Advances in Parallel Computing Algorithms, Tools and Paradigms
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC220007

Different Approaches on Security, Privacy and Efficient Sharing of Electronic Health Records Using Blockchain Technology

SunithaBJ[a,1], K.Sankar[b], Amreena Ayesha[c] and Dr. M. Islabudeen[d]
[a,b,c,d]*Assistant Professor, Presidency University*

Abstract. Electronic health records (EHRs) are both important and sensitive since they store crucial data that is routinely shared across various parties, such as clinics, pharmacies, and medical practices. These health files require increased safety and confidentiality to prevent leakage or misuse by a third party. There have been instances where a security breach in a patient's electronic medical records has occurred. Blockchain technology may be useful in providing privacy for these documents. The fundamental goal of the work mentioned in this article is to improve the security, privacy, management, and efficient sharing of medical records. In this study, we will present a complete assessment of several strategies for safeguarding EMR privacy using blockchain technology.

Keywords. Blockchain, Electronic Health Records (EHRs), authorized, Secure Sharing.

1. Introduction

A happy lifestyle is built on the foundation of perfect health. Public healthcare has traditionally been a major part of public concern [1]. Electronic medical records (EMRs) are vital healthcare data that doctors and nurses use to diagnose and treat patients. However, this data is considered very confidential and private, and it must be stored securely and protected from unwanted access. Patients' private details, such as name, gender, age, address, phone number, and diagnostic features, such as diagnosis, prescription, and lab findings, are stored in electronic medical records. In recent times, medical institutions have embraced EHR systems, which are data models that save and organise patients' medical records to increase the effectiveness of the healthcare system. Comparing with conventional journal article health records, which have drawbacks [2] including being destroyed, damaged, lost, and not readily available, such systems are more adaptable, economical, and error-free for both health practitioners and patients.

With the expansion of IOT, technology's valuable asset to healthcare services has expanded as well, albeit with some difficulties. The majority of today's healthcare systems are centred on healthcare practitioners and have very limited interoperability. In today's world, patients do not limit themselves to a single hospital or doctor. They may indeed be transferred from one hospital to another, or for medical monitoring and therapy, they may visit various clinics or doctors. In such cases, exchanging the

[1]Amreena Ayesha, Assistant Professor, Presidency University, Bangalore, Karnataka, India. E.mail:amreenayesha@presidencyuniversity.in.

patient's health information for accurate treatment is necessary. The electronic medical records (EMRs) of one medical institution are not necessarily accessible to other medical institutions. Quality care is a well-known problem in healthcare that must be addressed. Patients also have little influence over their health records in these systems.

EMR sharing is thought to be a viable technique for improving healthcare quality, speeding biomedical discoveries, and lowering medical expenses [03]. Private health information, electronic medical records, and electronic health records have all emerged as valuable assets with the ability to influence people's quality of life all around the world. The WHO, with sharing going far beyond its core medical use [4], has previously designated personal health information as an asset. A greater understanding of trends and patterns in population health and sickness in order to provide better care. [5]; excellent advice for trainees or doctors [6] developing programmes that make the most of restricted national health-care funding for everyone's health and wellbeing, etc.,[7]. Medical data is dispersed across numerous medical hospitals and the information's standards of different medical hospitals differ, resulting in a poor level of medical information system interoperability among agencies. There is no assurance of the security and trustworthiness of patient information under the existing medical data management system oriented by medical institutions. Loss of medical files or hacking are unavoidable hazards, and this data is constantly subjected to data security, personal privacy breaches, and other difficulties. The majority of medical files are centralised in medical facilities, making them vulnerable to various risks, such as intentional destruction. Medical data leakage and loss can be caused by manipulation, malware, and natural calamities.

As a result, in this study, we provide a thorough assessment of blockchain options for EHR systems, with a concentration on confidential sharing. As part of the evaluation, we provide the necessary prior knowledge on both EHR systems and blockchain before analysing the (possible) blockchain applications in EHR systems. A variety of research difficulties and opportunities are discussed.

2. Literature Survey

One of the first and most prevalent blockchain uses in healthcare is in the transferring of health records. Health records are difficult to disclose because they are regarded as confidential material and involve patients' private information. Many researchers have investigated the need to employ blockchain in the context of healthcare for ten years. Blockchain technology has the potential to address a few difficulties with present electronic medical records solutions, as well as provide value to the treatment process, remote access to patients' health records, and the preservation of healthcare privacy protection. We did a lot of studies on the concepts of blockchain technology and how it may be used in healthcare for electronic medical records administration, as well as data storage, safe data transfer, and cryptographic techniques used for safe data sharing.

Azaria et al. [8] have developed MedRec, a blockchain platform for saving electronic healthcare records. The MedRec attempts to address issues such as data accessibility responsiveness, portability, and improved data integrity in healthcare. MedRec's design incorporates a private peer-to-peer network.TheEthereum framework can used to create a network (permissioned blockchain) and smart contracts. Monitor and track network state changes.

Dubovitskaya et al. [9], the model gives the topic of cloud computing, which can also aid in the creation of the latest designs for exchanging health files via blockchain, resulting in secure and much more dependable healthcare models in hospital practice. The authors suggest a cloud-based model that enables a blockchain-based database schema to link the network of transmission nodes. They have shown how to control the transfer of healthcare data using smart agreements and permanent, accessible bookkeeping.

Xia et al. [10] have discussed the discovery of a blockchain-based alternative for medical cloud service providers to share records. When employing activation triggers to accomplish operations with smart contracts, the solution intends to assist in creating a query layer (a visual tool for searching information) to link to the blockchain network and enable better ecosystem auditing and control access to records.

Sofia et al. [11] have presented a blockchain-based and intelligent contract-based EHR access and exchange method. They developed a blockchain technology dependent on a decentralised healthcare field, which would allow for greater preservation of patients' medical records while also creating an effective authentication scheme.

Hongyu Li et al. [12] developed a method for EHR retention. This system is based on blockchain and aims to protect patients' privacy while also providing a secure method for storing medical files and guaranteeing the authentication and primitiveness of information saved. They created a Preservation of Data prototype using the Ethereum domain, which is a permission less blockchain network.

2.1.Secure Data Storage

Al Omar et al. [13] suggested MediBchain is a blockchain-based medical system that encodes personal information over a security gateway using a cryptosystem technique (i.e. Elliptic Curve Cryptography (ECC)). Additionally, Lee and Yang suggested that sensing devices' information be posted to the public blockchain using a combination of distinct encryption keys to ensure that biological data is protected and secure. Key guardians (just under the threshold) would not cause data leakage.

Yue et al. [14] Healthcare Information Portal (HDG) is a mobile phone app built on blockchain and the MPC protocol. The system allows encrypted information computations to be performed immediately on the blockchain server, with the results acquired without disclosing the collected information.

In the healthcare blockchain, Guo et al. [15] introduced a multiple-authority essential element authentication mechanism (MA-ABS). Instead of the identification of the person who supports a communication, the signature of this approach testifies to a hold (like an access control mechanism) on the characteristics assigned by a certain agency. However, the network can resist cooperation attempts by disseminating hidden pseudorandom function (PRF) keys amongst officials.

To prevent hacking attempts, medical systems must replace the cryptographic keys in basic ways on a regular basis (e.g. statistical attacks). Since these previous keys should be maintained appropriately in order to decode particular prior data in the future, the cost of maintaining and managing a large number of historical keys will rise.

Zhao et al. [16] devised a minimalist data retrieval secret management scheme for body sensor networks (BSNs) to safeguard the confidentiality of sensor data from the body while reducing private key keeping expenses. Fuzzy banking innovation was utilised to produce, backup, and restore keys without storing any encryption keys, with

BSNs conducting key retrieval. The hacker will also have a tough time accessing sensor information since it is encrypted using asymmetric strong encryption.

Liu et al., [17] built a system for preserving medical information in the cloud in a secure manner using CP-ABE-based access control (CCAC). Data recipients have access to data stored in the cloud. This includes a request for data integrity verification to validate the validity and integrity of the requested data.

2.2. Data Sharing

Hospitals, clinics, laboratories, and other healthcare facilities rely on a variety of data sources maintained in various systems. Patient information should be preserved, accessed, and altered by different healthcare providers for clinical objectives. Unfortunately, such a health information exchange method is problematic due to the varied information infrastructure among various institutions. It is critical to ensure data compatibility among distinct entities before sharing information. First, we will discuss compatibility.

The approach described by Peterson et al., [18] uses Uniform Resource Locators (URLs) preserved with blockchain to refer to FHIR resources, keeping sensitive data off the same blockchain. It also gives Evidence of Interoperability (POI) based on adherence to the FHIR protocol. Miners must guarantee that their data meets specified structural and semantic criteria. must verify incoming messages. This method overcomes a few of the limitations of Proof of Work (PoW) along with increasing compatibility.

Azaria et al., [19] MedRec is a decentralised system for managing records built on the blockchain. Patient-Provider Relationship Contracts are used in this system to connect any two nodes where patients have control over their medical records and can share them with healthcare professionals. Clinicians have the ability to add or change patient authorization records. When malevolent entities break data access rights, a record is kept in the block to trace them down. They also created a user-friendly GUI that enables patients to communicate off-chain information while maintaining fine-grained access control.

Nguyen et al., [20] When mobile users send requests, the admin component builds an access-control protocol based on smart contracts. Smart contracts will verify any transaction using current access standards policies that prevent malicious attacks and ensure trustworthy EHR sharing. However, during the mining process, interested miners may deduce personal information from handling transactions, including such region IDs as cellular port IDs and client IDs.

Liang et al., [21] Hyper ledger Fabric's channel concept, which isolates various forms of activities for clients in various channels to share a variety of fine-grained information, was creatively used. Chain code (smart contract) with various access types, allowed to access functions, and selected shared data indicated in the certificate by the owner of information can be launched in the channel. A channel system like this makes effective use of fabric to improve data preservation in addition to data exchange.

Yue et al., [22] Healthcare Data Gateway is a blockchain-based app architecture for smartphones and computers (HDG). They presented a purpose-centric access control paradigm with two sorts of data depending on purposes: raw information (medical service) and statistical information (medical based research). Throughout the methodology, each transfer procedure uses various sharing mechanisms for various

goals. This system enables patients to simply control and manage the sharing of their health records.

Maesa et al., [23] for smart contract compatibility, depending on blockchain parameters, an access control mechanism based on the XACML protocol was developed. They go into great detail about how to establish and translate access protocols. Their method ensures that valid requestors are properly assessed, while malicious or malfunctioning entities are denied access to any resources.

Dias et al., [24] to handle access control management across diverse entities; a comparable permission matrix for control coupled with consortium blockchain was adopted. To resolve the complexity of various companies owning medical files, blockchain is being utilised to preserve transactions about access permissions.

2.3. Cryptography technology for data sharing

Xia et al., [25] built a model that provides permission for clients to request records from a shared sensitive data repository after confirming their identities and granting keys. In this system, the Consumer Protocol was utilised to generate a participation confirmation essential and a transactional key. The User-Verifier Protocol (UVP) is a protocol that allows users to verify used to verify membership, and only valid users are allowed to send data requests to the system.

Ramani et al., [26] to improve the security of permissioned requests, we used lightweight public key cryptographic procedures (edited, fetch). Nobody can update the information of patients without notifying them, because the requested transaction will be reviewed to see if the client has signed it before being recorded on a private blockchain.

Wang et al., [26] created a platform that utilizes Ethereum and essential element encryption (ABE) techniques to provide perfectly fine access control in a distributed storage solution without the use of a trustworthy secret key generation (PKG). The file's encryption key is kept in an encrypted format on the blockchain using the AES technique. The file encryption key can be decrypted and the encrypted file downloaded from IPFS by requestors whose attributes match the access policies. Furthermore, the smart contract's keyword search.

Zhang et al. [27] created a policy for sharing medical records between nodes in a pervasive social network (PSN). The healthcare data is generated by the wireless body area network. To use an improved version of the show-authorized connection, PSN nodes can install and configure connections for the WBAN. Finally, if the validation is successful, allow entry to exchange network information without imposing a huge storage or processing strain on the sensors, owing to the large number of systems and wireless devices maintained in the blockchain. Furthermore, because all data is saved in smart devices and body sensors, data from illegal behaviour is prevented from leaking.

Liu et al.,[28] The BPDS scheme is a blockchain dependent privacy securing data exchange strategy for EMR. To handle the privacy problem with various groups utilising group signatures and secure the dependability of information from organizations, the system used content extraction signature (CES) to create in the virtualized environment, a blockchain-based data-sharing method. Requestors to verify the confidential nature of shared data can use the immutable ledger record. When a disagreement emerges, the organisations in control of all the team members in the

signatures can determine the data owner's identity. It is evident that data interchange with traceability aids in the improvement of trust connections between businesses.

3. Conclusion

Blockchain has shown significant promise in revolutionising the healthcare business, as we know it. In this study, we looked at how blockchain technology can help the healthcare industry and how it can be used for electronic health records. The blockchain infrastructure combines secure record storage with fine-grained access controls. However, there are still a number of scientific and operational challenges to overcome when attempting to fully integrate blockchain technology with conventional EHR systems. In this paper, we review and describe some of these existing techniques.

References

[1] Mark, A.E, Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technology Innovation Management Review, 2017. 7(10).
[2] Lefeuvre, D., et al., Quality comparison of electronic versus paper death certificates in France. Population Health Metrics, 2014. 12(1): p. 3.
[3] Jingwei Liu, X. L. (2018). BPDS: A Blockchain based Privacy-Preserving Data Sharing for Electronic Medical Records. Global Communications, (pp. pp. 1-6).
[4] E. B.-B. (2018). A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data.International Conference on e-Health Networking, Applications and Services.
[5] NeeshaJothia, N. A. (2015). Data Mining in Healthcare – A Review. Procedia Computer Science . Penang Malaysia .
[6] Yin Zhang, M. C. (2015). iDoctor: Personalized and professionalized medical recommendations based on hybrid matrix factorization. Future Generation Computer Systems.
[7] One-way Hash Function. (n.d.). Retrieved from http://www.aspencrypt.com: http://www.aspencrypt.com/crypto101_hash.html
[8] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. 2016. MedRec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 25–30.
[9] AlevtinaDubovitskaya, Zhigang Xu, Samuel Ryu, Michael Schumacher, and Fusheng Wang. 2017. Secure and trustable electronic medical records sharing using blockchain. CoRR abs/1709.06528 (2017), 1–10.
[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani. 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 5 (2017), 14757–14767. DOI:https://doi.org/10.1109/ ACCESS.2017.2730843
[11] Alexaki, S., et al. Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions. in 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). 2018
[12] Li, H., et al., Blockchain-Based Data Preservation System for Medical Data %J J. Med. Syst. 2018. 42(8): p. 1-13.
[13] Al Omar, A., Rahman, M.S., Basu, A., Kiyomoto, S., 2017. Medibchain: a blockchain based privacy preserving platform for healthcare data. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, pp. 534–543.
[14] Zhang, J., Xue, N., Huang, X., 2016. A secure system for pervasive social network-based healthcare. IEEE Access 4, 9239–9250. Zhang, P., White, J., Schmidt, D. C., Lenz, G., 2017. Applying software patterns to address interoperability in blockchain-based healthcare apps
[15] Guo, R., Shi, H., Zhao, Q., Zheng, D., 2018. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access 6, 11676–11686.
[16] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., Guizani, M., 2018. Bpds: A blockchain based privacy-preserving data sharing for electronic medical records. In: 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 1–6.

[17] Peterson, K., Deeduvanu, R., Kanjamala, P., Boles, K., 2016. A blockchain-based approach to health information exchange networks. In: Proc. NIST Workshop Blockchain Healthcare, 1, pp. 1–10.
[18] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., 2016. Medrec:using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD). IEEE, pp. 25–30.
[19] Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A., 2019. Blockchain for secure EHRS sharingof mobile cloud based e-health systems. IEEE Access.
[20] Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D., 2017. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, pp. 1–5.
[21] Yue, X., Wang, H., Jin, D., Li, M., Jiang, W., 2016. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. 40 (10), 218
[22] Maesa, D., Mori, P., Ricci, L., 2018. Blockchain based access control services. 10.1109/ Cybermatics_2018.2018.00237.
[23] Dias, J. P., Reis, L., Ferreira, H. S., Martins, Â., 2018. Blockchain for access control in e-health scenarios. arXiv:1805.12267.
[24] Xia, Q., Sifah, E., Smahi, A., Amofa, S., Zhang, X., 2017. Bbds: blockchain-based data sharing for electronic medical records in cloud environments. Information 8 (2),
[25] Ramani, V., Kumar, T., Bracken, A., Liyanage, M., Ylianttila, M., 2018. Secure and efficient data accessibility in blockchain based healthcare systems. In: 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 206–212.
[26] Wang, S., Zhang, Y., Zhang, Y., 2018. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access 6, 38437–38450.
[27] Zheng, X., Mukkamala, R.R., Vatrapu, R., Ordieres-Mere, J., 2018. Blockchain-based personal health data sharing system using cloud storage. In: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, pp. 1–6.
[28] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., Guizani, M., 2018. Bpds: A blockchain based privacy-preserving data sharing for electronic medical records. In: 2018 IEEE Global Communications Conference (GLOBECOM).