2024 3rd International Conference for Innovation in Technology (INOCON)
Karnataka, India. Mar 1-3, 2024

A Comprehensive Review of Blockchain based Secure EHR: Addressing Challenges and Unlocking Opportunities in Healthcare Data Management

Divyashree D[1]
School of Science Studies, Research Scholar,
CMR University,
Bengaluru, India.
divyashree.d@cmr.edu.in

Chitra Ravi[2]
School of Science Studies, Director & Professor,
CMR University,
Bengaluru, India.
chitraravi@cmr.edu.in

2024 3rd International Conference for Innovation in Technology (INOCON) | 979-8-3503-8193-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/INOCON60754.2024.10511953

***Abstract*- In the rapidly evolving landscape of healthcare, the secure sharing of Electronic Health Records (EHRs) has become a critical component that has garnered significant attention due to concerns regarding security. Furthermore, the recent adoption of blockchain for EHRs has shown potential in enhancing secure sharing. This review work delves into the realm of blockchain-based EHRs, focusing on addressing challenges and opportunities. The main objective of this review paper is to address the challenges while unlocking the opportunities presented by blockchain technologies in designing secure and efficient EHR sharing models. Moreover, this review systematically analyzes existing literature and adoption trends, providing a critical analysis of their implications. The article identifies key challenges such as privacy preservation, data security, and interoperability, and discusses the existing solutions aimed at mitigating these issues. Furthermore, the review primarily concentrates on highlighting the role of blockchain technology in mitigating data breaches, managing patient consent, and facilitating data exchange among stakeholders. Finally, it addresses the research gap in the context of Blockchain-EHR and outlines potential future directions for EHR research.This review paper offers valuable insights into the integration of blockchain technology with EHRs, showcasing its potential benefits and challenges, and providing a foundation for further research in this rapidly evolving field.**

Keywords: EHR, healthcare data management, security blockchain.

I. INTRODUCTION

The world's population is expected to more than double from its present 7.7 billion people by the year 2050, according to a report released by the United Nations (UN) in 2019 [1]. This population growth poses a substantial challenge for healthcare centers worldwide as they strive to enhance their services. However, the current state of healthcare is marred by various issues, including insufficient treatment options, high costs, limited availability of human and medical resources, and vulnerabilities in data security [2][3]. These difficulties underscore the urgent requirement for a reliable along with secure healthcare data records management system that can accommodate the changing needs of healthcare providers while protecting patient information. In the era of rapid advancements in information technology and the pervasive influence of the Internet, Electronic Health Records (EHRs) have emerged as a modern solution to replace traditional paper-based patient records. Figure 1 shows the EHR components

Fig. 1. Electronic Health Record

By transitioning to digital records, healthcare facilities can overcome the limitations associated with physical documents, such as the risk of loss, difficulties in long-term preservation, and inconvenience in portability [1]. For medical researchers and practitioners, access to a comprehensive collection of EHRs is invaluable in their quest to analyze and compare similar or related diseases, thus enabling the development of improved treatment methods. Furthermore, EHR sharing plays a vital role in enhancing disease diagnosis accuracy by equipping healthcare professionals with a holistic view of patients' medical history and symptoms. As shown, one of the main benefits of using cloud-environment based EHR (Electronic Health Records) is the ability to give different authorized users, such as patients, hospitals, laboratories, doctors, and other healthcare professionals, access to up-to-date clinical data from remote servers in various ways.

The practice of sharing EHRs has attracted considerable attention and has become a subject of extensive research in both industry and academia. Among the many facets explored, three key aspects have gained prominence: privacy preservation, data security, and interoperability [2]. The sensitive nature of EHRs, which contain personal and confidential information, necessitates stringent privacy preservation measures to safeguard patient privacy, maintain their reputation, and protect their overall well-being. Moreover, the authenticity and integrity of EHR data are of paramount importance in ensuring the reliability and effectiveness of medical treatments. By combating the presence of forged or modified data, healthcare providers can

rely on accurate and trustworthy information for making informed decisions. Additionally, the establishment of interoperability standards for EHRs empowers patients to maintain control over the accessibility of their records and facilitates seamless data exchange across diverse healthcare institutions. As healthcare systems strive to adapt to the growing demands imposed by a burgeoning population, the effective management and utilization of EHRs play a pivotal role in delivering improved healthcare services. Figure 2 shows the traditional EHR system.

Fig. 2. Traditional EHR system

Addressing the challenges surrounding privacy, security, and interoperability in EHR sharing not only enhances patient care but also paves the way for more efficient healthcare practices, reduced costs, and improved overall healthcare outcomes, blockchain has been the recent adoption to address these challenges.

A. Blockchain

Blockchain technology has drawn a lot of interest as a potential remedy for the problems EHR systems are now experiencing. By leveraging the unique characteristics of blockchain, EHR systems can benefit from improved security, privacy, data integrity, and interoperability. Blockchain, at its core, is a decentralized, unchangeable ledger that logs data or transactions in a visible, chronological order. Blockchain functions as a distributed database in the context of EHR, storing medical data and transactions in a safe and unchangeable manner. The key features of blockchain that make it suitable for EHR systems are:

1) Decentralization:

Each node in the blockchain's network, which is made up of many nodes, possesses a copy of the whole blockchain. Since there is no longer a requirement for a centralized authority, there is less chance of a single point of failure and the system is more resilient as a result of its decentralized structure.

2) Immutability:

Once information is stored on the blockchain, it is very hard to change or remove it. It prevents illegal adjustments and preserves an auditable trail of changes, ensuring the validity and integrity of medical records.

3) Transparency:

Blockchain offers transparency by providing a shared view of transactions to all authorized participants. This transparency enhances trust among healthcare providers, patients, and other stakeholders, as they can verify the integrity and accuracy of shared medical records.

4) Security and Privacy:

Blockchain employs cryptographic techniques to secure data and control access to sensitive information. Patient data can be encrypted, and access can be granted based on permissions and consent mechanisms, ensuring data privacy and reducing the risk of unauthorized data breaches.

5) Interoperability:

Blockchain facilitates seamless data exchange and interoperability between different EHR systems. Through standardized protocols and smart contracts, healthcare providers can securely share medical records, enabling comprehensive patient care and reducing duplication of tests or procedures.

6) Auditability:

The transparent as well as the immutable behavior of blockchain enables easy auditing of EHR transactions. Healthcare organizations can track and verify data access, sharing, and modifications, enhancing accountability and compliance with regulatory requirements.

B. Blockchain based HER

Blockchain-based EHR have emerged as a promising solution in the healthcare industry. This innovative approach utilizes technology of blockchain to enhance the EHR security along with privacy, as well as interoperability of patient health records. The decentralized nature of blockchain-based EHRs is one of its main benefits. Traditional EHR systems often rely on a centralized authority or database, which can be vulnerable to data breaches and unauthorized access. In contrast, blockchain technology distributes and stores EHR data across a network of computers, ensuring transparency and reducing the risk of a single point of failure. This decentralized structure enhances data security and resilience. Another significant benefit of blockchain-based EHR is the immutability and tamper-proof nature of the technology. The blockchain keeps an unalterable record of all EHR transactions by recording each one as a block. This feature ensures the integrity and accuracy of EHR data, as any attempted modification or tampering with the records would require consensus from the entire network, making it highly secure and trustworthy.

Moreover, blockchain-based EHR promotes patient privacy by granting individuals more control over their health data. Patients can provide consent for access to their EHRs, enabling them to manage who can view and update their medical information. This patient-centric approach empowers individuals to maintain ownership and privacy of their sensitive health data, promoting trust and confidentiality.

Interoperability is another key advantage of blockchain-based EHR. As healthcare providers often operate with different EHR systems, interoperability challenges can arise when sharing patient information. Blockchain technology facilitates secure and seamless data exchange between different institutions, ensuring data integrity and streamlining healthcare processes. This interoperability promotes

improved collaboration and continuity of care across the healthcare ecosystem.

Despite these advantages, blockchain-based EHR also faces certain challenges. It takes a lot of technical expertise and resources to deploy and integrate blockchain technology. The decentralised characteristics of the blockchain network might lead to scalability and performance difficulties. Additionally, regulatory and legal frameworks surrounding patient privacy and data protection need to be carefully considered and addressed. Figure 3 shows the blockchain based EHR.

Fig. 3. Blockchain based EHR

1) Motivation:

The motivation behind conducting research on blockchain-based Electronic Health Records (EHR) systems, specifically focusing on Content-Aware Peer-to-Peer Medical Record Sharing through Self-Certified File Systems (SFS), arises from the urgent need to address the issues with conventional EHR systems and utilize the blockchain in healthcare. The existing EHR systems often encounter issues related to data security, privacy breaches, interoperability limitations, and lack of patient control over their medical records. These difficulties make it difficult for healthcare practitioners to collaborate and communicate data easily, possibly jeopardizing patient care and slowing the progress of medical research. By integrating blockchain technology into EHR systems, we can establish a secure, transparent, and decentralized infrastructure that addresses these concerns. The use of self-certified file systems (SFS) and content-aware peer-to-peer medical record sharing further enhances data privacy, fine-grained access control, and patient empowerment.

2) Contribution:

This review paper contributes to the study for secure EHR sharing as well as healthcare data management in a number of ways. It provides a thorough review of the difficulties and possibilities related to this technique. The article identifies key challenges such as privacy preservation, data security, and interoperability, and evaluates existing solutions in addressing these issues. By synthesizing findings from various research studies, it presents a comprehensive understanding of the current research landscape. Additionally, the article proposes future directions for research and development in secure EHR sharing, offering insights for practitioners, policymakers, and researchers. Overall, this review article contributes to the existing knowledge by providing a comprehensive analysis, identifying research gaps, and guiding future research efforts in the field of secure EHR sharing. By encouraging the implementation of blockchain technologies and SFS in EHR, the research ultimately seeks to contribute to the improvement of healthcare systems, facilitating secure and efficient medical record sharing, enhancing patient privacy and control, and fostering collaboration among healthcare providers for improved patient care and research outcomes.

II. Related Work

Due to the blockchain's quick growth, the medical sector has begun to pay close attention to the technology's decentralized, traceable, as well as anonymous features. For many academics, the privacy and security of exchanging electronic health records (EHRs) utilizing blockchain technology has taken center stage.

Numerous research have looked into using blockchain to preserve health data in order to protect individuals' privacy about their health. A searchable encryption strategy for EHRs based on blockchain, for instance, was presented by [6]. The EHR indices created using this method are kept on the blockchain and can be searched using expressions. It does this by employing sophisticated logical expressions to form the indices. Owners of the data can still fully manage their EHRs by merely moving the index to the blockchain. Similarly, [7] unveiled Healthchain, a large-scale blockchain-based privacy protection system for health data. Using transactions for key management, Healthchain's encryption of health data allows for fine-grained control of access and lets users manage approved doctors. The use of blockchain ensures the immutability of both IoT data and doctor diagnoses, minimizing the risk of medical disputes. Furthermore, [8] put out a cutting-edge blockchain-based framework for security and privacy protection when sharing EHRs.

This protocol creates a data structure and consensus mechanism using either a private blockchain or a consortium blockchain. EHRs are maintained on the private blockchain, while secure EHR indexes are kept on the consortium blockchain. For the healthcare blockchain, [9] presented an attribute-based multiauthority signing system. In addition to preventing collusion attacks using shareable pseudorandom function seeds across authorities, this technique focuses on demonstrating the ownership of particular traits for authority delegation. These studies mostly ignore the actual data transfer in favor of examining the use of blockchain to safeguard the index or storing of EHRs. Access control for health information should be implemented, though, with data privacy protections in place.

A blockchain architecture that combines intelligent contracts with user-generated acceptable policies was proposed by [10] in order to promote the easy and secure usage and sharing of personal health data. Through restricted data sharing, this architecture guarantees security control

over personal data in the transmission of health information. Similar to this, [11] put out a conceptual framework for personal continuous dynamic health data sharing that makes use of blockchain technology and cloud storage. This design enables safe and transparent sharing of personal health-related information. Furthermore, [12] introduced an identity and access management system utilizing blockchain technology, specifically within the Hyperledger Fabric framework, for authentication and authorization in digital systems. This system ensures secure identity management and access control. In addition, [13] proposed an attribute-based signature scheme with multiple authorities to ensure the integrity of encapsulated EHRs in the blockchain. In this plan, patients vouch for communications based on their characteristics and offer proof of their attestation.

To increase the security of EHR sharing, several strategies mix blockchain and cloud technologies. As an illustration, [14] presented a cloud-assisted secure eHealth solution that makes use of blockchain to shield outsourced EHRs kept in the cloud from unwanted changes. The system makes sure that only verified users are able to outsource EHRs, and it also guarantees that every action performed on the outsourced EHRs is documented as a transaction on the public blockchain. Similar to this, [15] unveiled the BPDS privacy-preserving data sharing protocol, which uses a consortium blockchain to share EMR indexes while securely storing actual electronic medical records (EMRs) in the cloud. By guaranteeing the immutability of EMRs, this system lowers the possibility of medical data leakage. Furthermore, [16] put out a cloud-based and blockchain-based storage plan and service structure for using medical data.

This plan allows for the use of blockchain technology for applications involving individual medical data without jeopardizing privacy issues. Addressing security and access control concerns in EHR sharing over the blockchain is a second area of research. For instance, [17] suggested a private data exchange strategy based on blockchain-based technology as well as proxy re-encryption techniques to enable a personal health record system. This paradigm handles three major issues: the confidentiality of on-chain data, the storage capacity limitations for massive medical data, and the revocation of consent. Similarly, [18] described a blockchain-based system architecture that provides auditable medical data exchange and healthcare data access authorization management. Another work by [19] developed a blockchain-based searchable encryption strategy for exchanging electronic health records, which improves data searchability by using sophisticated logical expressions as EHR indexes stored on the blockchain. With this method, the EHRs of data owners may be completely controlled by those who have access to them.

Data integrity, anti-interference, and traceability are all maintained by utilizing the decentralized structure of blockchain. Additionally, [20] suggested an attribute-based cryptosystem and a blockchain-based secure EHR system. By combining confidentiality, authentication, medical data integrity, and fine-grained access control, this system makes it possible to administer EHRs effectively while preserving data traceability and integrity. [21] a private blockchain was put in place to link EHR systems from different providers and enable health information exchange (HIE) and ongoing clinical trial monitoring. A different method, called MedBlock, was put up by [22]. It is a blockchain-based health information management system made to efficiently handle patients' electronic medical records (EMRs) and make them accessible and retrievable. Additionally, [23] developed a blockchain approach that makes use of a multiple-authority attribute-based signature system to ensure the authenticity of EHRs without the requirement for a single, reliable authority. While respecting patient privacy, our method guarantees information immutability.

By enabling decentralized data exchange among healthcare providers and boosting data relevance, transparency, and permission management, the Gem Health Network created a blockchain system based on Ethereum [24]. With the help of this technology, healthcare decision-making is made better by fostering greater interoperability and information exchange. Last but not least, [25] suggested an EHR solution built on top of the Ethereum blockchain, enabling patient-centric apps and obviating the requirement for third-party systems. This user-controlled system is accessible via desktop computers and mobile phones, promoting interoperability between healthcare providers and providing patient records in a uniform format. It is evident that blockchain technology can serve as a platform for managing patient records, particularly when implemented as a private permissioned blockchain solution.

Researchers have also proposed various approaches to enhance privacy, access control, and security in EHR sharing. For instance, [26] presented a searchable encryption method with granular access control for blockchain-assisted cloud-based EHR sharing. This system gives consumers control over EHR access by offloading computational chores to edge servers. Data integrity and transaction fairness are guaranteed by the use of blockchain technology and smart contracts, while the efficiency of the system is improved by a consensus process. A security architecture for patient data privacy protection in a mobile edge computing (MEC) environment was provided in a different research by [27]. For the purpose of encrypting electronic health records, the suggested approach uses a simple cryptographic method that incorporates a chaotic map with DNA sequences. A healthcare application portal's data integrity, privacy, permissions, as well as service availability were also ensured by [28] by using Hyperledger Fabric and blockchain. The creation of digital information hubs around the nation has expedited the process, which involves creating a unique identification profile for each user. A innovative access control method based on attribute-based encryption (ABE) that supports multi-level controlled access delegation was also suggested by [29]. In an e-health setting, this system illustrates how it may be used to securely share outsourced EHRs.

References	Methodology	Advantage	Limitation
[6]	Blockchain-based EHRs searchable encryption scheme	Allows data users to search EHR indices using expressions . Data owners retain full control over EHRs	Limited consideration for data sharing
[7]	Healthchain privacy protection scheme based on blockchain	Fine-grained access control for encrypted health data - Revocation and	Limited emphasis on data sharing

		addition of authorized doctors - Prevents data tampering and medical disputes	
[8]	Blockchain-based privacy and security protection EHR sharing protocol	Private and consortium blockchains for data storage and indexing - Improved security and effective treatment in TMIS	Insufficient focus on data sharing
[9]	Attribute-based multiauthority signature scheme in healthcare blockchain	Proves possession of specific attributes for authority delegation	Data sharing considerations are minimal
[11]	Conceptual design for personal continuous dynamic health data sharing using blockchain	Safe and transparent sharing of personal health information Supplementing with cloud storage for efficient sharing	Insufficient focus on access control
[14]	Cloud-assisted secure eHealth system using blockchain	Protection of outsourced EHRs in the cloud. Integration of authenticated participants and public blockchain transactions	Limited consideration for fine-grained access control
[17]	Confidential data sharing model for personal health record system	Ensures privacy of on-chain data and consent revocation Addresses limited storage for large medical data	Limited discussion on data integrity
[21]	Private blockchain for HIE and continuous monitoring of clinical trials	Connects EHR systems from multiple providers	Limited consideration for data integrity
[24]	Ethereum-based blockchain solution for decentralized data sharing	Enables decentralized access to healthcare information Improves relevance, transparency, and permission management	Limited emphasis on access control
[25]	EHR solution on top of the Ethereum blockchain for patient-centric application	Empowers patients to control their data	Insufficient focus on fine-grained access control
[28]	Hyperledger Fabric and Blockchain solution for data integrity and privacy	Ensures data integrity, privacy, and service availability - Unique identity creation for users	Insufficient focus on access control

A. *Future direction*

The integration of blockchain technology in Electronic Health Records (EHR) systems is a rapidly evolving field with numerous potential research directions and opportunities. The following issues need more research as blockchain implementation in healthcare increases:

Enhancing Privacy and Confidentiality: Although blockchain provides secure and transparent storage of data, ensuring patient privacy and confidentiality remains a critical concern. Research should concentrate on creating strong privacy-preserving methods, such as differential privacy and zero-knowledge proofs, to safeguard sensitive patient data while yet allowing secure data sharing as well as analysis.

Scalability and Performance Optimization: Blockchain networks face scalability challenges due to limitations in transaction throughput and data storage capacity. Exploring novel consensus algorithms, sharding techniques, or off-chain solutions can help improve the scalability and performance of blockchain-based EHR systems, ensuring they can handle the increasing volume of healthcare data.

Standards and Interoperability: Achieving seamless interoperability between different blockchain-based EHR systems is crucial for realizing the full potential of blockchain technology. Research efforts should focus on developing standardized protocols, data formats, and smart contract standards to enable efficient and secure exchange of medical records among various healthcare providers, ensuring continuity of care and reducing administrative burdens.

Legal and Ethical Consequences: The implementation of blockchain in EHR involves legal and ethical issues, including data ownership, consent management, liability, and adherence to laws like the General Data Protection Regulation (GDPR). Additional investigation is required to examine the ethical and legal frameworks underlying blockchain-based EHR systems, ensuring compliance with current legal and regulatory requirements while addressing new issues in this area.

User Experience and Adoption: User acceptance and adoption of blockchain-based EHR systems are critical for their successful implementation. Research should focus on understanding the needs, concerns, and preferences of healthcare professionals, patients, and other stakeholders to design user-friendly interfaces, education programs, and incentives that promote the adoption and utilization of blockchain-based EHR systems.

Real-World Deployment and Evaluation: While there are pilot projects and proof-of-concept implementations of blockchain-based EHR systems, real-world deployment and comprehensive evaluations are necessary to assess their effectiveness, efficiency, and impact on healthcare outcomes. Research should involve longitudinal studies, comparative analyses, and user feedback to validate the benefits and limitations of blockchain-based EHR systems in diverse healthcare settings.

III. Conclusion

The integration of blockchain technology in Electronic Health Records (EHR) systems holds significant promise for

addressing the challenges faced by traditional systems and transforming healthcare data management. The concept of Content-Aware Peer-to-Peer Medical Record Sharing through Self-Certified File Systems (SFS) further enhances the security, privacy, and patient control aspects of blockchain-based EHR. Through this review, we have explored the benefits, challenges, and potential solutions associated with blockchain-based EHR systems, with a specific focus on SFS. The research has highlighted the potential of blockchain in improving data security, privacy, integrity, and interoperability in healthcare. Additionally, the concept of SFS allows for fine-grained control over medical record sharing, empowering patients and ensuring content relevance.

REFERENCES

[1] S. Alzahrani and T. Daim, "The adoption and use of tethered electronic personal health records for health management," in R&D Management in the Knowledge Era: Challenges of Emerging Technologies, T. Daim, M. Dabi´c, N. Ba¸so ˘glu, J. R. Lavoie, and B. J. Galli, Eds. Cham, Switzerland: Springer, 2019, pp. 95–143.

[2] S. Ramzan, A. Aqdus, V. Ravi, D. Koundal, R. Amin and M. A. Al Ghamdi, "Healthcare Applications Using Blockchain Technology: Motivations and Challenges," in IEEE Transactions on Engineering Management, vol. 70, no. 8, pp. 2874-2890, Aug. 2023.

[3] A. N. Gohar, S. A. Abdelmawgoud and M. S. Farhan, "A Patient-Centric Healthcare Framework Reference Architecture for Better Semantic Interoperability Based on Blockchain, Cloud, and IoT," in IEEE Access, vol. 10, pp. 92137-92157, 2022.

[4] A. Haddad, M. H. Habaebi, M. R. Islam, N. F. Hasbullah and S. A. Zabidi, "Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems," in IEEE Access, vol. 10, pp. 94583-94615, 2022.

[5] S. Alzahrani, T. Daim and K. -K. R. Choo, "Assessment of the Blockchain Technology Adoption for the Management of the Electronic Health Record Systems," in IEEE Transactions on Engineering Management, vol. 70, no. 8, pp. 2846-2863, Aug. 2023.

[6] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," Future Gener. Comput. Syst., vol. 95, pp. 420–429, Jun. 2019.

[7] J. Xu et al., "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," IEEE Internet Things J., vol. 6, no. 5, pp. 8770–8781, Oct. 2019.

[8] S. Shamshad, K. Mahmood, S. Kumari, C.-M. Chen, "A secure blockchain-based e-Health records storage and sharing scheme," J. Inf. Security Appl., vol. 55, Dec. 2020, Art. no. 102590.

[9] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 6, pp. 11676–11686, 2018.

[10] S. Amofa, E. B. Sifah, K. O.-B. Agyekum, S. Abla, Q. Xia, J. C. Gee, and J. B. Gao, ''A blockchain-based architecture framework for secure sharing of personal health data,'' in Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom). Ostrava, Czech Republic, 2018, pp. 1–6.

[11] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, ''Blockchain-based personal health data sharing system using cloud storage,'' in Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom). Ostrava, Czech Republic, Sep. 2018, pp. 1–6.

[12] T. Mikula and R. H. Jacobsen, ''Identity and access management with blockchain in electronic healthcare records,'' in Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD), Prague, Czech Republic, 2018, pp. 699–706.

[13] R. Guo, H. Shi, Q. Zhao, and D. Zheng, ''Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,'' IEEE Access, vol. 6, pp. 11676–11686, 2018.

[14] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, ''Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain,'' Inf. Sci., vol. 485, pp. 427–440, Jun. 2019.

[15] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, ''BPDS: A blockchain based privacy-preserving data sharing for electronic medical records,'' in Proc. IEEE Global Commun. Conf. (GLOBECOM). Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.

[16] Y. Chen, S. Ding, Z. Xu, H. D. Zheng, and S. L. Yang, ''Blockchain-based medical records secure storage and medical service framework,'' J. Med. Syst., vol. 43, no. 5, Jan. 2019

[17] T. T. Thwin and S. Vasupongayya, ''Blockchain based secret-data sharing model for personal health record system,'' in Proc. 5th Int. Conf. Adv. Inform., Concept Theory Appl. (ICAICTA), Krabi, Thailand, 2018, pp. 196–201.

[18] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, ''On the design of a blockchain-based system to facilitate healthcare data sharing,'' in Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE), New York, NY, USA, Aug. 2018, pp. 1374–1379.

[19] L. X. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, ''Blockchain based searchable encryption for electronic health record sharing,'' Future Gener. Comput. Syst., vol. 95, pp. 420–429, Jun. 2019.

[20] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute based cryptosystem and blockchain," J. Med. Syst., vol. 42, no. 8, Jul. 2018, Art. no. 152.

[21] Y. Zhuang, L. Sheets, Z. Shae, J. J. P. Tsai, and C.-R. Shyu, "Applying blockchain technology for health information exchange and persistent monitoring for clinical trials," AMIA Annu. Symp. Proc., vol. 2018, pp. 1167–1175, Dec. 2018.

[22] .K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain," J. Med. Syst., vol. 42, no. 8, Jun. 2018, Art. no. 136.

[23] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 6, pp. 11676–11686, Feb. 2018.

[24] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in Proc. 18th Int. Conf. E-Health Netw., Appl. Serv., Sep. 2016, pp. 1–3.

[25] T. Fatokun, A. Nag, and S. Sharma, "Towards a blockchain assisted patient owned system for electronic health records," Electronics, vol. 10, no. 5, Mar. 2021, Art. no. 580.

[26] H. Gao, H. Huang, L. Xue, F. Xiao and Q. Li, "Blockchain-enabled Fine-Grained Searchable Encryption With Cloud-edge Computing for Electronic Health Records Sharing," in IEEE Internet of Things Journal.

[27] A. Singh, K. Chatterjee, A. K. Singh and N. Kumar, "Secure Smart Healthcare Framework Using Lightweight DNA Sequence and Chaos for Mobile-Edge Computing," in IEEE Internet of Things Journal, vol. 10, no. 6, pp. 4883-4890, 15 March15, 2023.

[28] M. A. Islam et al., "Distributed Ledger Technology Based Integrated Healthcare Solution for Bangladesh," in IEEE Access, vol. 11, pp. 51527-51556, 2023.

[29] H. S. G. Pussewalage and V. Oleshchuk, "A Delegatable Attribute Based Encryption Scheme for a Collaborative E-Health Cloud," in IEEE Transactions on Services Computing, vol. 16, no. 2, pp. 787-801, 1 March-April 2023.