Securing patient Health Record in Blockchain With Abe Access Control

M.Mohan[1], B.J.Nirmal[2] , R.Sophie Angela[3] , R.Nivetha Angel[4],A.Joseph Praveen[5]

[1,2]Assistant Professor Department of Information Technology, CSI College of Engineering, Ketti, Tamil Nadu, India.

[3,4,5]UG Scholar, Department of Information Technology, CSI College of Engineering, Ketti, Tamil Nadu, India.

m.mohansan@gmail.com[1]

Abstract

Electronic Health Record which is also known as EHR which is considered as the replacement of the paper records of the patients in a digital format in the health organizations. EHR plays a major role in treating the patients in all the departments of the medicine. These records consist of the medical history of patients. EHR acts as a medium of communication among healthcare practitioners. A decade ago, EHRs were touted as a key for increasing quality care. Today, providers are using data from patient records to improve quality outcomes through their care management programs. One of the key features of an EHR is that health information can be created and managed by authorized providers in a digital format capable of being shared with other providers across more than one health care organization. EHRs are built to share information with other health care providers and organizations such as laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and school and workplace clinics.

Keywords: EHR, patient records, digital format, health organizations, quality care, created and managed.

1. Introduction

Block chain is a distributed system recording and storing transaction records. It is a decentralized unit. It allows each participant in a network to interact without preexisting trust between parties. The main concept is transactions between two users will not be known by others. For transaction Bitcoin is used which is a digital currency. The transaction is saved in a digital ledger which was verified by miner and hash value is obtained which helps in achieving the transaction successfully. This presentation is about study and working of Block chain and our implementation in Electronic health record. Block chain technologies present an opportunity to improve the operations of EHR by sharing the patients document among the organizations. 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.[1−2].

1.1 Objectives:

•The main objective of the project is to allow patients to assign access rules for their medical data.

•With block chain technology patients can connect to other hospitals and collect their medical data automatically.

•The use of block chain concept in EHR will make the patients stress free and also reduces the complications of medical data transactions.

•The main advantage of block chain is it can change the EHR market on its head by creating secure, flexible and enforceable business associate agreements.

•Now a days many patients are getting confused about the medications to be taken for a particular disease.

•By using blockchain the patients are able to get suggestions from other health care organizations for their quality care.

•Essentially, with the block chain ledger, you'll get to know the status of the patient medical history from beginning till the end of the checkup.

•We want to help the patients understand exactly what are the possibilities in the block chain and how they can play a part in it.

•Block chain has so far been most useful in medical applications in terms of understanding the work flow of tracking the medical process.

2. Steps in Working of Blockchain:

➢ Transaction data. (patient medical record)
➢ Chaining the blocks (with a hash) (each time a patient pays a visit along with the medications and treatments suggested by other health care providers)
➢ How the signature (hash) is created? (using Cryptography)
➢ When does the signature qualify? (when the access control is provided)
➢ How does this make the block chain immutable? (using hash function)
➢ How is the block chain governed? Who determines the rules? (the Admin, who checks the entire workflow)

2.1 How Blockchain Can Be Implemented:

• Understand what block chain is.
• Develop a business case.
• Choose your block chain carefully.
• Build an EHR ecosystem.
• Design Deliberately.
• Navigate uncertainty.

2.2 Why Blockchain In EHR?

•Standardization of problem lists in the healthcare industry is needed to enable more efficient exchange of information between health providers and especially to patients.

•Paper-based structures do not work in electronic environments and some forms of problem list preparation, such as auto-population of lists, represent significant compliance and patient safety concerns.

•Block chain could reinvent the way patient's EHRs are shared and stored by providing safer mechanisms for health information exchange of medical data the health care industry.

2.3 System Architecture:
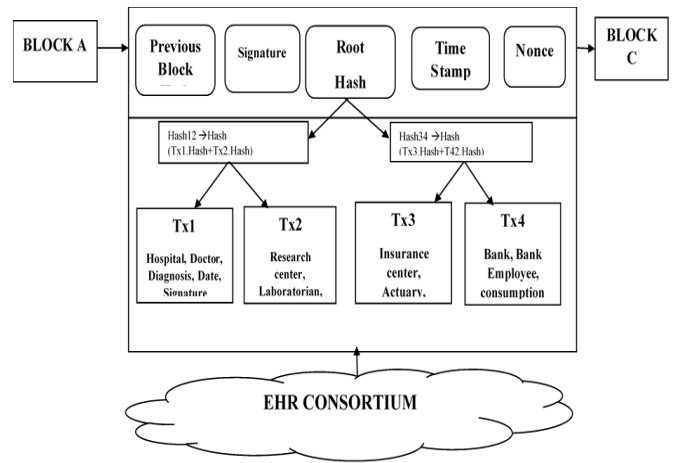
Assuming that there is an EHRs system in a cloud storage platform, which consists of some departments, such as hospitals, pharmaceutical departments, insurance departments, disease research departments and so on, EHRs systems can be jointly managed. All departments can offer services for patients together and restrict the rights of each department to prevent EHRs abuse. Thus, an EHRs system with a blockchain structure is designed as shown above. Suppose that every patient owns one blockchain of healthcare alone. After being treated in a hospital, all the information including EHRs, consumption records, insurance records, etc. Patient treatments at different times will be generated in different blocks. Then, a series of blocks are generated according to the time sequence and a healthcare blockchain of this patient is constructed. [3−5].

2.4 Algorithm:

1. First Build The Genesis Block.
2. With The Help Of The Root Hash (Genesis Block) Generate The Next Blocks To Form The Chain Of Blocks.
3. Enter The Corresponding Details.
4. Initially The Input Block Id Is Required.
5. Fetch The Contents Of The Block.
6. Unzip The Content Of The Block.

7. Extract The Root Hash Of The Block Which Is Currently Used In Order To Create The Next Block.
8. The Corresponding Details Are Uploaded In This Block For The Future Use.
9. Check The Equivalence Of Hashes I) If Yes
10. A)The Block Is Not Corrupted
11. Ii)If No
12. B)The Block Is Corrupted
13. Hence The Process Knock Off.

A Block chain is a growing list of records, called blocks that are linked using cryptography. Each block contains a hash value of the previous block, a timestamp, and transaction data. EHR block chain is one of the compelling use cases that make the process of medical transactions simpler. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers. Interoperability challenges between different providers, hospitals, research institutions, etc. add extra barriers to high-performance data sharing. For this problem we have introduced one new research of using the block chain in EHR system. Each patient will have a separate block which consists of their personal details such names, their phone number, their medical details (prescription, lab records). These details are encrypted using cryptography with the help of public key. Once a blockchain has been introduced to manage electronic health records, it becomes the long sought after standardized method of digital health data management.

Hospitals and care providers will no longer require specific software or databases to access patient data. The first visit of the patient's data is added to the block for the first time and the formation of the chain continues in the further visits. The main purpose of this project is to give access to the patients by taking this as an advantage the patient who is considered as the user here can view the medical details and has the privileges to modify their personal details. The Admin is the one who plays a major role in the entire system and gives access and privileges to all the other modules who is the one responsible for organizing and overseeing the health services and daily activities of a hospital or healthcare facility. They manage staff and budgets, communicate between departments and ensure adequate patient care amongst other duties. The Data owner allows health systems to create holistic views of patients, personalize treatments, advance treatment methods, improve communication between doctors and patients, and enhance health outcomes. File Auditor who will assess, evaluate and improve care of patients in a systematic way and forms part of clinical governance, which aims to safeguard a high quality of clinical care for patients. This idea will make the growth of EHR and life of patients in a high level. The advantages of using block chain in EHR is cost reduction, building confidence and scalability. Blockchain technology could be quite complementary in the possibility space for a future world.

3. Implementation Analysis

Step 1: Let us now upload a sample health record of a patient in the EHR system which has some common information about the patient, doctor and the patient's clinical history.

Step 2: The format of the file should begiven and then choose the file and upload. In the EHR system the DATAOWNER is having the privileges to upload.
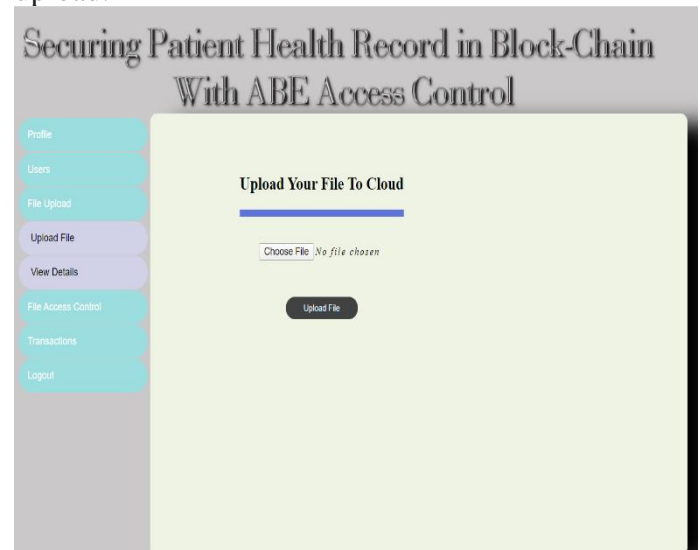

Fig.1. In the EHR system the DATAOWNER is having the privileges to upload.

Step 3: Now an acknowledgement message is received and its hows on which cloud the file is stored.

Fig.2.Cloud file storage

Step 4: And now the file has been uploaded in the cloud along with timestamp.

Fig.3. File has been uploaded in the cloud along with timestamp.

Step 5: The cloud gives a download option and now the zip format of the file is downloaded and the timestamp of the file is downloaded only by the authorized user and this is one of the greatest advantage in order to get rid of the file tamper.

Fig.4.Cloud Download

Step 6: To decrypt the file the file requester should have the exact matching replica of the private key in order to fetch the file and read the contents. If the unauthorized user tries to match the key then the document will be displayed as shown below. In case of unauthorized user corruption, it pings a message

that the file is corrupted and all these are handled by the file auditor.

Table.1 Difference Between Normal Health Records and Blockchain Based Health Records:

Normal health Records	Block chain opportunities
Hand written paper records.	Converted pen-paper data into digital form.
Varying data standards.	Shared data.
Not secure.	Distributed, secure access.
Difficulty in managing records.	Manage and transfer records easily.

Table.2. Software Requirements:

Operating system	Windows XP / 7
Coding Language	Java (Jdk 1.7)
Web Technology	Servlet, JSP
Web Server	TomCAT 6.0
IDE	Eclipse Galileo
Database	My-SQL 5.0
UGI for DB	SQLyog
JDBC Connection	Type 4

3.1 Steps to Build A Blockchain Network:
Step 1: Installing the prerequisites.
Step 2: Identify a suitable use case.
Step 3: Design a workflow for blockchain integration.
Step 4: Choose the most suitable version of blockchain.
Step 5: Choose between private and public blockchain.
Step 6: Design the admin and the user interface.
Step 7: Modelling our business network.
Step 8: Adding logic for our transactions.
Step 9: Building block.

3.2 Advantages of Blockchain:
- ✓ Cost reduction.
- ✓ Scalability.
- ✓ Greater Transparency.
- ✓ Increased Efficiency.
- ✓ Better Security.
- ✓ Improved Traceability.

3.3 Advantages of Using Blockchain In EHR:
- Public health and improves data security.
- Data transparency is more.
- Simplified claim Process.
- Patient generated information and data.
- Providing accurate, up-to-date and complete information.
- Enabling quick access to patient records.

4. Future Enhancement:

In the present system, they are using only a single attribute. In our project, we are adding multiple attributes. In Enhancement work, we are planning to create hybrid cloud setup. Which mean softwares are running in private servers and data are store in public server in block chain. In present system, they used Diffie-Hellman encryption technique. In future work, we can use RNS crypto system (RNS-Residual Number System) and plan to implement the payment module in the existing framework.

Conclusion:

Block chain technology could be quite complementary in the possibility space for the future world. This includes both centralized and decentralized models. Block chain could transform the medical field, but that outcome is very much in the future. In this paper we discussed how blockchain technology can be useful for healthcare sector and how it can be used for electronic health records. 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. Like any new technology block chain is an idea that initially disrupts. It could promote the development of a larger health care ecosystem that includes both the old way and new innovation.

References:

[1]. M. Ali, S. U. Khan, and A. V. Vasilakos, ``Security in cloud computing Opportunities and challenges,'' Inf. Sci., vol. 305, pp. 357_383, Jun. 2015.

[2]. Z. Wan, J. Liu, and R. H. Deng, ``HASBE: A hierarchical attribute-based solution for _exible and scalable access control in cloud computing,'' IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743_754, Apr. 2012.

[3]. D. X. Song, D. Wagner, and A. Perrig, ``Practical techniques for searches on encrypted data,'' in Proc. IEEE Symp. Secur. Privacy, May 2000, pp. 44_55.

[4]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, ``Public key encryption with keyword search,'' in Eurocrypt, vol. 3027. Berlin, Germany: Springer, 2004, pp. 506_522.

[5]. K. Kurosawa and Y. Ohtaki, ``UC-secure searchable symmetric encryp- tion,'' in Financial Cryptography, vol. 7397. Berlin, Germany: Springer, 2012, pp. 285_298.