International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 6 No. 22 March - April - 2025

Electronic Health Records Management Using Blockchain Technology

Sanjana S. Pol
Department of Computer Science, S. M. Joshi College of Arts, Commerce, Science, Hadapsar Savitribai Phule University of Pune.
Corresponding Author – Sanjana S. Pol
DOI - 10.5281/zenodo.15501571

Abstract:

In the recent years, blockchain technology has gained significant attention in the healthcare sector. It has the potential to alleviate a wide variety of major difficulties in electronic health record systems. This study presents an elaborate overview of the existing research works on blockchain applications in the healthcare industry[10] In the healthcare industry, managing electronic health records (EHRs) effectively and securely has always been difficult. However, blockchain technology offers a chance since it can provide information confidentiality, data consistency, and patient ownership over medical history. Blockchain resists corrosion because it is decentralized by nature. This significantly reduces the likelihood of data infringement and ill-advised access while facilitating the easy exchange of medical records between practitioners. Patients gain from this development because it increases their trust, enhances healthcare coordination, gradually lowers administrative costs, and—above all—makes the systems less opaque and more patient-centred.

Keywords: Blockchain, Electronic Health Records (EHR), Medical Research, Healthcare, Privacy, Security Encryption & decryption, Interoperability, Distributed ledger technology, Control, Distributed information system, Patient monitoring.

Introduction:

In today's digital era, healthcare systems worldwide are rapidly adopting Electronic Health Records (EHRs) to improve efficiency, accuracy, and accessibility of patient information. EHRs have revolutionized medical data management by enabling seamless information exchange between healthcare providers, reducing paperwork, and minimizing errors[4]. However, despite their advantages, traditional EHR systems face several critical challenges, including data security threats, lack of interoperability, unauthorized access, and data integrity issues. These concerns have raised the need for a more secure, transparent, and decentralized approach to managing healthcare records [3].

Instead of being controlled by a single organization, medical records are safely stored across numerous nodes in a distributed ledger, which is the foundation of a blockchain-based EHR system [4,7]. To ensure data integrity and traceability, every transaction (or update) in the patient's record is cryptographically encrypted and documented in an unchangeable chain. Blockchain technology known as smart contracts can automate access rights, limiting access to medical records to authorized personnel only. This removes the possibility of illegal changes and data breaches, which are frequent problems with centralized EHR systems[4,6].

Additionally, by making it possible for hospitals, clinics, pharmacies, and insurance companies to share data easily,

blockchain technology improves data interoperability. It can be challenging for medical personnel to obtain thorough patient histories in traditional healthcare systems due to fragmented data storage, which occurs when patient records are dispersed among several organizations. Blockchain offers a single, decentralized database that guarantees instant access to precise patient data, thereby enhancing patient outcomes, diagnosis, and treatment.

The empowerment of patients is perhaps another important benefit of blockchain in EHR management[1]. Patients have little control over their medical records under traditional systems, and obtaining medical histories frequently necessitates a lot of paperwork. Blockchain makes it possible to maintain patient-centred health records, allowing users to use cryptographic keys to grant or withdraw access to their data. This promotes confidence between patients and healthcare professionals by improving patient autonomy, privacy, and security.

Originally designed for keeping a financial ledger, the blockchain paradigm can be extended to provide a generalize framework for implementing decentralized compute resources [12].

High maintenance and management costs are the dire problems that modern healthcare systems face [1]. The healthcare system is highly complex, containing several domains, each comprising physicians, researchers, practitioners, supportive staff, management employees, and patients. As a result, categorization and management of patient data becomes a daunting challenge. This challenge is further exacerbated by dissimilar data structures and disparate workflows in different healthcare domains. For these reasons, the lack of efficient interchange of healthcare-related information among various healthcare domains poses a great hindrance.

Blockchain technology has emerged as a revolutionary solution to address these challenges[12]. Initially developed as the foundation for cryptocurrencies like Bitcoin, blockchain is now being explored for various applications, including healthcare data management. The decentralized, immutable, and secure nature of blockchain makes it an ideal candidate for transforming EHR systems[16]. By leveraging blockchain, healthcare providers can ensure secure and tamper-proof patient data storage, enhance interoperability, and empower patients with greater control over their medical information[14].

The Proof of Work consensus algorithm and its underlying peer-to-peer protocol secure the state- machines' state and transitioning logic from tampering, and also share this information with all nodes participating in the system. Nodes can therefore query the state-machines at any time and obtain a result which is accepted by the entire network with high certainty[8].

Literature Review:

1) Designing a system for patients controlling providers: J. C. Leventhal, J. A. Cummins, P. H. Schwartz, D. K. Martin, and W. M. Tierney.

The usage of electronic health records, or EHRs, is increasing due to financial incentives. In order to apply Fair Information Practice principles to EHRs, clinicians' data needs to offer safe, high-quality care must be balanced with patients' rights to retain their personal information. We outline the organizational and technical difficulties in determining patient preferences for patient-controlled EHR access and implementing those preferences within an already-existing EHR.

2) Public key encryption with keyword search: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano

We examine the challenge of conducting searches on material that has been encrypted with a public key method. In order

to route emails appropriately, an email gateway wants to know if the email contains the word "urgent." Without knowing anything else about the email, we develop and build a system that allows Alice to supply a key to the gateway, allowing the gateway to determine whether the word "urgent" is a keyword in the email. We call this method "keyword search public key encryption."

3) Public key encryption schemes supporting equality test with authorisation of different granularity: Q. Tang

In this paper, we extend the work about public key encryption schemes supporting fine-grained authorisation (FG-PKEET), done by Tang (2011b). First of all, we correct some flaws in Tang (2011b) and discuss how to extend the proposed cryptosystem to support approximate equality test. Secondly, we present a comparison between FG-PKEET and other similar primitives including AoN-PKEET by Tang (2011a) and PKEET by Yang et al. (2010), and demonstrate their differences in complexity and achieved security. Thirdly, to mitigate the inherent offline message recovery attacks, we extend FG-PKEET to a two-proxy setting, where two proxies need to collaborate in order to perform an equality test. Finally, we propose a cryptosystem and prove its security in the two-proxy setting.

4) Efficient verifiable public key encryption with keyword search based on KP-ABE: P. Liu, J. Wang, H. Ma, and H. Nie

Public key encryption with keyword search (PEKS) is a very appealing cryptographic primitive that allows users to search encrypted data, making it suitable for cloud computing environments. Verifiable attribute-based keyword search (VABKS) is a new cryptographic technique that Zheng just suggested. It enables a data user to search the encrypted data file and validate the search result if their credentials meet the data owner's access control policy. In this work, based on key policy attribute-based keyword search (KP-ABKS) of VABKS, we present a new system that "removes secure channel" and provide a novel approach for confirming the searched result from the cloud server. Our verification simulation demonstrates that our scheme is more feasible thanVABKS.

5) Hybrid Blockchain-Edge Architectures: Guo et al.

In order to efficiently manage EHRs, recent research has investigated hybrid architectures that combine blockchain technology with edge computing. Guo et al. (2023) presented a system that combines Paillier homomorphic encryption with multi-authority attribute-based encryption and attribute-based signature aggregation. With all activities documented as unchangeable blockchain transactions, this solution protects EHRs and guarantees patient anonymity. Performance reviews show that this method is robust against unwanted access and satisfies real- world needs.

6) Self-Sovereign Identities in Healthcare: Siqueira et al. (2021)

Blockchain-enabled Self-Sovereign Identity (SSI) gives people more control over their medical records. A thorough review by Siqueira et al. (2021) shown how SSI may empower users by giving them control over their data. The report did point out that there haven't been many SSI deployments in the healthcare industry yet, indicating that the practice is still in its infancy.

7) Challenges in Blockchain Applications: Nguyen (2023).

Blockchain has many obstacles when it comes to digital health applications, despite its potential. Key concerns such network effects, energy usage, data standards, regulatory compliance, and technology accessibility were noted by Nguyen (2023). For blockchain technology to be successfully implemented in healthcare settings, certain issues must be resolved.

8) Privacy and Security Considerations:
Esmaeilzadeh et al. (2023)

Ensuring privacy and security in EHR systems is paramount. A systematic review by Esmaeilzadeh et al. (2023) analyzed blockchain- based approaches for enhancing privacy and security in electronic health systems. The study reviewed 51 papers published between 2018 and December 2022, discussing main ideas, types of blockchains used, evaluation metrics, and tools employed. The review also highlighted future research directions and open challenges in this area.

Proposed Frameworks for EHR Management:

Blockchain-based innovative frameworks have been developed to improve EHR management.

A blockchain-based architecture for managing medical information was presented in a paper that was published in Technologies with the goal of improving security, privacy, and interoperability. The suggested architecture uses smart contracts to enhance the administration and exchange of patient health records while maintaining patient sovereignty over their data, and it incorporates decentralized blockchain technology to mitigate single-point-of-failure problems in current centralized EHR systems.

Blockchain Personal Health Records:

To determine its viability and deployment, the use of blockchain technology in personal health records (PHRs) has been thoroughly examined. In a study that was published in the Journal of Medical Internet Research, the current state of blockchain-based PHRs was analyzed, along with trends and constraints. The study also identified characteristics of different implementations. According to the research, blockchain offers a strong substitute for PHR systems, with advantages like enhanced data security and patient empowerment.

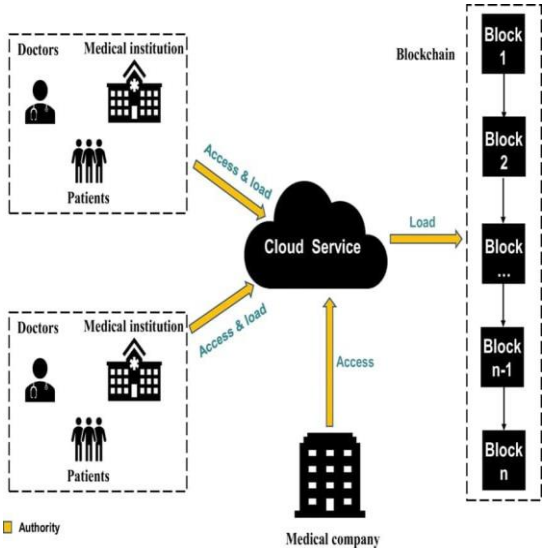

Fig.1 Architecture of EHR[16]

The image illustrates a healthcare data management system integrating cloud computing and blockchain technology. In order to access and load data, medical organizations—including physicians and patients—interact with cloud services. By serving as a middleman, the cloud service manages and stores medical data while guaranteeing safe access. The cloud service is also available to a medical organization, most likely for analytics or data processing.

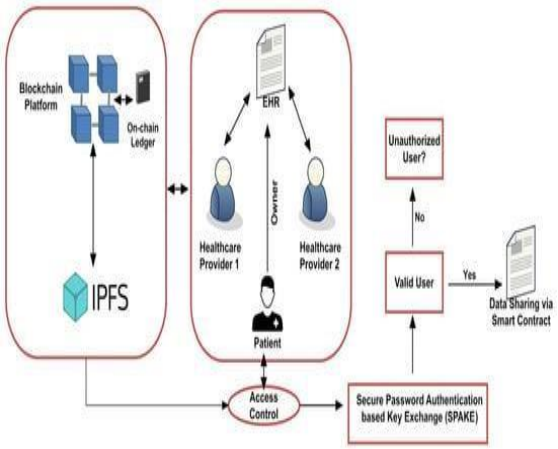

Fig.2 Working of EHR [17]

In fig.2 (Working of EHR)We can see the Data storage that is safe and impenetrable is accomplished through the blockchain component. In order to maintain

integrity and transparency, data is imported from the cloud service onto the blockchain and stored in successive blocks. Data loading and access are supervised by authorities, who are shown via yellow-highlighted connections. This system improves healthcare data management's security, usability, and dependability.

Material and Method:

A blockchain-based EHR system requires hardware such as servers for hosting nodes, computing devices for access, and secure storage solutions[7]. Software components include blockchain frameworks (Hyperledger Fabric, Ethereum), databases (SQL/NoSQL), smart contract tools (Solidity, Chaincode), and identity management solutions (uPort, Sovrin). Security measures involve encryption (AES, SHA-256), authentication (MFA, biometrics), and consensus mechanisms (PoA, PBFT) to validate transactions[9].

Method:

The implementation starts with designing the system architecture, defining blockchain type (public/private/consortium), and identifying stakeholders[10]. Patient data is stored off-chain while blockchain stores hashed records for integrity[8]. Smart contracts automate access control and data updates, while cryptographic techniques like PKC and zero-knowledge proofs enhance security[11]. Interoperability is ensured using IPFS for decentralized storage and FHIR standards for seamless data exchange[17]. APIs integrate blockchain with existing EHR systems. The system undergoes functional, load, and security testing before deployment on cloud platforms like AWS or Azure. Continuous monitoring and regular audits ensure compliance with regulations like HIPAA and GDPR[5].

Result:

The implementation of blockchain technology for Electronic Health Records (EHR) management enhances data security, transparency, and interoperability. By storing patient data off-chain and using blockchain for record hashing, the system ensures integrity while maintaining scalability. Smart contracts automate access control, allowing only authorized users to retrieve medical records, reducing administrative overhead. Encryption techniques and decentralized identity management improve data privacy and prevent unauthorized access. The integration of IPFS and FHIR standards facilitates seamless data exchange between healthcare providers. Performance testing shows that the system efficiently handles high transaction volumes with minimal latency. Security assessments confirm resilience against cyber threats, ensuring compliance with regulations like HIPAA and GDPR. Overall, blockchain-based EHR management proves to be a secure, efficient, and interoperable solution for modern healthcare systems.

Discussion:

By tackling important issues like data security, interoperability, and patient privacy, the use of blockchain technology to the administration of lectronic Health Records (EHRs) has the potential to completely transform the healthcare industry. Data breaches, fragmented information across several providers, and a lack of patient control over medical data are problems with traditional EHR systems. With its decentralized and unchangeable structure, blockchain presents a viable way to address these issues and guarantee security, efficiency, and transparency in the handling of health data.

Improving the Security and Integrity of Data:

Data security is one of the major issues facing the healthcare industry. Because traditional EHR systems are frequently centralized, they are susceptible to illegal access and cyberattacks. By encrypting patient data and only keeping hashed entries on the distributed ledger, blockchain improves security. Because any illegal alteration of records is instantly detectable, this guarantees data integrity. Additionally, using cryptographic methods like zero-knowledge proofs (ZKP) and public-key cryptography (PKC) guarantees that only authorized parties can access private health data.

Enhancing Data Sharing and Interoperability:

Because different hospitals and healthcare providers use incompatible EHR systems, interoperability is still a significant barrier in the healthcare industry. Through the integration of decentralized storage systems such as the Fast Healthcare Interoperability Resources (FHIR), blockchain can standardize the transmission of health data.

Giving Patients Ownership of Their Data:

Hospitals and other healthcare facilities control patient data in traditional EHR systems, which restricts patient access and control. Through smart contracts, patients can grant or cancel access to their medical records thanks to blockchain's decentralized identity management capabilities. By guaranteeing that medical information is only disclosed to reliable healthcare professionals, researchers, or insurers, this improves patient autonomy. Multi-factor authentication (MFA) and digital signatures allow patients to safely control their medical records without depending on centralized authority.

Considerations for Scalability and Performance:

Blockchain-based EHR systems' scalability is still an issue because large transaction volumes might cause network congestion and processing delays. By employing consensus techniques like Practical Byzantine Fault Tolerance (PBFT) to enhance performance, permissioned blockchains such as Quorum and Hyperledger Fabric provide effective substitutes. Sidechains and Layer 2 solutions can also aid in improving scalability while preserving decentralization and security.

Prospects for the Future and Adoption Difficulties:

Despite its benefits, obstacles like high installation costs, reluctance to change, and the requirement for technical know-how prevent blockchain from being widely used in EHR management. To create standardized frameworks and procedures for blockchain-based EHR systems, cooperation between healthcare organizations, technology companies, and regulatory agencies is essential.

Predictive analytics, remote patient monitoring, and real-time health data management may all be further improved by future developments in artificial intelligence (AI) and Internet of Things (IoT) integration with blockchain.

Conclusion:

Data security, transparency, and interoperability are improved when blockchain technology is integrated into the administration of electronic health records (EHRs). Healthcare organizations may guarantee the confidentiality and integrity of patient records while facilitating easy access among authorized entities by utilizing blockchain's decentralized and impenetrable features. This strategy lessens administrative inefficiencies, decreases data breaches, and gives patients more control over their medical records. Blockchain has the ability

to completely transform EHR systems as its use in healthcare develops, promoting efficiency, trust, and better patient outcomes. Healthcare providers may increase patient trust, lower costs, and improve data integrity by utilizing blockchain technology, all of which will improve patient outcomes.

Acknowledgment:

It has been enlightening and stimulating to start the exploration of Blockchain Technology for Electronic Health Records (EHR) Management. Without the steadfast assistance, direction, and encouragement of numerous people and organizations that have greatly influenced its course, this endeavor would not have been feasible.

First and foremost, I would want to express my sincere gratitude to [Mrs. Namita Mane], whose knowledge, tolerance, and priceless ideas have been crucial in helping to improve this study. Their advice has not only improved my comprehension of blockchain applications in healthcare but also motivated me to consider its potential ramifications in the future.

I am incredibly grateful to my classmates and coworkers who participated in stimulating conversations, questioned my beliefs, and offered helpful criticism during this process. Finally, I would want to express my profound gratitude to the blockchain technology pioneers and the larger scientific community, whose innovative work has made this investigation possible. Their contributions keep spurring creative fixes that aim to create a healthcare system that is safer, more effective, and more patient-centred.

This acknowledgement is a sincere way to thank everyone who has helped with this project, whether directly or indirectly. It is not just a formality. We are getting closer to a time when technology will profoundly benefit humanity through teamwork and knowledge sharing.

REFERANCES

1. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, (2016). Medrec: using blockchain for medical data access and permission management. 2016 2nd international conference on open and big data (OBD), pp. 25-30. Doi: 10.1109/obd.2016.112. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). [1].
2. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk AI systems, 40(10), 218. Doi: 10.1007/s10916-016-0574-63.
3. Zhang, P., White, J., Schmidt, D. C., Lenz, G., Rosenbloom, S. T. (2018). [2] Fhirchain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16, 267-278. Doi: 10.1016/j.Csbj.2018.07.0044. Kuo, T.-T.,
4. Kim, H.-E., & Ohno-machado, L. (2017).[3] Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the american medical informatics association, 24(6), 1211–1220. Doi: 10.1093/jamia/ocx0685.
5. Gordon, W. J., & Catalini, C. (2018).[4] Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and structural biotechnology journal, 16, 224-230. Doi: 10.1016/j.Csbj.2018.06.0036.
6. Shuaib, K., Saleh, H., & Badsha, S. (2020). [5] A blockchain-based framework for securing electronic health records. IEEE access, 8, 226719-226730. Doi: 10.1109/access.2020.30437657.
7. Radanović, I., & Likić, R. (2018). [6] Opportunities for use of blockchain technology in medicine. Applied health economics and health policy, 16(5), 583-590. Doi: 10.1007/s40258-018-

0412-88. Esposito, C.,
8. De santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). [7] Blockchain: A panacea for healthcare cloud- based data security and privacy? IEEE cloud computing, 5(1), 31-37. Doi: 10.1109/mcc.2018.0117917129. Xia, Q., Sifah,
9. E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). [8] Medshare: trust-less medical data sharing among cloud service providers via blockchain. IEEE access, 5, 14757-14767. Doi: 10.1109/access.2017.273084310.
10. Dey, T., Jaiswal, A., & Sunderkrishnan, S. (2020). Blockchain in healthcare: A review of current applications and challenges. Journal of systems and software, 173, 110871. Doi: 10.1016/j.Jss.2020.110871.[10]
11. Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.K.R. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. IEEE Trans. Eng. Manag. 2023, 70, 353–368. [CrossRef][11]
12. Xing, W.; Bei, Y. Medical Health Big Data Classification Based on KNN Classification Algorithm. IEEE Access 2020, 8, 28808–28819. [CrossRef][12]
13. Khan, A.A.; Wagan, A.A.; Laghari, A.A.;
14. Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. IEEE Access 2022, 10, 78887–78898. [CrossRef][13]
15. Quadery, S.E.U.; Hasan, M.; Khan, M.M. Consumer side economic perception of telemedicine during COVID-19 era: A survey On Bangladesh's perspective. Inform. Med. Unlocked 2021, 27, 100797. [CrossRef] [PubMed][14]
16. Tomlinson, M.; Rotheram-Borus, M.J.; Swartz, L.; Tsai, A.C. Scaling up mhealth: Where is the evidence. PLoS Med. 2013, 10, e1001382. [CrossRef] [15].
17. Yuan, WX., Yan, B., Li., W.et al. Blockchain-based on medical health record access control scheme with efficient protection mechanism and patient control. Volume 82, 2023.[16]
18. Rahul Sonkamble , Anupamkumar M. Bongale, Shraddha Phansalkar, Abhishek Sharma, Shailendra Rajput. Secure data transmission of electronic health record using blockchain technology 2023[17].