International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

PERSONAL HEALTHCARE DATA SHARING FRAMEWORK USING BLOCKCHAIN

Kasthuri Ayswarya .V.S , Puvana Preethika .M ,Sanuja .S.B , Ajitha.P

UG Student , Assistant professor/CSE

St.Xavier's Catholic College of Engineering, Chunkankadai

ABSTRACT: In this chapter we provide an overview of the concept of block chain technology and its potential to transform our current use of technology and software infrastructure. Block chain is disruptive technology that is playing a vital role in many sectors. The decentralized nature of block chain application can be used to change information technology systems. Block chain can potentially solve these issues. Block chain technology is the most reliable cryptosystem that provides a framework for securing transaction over networks. In this paper, we suggest healthcare data sharing framework that employs block chain technology to provide a tamper protection application by considering safe policies. Block chain technology is proposed in which third party organization can be replaced with distributed database where sensitive data is maintained securely in blocks lock down by clever cryptography. Block chain technology is proposed in which third party organization can be replaced with distributed database where sensitive data is maintained securely in blocks lock down by clever cryptography. Block chain technology is proposed in which third party organization can be replaced with distributed database where sensitive data is maintained securely in blocks, lock down by clever cryptography.

Keywords: Privacy and security; Block chain; Access control

1.INTRODUCTION

Cloud computing is an emerging paradigm of dynamic delivery of Information Technology services likehardware, software and capabilities as a service over the network. The increased popularity of cloud based data services, data owners are highly motivated to store their huge amount of potentially sensitive personal data file on remote servers. Nevertheless, it also brings many security issues since the data stored in cloud is vulnerable to various source of attacks. To ensure confidentiality, data owners encrypt the data before outsourcing to cloud. However, in order to achieve data sharing with sensitive information hiding with other users of cloud ,encrypting the whole file that is to be shared will achieve sensitive data hiding but the shared file will not be accessible to others. In cloud based storage systems like Electronic Health Record system, organization struggle to keep patient data secure, up-to-date, auditable and accessible to all parties together with hiding sensitive data**.** The advantages of blockchain are (i) Decentralized (ii) peer to peer (iii) history cannot be changed. It has been involved with information between patients, business entities such as different hospital systems, pharmaceutical companies, etc. It is a mechanism for digitally storing a patient's health data. Fraud detection and mitigation is increasingly becoming a policy issue for state Medicaid programs. It provide an efficient tool for solving malicious access to the PHR. Other research finds that Medicaid fraud could be as high as 15-22% of total spend as a result of over billing for services.

The rest of the article is arranged as follows. Section 2 briefly describes the blockchain Components, transactions and data store 3 application in healthcare. Section 4 introduces the architecture of our proposed framework. In Section 5, data sharing and management. In Section 6, we discuss our experiments by considering various types of attacks and exhibiting the performance analysis. Finally, Section 7 concludes the remarks of our contributions.

2.BLOCKCHAIN COMPONENTS

Blockchain has basic building blocks and components that are independent of blockchain type.The implementation of the components may differ depending on the type and application.

A.BLOCKCHAIN TRANSACTIONS

The transaction of blockchain enable the transfer of information between two parties without the need of the trusted third party. The transactions are programmable. The transaction is initiated by the center which must include the receiver public address, transaction value and the message digital signature which is used to prove the authenticity. The transaction is then transmitted to the network where the nodes need to check the transaction using digital signature and if validated it gets transferred to the transaction tool. The transaction in blockchain are stored in blocks and histories of all transactions are maintained by nodes in the network.

B.DATASTORE

The transactions from the unconfirmed pool are bound in blocks using the AS algorithm and is chained to previous blocks. Each blocks includes the hash output of the previous block in the blockchain.

Problem Statement

Cross-institutional sharing of healthcare data is a complex undertaking with the potential to significantly increase research and clinical effectiveness. First and foremost, institutions often are reluctant to share data because of privacy concerns, and may fear that sending information will give others a competitive advantage. Next, even if privacy concerns could be addressed, there is no broad consensus around the specific technical infrastructure needed to support such a task. Finally, healthcare data itself is complex, and sending information across institutional boundaries requires a shared understanding of both data structures and meaning. Even assuming data can be shared efficiently and securely, these interoperability issues left unchecked will limit the utility of the data. Despite evidence that the value of healthcare data exchange is large, these issues, described below, remain significant barriers.

3.Blockchain application in healthcare

Storing the health records in the blockchain will support health research by having access to private pseudonymous records of the patient that is required for research. With the progress in electronic health-related data, cloud healthcare data storage and patient data privacy protection regulations, new opportunities are opening for health data management, as well as for researchers convenience to access the health data. Securing data, storage, transaction,

and managing their smooth integration are immensely valuable to any data-driven organization,

especially in healthcare where blockchain technology has the potential to resolve these critical issues in a robust and effective way.

Blockchain Technology to secure the personal data of the patient. The Researches needs only the details of patient's disease and not their personal details. Therefore the details of Patient's disease is directly stored in the database which can be accessed by the Researchers. And the personal data such as the Name, Age, etc. are stored in the Blockchain which is transmitted to the Nodes and the Miners verify the data. Finally the verified data is stored in the Blockchain which is accessed only by the Authorized persons.

Blockchain technology has the potential to be the infrastructure that is needed to keep health data private and secure. In this framework the block chain is employed to maintain non repudiation accountability and tamper proof attributes

EXISTING SYSTEM

Much like the Bitcoin approach, the previous method is a Merkle Tree-based structure. The leaf nodes of this tree represent patient record transactions, and describe the addition of a resource to the official patient record. Transactions, however, do not include the actual record document. Instead, they reference FHIR Resources via Uniform Resource Locators (URLs). This allows

institutions to retain operational control of their data, but more importantly, keeps sensitive patient data out of the blockchain. FHIR was chosen as an exchange format not only because it is an emerging standard, but also because it contains inherent support for provenance and audit trails, making it a suitable symbiotic foundation for blockchain ledger entries. FHIR in conjunction with the blockchain can serve to preserve the integrity and associated context of data transactions.

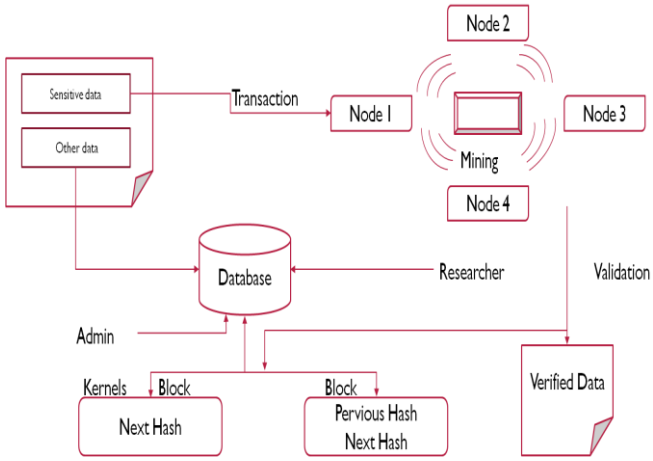
Fast Healthcare Interoperability Resources (FHIR) is an emerging standard that depicts data formats and elements, along with providing publicly accessible Application Programming Interfaces (APIs) for the purpose of exchanging Electronic Health Records. The standard was created and is managed by the Health Level Seven International (HL7) healthcare standards organization. FHIR is licensed without restriction or royalty requirements, which should serve to further facilitate its broader adoption. FHIR offers the potential for increased utilization of mobile and cloud-based applications, medical device integration, and flexible/customized healthcare workflows. FHIR enables the separation of EHR data elements into defined structured data types known as resources. Two of the resource types pertain to identification (providers and patients) and common clinical activities. The segmented resource constructs of FHIR facilitate the transfer of portions of EHR data where appropriate or desired. FHIR resources follow Representational State Transfer (ReST) principles, and can be validated for structural conformance to the standard as well as further refined by additional conformance statements called Profiles.

Blocks:

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.

Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher score can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low. For example, bitcoin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

4.Architecture



- Primary data is generated by the interaction between a patient and their doctors and specialists. This data consists of medical history, current problem and other physiological information.
- A block is created for each doctor and researcher using the primary data collected in the first step.
- Parties who want to access such valuable information must request permission which is forwarded to the blockchain, and the blockchain will decide to whom access will be granted

.

- These four steps are part of the core of the whole process including database , the blockchain, and cloud storage.

- Database and cloud storage store the records in a distributed manner and a blockchain provides extreme privacy to ensure customized authentic user access.

- For example, no matter where you are treated in the globe, your health record will be available and accessible on your phone and validated through a distributed ledger such as blockchain, to which healthcare providers would continue to add to over time.

SHA256

The SHA (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a data set. If you would like to compare two sets of raw data (source of the file, text or similar) it is always better to hash it and compare SHA256 values. It is like the fingerprints of the data. Even if only one symbol is changed the algorithm will produce different hash value. SHA256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is so called a one-way function. This makes it suitable for checking integrity of your data, challenge hash authentication, anti-tamper, digital signatures, blockchain.

With the newest hardware (CPU and GPU) improvements it is become possible to decrypt SHA256 algorithm back. So it is no longer recommended to use it for password protection or other similar use cases. Some years ago you would protect your passwords from hackers by storing SHA256 encrypted password in the data base. This is no longer a case. SHA256 algorithm can be still used for making sure you acquired the same data as the original one. For example, if you download something you can easily check if data has not changed due to network errors or malware injection. You can compare hashes of your file and original one which is usually provided in the website you are getting data or the file from. SHA-256 is one of the successor hash functions to SHA-1, and is one of the strongest hash functions available. Using this online tool you can easily generate SHA256 hashes.

5.DATA SHARING AND MANAGEMENT

Sharing of healthcare and medical data is one main and essential step to improve the quality of healthcare providers and make the healthcare system smarter. Every transaction in a healthcare based blockchain is stored in blocks on decentralized storage system. The operational mechanism of today's health-related systems has some limitations. One limitation is that patients hardly have access to their health records. So, they have no idea about the sharing of their own health data among unknown parties. To improve the interaction and collaboration with the healthcare industry, blockchain technology could play a important role, enabling and securing a convenient sharing mechanism of electronic health data. In another contribution made by Genestieret al. , a new idea of reshaping the consent management in the healthcare system which mainly provides user to control the whole health record data by using blockchain was introduced. In another study, Zhu et al. proposed an approach for achieving a controllable blockchain data management in the cloud environment to address the concerns of users about the lack of control on the posted ledgers. In their model, they designed a special trust authority node to allow users to terminate and prevent any potentially malicious actions even in a majority attack. However, there is no authorization design and no access control in their implementation. The idea behind implementing the cloud is to keep the data distributed and safe under the same

roof without involving third parties. Cloud storage technology has its advantages of fast transmission, good sharing, storage capacity, low cost, easy access, and dynamic association. Many research work was developed to design blockchain technology in order to secure, share, and store data. This is stored by deploying cloud encryption under the chain. Cloud storage is mainly the composition of numerous storage devices, connected all together to form a large volume of storage, to accommodate a lot of Information. Healthcare organizations need not compete among themselves because they all have access to the same information. Blockchain technology has the potential to transform healthcare systems because it places the patient at the center of the health care system.

6.CONCLUSION

The blockchain technology is gaining significant attention from individuals, as well as organizations of nearly all kinds and dimensions. The process will be transparent and secure, but also the quality of healthcare will be increased at a lower cost. We utilized the smart contracts in blockchain technology to provide security policies that patients can manage the access rules of other participants in the healthcare system. The patients will have the right to decide who can and cannot access their data and for what purpose. Our system affords historian records.