carefully addressed to ensure the effective and secure implementation of blockchain in healthcare and other critical sectors.

1. **Technical or technological threats**: The scalability problem with blockchain technology was due to the network's constrained processing capacity for transactions. Additionally, according to two studies, the exchange between trading volume and the amount of processing power needed to handle those transactions is the major limitation of scalability. Authorisation and security were issues and constraints associated with blockchain technology. According to several studies, distributed ledger technology is vulnerable to assaults. Other research studies identified significant issues, particularly in blockchain networks, including high energy consumption and sluggish processing speeds due to a significant increase in network users.
2. **Social threats:** According to the societal acceptability of blockchain technology was a key obstacle to implementation. Scholars revealed that it is challenging for the legal authorities to grant access due to the

decentralization of medical data and the withdrawal of a trusted third-party, emphasizing privacy as a valid concern. It emphasized the absence of governance norms and standards as a barrier to blockchain adoption in the healthcare industry.

3. **Organizational threats:** The compatibility is one of the main problems with blockchain adoption in the healthcare sector from an organizational standpoint. Studies described interoperability issues as lack of confidence among parties and absence of transparent standards, which make it difficult for healthcare organizations to communicate full patient data. The maintenance of an interconnected pharmaceutical supply chain for networks lacking the technical knowledge to manage it was another issue noted by the research. In addition, the initial cost of installation is rather significant for blockchain, even though it can save costs in the long term.

D. Blockchain as Platform for Medical Records

By allowing data exchange between providers and electronic health record (EHR) systems, Blockchain technology has the potential to change healthcare delivery[19]. But major barriers prevent this technology from being generally implemented in the healthcare industry [20]. Two of the main issues related to the use of Blockchains to share information in health care are: securing sensitive health information and deploying and installing Blockchain software in various hospital contexts. Blockchain solution with a distributed microwave architecture to enable system' s -core functions to be encapsulated in single services that can be scaled on a specific level based on the needs of a particular hospital system deployment. To ensure easy implementation in a hospital system, designed essential components for handling cryptographic secrets safely, connecting with Blockchain nodes, simplifying big file sharing, enabling secondary-index based lookups, and integrating external business logic that regulates how users interact with Smart Contracts as part of this architecture.

III. BLOCKCHAIN APPLICATIONS IN MEDICAL RECORD MANAGEMENT

Blockchain technology can revolutionize the health sector via the introduction of secured algorithms to manage patients' confidential health records [21]. According to IBM, 70% of healthcare executives are optimistic about the benefits the integration of blockchain technology will bring to the health sector, especially by enabling distributed, transparent architectures for the dissemination of EMRs. The processing of medical data and patient records is essential for analysing previously prescribed medicines and understanding the severity of prior ailments [22]. In essence, trustworthy, tamper-proof, and immutable systems should be utilised to store, secure, and disseminate health information appropriately. Consequently, privacy and security are serious concerns for maintaining patients' confidential data in the health domain[23]. Thus, blockchain technology enhances the healthcare system by improving transparency and privacy for patients and practitioners, despite its inherent shortcomings.

A. Key Benefits of Blockchain in Medical Records

The benefits of blockchain technology adoption in the quest to actualize healthcare digitization are enormous. A few of these benefits are outlined in a cursory format below:

1. **Accuracy of Health Information**:

The history of the medical data of a patient is fragmented among many platforms, like hospitals, insurance companies, etc. By using blockchain, the collection of data is automated and always up-to-date. The record is transparent, as every transaction is imitable and auditable on the network. The immutable and secure data structure allows medical professionals to view the entire health history on the blockchain, allowing them to provide better treatment.

2. **Accentuated Interoperability of MIR Platforms:**

Many health record systems suffer from compatibility issues. This is because there are many manufacturers with a lot of technical differences. Thus, electronic information sharing is limited. With blockchain technology as the hub of digital healthcare record security and with decentralized applications managing the MIR distribution process at the front end, interoperability is achieved seamlessly across different healthcare delivery platforms.

3. **Authentic Protection of Health Records:**

The centralised nature of most medical record databases makes successful cyberattacks easy. Due to these centralization characteristics [24], unauthorized modification of medical records is possible. However, blockchain technology prevents data loss in the event of unexpected natural disasters.

4. **Alleviation of Administrative and Handling Costs:**

Medical data saved on a public blockchain is complete and accessible from anywhere. This saves costs and time spent in gathering fragmented data scattered across different databases in most current medical record management systems [25].

5. **Authorised Global Accessibility of MIRs:**

Apart from a reduction in the cost of accessing medical records, putting medical data on the blockchain also allows professionals to have full access to the medical history of patients to enable proper drug prescription and straight-to-the-point conclusions on the likely cause of a medical issue [26], especially when an emergency procedure needs to be carried out.

B. Functional Capabilities of Blockchain Supporting Global Healthcare

Blockchain tech comes with an extensive set of functionalities that have a direct impact on global healthcare operations. The decentralized nature of the blockchain ledger makes sure that the transfer of medical information is done in a secure and transparent manner, thus, allowing easy sharing of electronic health records (EHRs), reinforcing drug supply chain traceability and making privacy-preserving genomic data management possible[27]. Blockchain promotes trust between the various healthcare actors, like hospitals, laboratories, insurers, and research centres, by making it possible to use secure storage for data that cannot be changed and providing a way to see the history of transactions.

Moreover, blockchain supports several essential healthcare functions, including patient data protection, interoperable electronic data management, digitalised tracking of medical assets, outbreak surveillance, and secure identity authentication[28]. These capabilities promote the development of more resilient and interconnected healthcare ecosystems worldwide, enabling improvements in telemedicine, cross-border health information exchange, and collaborative biomedical research. Figure 2 illustrates the key functional capacities and enabling features of blockchain that contribute to the design of scalable, secure, and globally integrated healthcare solutions.

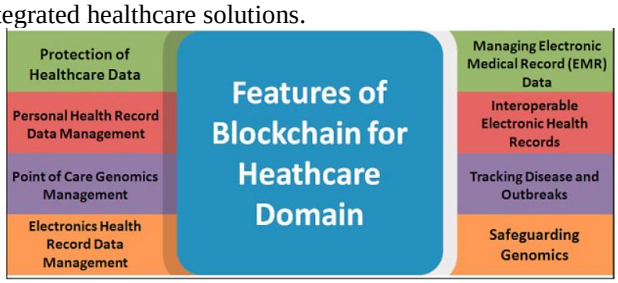

Fig. 2. Capacities of blockchain technology for healthcare domain

C. Energy Efficiency Concerns in Blockchain-Based Medical Record Systems

Energy consumption on the whole, however, this significantly limits the application of the so-called permission less blockchain systems especially those employing the Proof-of-Work (PoW) consensus mechanism. The PoW process involves miners constantly executing very resource-intensive hashing algorithms to arrive at the solution to a cryptographic puzzle, a process nicknamed “trial and error” because of the unpredictable nature of hash outputs [29]. Consequently, this leads to extremely high energy consumption, as in the case of Bitcoin, where the establishment of a new block about every ten minutes leads to the miners doing heavy computational work and consuming vast amounts of electricity[30]. So, while PoW brings along the positives of strong security and high resistance to counterfeiting, it can still be ruled out as the method of choice for an active health care environment because of the high energy demand that it imposes on the facility and hence, the need for a sustainable and resource-efficient digital infrastructure for medical records storage and access.

New blockchain models are trying to get rid of hashing altogether and let nodes control their block creation rates directly, rather than through a difficulty-based method. This shift poses the problem of creating mechanisms that keep block production steady and at the same time cut down on energy use to a large extent [31]. For storing and sharing of patient records, the consumption of energy in the case of PoS, PoA, and PoET is less as compared to that of PoW but the security guarantees are as strong.

D. Technical Issues in Blockchain for Medical Record Storage

The medical record systems that are based on blockchain have to deal with a number of technical issues which affect their trustworthiness, productivity, and future adoption. These problems are a result of the basic consensus mechanisms, security drawbacks that are not addressed by the standard cryptography, and the limitations of the decentralized medical settings.

1. Consensus Mechanisms and Energy Demand:

Consensus mechanisms may considerably affect the performance and energy consumption of a Blockchain network. As Blockchain is a decentralised ledger that does not need a central authority to manage it, a consensus mechanism is used to determine the validity of a new transaction before adding a new block to the chain [32]. The adopted mechanism determines crucial properties, including data consistency, consensus finality, speed, network scalability, and robustness against malicious nodes.

1. **Proof of Work (PoW):** PoW was developed to alleviate double-spending in the network. A proof-of-work system requires that nodes verifying transactions (known as miners) perform a complex computation to assert the validity of entities in the network. In Bitcoin, mining nodes compete to validate transactions by solving a cryptographic challenge to build a valid block.
2. **Proof of Stake (PoS):** PoS was introduced as an alternative to PoW to reduce energy consumption. The voting weight is related to the assets (owned units of the cryptocurrency, which are finite, visible, and thus verifiable within the Blockchain network) rather than the resource's computing power.
3. **Delegated Proof of Stake (DPoS):** DPoS works similarly to PoS, giving priority to the nodes with more stake on the network. However, the significant difference between PoS and DPoS is that, in PoS, validators are randomly chosen based on their stake, whereas in DPoS, validators are elected by other nodes on the network to validate and append new blocks.
4. **Proof of Luck (PoL):** PoL was proposed to leverage trusted execution environments (TEEs) to build a consensus mechanism that randomizes validators’ selection.
5. **Proof of Elapsed-Time (PoET):** Proof of Elapsed Time is a consensus mechanism introduced for private (permissioned) Blockchain networks. PoET was developed by Intel in tandem with their Software Guard Extension (SGX) 3 technologies and deployed in the open-source Hyperledger Sawtooth Blockchain platform.

2. Security Issues Beyond Traditional Encryption

Even though blockchain is built in a way that prevents unauthorized data tampering, actually a lot of security problems still exist which conventional encryption cannot deal with. For instance, healthcare IoT devices which encompass wearables and smart monitoring appliances are open to attacks where such devices may pass on the compromised data to the blockchain network.

3. Data Privacy and Regulatory Compliance Constraints

The healthcare data governance frameworks, which include HIPAA in the U.S. and GDPR in the E.U., set very high standards for confidentiality, access control, and even patient rights. On the other hand, the blockchain's inherent immutability is at odds with the GDPR's "right to be forgotten," which requires the complete removal of personal data upon the patient's request[33]. Moreover, methods such as transferring data to off-chain storage or encrypting on-chain references have emerged, but reconciling compliance with the law and the unchangeability of the blockchain remains a major challenge**.**

4. On-Chain vs. Off-Chain Data Storage Constraints

Electronic medical records consist of diverse, large data types, such as radiology images, genomic sequences, and diagnostic videos, which render complete on-chain storage impractical due to the limited capacity and high storage costs of the blockchain. The majority of health tech solutions use a hybrid architecture in which only hashed pointers or metadata are kept on-chain, while the actual data are stored in distributed file systems like IPFS or in protected cloud repositories. However, the above-mentioned solution creates difficulties with storage scalability, integrity verification, and risks in the off-chain infrastructure.

IV. SCALABILITY ISSUES IN BLOCKCHAIN FOR MEDICAL RECORD STORAGE

Scalability is a significant concern in adopting blockchain technology for medical record storage. A system is considered scalable if it can handle increased workloads, such as a rising number of users, records, or transactions, without compromising its performance [34]. In the healthcare domain, this means managing large volumes of electronic medical records (EMRs) with high availability and minimal latency. Scalability also reflects a system's ability to remain resilient and flexible as demand grows.

In the context of blockchain, scalability refers to the network's capacity to grow without experiencing slowdowns or congestion. This paper evaluates existing blockchain-based medical record systems across three key scalability dimensions: throughput, storage, and cost[35]. Throughput refers to the number of transactions processed per second and is heavily influenced by the underlying consensus mechanism. The choice of consensus protocol determines how efficiently nodes reach agreement while maintaining the confidentiality and validity of patient data.

A. Storage Requirements and Growth of Medical Data:

The rapid growth of medical data driven by electronic health records (EHRs), imaging, and wearable devices poses significant storage challenges for blockchain systems. Due to data replication across nodes, blockchain inherently consumes more storage and energy compared to centralized systems. Storing large, sensitive medical files directly on-chain is inefficient and unsustainable, prompting the use of off-chain solutions such as IPFS or cloud storage, with only hashes stored on the blockchain. While these approaches enhance scalability and reduce storage pressure, they also introduce complexity in maintaining data integrity and security. Efficient storage design is thus essential to ensure blockchain-based medical systems remain both scalable and energy-efficient.

B. Network Congestion and Bottlenecks:

Network congestion and bottlenecks are critical challenges in blockchain-based medical record systems, particularly as transaction volume and user base grow. In permissionless blockchains, limited block sizes and transaction throughput can lead to significant delays, especially during peak usage, which is unacceptable in time-sensitive healthcare scenarios. This congestion results in higher latency and reduced system responsiveness, making real-time data sharing difficult. Moreover, the consensus mechanism used, such as Proof of Work (PoW) or even some permissioned models, can exacerbate bottlenecks by limiting the rate at which transactions are validated. To address this, many healthcare-focused blockchain frameworks explore solutions such as sharding, sidechains, and hybrid architectures to maintain network efficiency, reduce transaction latency, and ensure timely access to medical records.

V. LITERATURE OF REVIEW

These literature reviews explore blockchain-based healthcare solutions, focusing on security, privacy, authentication protocols, data sharing, and innovative models for improving healthcare data management, efficiency, and resilience against cyber threats.

Ryu and Kim, (2025) propose a new authentication protocol to prevent and address such issues within hospital systems. The proposed protocol encrypts medical records on a private blockchain, enabling secure sharing among institutions, hospitals, and insurance companies and ensuring data recovery even if a ransomware attack paralyzes the server. Additionally, the protocol facilitates the systematic sharing of patient medical records between hospitals or between hospitals and insurance companies by distributing session keys [36].

Ul *et al.*, (2024) presents a framework for adopting blockchain technology in EHR systems, providing a comprehensive, modular, and straightforward approach. Our proposed framework addresses the constraints of existing EHR systems by providing a platform for connected and interoperable EHRs. The proposed blockchain-based patient health records management framework demonstrates the potential to address the limitations of current centralized health records systems. It offers benefits such as data privacy and security, interoperability, audibility, decentralization, and automation through the use of smart contracts. The proposed framework is implemented in Ethereum [37].

Almalawi *et al.*, (2023) to improve the safety and security of medical professionals' access to cloud-based patient-sensitive data. The experiment's findings suggest that

the secret keys generated are sufficiently random and unique to provide adequate protection for the data stored in modern healthcare management systems. The proposed method minimizes the time needed to encrypt and decrypt data and improves privacy standards [38].

Wenhua *et al.*, (2023) focuses on healthcare security issues in blockchain and identifies security risks across the six layers of blockchain technology by comparing and analyzing existing security measures. It also explores and defines the different security attacks and challenges when applying blockchain technology, which promotes theoretical research and robust security protocol development in the current and future distributed work environment [39].

Taherdoost, (2023) presents research on blockchain's privacy and security in healthcare from 2017 to 2022. In light of the existing literature, this critical evaluation assesses the current state of affairs, with a particular emphasis on papers that deal with practical applications and difficulties. By providing a critical evaluation, this review provides insight into prospective future study directions and advances [40].

Dwivedi *et al.*, (2022) discuss all the existing EMR systems and discuss their drawbacks. Keeping all the drawbacks in their mind, they propose a blockchain-based medical record system that utilizes clouding technology for storage purposes. Furthermore, designed a smart contract and consensus algorithm for the proposed EMR. Its system only uses a permissioned blockchain model so that only verified and authenticated users can generate their data and participate in the data-sharing system [41].

Table 1 summarizes research on blockchain applications in healthcare, highlighting key topics such as secure data sharing, encryption, transaction protocols, and privacy, with insights into improving security, privacy, and efficiency.

Table 1: Literature Summary on Blockchain in Medical Record Storage

Reference	Focus Area	Objectives	Challenges	Key Findings	Future directions
Ryu et.al. (2025)	Blockchain-based authentication for hospital systems	To design a secure authentication protocol for medical record sharing using private blockchain and encrypted session keys	Ransomware attacks, insecure data sharing, server paralysis during attacks	The encrypted private-chain protocol ensures secure inter-hospital and insurance data sharing; enables data recovery even during system paralysis; session-key distribution improves interoperability	Improve protocol scalability; test interoperability across larger national health networks; integrate with AI-driven anomaly detection
Ul et al. (2024)	Blockchain framework for interoperable EHR systems	To design a modular, comprehensive blockchain-based EHR adoption framework on Ethereum	Lack of interoperability, centralized EHR vulnerabilities, privacy issues	Framework enhances data privacy, auditability, automation via smart contracts; interoperable EHR exchange demonstrated on Ethereum	Extend framework to multi-chain settings; evaluate performance in real-world hospital deployments; integrate lightweight consensus mechanisms
Almalawi et al. (2023)	Secure key generation for cloud-based healthcare systems	To improve access security for clinicians using cloud-stored sensitive medical data	Weak key randomness, encryption inefficiency, data privacy risks	Proposed method generates unique, random keys; accelerates encryption/decryption; enhances privacy for cloud-based healthcare systems	Extend method to IoT-based healthcare; integrate quantum-resistant cryptography; evaluate performance for large-scale hospital datasets
Wenhua et al. (2023)	Security vulnerabilities in blockchain layers for healthcare	To analyze security risks across six blockchain layers and assess attacks relevant to healthcare applications	Security attacks across network, consensus, application layers; lack of unified security standards	Provides a taxonomy of blockchain security risks; supports development of stronger security protocols; highlights gaps in existing healthcare blockchain defenses	Development of cross-layer security standards; improved intrusion detection for blockchain healthcare apps; research into adaptive security protocols
Taherdoost et.al. (2023)	Privacy and security review of blockchain in healthcare (2017–2022)	To critically evaluate practical blockchain applications and limitations in healthare	Fragmented solutions, lack of large-scale deployments, privacy concerns	Reviews practical applications and identifies gaps; highlights challenges in scalability, adoption, privacy, and regulatory issues	Proposes future research on compliance frameworks, large-scale pilots, and enhanced privacy-preserving techniques
Dwivedi et al. (2022)	Blockchain-based EMR using cloud storage	To design an EMR system combining blockchain and cloud storage with smart contracts	Limitations of existing EMR systems—centralization, lack of security, poor data sharing	Permissioned blockchain improves security, authentication, and controlled participation; cloud layer supports scalable storage	Expand to hybrid-cloud architecture; include advanced consensus mechanisms; test with multi-institution healthcare systems

VI. CONCLUSION AND FUTURE WORK

The popular blockchain technology has a strong potential in revolutionizing medical record management in terms of providing a secure, transparent, and interoperable exchange of data in a variety of healthcare settings. It has a decentralized structure which makes it immutable, improves patient privacy, and builds trust between hospitals, insurers, and laboratories and regulatory agencies. According to this survey, the advantages of blockchain are remarkable as it can enhance the accuracy of medical data, ensure free interoperability,

minimize administrative overhead, and provide a legitimate universal access to electronic medical records. Nevertheless, these benefits do not stem out of the many technical, organizational, and social obstacles, which limit mass adoption. The issue of scalability is one of the key ones since the amounts of healthcare data are constantly increasing. The solutions to these limitations are needed to maximize the potential of blockchain and construct effective, resilient, and sustainable medical record systems.

Additional studies to be developed in the future include energy-efficient consensus protocols, sophisticated privacy-saving methods, and scalable hybrid storage systems. The further adoption of blockchain will be achieved by integrating AI-based analytics, improving interoperability, and creating regulatory-compliant frameworks. Real-world clinical implementations are necessary to pilot-test and confirm performance, usability, and long-term sustainability.

REFERENCES

[1] C. S. Kruse, M. Mileski, A. G. Vijaykumar, S. V. Viswanathan, U. Suskandla, and Y. Chidambaram, "Impact of electronic health records on long-term care facilities: systematic review," *JMIR Med. informatics*, vol. 5, no. 3, p. e7958, 2017.

[2] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, 2023, doi: 10.56975/tijer.v10i6.158517.

[3] S. Ghaith, G. P. Moore, K. M. Colbenson, and R. A. Lindor, "Charting practices to protect against malpractice: case reviews and learning points," *West. J. Emerg. Med.*, vol. 23, no. 3, p. 412, 2022.

[4] R. La Russa *et al.*, "Analysis of inadequacies in hospital care through medical liability litigation," *Int. J. Environ. Res. Public Health*, vol. 18, no. 7, p. 3425, 2021.

[5] S. O. Ajakwe *et al.*, "Medical IoT Record Security and Blockchain: Systematic Review of Milieu, Milestones, and Momentum," *Big Data Cogn. Comput.*, vol. 8, no. 9, 2024, doi: 10.3390/bdcc8090121.

[6] N. R. de Oliveira *et al.*, "Storage Standards and Solutions, Data Storage, Sharing, and Structuring in Digital Health: A Brazilian Case Study," *Information*, vol. 15, no. 1, 2024, doi: 10.3390/info15010020.

[7] A. Odeh, I. Keshta, and Q. A. Al-Haija, "Analysis of Blockchain in the Healthcare Sector: Application and Issues," *Symmetry (Basel).*, vol. 14, no. 9, 2022, doi: 10.3390/sym14091760.

[8] A. L. A. Fonsêca *et al.*, "Blockchain in Health Information Systems: A Systematic Review," *Int. J. Environ. Res. Public Health*, vol. 21, no. 11, 2024, doi: 10.3390/ijerph21111512.

[9] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, pp. 16–22, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[10] M. Javaid, A. Haleem, R. P. Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," *Blockchain Res. Appl.*, vol. 2, no. 4, p. 100027, 2021.

[11] J. N. Chanda, I. A. Chowdhury, M. Peyaru, S. Barua, M. Islam, and M. Hasan, "Healthcare monitoring system for dedicated COVID-19 hospitals or isolation centers," in *2021 IEEE Mysore Sub Section International Conference (MysuruCon)*, 2021, pp. 405–410.

[12] S. Khadija, A. Abdessadek, A. Khalid, C. Bouchaib, and others, "Impact of Blockchain technology in Healthcare," in *ITM Web of Conferences*, 2022, p. 1007.

[13] V. Singh, D. Pathak, and P. Gupta, "Integrating Artificial Intelligence and Machine Learning into Healthcare ERP Systems: A Framework for Oracle Cloud and Beyond," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 2, pp. 171–178, 2023.

[14] I. M. P. Barbalho *et al.*, "Digital health solution for monitoring and surveillance of Amyotrophic Lateral Sclerosis in Brazil," *Front. Public Heal.*, vol. 11, p. 1209633, 2023.

[15] K. Yaeger, M. Martini, J. Rasouli, and A. Costa, "Emerging blockchain technology solutions for modern healthcare infrastructure," *J. Sci. Innov. Med.*, vol. 2, no. 1, 2019.

[16] A. Gaggioli, "Blockchain technology: Living in a decentralized everything.," *CyberPsychology, Behav. \& Soc. Netw.*, vol. 21, no. 1, 2018.

[17] G. Sarraf, "Privacy-Preserving Blockchain for Healthcare : Addressing Security Challenges Through Decentralized Architecture," *TIJER - Int. Res. J.*, vol. 10, no. 11, pp. 111–117, 2023.

[18] F. M. AbdelSalam, "Blockchain Revolutionizing Healthcare Industry: A Systematic Review of Blockchain Technology Benefits and Threats.," *Perspect. Heal. Inf. Manag.*, vol. 20, no. 3, pp. 1–19, 2023, [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10701638/

[19] Godavari Modalavalasa, "Exploring Big Data Role in Modern Business Strategies: A Survey with Techniques and Tools," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 431–441, Jan. 2023, doi: 10.48175/IJARSCT-11900B.

[20] G. Huang and A. Al Foysal, "Blockchain in Healthcare," *Technol. Invest.*, vol. 12, no. 03, pp. 168–181, 2021, doi: 10.4236/ti.2021.123010.

[21] A. Razzaq, S. A. H. Mohsan, S. A. K. Ghayyur, N. Al-Kahtani, H. K. Alkahtani, and S. M. Mostafa, "Blockchain in healthcare: a decentralized platform for digital health passport of COVID-19 based on vaccination and immunity certificates," in *Healthcare*, 2022, p. 2453.

[22] M. Alnafrani and S. Acharya, "SecureRx: A blockchain-based framework for an electronic prescription system with opioids tracking," *Heal. Policy Technol.*, vol. 10, no. 2, p. 100510, 2021.

[23] R. Q. Majumder, "Designing an Intelligent Fraud Detection System for Healthcare Insurance Claims Using a Machine Learning Approach," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–6. doi: 10.1109/GINOTECH63460.2025.11076870.

[24] F. A. Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid, "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development," *Sustain. Cities Soc.*, vol. 55, p. 102018, 2020.

[25] M. Kassab, J. DeFranco, T. Malas, P. Laplante, G. Destefanis, and V. V. G. Neto, "Exploring research in blockchain for healthcare and a roadmap for the future," *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 4, pp. 1835–1852, 2019.

[26] G. Vonitsanos, T. Panagiotakopoulos, and A. Kanavos, "Issues and challenges of using blockchain for iot data management in smart healthcare," *Biomed. J. Sci. Tech. Res*, vol. 40, no. 2, pp. 32052–32057, 2021.

[27] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Intell. Networks*, vol. 2, pp. 130–139, 2021, doi: 10.1016/j.ijin.2021.09.005.

[28] J. Chanchaichujit *et al.*, "Blockchain technology in healthcare," *Healthc. 4.0 Next Gener. Process. with Latest Technol.*, pp. 37–62, 2019.

[29] X. Wang and L.-Y. Wu, "Toward energy-efficient blockchain system: A game theoretic analysis," *Comput. Ind. Eng.*, vol. 200, p. 110821, 2025, doi: https://doi.org/10.1016/j.cie.2024.110821.

[30] R. Patel, "Sustainability and Energy Management : Trends and Technologies for a Greener Industrial Future," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 1, 2024, doi: 10.48175/IJARSCT-19200E.

[31] E. Ghosh and B. Das, "A Study on the Issue of Blockchain's Energy Consumption," 2020, pp. 63–75. doi: 10.1007/978-981-15-0361-0_5.

[32] A. O. Bada, A. Damianou, C. M. Angelopoulos, and V. Katos, "Towards a Green Blockchain: A Review of Consensus

Mechanisms and their Energy Consumption," *Proc. - 17th Annu. Int. Conf. Distrib. Comput. Sens. Syst. DCOS 2021*, pp. 503–511, 2021, doi: 10.1109/DCOSS52077.2021.00083.

[33] S. Gupta, "Zero-Knowledge Proofs For Privacy-Preserving Systems: A Survey Across Blockchain, Identity, And Beyond," *Eng. Technol. J.*, vol. 10, no. 07, Jul. 2025, doi: 10.47191/etj/v10i07.23.

[34] T. Alghamdi, R. Khalid, and N. Javaid, "A Survey of Blockchain Based Systems: Scalability Issues and Solutions, Applications and Future Challenges," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3408868.

[35] V. Prajapati, "Blockchain-Based Decentralized Identity Systems : A Survey of Security , Privacy , and Interoperability," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 3, 2025.

[36] J. Ryu and T. Kim, "Enhancing Hospital Data Security: A Blockchain-Based Protocol for Secure Information Sharing and Recovery," *Electronics*, vol. 14, no. 3, 2025, doi: 10.3390/electronics14030580.

[37] N. Ul *et al.*, "Blockchain-Based Healthcare Records Management Framework : Enhancing Security , Privacy , and Interoperability," vol. 12, pp. 1–19, 2024.

[38] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing Security of Healthcare Data for a Modern Healthcare System," *Sensors*, vol. 23, no. 7, 2023, doi: 10.3390/s23073612.

[39] Z. Wenhua, F. Qamar, T.-A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends," *Electronics*, vol. 12, no. 3, 2023, doi: 10.3390/electronics12030546.

[40] H. Taherdoost, "Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives," *Sci*, vol. 5, no. 4, 2023, doi: 10.3390/sci5040041.

[41] S. K. Dwivedi, R. Amin, J. D. Lazarus, and V. Pandi, "Blockchain-Based Electronic Medical Records System with Smart Contract and Consensus Algorithm in Cloud Environment," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/4645585.