Blockchain-Based Electronic Health Records Management

Binisha R
Department of Computer Science and Engineering
(Associate Professor)
Dr.Mahalingam College of Engineering and Technology
Pollachi, India

Baranisri M
Department of Computer Science and Engineering (Student)
Dr.Mahalingam College of Engineering and Technology
(Anna University)
Pollachi, India

Madhana Nateswar B
Department of Computer Science and Engineering (Student)
Dr.Mahalingam College of Engineering and Technology
(Anna University)
Pollachi, India

Shivapriyan K
Department of Computer Science and Engineering (Student)
Dr.Mahalingam College of Engineering and Technology
(Anna University)
Pollachi, India

***Abstract* —EHRs are digital records containing patients' medical histories and other health-related data, and their management is often plagued by issues such as data fragmentation, privacy, and security concerns. Blockchain technology can address these challenges by providing a decentralized, secure, and tamper-proof platform for storing and managing EHRs. This ensures that patients have control over their data and can grant access to healthcare providers as needed, while also improving data sharing and interoperability between different providers. Blockchain-based EHR management has the potential to streamline administrative processes, reduce medical errors, and create a more patient-centric system, thus transforming the healthcare industry.**

Keywords –Electronic Health Records (EHR).

I. INTRODUCTION

Electronic health records (EHRs) are a critical component of modern healthcare systems. They provide healthcare providers with timely access to a patient's medical history, diagnoses, treatments, and medications, allowing for better-informed decision-making and improved patient outcomes. However, the management of EHRs is often plagued by challenges such as data fragmentation, privacy, and security concerns, and interoperability issues. Enter blockchain technology, which has the potential to transform the management of EHRs by providing a decentralized, secure, and tamper-proof platform for storing and managing patient data. Blockchain technology is a distributed ledger that records transactions and data in a secure and transparent manner, making it ideal for managing sensitive healthcare data. Blockchain-based EHR systems can provide patients with greater control over their health data. With a blockchain-based EHR system, patients can store their health data on the blockchain and grant access to healthcare providers as needed. This can help address concerns around privacy and data ownership, as patients can be assured that their health data is secure and under their control. Furthermore, blockchain technology can improve data sharing and interoperability between different healthcare providers. Today, EHRs are often fragmented across multiple systems, making it difficult for healthcare providers to access a patient's complete medical history. A blockchain-based EHR system could provide a single, secure source of patient data that is accessible to authorized healthcare providers, allowing for better-informed decision-making and improved patient outcomes. In addition to improving data sharing and patient control, blockchain-based EHR systems can also streamline administrative processes and reduce the likelihood of medical errors. For example, blockchain technology can enable automated billing and payment processes, reducing the time and resources required for administrative tasks. Additionally, the secure and transparent nature of blockchain technology can help reduce the risk of medical errors by ensuring that all healthcare providers have access to the same accurate and up-to-date patient data. However, the implementation of blockchain-based EHR systems is not without challenges. For example, healthcare providers must ensure that the data stored on the blockchain is accurate and up-to-date and that patient privacy and confidentiality are maintained. Additionally, the interoperability of blockchain-based EHR systems with legacy EHR systems may be a challenge, and the upfront costs of implementing a blockchain-based system can be significant. Despite these challenges, the potential benefits of blockchain-based EHR systems are significant. They offer a secure, efficient, and patient-centric system for managing EHRs, improving data sharing, and interoperability, and reducing the likelihood of medical errors. As the healthcare industry continues to evolve, it is likely that blockchain technology will play an increasingly important role in the management of EHRs.

II. LITERATURE SURVEY

Blockchain, as suggested by Peng Zhang et al. in this work, is a decentralized, trustless system that combines transparency, immutability, and consensus features to enable safe, pseudo-anonymous transactions. Smart contracts are constructed on top of blockchains to enable on-chain storage and Decentralized Apps (DApps) to interact with the blockchain programmatically. Programmable blockchains have piqued the interest of healthcare professionals as a potential solution to important issues such as a lack of communication, inefficient clinical report delivery, and fragmented health data. This study gives assessment metrics

for blockchain-based DApps in the healthcare industry in terms of feasibility, expected capabilities, and compliance. Blockchain is a novel platform that eliminates the need for a single, centralized authority while yet allowing for safe and pseudo-anonymous transactions and agreements to be made directly amongst interacting parties. Through cryptography and game theory, it provides decentralization, immutability, and consensus. Smart contracts are pieces of code that are constructed on top of a blockchain and may be executed based on predetermined criteria. They allow the creation of Decentralized Apps (DApps) that interface with blockchains and provide on-chain storage. Blockchains provide decentralization, transparency, and immutability qualities that can be used to improve healthcare interoperability. However, existing literature gives few/no measures/guidelines for evaluating/creating blockchain-based healthcare apps. To close this gap, this research proposed a set of assessment measures from both the technical and domain viewpoints that may be used to grade healthcare DApps created with this unique technology and serve as a starting point for future applications in this domain. In the future, we will broaden our research to investigate other acceptable assessment measures and test our findings with specific blockchain-based healthcare use cases.[1]

Key management is one of the most crucial aspects of blockchain security, and effective key management practices are essential for ensuring the confidentiality and integrity of healthcare data. It is essential to use secure key management protocols that can protect the private keys used for signing transactions. Multi-factor authentication (MFA) is a key element of effective key management for health blockchain. MFA can be used to verify the identity of users before granting access to the blockchain network. This can be achieved through the use of biometric authentication, smart cards, or one-time passwords. Hardware Security Modules (HSMs) can be used to provide an added layer of security to private keys. HSMs are physical devices that store and protect private keys and can be used to securely sign transactions on the blockchain. HSMs are often used in healthcare blockchain applications that require a high level of security. Key rotation is an essential key management practice that involves regularly changing private keys to reduce the risk of key compromise. Regular key rotation can help protect against potential security breaches and healthcare blockchain applications. Key recovery mechanisms are essential for healthcare blockchain applications, especially in situations where users lose or forget their private keys. Key recovery mechanisms can include the use of backup keys or the use of secure multi-party computation protocols that enable key recovery without compromising security. Key-sharing mechanisms can be used to enable multiple users to access and use a single private key. Key sharing can be achieved through the use of threshold cryptography or through the use of multi-signature transactions that require multiple parties to sign a transaction. Key revocation is an essential aspect of key management that involves revoking access to a private key in the event of a security breach or other security incident. Healthcare blockchain applications should have key revocation policies in place that are consistent with industry best practices. [2]

A Blockchain Consensus Protocol for Accurate Medical Decisions and Disease Reduction Burden" is a paper that proposes a consensus protocol for healthcare blockchains that can be used to reduce the burden of diseases. The paper proposes a consensus protocol that can be used to accurately identify the causes of diseases and reduce the burden of diseases. The consensus protocol is based on a voting mechanism that involves healthcare providers, patients, and medical researchers. The proposed consensus protocol is implemented on a healthcare blockchain that can securely store and share medical data. The healthcare blockchain is designed to be scalable, efficient, and secure, and it is based on a permission blockchain architecture. The paper highlights the potential benefits of blockchain in healthcare, including increased data security, improved data privacy, and enhanced data interoperability. The use of blockchain can also facilitate the sharing of medical data among different stakeholders, including patients, healthcare providers, and researchers. The paper also discusses the challenges of implementing blockchain in healthcare, including regulatory issues, interoperability challenges, and scalability issues. The paper proposes solutions to these challenges, such as the use of permissioned blockchain architectures and the development of standardized data formats The paper evaluates the proposed consensus protocol through simulation experiments and compares it with other consensus protocols used in healthcare blockchains. The results of the experiments show that the proposed consensus protocol can achieve high accuracy in identifying the causes of diseases and can significantly reduce the burden of diseases. [3]

An effective authentication scheme is critical to ensure the privacy and security of electronic health records (EHRs). Blockchain technology has been proposed as a potential solution to address the security and privacy concerns of EHRs. Blockchain is a decentralized and immutable ledger that provides a secure and transparent way to store and share data. The use of blockchain technology in healthcare can help to improve the security and privacy of EHRs by providing a tamper-proof and transparent system for storing and sharing health data. The paper proposes an authentication scheme for EHRs based on blockchain technology. The proposed scheme uses a combination of public and private keys to authenticate users and provide access to EHRs. The scheme also incorporates multi-factor authentication to enhance the security of the system. The proposed authentication scheme ensures the privacy and security of EHRs by providing a secure and transparent system for storing and sharing health data. The use of blockchain technology ensures that the data is tamper-proof and transparent, while multi-factor authentication ensures that only authorized users can access the data. The paper provides a detailed description of the implementation of the authentication scheme for EHRs based on blockchain. The implementation includes the use of a permissioned blockchain to ensure that only authorized users can participate in the network. The implementation also includes the use of smart contracts to automate the authentication

process and ensure the integrity of the system. The paper evaluates the proposed authentication scheme through simulation experiments and compares it with other authentication schemes used in healthcare. The results of the experiments show that the proposed scheme is more secure and efficient than other authentication schemes. [4]

Secure and privacy-protecting medical data sharing is an important issue in healthcare, as it involves the sharing of sensitive patient data among different stakeholders, including patients, healthcare providers, and researchers. Medical data is sensitive information that requires strong privacy and security protections. The sharing of medical data among different stakeholders can pose significant privacy and security risks, including the risk of data breaches, identity theft, and unauthorized access to patient data. Blockchain technology has been proposed as a potential solution to address the privacy and security concerns of medical data sharing. The use of blockchain technology can provide a tamper-proof and transparent system for storing and sharing medical data while ensuring the privacy and security of the data. Consent management is a critical component of secure and privacy-protecting medical data sharing. Patients should have control over their medical data and should be able to provide or revoke consent for the sharing of their data. Blockchain technology can be used to create a secure and transparent system for consent management. Interoperability is also an important issue in medical data sharing. Different stakeholders use different systems and data formats, which can make it challenging to share medical data. Blockchain technology can provide a standardized system for data storage and sharing, which can facilitate interoperability among different stakeholders. There have been several studies that have evaluated the use of blockchain technology for secure and privacy-protecting medical data sharing. These studies have shown that blockchain-based systems can provide a secure and transparent system for medical data sharing while ensuring the privacy and security of the data. [5]

III. Proposed Methodology

We present a secure multi-owner data-sharing mechanism. It means that any user in the group can safely exchange data with others using the Untrusted cloud. Our suggested method is able to support dynamic groups efficiently. Specifically, newly permitted users can immediately decrypt data files posted before their involvement without communicating with data owners. User revocation may be readily performed using an innovative revocation list without altering the secret keys of the remaining users. The size and processing overhead of encryption is constant and independent of the number of revoked users. We give safe and privacy-preserving access control to users, which assures every member of the group can anonymously utilize the cloud resource. Moreover, the genuine names of data owners might be exposed by the group admin when disagreements develop. SHA algorithm is utilized as the proposed model.

A. Group Member Registration & Login

The initial user in this module enters his username, and password, and selects any one group id before registering with Data Cloud Server. The group signature system allows any member of the group to sign messages while remaining anonymous to verifiers. Furthermore, when a disagreement arises, the appointed group manager can divulge the name of the signature's creator, which is referred to as traceability.

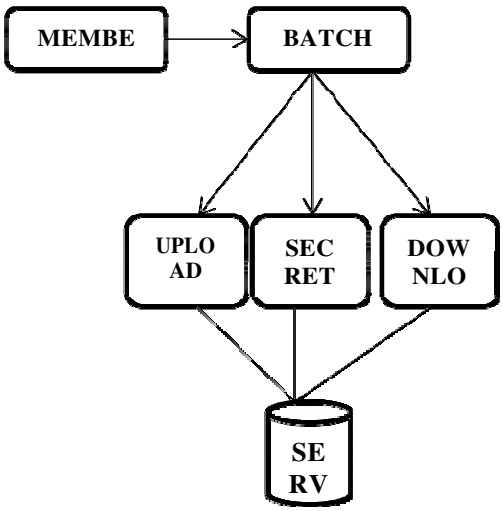
B. Key Generation

Every user in the group produces his or her own public and private keys in the Key Generation module. The user produces a random p and outputs both the public and private keys. Asymmetric cryptography is used in digital signatures. A correctly designed digital signature offers the recipient reason to assume the message was sent by the stated sender when sent via an unsecured channel. In many ways, digital signatures are equal to traditional handwritten signatures; correctly implemented digital signatures are more difficult to falsify than handwritten signatures. Digital signature systems in this context are cryptographically based and must be correctly implemented to be successful. Digital signatures can also provide non-repudiation, which means that the signer cannot successfully claim that they did not sign a message while also claiming that their private key is secret; additionally, some non-repudiation schemes provide a time stamp for the digital signature, so that even if the private key is exposed, the signature remains valid.

C. Upload File To Data Cloud Server

The user wants to upload a file in this module. As a result, he divided the files into multiple chunks. He then encrypts each block using his public key.

D. Download the File From Data Cloud Server



The next user or group member in this module wants to download a file. As a result, he provides the filename and obtains the secret key. Any party (i.e., the signatory, the intended receiver, or any other party) may perform signature verification using the signatory's public key. A signatory may want to double-check the calculated signature before transmitting the signed communication to the intended

recipient. To confirm the legitimacy of the signature, the intended receiver (or any other person) checks it. Prior to validating the signature of a signed message, the domain parameters, as well as the claimed signatory's public key and identity, must be made authentically available to the verifier. The public key can be received in the form of a certificate issued by a trustworthy institution (such as a Certification Authority) or in person with the public key owner.

E. Public Auditing With User Revocation In Public Verifier

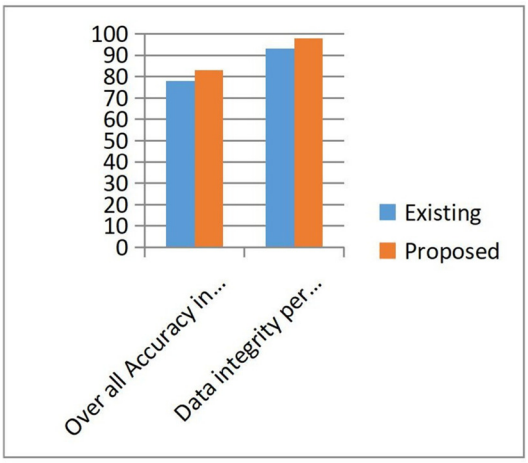
In this module, a user who enters the incorrect secret key is blocked by the public verifier. He then added a public verifier and revoked the user list. The group manager performs user revocation through a publicly available revocation list (RL), on which group members can encrypt their data files and maintain secrecy The Electronic Health Records Management, or EHR, is a network of these software agents, sometimes known as web agents. The MQTT protocol is used to connect to these software agents, which are identified by their IP addresses. In response to a network request, the software agents communicate a complicated set of patient data in a package with a prescribed structure and content. To distinguish it from the partnering hospital's Hospital Information System (HIS), we call this sophisticated data to bundle the Electronic Health Record (EHR).

IV. RESULT ANALYSIS

When comparing results when information is on a circle vs. in storage, it is revealed that while going to all squares, plate throughput restricts IB presentation. DPDP's Except for the core squares of a document, I/O, and test computation occur simultaneously. As a result, IB-DPDP generates confirmations faster than the plate can transmit data: 1.0 seconds vs 1.8 seconds for a 64 MB record. Because I/O constrains execution, no convention can outperform IB-DPDP by more than the initial costs. While faster, multiple plate stockpiling may eliminate the I/O constraint today. After some time, the speeds will exceed the capacity of the circular transmission and the I/O bound will be maintained.

Algorithm	Overall Accuracy in percentage	Data integrity per block(for 100 percentage)
Existing	78	93
Proposed	83	98

Plate I/O adds around 0.04 seconds to the runtime for larger record sizes when compared to in-memory results. Examining execution explains the benefits of IB-DPDP. Probabilistic guarantees make it practical to use public-key cryptography developments to verify ownership of massive informational indexes. Tables 1 and 2 exhibit the proposed and current frameworks' preprocessing exactness and overall accuracy.



Testing breaks the straight scaling relationship between an optimal chance to demonstrate proof of information ownership and record size. IB-DPDP can provide proof of ownership for any record up to 64 MB in size with 99% confidence in around 0.4 seconds.

CONCLUSION

Blockchain-based electronic health records (EHR) management has the potential to improve the security, privacy, and interoperability of healthcare systems. Blockchain technology provides a tamper-proof and transparent system for storing and sharing health data, which can help to address the privacy and security concerns of EHRs. The use of smart contracts can automate the process of managing EHRs, which can reduce the administrative burden on healthcare providers and improve the efficiency of the system. Additionally, the use of blockchain technology can facilitate interoperability among different stakeholders by providing a standardized system for data storage and sharing. Several studies have shown that the use of blockchain technology for EHR management can provide significant benefits, including improved security, privacy, and efficiency. However, there are also challenges associated with the implementation of blockchain-based EHR systems, including the need for robust key management, scalability, and regulatory compliance. Overall, blockchain technology has the potential to transform the healthcare industry by providing a secure and transparent system for managing EHRs. As the technology continues to evolve, it is likely that we will see more widespread adoption of blockchain-based EHR systems in the future, which could help to improve the quality of healthcare and enhance patient outcomes.

REFERENCES

[1] "Metrics for judging blockchain-based healthcare decentralized apps," P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, in Proc. IEEE 19th Int. Conf. e-Health Netw., Appl. Services (Healthcom), Oct. 2017, pp. 1-4.

[2] "Efficient key management strategy for health blockchain," H. Zhao, P. Bai, Y. Peng, and R. Xu, CAAI Trans. Intell. Technol., vol. 3, no. 2, June 2018, pp. 114-118.

[3] A. K. Talukder, M. Chaitanya, D. Arnold, and K. Sakurai, "Proof of Disease: A Blockchain Consensus Protocol for Accurate Medical Decisions and Disease Reduction," in Proc. IEEE SmartWorld,

Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov.

[4] "An efficient authentication strategy for blockchain-based electronic health records," F. Tang, S. Ma, Y. Xiang, and C. Lin, IEEE Access, 2019, vol. 7, pp. 41678-41689.

[5] "A review of safe and privacy-preserving medical data exchange," H. Jin, Y. Luo, P. Li, and J. Mathew, IEEE Access, 2019, vol. 7, pp. 61656-61669.

[6] G. Jetley and H. Zhang, "Electronic health records in IS research: Quality issues, essential thresholds and remedial actions," Decis. Support Syst., pp. 113–137, 2019.

[7] K. Wisner, A. Lyndon, and C. A. Chesla, "The electronic health record's impact on nurses' cognitive work: An integrative review," Int. J. Nurs. Stud., vol. 94, pp. 74–84, 2019.

[8] T. Vehko et al., "Experienced time pressure and stress: electronic health records usability and information technology competence play a role," BMC Med. Inform. Decis. Mak., vol. 19, no. 1, p. 160, Aug. 2019.

[9] W. W. Koczkodaj, M. Mazurek, D. Strzałka, A. Wolny-Dominiak, and M. Woodbury-Smith, "Electronic Health Record Breaches as Social Indicators," Soc. Indic. Res., vol. 141, no. 2, pp. 861–871, 2019.

[10] S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault, "The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review," BMC Med. Inform. Decis. Mak., vol. 19, no. 1, pp. 1–11, 2019.

[11] D. Spatar, O. Kok, N. Basoglu, and T. Daim, "Adoption factors of electronic health record systems," Technol. Soc., vol. 58, no. February, p. 101144, 2019.

[12] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," Cryptography, vol. 3, no. 1, p. 3, 2019.

[13] M. G. Kim, A. R. Lee, H. J. Kwon, J. W. Kim, and I. K. Kim, "Sharing Medical Questionnaries based on Blockchain," Proc. - 2018 IEEE Int. Conf. Bioinforma. Biomed. BIBM 2018, pp. 2767–2769, 2019.

[14] S. Gupta and M. Sadoghi, "Blockchain Transaction Processing," Encycl. Big Data Technol., pp. 366– 376, 2019.

[15] InterPlanatery File System (IPFS)." [Online]. Available: https://ipfs.io/. [Accessed: 04-Feb-2019].