Blockchain Based Medical Data Sharing and Protection Scheme

Amal Benny[1*], Bhavana S[2], Husna Fathima A S[3], Meghana C M[4] , Mrs. Shweta Muddebihal[5]

[1-4]Student, Computer Science Engineering, Sri Venkateshwara College of Engineering, Bangalore, India
[5]Assistant Professor, Computer Science Engineering, Sri Venkateshwara College of Engineering, Bangalore, India

---***---

Abstract—Electronic health record (EHR) records the process of how a disease occurs, its development and the treatment for that disease. In EHR the most important aspects of the patients medical data are data sharing and privacy preservations. Blockchain technology holds as an apt solution to the above mentioned problems since it holds the features such as decentralization and tamper resistance. To improve the electronic health system of the hospital we make use of medical data sharing and protection scheme. The system can satisfy various security properties such as decentralization, openness, and tamper resistance. An efficient approach is made for the doctors to store the medical data and access the historical data of patients which in turn meets privacy concerns. It helps the doctors in symptom-matching mechanism between the patients and helps in conducting mutual authentication and create a session for their future communication about their illness.

Keywords—Block chain, Electronic Heath Record, Medical Data, Sharing and Protection, Symptoms-Matching.

1. INTRODUCTION

After the development of computer and communication technology, EHR has become an essential tool for medical services. This system requires some electronic devices such as the computer to manage digital medical records, as it is easy to use, more appropriate and saves time. EHR helps in providing important data for diagnosis and scientific research along with judgement for handling medical disputes. Hence, it has attracted a huge range of attention in the departments like government, medical and cyber security. As we know, nowadays medical data is crucial for the diagnosis, and it is personal and sensitive for patients. So, data sharing and privacy preservation are the most important aspects in EHR.

The EHR system is mainly developed with the help of cloud computing. These schemes tend to have some flaws. For example, they have a dependency on the cloud provider. If some attacks to the cloud provider are made, then the sensitive information leakage is encountered and also in the worst case the server may abruptly stop if the cloud providers would go bankrupt or be swallowed up by the larger companies. Thus, the security of EHR will be compromised. The reason blockchain was introduced in 2008 was because of the flaws that was encountered in EHR system. Hence the blockchain can be viewed as a distributed database and satisfies the features of decentralization, tamper resistance, and asymmetric encryption. This technology can provide prominent way to manage and store the sensitive medical data of the patients. Hence blockchain is the promising solution for EHR.

2. LITERATURE SURVEY

Nowadays many advanced technologies are used for Medical Data Sharing and Protection Scheme. Many authors and scholars researched about the same. This section consists of comparison of several authors related to the above technology.

In 2017, Xue et al designed a blockchain-based sharing model for medical data. The scheme solves the problem of checking, saving, and synchronizing medical data among different medical institutions by improving the consensus mechanism. But it has some disadvantages in data storage since the scheme does not possess the ability of machine learning algorithm.

In 2018, Yang and Li [9] presented a blockchain-based architecture for EHR. It prevents tampering and misuse of EHR by keeping track of all events occurring in the database. Also, the system introduces a new incentive mechanism to create new blocks in the block chain.

Zhang et al. proposed a medical data sharing scheme based on block chain to improve the diagnosis level. They utilized the private blockchain possessed by the hospital to store personal health data of patients while the consortium block chain is used to keep the security indexes.

3. PROPOSED SYSTEM

Blockchain is being considered as a new technological revolution with peer-to-peer distributed ledger technology to record transactions, agreements, and sales. The benefits of the blockchain technology are decentralized maintenance, data saving in the block-then-chain structure, secure transporting and accessing of data as well as anti-tamper and undeniable data security. Taking advantage of these distinguishing features above, blockchain enables efficient and precise management of authentication, confidentiality, accountability and data sharing while handling private information, medical resource saving and facilitating the patient.

The major contributions of this paper are listed as follows.

- Providing lethal and exhaustive information about patients at the point of care and enabling quick access to patient records for more coordinated, efficient care.
- Sharing electronic information securely with patients and other clinicians.
- Helping providers more effectively diagnose patients with reduce medical errors, and provide safer care.
- Improving patient and provider interaction, as well as health care convenience and, enabling safer and more reliable prescribing.

4. METHODOLOGY

A.BLOCKCHAIN

Blockchain mainly solves the trust and security issues of transactions, and it is a kind of distributed database combining data blocks in chronological order. Generally, the block chain is divided into three classes: private blockchain, consortium blockchain, and public blockchain. As shown in Figure 1, each blockchain consists of many blocks, and each block contains a block header and a block body. Block header contains multiple meta-information about the current block. For example, timestamp, a hash value for the blockchain body, and a hash value for the previous block. Block body is usually used to record the real data of the current transactions.A Blockchain can be defined as growing list of records known as blocks. Every block contains a block header and a block body.Block header contains a cryptographical hash of the previous block, a timestamp and hash price for the blockchain body. Block body contains current transactions. We have used blockchain to resolve the trust and security problems with transactions. The main characteristics of blockchain are :

Decentralization: All the nodes measure equal, there is no central node. Multiple nodes distributed in numerous places perform transaction records and every node records and keeps a whole account. All nodes will supervise the transaction and collectively testify for it.

Tamper resistance: The hash value of the previous block is maintained. If any of the block is changed then all the blocks at the moment are recalculated. Therefore, modification of the medical data by a single node is invalid.

Openness: The data of blockchain is open source through public interface, provided the personal data of all parties concerned within the transaction is being encrypted.

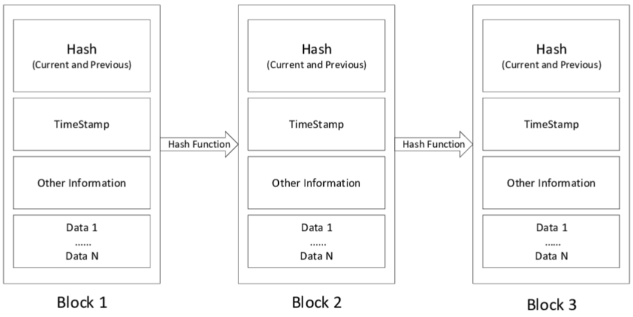

Figure 1. Structure of Block chain.

B.SYSTEM ANALYSIS

Initially medical data is uploaded to the EHRs. RSA private key and public key is generated at the time of user creation by the data owner and encrypted using RSA algorithm. Hashcode is generated using SHA256 algorithm and the hashcode will be stored in the block header. Hashcode of previous block is fetched and stored in the block header which helps the validation protocols and algorithms to detect tampering of data. Timestamp and random number is generated and stored in block header. Block is generated which contains the actual data and the block header. A connection between local database and working platform and the cloud storage server is established and an FTP connection is established for transfer of files. The generated block is uploaded to the cloud storage where each block is stored as a zip file as seen in Figure 2.

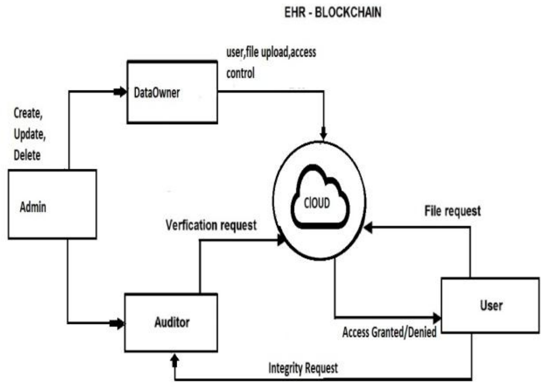

Figure 2. System Block diagram.

5. CONCLUSION

The important features of blockchain technology such as the decentralization and tamper resistance make it apt for the protection and sharing of medical data. Here a lightweight medical data sharing scheme based on blockchain is proposed and implemented. Proxy re-encryption technology is used by doctors to retrieve the medical data history of the patient. It can ensure the security of the data since the information is transmitted in a ciphertext format. Also an improved DPOS mechanism is adopted to act as a convinient mechanism that is lightweight and reliable. Finally, this scheme provides the symptoms-matching mechanism that allows two patients with the same symptoms to communicate about their illness. The analysis results show that the proposed scheme satisfies many requirements and has a low computational and communication cost.

6. FUTURE SCOPE

Whereas single attribute is used in the present system, multiple attributes might be added in the future systems. Enhancement work is done by creating a hybrid cloud setup which runs softwares in private servers and stores data in public server in the block chain. Diffie-Hellman encryption technique and RSA cryptosystem used in the present system can be substituted by EHR in pharmaceutical industry and research as it is a promising advancement. There is a large potential which facilitates the patient and physician access to medical records, prescription sharing and much more.

REFERENCES

[1] Medical data sharing scheme based on blockchain to improve the diagnosis level proposed by Zhang et in the yesr of 2018.

[2] Blockchain based architecture for EHR which prevents tampering and misuse of EHR presented by G.Yang and C.L.Li in 2018.

[3] G.Zyskind, O.Nathan, and A.Pentland bring forword "Decentralizing privacy:using blockchain",work-space,San Jose CA,USA, May 2015.

[4] T. F. Xue, Q.-C. Fu, C. Wang, and X.-Y. Wang, ''A medical data sharing model via blockchain,'' ActaAutomaticaSinica, vol. 43, no. 9, pp. 1555–1562, 2017.

[5] AES-The Advanced Encryttion standard by J.Daemen and V.Rijmen.

[6] Z.Zheng, S.Xie, H.Dai, X.Chen anf H.Wang "A overview of blockchain technology: Architecture, consensus and future trends",in Jun 2017.

[7] Security and Privacy of in EHR system based on blockchain by A.Zhang, X.Lin in 2018.

[8] "The use of health information technology in seven nation",proposed by A.K.Jha, D.Doolan and D.Grandt in 2008.

[9] G. Yang and C. L. Li, ''A design of blockchain-based architecture for the security of electronic health record (EHR) systems,'' in Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci., Nicosia, Cyprus, Dec. 2018, pp. 261–265.