Significance and Challenges in Blockchain-Based Secure Sharing of Healthcare Data

Rashmi Pathak, Badal Soni, and Naresh Babu Muppalaneni

Abstract Both service providers and patients require healthcare information. Electronic Healthcare Records (EHR) must be shared and maintained in a more secure manner. Blockchain technology has the potential to address many of the issues confronting the healthcare industry, including electronic health record security and privacy (EHRs). Blockchain technology, with its decentralised and transparent ledger, can provide a secure and efficient platform for healthcare data sharing and management. This can help to improve the privacy and security of patient data, the efficiency of healthcare processes, and the ability of healthcare providers to collaborate more effectively. However, issues such as interoperability, scalability, regulation, governance, and security must still be addressed. This article offers a summary of the potential benefits and challenges of blockchain technology in healthcare, with a particular emphasis on EHR security and privacy. It investigates the various blockchain-based models that can be used to secure EHRs, such as public, private, hybrid, and federated models, and discusses the key challenges that must be overcome to ensure the successful implementation of blockchain-based EHRs. While challenges remain, the sustained development and adoption of blockchain-based solutions in healthcare has enormous potential for getting better patient outcomes and transforming healthcare delivery.

Keywords Blockchain · Healthcare · Secure · Access · Storage · Privacy

1 Introduction

Security and privacy must be maintained when storing and sharing medical records. Centralized systems, which are typically used in data sharing systems, can be a significant point of failure. Since the introduction of bitcoin about ten years ago,

R. Pathak (✉) · B. Soni · N. B. Muppalaneni
National Institute of Technology, Silchar, Assam, India
e-mail: rashmi.pathak3012@gmail.com

A. Kumar and S. Mozar (eds.), *Proceedings of the 6th International Conference on Communications and Cyber Physical Engineering*, Lecture Notes in Electrical Engineering 1096, https://doi.org/10.1007/978-981-99-7137-4_74

numerous blockchain variations have been introduced. The health industry is one of the fields where blockchain is finding success.

Data on healthcare is pertinent to everyone. It keeps a physical record of our bodies. The healthcare industry is facing significant challenges in managing and securing electronic health records, which contain sensitive and confidential patient information. Electronic health records (EHRs) have emerged as the standard method for storing and sharing the vast majority of the sensitive data that healthcare organisations handle. Although the security and privacy of EHRs are of the utmost importance, current systems are sadly not completely secure. Sensitive patient data can be compromised by cyberattacks and data breaches, with serious repercussions for patients and healthcare professionals. With its secure and decentralised platform for managing healthcare data, blockchain technology has emerged as a promising approach to overcoming these problems. It is crucial for the identification and management of diseases [1]. Medical data has become a valuable resource as artificial intelligence has quickly advanced. It can aid in diagnosis and be used to build diagnostic models for artificial intelligence [2]. Electronic medical records (EMR) are more convenient for data access and storage than the original paper records, but more care still needs to be taken to ensure that the privacy of the data is protected [3]. The decentralised and immutable nature of blockchain technology is its main benefit. Blockchain technology can offer a secure and open platform for managing healthcare data by distributing and encrypting data across numerous nodes [4]. It may provide a number of advantages, including improved data integrity, better data sharing, and effective management of health data. In order to prevent data privacy leaks, many hospitals and institutions have reduced data transfer and sharing. Figure 1 illustrates how the fusion of blockchain and e-health can improve user-centered smart healthcare solutions.

This article's overall goal is to give a thorough overview of the potential advantages and difficulties of blockchain technology in healthcare and EHR security. Blockchain technology can aid healthcare organisations in enhancing patient outcomes and bettering healthcare delivery by addressing these issues.

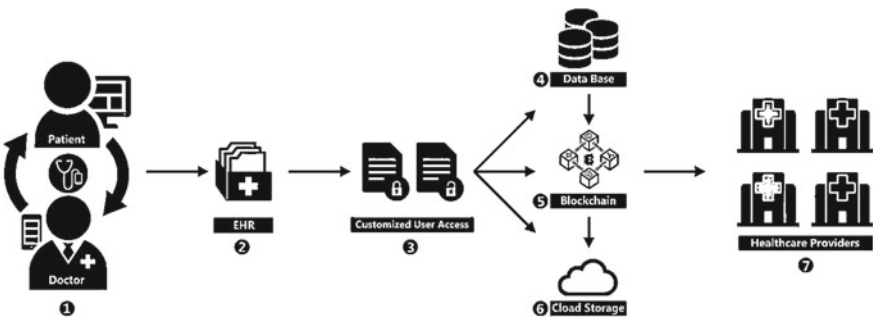

Fig. 1 Block chain mechanism in healthcare

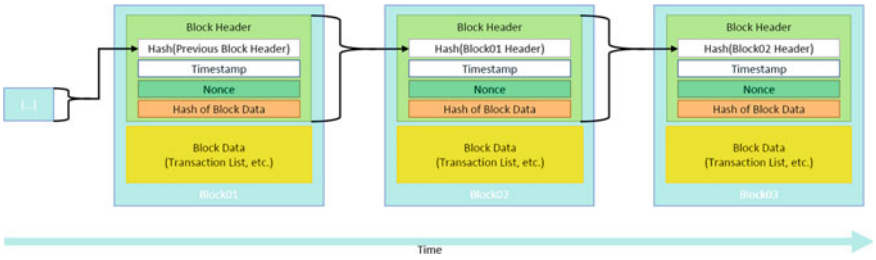

Fig. 2 Structure of block chain

2 Significant Attributes of BlockchainTechnology

2.1 Background Details of Blockchain

Stuart Haber and W. Scott Stornetta, two research scientists, first discussed blockchain technology in 1991. Since Satoshi Nakamoto's invention of Bitcoin, blockchain has received considerable attention. Blockchain is a distributed digital ledger technology that was originally developed as the underlying technology behind the cryptocurrency Bitcoin [5]. The basic concept of blockchain is to create a decentralized and immutable record-keeping system, where data is stored in a network of computers rather than in a central server or database.

The blockchain network is made up of a series of interconnected nodes, each of which stores a copy of the ledger. When a new transaction is made, it is broadcast to all the nodes on the network. Each node then validates the transaction using complex cryptographic algorithms before adding it to the blockchain. The data in a blockchain is organized into blocks, with each block containing a certain number of transactions. Once a block is filled with transactions, it is added to the blockchain and cannot be altered or deleted [6]. This makes blockchain an immutable and tamper-proof record of all transactions that have ever taken place on the network.

In addition to Bitcoin, blockchain technology has found applications in a wide range of industries, including finance, supply chain management, healthcare, and more [7]. Some of the key benefits of blockchain technology include increased security, transparency, efficiency, and accountability. Figure 2 depicts the blockchain's structure.

2.2 Types of Blockchain Methodologies

Blockchain can be classified into several types based on different criteria. Here are some common classifications of blockchain:

- Public blockchain: Also known as a permission less blockchain, this type of blockchain is open to anyone who wants to join and participate. Anyone can create a new block, validate transactions, and become a part of the network. Bitcoin and Ethereum are examples of public blockchains.
- Private blockchain: Also known as a permissioned blockchain, this type of blockchain is only open to a select group of participants who have been given permission to join the network. This type of blockchain is often used by businesses and organizations that want to maintain control over who can access and participate in the network.
- Consortium blockchain: A consortium blockchain is a hybrid between public and private blockchains. It allows multiple organizations to participate in the network and validate transactions, but the consensus mechanism is controlled by a predefined group of nodes. This type of blockchain is often used in industries where multiple parties need to work together, such as supply chain management.
- Hybrid blockchain: A hybrid blockchain combines the features of both public and private blockchains. It allows users to choose between a public or private network depending on their needs. For example, a user may want to keep some transactions private, but allow others to be public.
- Federated blockchain: A federated blockchain is a type of private blockchain where multiple organizations control the network. It is often used in industries where several organizations need to work together, but each organization wants to maintain control over its own data.
- Sidechain: A sidechain is a separate blockchain that is connected to the main blockchain but operates independently. It allows developers to experiment with new features and applications without affecting the main blockchain.

3 Blockchain in Healthcare Data

Blockchain technology has the potential to transform the healthcare industry by enhancing data security, improving data interoperability, and enabling efficient and secure data sharing among stakeholders [8]. In healthcare, blockchain technology can be used to create a decentralized, secure, and tamper-proof ledger of patient health data. This ledger can store patient health data, including medical records, test results, and prescription history, in a secure and immutable manner [9].

By implementing blockchain technology in healthcare, patients can have better control over their health data, and healthcare providers can easily access and share patient data across various healthcare systems [10]. In Fig. 3. The merits of Block chain in Health care are provided in clear manner. Blockchain technology can also facilitate data interoperability among different healthcare providers and organizations, improving the overall quality of patient care. One notable use case of blockchain technology in healthcare is the creation of a patient-centric health information exchange platform. This platform allows patients to securely store and share their health information with healthcare providers and organizations of their choice.

Fig. 3 Merits of block chain in health care

Patients have complete control over who has access to their health data and can grant or revoke access at any time [11–14]. Another use case of blockchain technology in healthcare is in the management of clinical trials. Blockchain technology can be used to create a tamper-proof record of clinical trial data, ensuring transparency and accuracy of the trial results. This can help improve the overall efficiency and effectiveness of clinical trials [15, 16].

Overall, blockchain technology has the potential to revolutionize the healthcare industry by enhancing data security, improving data interoperability, and enabling efficient and secure data sharing among stakeholders [17].

3.1 Concept of Security Storage and Access via Block Chain

Blockchain technology can be used for data security storage and access in a variety of industries, including healthcare, finance, and supply chain management. By leveraging the decentralized and immutable nature of blockchain, sensitive data can be stored securely and accessed only by authorized parties [18, 19].

In traditional centralized systems, data is stored on a server controlled by a single entity. This creates a single point of failure, making the system vulnerable to cyber attacks and data breaches. Blockchain technology, on the other hand, stores data across a network of computers, making it much more difficult for attackers to compromise the system [20].

Additionally, blockchain technology uses cryptography to protect data and ensure that it is tamper-proof. This means that once data is stored on the blockchain, it cannot be altered or deleted without the permission of all parties involved. This provides a high level of security and trust in the data. In terms of access control, blockchain technology can be used to create a permissioned network where only authorized parties have access to specific data [21]. For example, in healthcare, patient data can be stored on a blockchain, and only healthcare providers with permission from the patient can access that data. This provides patients with greater control over their health information and ensures that sensitive data is only accessed by those who need it [22].

3.2 *Blockchain with IOMT*

The Internet of Medical Things (IoMT) refers to the network of medical devices and sensors that are connected to the internet and can transmit data to other devices and systems. Blockchain technology can be used to enhance the security, privacy, and interoperability of IoMT devices and data. By leveraging blockchain technology, the data generated by IoMT devices can be stored in a secure and decentralized manner. This ensures that the data is not vulnerable to cyber-attacks or data breaches, as it is not stored in a single location. Additionally, blockchain technology uses cryptography to protect data, ensuring that it cannot be altered or deleted without the permission of all parties involved.

Blockchain technology can also improve the interoperability of IoMT devices by creating a standardized platform for data sharing as shown in Fig. 4. This platform can enable seamless data sharing and communication between different devices and systems, allowing for more efficient and effective patient care. One potential use case of blockchain technology in IoMT is in the management of electronic health records (EHRs). EHRs contain sensitive patient data, and blockchain technology can be used to create a secure and tamper-proof ledger of EHRs. This can enhance the privacy and security of patient data, while also allowing for easy and secure data sharing between healthcare providers.

Another potential use case of blockchain technology in IoMT is in the management of clinical trials. Blockchain technology can be used to create a tamper-proof record of clinical trial data, ensuring transparency and accuracy of the trial results. This can help improve the overall efficiency and effectiveness of clinical trials. Overall, blockchain technology has the potential to enhance the security, privacy, and interoperability of IoMT devices and data. By leveraging the decentralized and immutable nature of

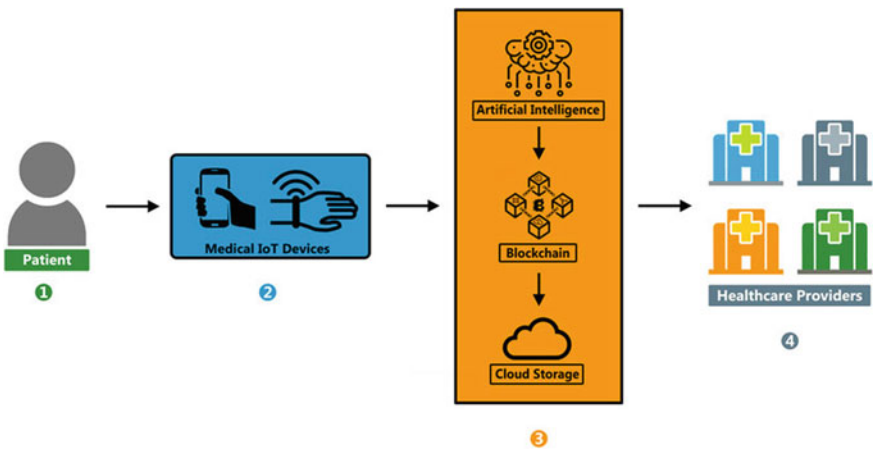

Fig. 4 Structure of blockchain with IOMT

blockchain technology, IoMT data can be stored and shared securely, creating a more efficient and effective healthcare system.

3.3 Blockchain-Based IOMT Models

There are different blockchain-based models that can be used to secure IoMT data, each with its own strengths and weaknesses. Here are a few examples of blockchain-based models for IoMT and their characteristics:

i. **Public blockchain model**: In this model, data is stored on a public blockchain, where anyone can participate in the network and verify transactions. This model offers transparency and immutability, but may not be suitable for sensitive health data due to privacy concerns.
ii. **Private blockchain model**: In this model, data is stored on a permissioned blockchain, where only authorized parties have access to the data. This model offers more privacy and security than public blockchain models, but may be less transparent and immutable.
iii. **Hybrid blockchain model**: This model combines aspects of both public and private blockchains. Data is stored on a permissioned blockchain, but certain data may be made public for transparency purposes. This model offers both privacy and transparency, but may be more complex to implement.
iv. **Federated blockchain model**: In this model, multiple organizations participate in a network of permissioned blockchains. Each organization operates a node on the blockchain, and all nodes must reach consensus before transactions can be validated. This model offers scalability and interoperability, but may be more difficult to manage due to the involvement of multiple organizations.

The choice of blockchain-based model for IoMT will depend on the specific use case and the needs of the organization. Factors such as privacy requirements, transparency, security, and scalability should all be considered when selecting a blockchain-based model for IoMT.

4 Key Challenges in Data Sharing via Blockchain

While blockchain technology has the potential to enhance the security and privacy of healthcare data sharing, there are still several challenges that need to be addressed. Here are some of the key challenges of blockchain-based healthcare data sharing:

i. Interoperability: One of the biggest challenges in healthcare data sharing is interoperability, or the ability of different systems to communicate and exchange data with each other. While blockchain technology can provide a standardized platform for data sharing, there are still issues with interoperability between different blockchain platforms and other healthcare systems.

ii. Scalability: Blockchain technology can be resource-intensive, which can be a barrier to scalability in healthcare data sharing. As more data is added to the blockchain, it becomes increasingly difficult to process transactions in a timely manner, which can slow down the system and limit its scalability.
iii. Regulation: Healthcare data is subject to strict regulatory requirements, such as HIPAA in the United States, which can complicate the implementation of blockchain-based healthcare data sharing. Ensuring compliance with these regulations can be challenging when using a decentralized and distributed system like blockchain.
iv. Governance: Governance of the blockchain network is another challenge in healthcare data sharing. Decisions about how the network is managed, who has access to the data, and how the data is used must be made in a transparent and accountable manner, which can be difficult to achieve in a decentralized system.
v. Security: While blockchain technology can enhance the security of healthcare data sharing, it is not immune to security threats. There is still the risk of cyber attacks, data breaches, and other security threats that must be addressed to ensure the security of the system.

Ultimately, while blockchain technology has the potential to improve the security and privacy of healthcare data sharing, there are still several challenges that must be addressed before blockchain-based healthcare data sharing can be effectively implemented.

5 Conclusions

By providing a secure, decentralised, and transparent platform for data sharing and management, blockchain technology has the potential to revolutionise the healthcare industry. Healthcare organisations can improve the privacy and security of patient data, enhance the efficacy of health systems, and facilitate more effective collaboration among healthcare providers by leveraging the immutability and transparency of blockchain technology. However, several challenges remain to be overcome in order to ensure the effective deployment of blockchain technology in healthcare. Interoperability, scalability, regulation, governance, and security are among the challenges. When creating and carrying out blockchain-based solutions, healthcare organisations must carefully consider these challenges.

Despite these obstacles, the potential benefits of blockchain technology in healthcare are significant, and many organisations are already investigating blockchain-based solutions for a variety of use cases, such as electronic health records, clinical trials, supply chain management, and more. Overall, blockchain technology has the potential to transform the healthcare industry by enabling secure and efficient data sharing and management. While there are still challenges to overcome, the continued development and adoption of blockchain-based healthcare solutions holds great promise for improving patient outcomes and transforming healthcare delivery.

References

1. Stanfill MH, Marc DT (2019) Health information management: implications of artificial intelligence on healthcare data and information management. Yearb Med Inform 28:056–064
2. Adamu J, Hamzah R, Rosli MM (2020) Security issues and framework of electronic medical record: a review. Bull Electr Eng Inform 9:565–572
3. Enaizan O, Zaidan AA, Alwi NHM, Zaidan BB, Alsalem MA, Albahri OS, Albahri AS (2020) Electronic medical record systems: decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. Health Technol 10:795–822
4. Agbo CC, Mahmoud QH, Eklund JM (2019) Blockchain technology in healthcare: a systematic review. Healthcare 7:56
5. Dang H, Dinh TTA, Loghin D, Chang EC, Lin Q, Ooi BC (2019) Towards scaling blockchain systems via sharding. In: Proceedings of the 2019 international conference on management of data, Amsterdam, The Netherlands, 30 June–5 July 2019, pp 123–140
6. Graf M, Rausch D, Ronge V, Egger C, Küsters R, Schröder D (2021) A security framework for distributed ledgers. In: Proceedings of the 2021 ACM SIGSAC conference on computer and communications security, virtual event, Republic of Korea, 15–19 Nov 2021, pp 1043–1064
7. Bhat SS, Ansari GA (2023) A domain oriented framework for prediction of diabetes disease and classification of diet using machine learning techniques. In: AI and blockchain in healthcare. Springer Nature Singapore, Singapore, pp 203–223
8. Ali S, Hafeez Y, Jhanjhi N, Humayun M, Imran M, Nayyar A et al (2020) Towards pattern-based change verification framework for cloud-enabled healthcare component-based. IEEE Access. 8:148007–148020. https://doi.org/10.1109/ACCESS.2020.3014671
9. Reddy PB, Obaid AJ, Reddy VS, Saikumar K (2023) Real-time data mining-based cancer disease classification using KEGG gene dataset. In: AI and blockchain in healthcare. Springer Nature Singapore, Singapore, pp 175–188
10. Javed AR, Faheem R, Asim M, Baker T, Beg MO (2021) A smartphone sensors-based personalized human activity recognition system for sustainable smart cities. Sustain Cities Soc 71:102970. https://doi.org/10.1016/j.scs.2021.102970[CrossRef][GoogleScholar]
11. Singha A, Noel JRS, Adhikrishna RV, Suthahar N, Abinesh S, Poorni SJS (2023) Fetal health status prediction during labor and delivery based on cardiotocogram data using machine and deep learning. In: AI and blockchain in healthcare. Springer Nature Singapore, Singapore, pp 105–135
12. Sun Y, Liu J, Yu K, Alazab M, Lin K (2021) PMRSS: privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare. IEEE Trans Indus Inform 18:1981–1990. https://doi.org/10.1109/TII.2021.3070544
13. Kumar S, Gunjan VK, Ansari MD, Pathak R (2022) Credit card fraud detection using support vector machine. In: Proceedings of the 2nd international conference on recent trends in machine learning, IoT, smart cities and applications: ICMISC 2021. Springer Singapore, pp 27–37
14. Pathak R, Prasad PS, Gunjan VK, Solanki VK (2020) Normalization techniques in multi modal biometric. In: ICCCE 2019: proceedings of the 2nd international conference on communications and cyber physical engineering. Springer Singapore, pp 425–431
15. Pathak R, Soni B, Muppalaneni NB (2023) Role of blockchain in health care: a comprehensive study. In: Proceedings of 3rd international conference on recent trends in machine learning, IoT, smart cities and applications: ICMISC 2022. Springer Nature Singapore Singapore, pp 137–154
16. Gunjan VK, Prasad PS, Pathak R, Kumar A (2020) Machine learning methods for extraction and classification for biometric authentication. In: ICDSMLA 2019: proceedings of the 1st international conference on data science, machine learning and applications. Springer Singapore, pp 1984–1988
17. Pathak R, Gupta SS (2020) A study on natural computing: a review. In: ICDSMLA 2019: proceedings of the 1st international conference on data science, machine learning and applications. Springer Singapore, Singapore, pp 1975–1983

18. Kaur I, Gupta V, Verma V, Kaur S (2023) Securing healthcare records using blockchain: applications and challenges. AI and blockchain in healthcare, pp 57–66
19. Gunjan VK, Kumar S, Ansari MD, Vijayalata Y (2022) Prediction of agriculture yields using machine learning algorithms. In: Proceedings of the 2nd international conference on recent trends in machine learning, IoT, smart cities and applications: ICMISC 2021. Springer Singapore, pp 17–26
20. Singh N, Gunjan VK, Nasralla MM (2022) A parametrized comparative analysis of performance between proposed adaptive and personalized tutoring system "seis tutor" with existing online tutoring system. IEEE Access 10:39376–39386
21. Rudra Kumar M, Pathak R, Gunjan VK (2022) Diagnosis and medicine prediction for COVID-19 using machine learning approach. In: Computational intelligence in machine learning: select proceedings of ICCIML 2021. Springer Nature Singapore, Singapore, pp 123–133
22. Kaur G, Choudhary P, Sahore L, Gupta S, Kaur V (2023) Healthcare: in the era of blockchain. In: AI and blockchain in healthcare. Springer Nature Singapore, Singapore, pp. 45–55