INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 411-416

EXPLORING THE IMPLEMENTATION OF A DISTRIBUTED LEDGER APPROACH FOR BLOCKCHAIN-BASED INTEGRATED ELECTRONIC HEALTH RECORDS: A METHODOLOGY UTILIZING ETHEREUM SMART CONTRACTS

Y. Durga Bhargavi[1], Jukanti Anusha[2], Abhishek Jamnor[3], Raja Shivani[4], G. Anil Kumar[5]

[1]Assisstant Professor, Computer Science and Engineering, ACE Engineering College, India.

[2,3,4,5]Computer Science and Engineering, ACE Engineering College, India.

ABSTRACT

Blockchain has been an interesting research area for a long time and the benefits it provides have been used by several various industries. Similarly, the healthcare sector stands to benefit immensely from blockchain technology due to security privacy confidentiality, and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security integrity and management. In this paper, we discuss how blockchain technology can be used to transform EHR systems and could be a solution to these issues. We present a framework that could be used for the implementation of blockchain technology in the healthcare sector for EHR. Healthcare systems provide fewer security measures to secure health records. Blockchain is a distributed and decentralized ledger that plays a vital role in securing data and transactions. The aim of our proposed framework is firstly to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining granular access rules for the users of the proposed framework. Moreover, this framework also discusses the scalability problem faced by blockchain technology in general via the use of off-chain storage of the records. This framework provides the EHR system with the benefits of having a scalable secure and integral blockchain-based solution.

Keywords: Blockchain, Electronic Health Record

1. INTRODUCTION

In healthcare, electronic health records (EHRs) contain highly sensitive personal data for the diagnosis, treatment, and management of patients, which are regularly updated, accessed, and shared by multiple parties including doctors, nurses, hospitals, pharmacies, medical researchers, and insurance companies. This poses a major challenge to EHR management for storing, updating, and sharing EHRs without compromising their security or violating patients' privacy. For instance, according to the U.S. Department of Health and Human Services Office for Civil Rights (OCR), the largest Health Insurance Portability and Accountability Act (HIPAA) violation penalty of 2020 was imposed on the health insurer Premera Blue Cross for a data breach of 10,466,692 EHR records. Blockchain technology has been proposed as a potential solution for EHR management in recent years. However, to maximize the capability of blockchain-inspired EHR data management systems, all the following problems are still required to be fully considered. First is the privacy concerns of the patients and security problems for the EHR data. Due to blockchains' decentralized and transparent characteristics, any patient's sensitive and private data can not be saved directly in the new blockchain transaction. The second is the storage space for each block. Usually, the storage capacity of blocks in blockchain transactions is very limited to accept EHR information, including large-size medical images In India, the National eHealth Authority(NeHA) is a proposed organization that aims to set certain regulations in the field of eHealth care. This is being done to ensure standardization of eHealth records which would facilitate secure access to these records while ensuring privacy. The model proposed in this paper could be used for this very purpose. To provide absolute privacy and security, we have put to use the concepts of cryptography, blockchain, and IPFS. Blockchain is an immutable list of records, which are stored in blocks with each block being linked to the previous block. In a Blockchain, every transaction made between the accounts including between a user and a smart contract account is stored in a block. These transactions are public and irreversible once they have been stored in a block. So everyone can see who has accessed which smart contract. In Blockchain for Healthcare, the patient data is stored on the blockchain after being encrypted with the patient's private key. This data can be decrypted using the patient's public key which is provided to users such as hospitals and researchers to whom the patient has given permission. This is in stark contrast to our approach in which the patients have complete control over who can view their data. In our model, the patient's private key is required to decrypt the data instead of encrypting it. Also, we do not store the data on the blockchain but instead use IPFS for the same. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research makes use of the blockchain to store encrypted medical record details such as where it is stored(hashed pointers) and who has access to it. Only the owner of the data can change the access control

policies. All the data is stored in a data lake. For identity authentication, the suggested method in this model is a biometric system which would be more secure than a password. The difference between this approach and ours is the distributed nature in which the data is stored in our system.

2. LITERATURE SURVEY

As part of the Literature Survey, we have referred few project papers and the findings from them are:

Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain-Based Framework: MyBlockEHR Rahul Ganpatrao Sonkamble, Shraddha P. Phansalkar 2021 [1]

The paper investigates the critical issue of interoperability in Electronic Health Records (HER) management. By conducting a thorough literature review, the study addresses key questions related to standards for EHR storage, and cross-chain interoperability. The findings emphasize the potential of a blockchain-based HER framework, MyBlockEHR, which employs on-chain and off-chain storage portioning to enhance performance. The paper underscores challenges in adopting blockchain in HER management while proposing a solution that demonstrates improved efficiency. In conclusion, the research highlights the significance of HER interoperability for seamless healthcare services and presents a practical framework to address associated challenges.

Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records iIPFS Jin Sun, Xiaomin Yao, Shangping Wang, and Ying Wu 2020 [2]

This paper addresses the integrity and security challenges in Electronic Medical Records (EMR). They propose a novel approach using attribute-based encryption, blockchain, and IPFS for secure and efficient EMR storage and sharing. Attribute-based encryption controls access without compromising efficiency. Encrypted EMR is stored on decentralized IPFS for security, and blockchain ensures immutability and traceability. The scheme provides security against keyword attacks, demonstrated through simulations on real datasets. Despite these strengths, challenges exist in managing access privileges effectively, ensuring timely expiration of user access, and optimizing the functionality of data stored on the blockchain. Addressing these limitations will contribute to refining the overall effectiveness of the system in providing secure and controlled access to sensitive healthcare information.

Mobile Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain Shufen Niu, Lixia Chen, Jinfeng Wang and Fei Yu 2020 [3]

This study suggests a solution for the challenges in managing electronic health records (EHRs) by using permissioned blockchains. These digital ledgers ensure secure and controlled access to medical data through encryption. The system also protects patient identity while connecting keywords, enhancing privacy. It tackles issues like dishonest doctors uploading false EHRs by implementing secure keyword searches and storage on permissioned blockchains. This approach not only ensures precise access control but also promotes efficient sharing of medical information among institutions using blockchain technology, ultimately improving the speed and accuracy of patient diagnosis and hospital workflows.

Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain Yong Wang, Aiqing Zhang, Peiyun Zhang and Huaqun Wang 2019 [4]

This paper addresses the significance of sharing electronic health records for disease research and medical diagnoses. It highlights concerns with existing cloud-based EHR sharing due to centralized systems, posing threats to data security and privacy. The paper introduces a solution using blockchain technology, leveraging its decentralized, anonymous, unforgeable, and verifiable properties. The proposed protocol involves searching for relevant EHRs on a blockchain and obtaining re-encryption ciphertext from a cloud server with the data owner's authorization. Employing searchable encryption and conditional proxy re-encryption ensures data security, privacy, and access control. A proof of authorization serves as the consensus mechanism for the blockchain. Security analysis and performance evaluation on the Ethereum platform confirm the protocol's effectiveness, presenting a blockchain-based EHR sharing scheme with conjunctive keyword searchable encryption and conditional proxy re-encryption for secure and private data sharing among medical institutions.

Blockchain for Secure EHRs Sharing of Mobile Cloud-Based E-Health Systems Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding and Aruna Seneviratne 2019 [5]

This paper proposes a novel EHRs sharing scheme enabled by mobile cloud computing and blockchain. They identified critical challenges of current EHR sharing systems and proposed efficient solutions to address these issues through a real prototype implementation. In this work, their focus is on designing a trustworthy access control mechanism based on a single smart contract to manage user access to ensure efficient and secure EHR sharing. To investigate the performance of the proposed approach, they deployed an Ethereum blockchain on the Amazon cloud,

where medical entities can interact with the EHRs sharing system via a developed mobile Android application. They also integrated the peer-to-peer IPFS storage system with blockchain to achieve decentralized data storage and data sharing.

Using Blockchain for Electronic Health Records Ayesha Shahnaz, Usman Qamar, and Ayesha Khalid 2019 [6]

In this paper, the focus is on the application of blockchain technology to address persistent challenges in the healthcare sector, particularly in the context of electronic health records (EHR) systems. Despite notable advancements in healthcare and EHR technologies, certain issues still need effective solutions, and blockchain is proposed as an innovative approach. The outlined framework introduces a combination of secure record storage and granular access rules for these records. This integration aims to create a system that is not only secure but also user-friendly. One of the key challenges addressed is data storage, and the framework tackles this by leveraging the off-chain storage mechanism provided by the InterPlanetary File System (IPFS). Furthermore, the framework incorporates role-based access controls, ensuring that medical records are accessible only to trusted and relevant individuals. This not only enhances security but also addresses the problem of information asymmetry within EHR systems. Users can easily understand and navigate the system, promoting a more efficient and transparent healthcare record management process.

Expense An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records Fei Tang, Shuai Ma, Yong Xiang and Changlu Lin 2019 [7]

This literature survey addresses challenges in traditional electronic health records (EHRs), where information control among different hospitals hampers seamless sharing. While cloud-based EHRs offer a solution, they face centralization issues. The paper proposes a novel approach using blockchain technology (blockchain-based EHRs) to overcome centralization problems. The focus is on defining a system model within a consortium blockchain, emphasizing the importance of authentication in EHRs. The paper introduces an identity-based signature scheme with multiple authorities to enhance authentication in blockchain-based EHRs, emphasizing its resilience against collusion attacks. The proposed scheme is provably secure, operating efficiently with improved signing and verification algorithms compared to existing authentication methods. The ultimate goal is to establish a secure and decentralized paradigm for managing electronic health records.

A BlockChain-Based Medical Data Sharing and Protection Scheme Xiaoguang Liu, Ziqing Wang, Chunhua Jin, Fagen Li and Gaoping Li 2019 [8]

This paper explores how electronic health records (EHRs) are valuable for tracking medical histories and the challenges of sharing and protecting this data. It suggests a solution using blockchain, specifically private blockchains for hospitals, to ensure secure, open, and tamper-resistant data. The scheme lets doctors securely store and access patient information while preserving privacy. Patients with similar symptoms can authenticate and securely discuss their conditions. The proposed system, implemented using PBC improves electronic health systems in hospitals.

EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain Ahmed Raza Rajput, Qianmu Li, Milad Taleby 2019 [9]

This paper introduces the Emergency Access Control Management System (EACMS), a solution designed to address privacy and security concerns for patients' Personal Health Records (PHR) during emergencies. The system is built on Hyperledger Composer, a permission blockchain technology, ensuring that access to PHR data is restricted to known members of the blockchain network, as approved by the admin peer designated by consortium organizations. The framework outlines how access to a patient's PHR is managed during emergency conditions using the capabilities of the Hyperledger Fabric (HF) and Hyperledger Composer. Specific rules for emergency control management of PHR are established, providing a structured approach to handling sensitive health data in critical situations. One notable feature is the storage of patients' data in all transactions on the system, contributing to the comprehensive management of health data. By utilizing the HF blockchain, the proposed EACMS aims to ensure the security of patients' PHR data items while maintaining efficiency in terms of time, accessibility, privacy, and granular access control management. To validate the effectiveness of the framework, the EACMS is implemented and evaluated through the Hyperledger Fabric blockchain. Experimental results affirm that the proposed system successfully secures sensitive PHR data, ensuring efficient access, privacy protection, and granular control over data management during emergency scenarios.

Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in ElectronicHealth Records Systems Rui Guo, Huixian Shi, Qinglan Zhao and Dong Zheng 2018. [10]

Electronic Health Records (EHRs) are entirely controlled by hospitals instead of patients, which complicates seeking medical advice from different hospitals. Patients face a critical need to focus on the details of their healthcare and restore the management of their medical data. The rapid development of blockchain technology promotes population

healthcare, including medical records as well as patient-related data. This technology provides patients with comprehensive, immutable records, and access to EHRs free from service providers and treatment websites. In this paper, to guarantee the validity of EHRs encapsulated in blockchain, we present an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute the public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attacks out of N from N -1 corrupted authorities. Under the assumption of the computational bilinear Diffie-Hellman, we also formally demonstrate that, in terms of the unforgeability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. The comparison shows the efficiency and properties between the proposed method and methods proposed in other studies. Aiming at preserving patient privacy in an EHR system on blockchain, multiple authorities are introduced into ABS and put forward an MA-ABS scheme, which meets the requirement of the structure of blockchain, as well as guaranteeing the anonymity and immutability of the information. PRF seeds are needed among authorities and the patient's private keys need to be constructed, N 1 corrupted authorities can- not succeed in collusion attacks. Finally, the security of the protocol is proven under the CBDH assumption in terms of unforgeability and perfect privacy. The comparison analysis demonstrates the performance and the cost of this protocol increase linearly with the number of authorities and patient attributes as well.

3. COMPARISION ANALYSIS

S.No	Paper Title	Work done on paper	Future work	Drawbacks
1	Rahul, Shradda P, Vidyasagar, Anupkumam "Survey ofInteroperability in ElectronicHealth Records Management and Proposed Blockchainn BasedFrameworkk: MyBlock HER", 2021	Primarily focuses on addressing the importance ofElectronic Health Record(EHR) interoperability, emphasizingits significance for seamless information sharing amongvarious healthcare stakeholders.	Refining AI algorithms, enhancing budgeting recommendations, advanced financial risk assessments, investment diversification suggestions, further language support, and user education.	The computation burden may limit its furtherapplications for real-life scenarios and difficulties in obtaining better performance.
2	Jin Sun, Xiaomin Yao, ShangpingWang, and Ying Wu "Blockchain-based secure storage and access scheme", 2020	Developed a secure systemfor electronic medical records, ensuring controlled access, decentralized storage using IPFS, and tamper-proof blockchain technology.	Investigate potential improvements in search functionality and retrieval speed.	Unsuitable for large-scale scenarios, Poor Application Performance&Small Networks can be compromised.
3	Shufen Niu ,Lixia Chen , Jinfeng Wang and Fei Yu "Electronic Health Record Sharing Scheme With SearchableAttribute-Based Encryptionon Blockchain", 2020	Proposed a medical data-sharing scheme leveraging permissioned blockchains and ciphertext-based attribute encryption	Exploring scalability, addressing potential limitationsin the proposed scheme, and enhancingsystem robustness	High level of communication and computation overheads, Less Resiliency dueto Less Decentralization, Tedious message updating.
4	Yong Wang, Aiqing Zhang, Peiyun Zhang,and Huan Wang "Cloud-Assisted HER Sharing With Security and Privacy Preservation via	Blockchain-based EHR sharing scheme with conjunctive keyword searchable encryption and conditional proxy re-encryption to realize	Hyperledger Fabric and perfect smartcontracts for running the algorithms ofdata sharing.	Cannot be implemented in real time Heavyweight Difficult to beused in large-scale parallel computing.

	Consortium Blockchain", 2019	data securityand privacy preservationof data sharing between different medical institutions.		
5	Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding and Aruna Seneviratne "Blockchainn for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems", 2019	EHRs sharing scheme enabled by mobile cloud computing and blockchain.	Adapting theprotocol to evolving blockchain technologies.	Computation burden may limit its further application forreal scenarios. Additional configuration is required It is not an easy-to-use method
6	Ayesha Shahnaz, Usman Qamar,and Ayesha Khalid "Using Blockchain for ElectronicHealth Records.", 2019	How blockchain technology canbe useful for the healthcare sector and howit can be used for electronic health records.	Implement the payment module in theexisting framework	Narrowly specialized knowledge Significantly increases capital and operating expenditures,Prone to Errors
7	Fei Tang, Shuai Ma, Yong Xiang,and Changlu Lin "An Efficient Authentication Scheme for Blockchainn-Based Electronic Health Records", 2020	The authentication scheme of EHR systems is based onblockchain.	More efficient algorithm.	Significantly increases capital and operating expenditures Richer People can control the network Additional configuration is required
8	Xiaoguang Liu, Ziqing Wang, Chunhua Jin, Fagen Li and Gaoping Li "A Blockchainn-Based Medical Data Sharing and ProtectionScheme", 2016	The features of blockchain technology such as decentralization and tamper resistance make it very suitable for theprotection and sharing of medical data	Performancecan be improved.	Poor Application Performance Solutions have been proven ineffective High complexity, inaccuracy, and inadequacy
9	Ahmed RazaRajput, Qianmu Li, Milad Taleby Ahvanooey and Isma Masood "EACMS: EmergencyAccess Control Managementnt System for Personal Health Record Based on Blockchain", 2019	Emergency Access ControlManagement System called EACMS whichprovides privacy protection and security policies for thepatient's PHR in emergency condition	Design using Less processing power and tryto match the current network withthe business needs.	Cannot meet current networkbusiness demands. This system isOpportunistic and uncontrollableHigh Processing Power (Expensive)
10	Rui Guo,Huixian Shi, Qinglan Zhao, andDong Zheng "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in ElectronicHealth Records Systems", 2018	Aiming atpreserving patient privacy in an EHR systemon blockchain.	Supporting general non-monotone predicates in blockchain technology is the direction offuture work.	Unsuitable forlarge-scale scenarios. Difficulties in obtaining better performance Tedious message updating

4. FUTURE SCOPE

Blockchain technology, when used in a centralized manner, can enable secure and transparent access to records. However, the ability to access these records would still be controlled by the permissions set by the entity managing the blockchain. In the case of hospitals accessing records through Aadhar cards, it would depend on how the blockchain system is set up and whether Aadhar cards are used as a means of authentication and authorization.

5. CONCLUSION

In this paper, we discussed how blockchain technology can be useful for the healthcare sector and how it can be used for electronic health records. Despite the advancement in the healthcare sector and technological innovation in HER systems they still faced some issues that were addressed by this novel technology i.e. blockchain. Our proposed framework is a combination of secure record storage along with the granular access rules for those records. It creates such a system that is easier for the users to use and understand. Also, the framework proposes measures to ensure the system tackles the problem of data storage as it utilizes the off-chain storage mechanism. The role-based access also benefits the system as the medical records are only available to trusted and related individuals. This also solves the problem of information asymmetry in the EHR system.

6. REFERENCES

[1] Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR-Rahul Ganpatrao Sonkamble, Shraddha P. Phansalkar, Vidyasagar M. Potdar and Anupkumar M. Bongale 2021

[2] Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS - Jin Sun, Xiaomin Yao, Shangping Wang and Ying Wu- 2020

[3] Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain - Shufen Niu, Lixia Che, Jinfeng Wang and Fei Yu - 2020

[4] Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain - Yong Wang, Aiqing Zhang, Peiyun Zhang and Huaqun Wang – 2019

[5] Blockchain for Secure EHRs Sharing of Mobile Cloud-Based E-Health Systems Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding and Aruna Seneviratne 2019

[6] Using Blockchain for Electronic Health Records Ayesha Shahnaz, Usman Qamar and Ayesha Khalid Published 2019

[7] An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records Fei Tang, Shuai Ma, Yong Xiang, and Changlu Lin 2019

[8] A Blockchain-Based Medical Data Sharing and Protection SchemeXiaoguang Liu, Ziqing Wang, Chunhua Jin, Fagen Li and Gaoping Li 2019

[9] EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain Ahmed Raza Rajput, Qianmu Li, Milad Taleby Ahvanooey and Isma Masood 2019

[10] Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems Rui Guo, Huixian Shi, Qinglan Zhao and Dong Zheng 2018