Securing Medical Data using Block Chain Technology

K. Durga[1] and R. Kavipriya[2]

[1]*Research Scholar, Department of Computer Science, Kuppam Engineering College, Kuppam, Andhra Pradesh, India.*

[2]*Associate Professor, Dept. Of CSE, Kuppam Engineering College, AP, India.*

***Abstract*:** *Now a day's encrypting sensitive information like medical data has been tough even though a lot of security is provided. In olden days hospitals were maintaining paper-based record and were updated every six months and patient view their record rarely. Recently health sector has been digitized and coming to the health sector each and every patient's medical data has to be stored with high security and accessibility. Health care system uses digital methods to maintain Electronic Health Record (**EHR**). To overcome security issues in health records the proposed system introduces Block chain technology with hashing to secure the files stored on the cloud. From the Proposed work there is an opportunity to reduce the turnaround time for EHR sharingand improvedecision making for medical care, and reduce the overall cost. It provides a unique opportunity to develop a secure and trustable EHR data management and sharing system using Block chain.*

Keywords: Patients Record, Block chain Technology, Sharing data between health care,SHA.

1. Introduction

Past days, the patient's paper-based record has been secured and updated every six months once and patient viewed their record rarely. Technology has been improved accordingly; hospitals are updating their paper-based records to digitize. The Health care system are maintaining Electronic Health Records which contain Sensitive information for the diagnosis and treatment purpose that has to be frequently shared between healthcare providers, insurance companies, pharmacies, among others, which possess a challenge keeping patients record up-to-date. Sharing and storing data between different entities and maintaining access control through different situation can complicate the patient's treatment. Suppose a patient is suffering from a disease called Blood Cancer, patient has to maintain a long history for the treatment process. Patient has to maintain his laboratory reports for the monitoring and for the further treatment.

A patient may visit multiple doctors for consultation or patient can change hospital that is being referred by doctors. According to the rights a patient can set the rules and limit who can look and receive the patients' health information. When a patient is transferred from one city to another or country, or region it will be difficult to carry all his documents with him (based on the patient situation). But when it is digitized it is easy to review and the process of accessing and transferring via email with high security may be difficult. To overcome security issues in medical data management here the proposed system is integrated with block chain technology. Block chain has been categorized in to two types, one is permissioned and other is permission less block chain technology. In our framework we use permissioned block chain to maintain metadata and to access control policy, cloud service to store encrypted patient's data.

2. Literature Survey

Jose Luis [1] mentioned security and privacy can easily threatened by the hackers, viruses and worms. Researchers have gone through 29 articles and found that there is no security and privacy in medical records and data is simply encrypted and stored. Researchers proposed access control method and used symmetric key encryption method to encrypt data and communications in Electronic Health record are securely encrypted using SSL and TSL, Login/Password is the most common authentication method. This paper also specified systematic review, protocol and registration. In this paper security and privacy is given in the form of proxy method. Here the systematic review is a technique that collects all evidence in a particular field and to obtain conclusion and summarize the research, it also support the development of guidelines which are used by the professionals.

Shekha Chenthara [2] mentioned that securing data in cloud is being a tough job. This research paper mention about the cyber security to build the compressive security model for Electronic Health record. The work in the paper states two folds one is for cryptography and other is for Non-cryptography approaches. In cryptography, the work possess robust and verifiable hybrid multi authority CP-ABE access control scheme by combining threshold secret sharing and multi authority scheme for public storage. Even though the paper proposed ABE encryption technique and provided fine grain access control system it is still impractical for proper execution on Electronic Health Record and there is lot of key management complexities and access control attributes when structure grows. Non cryptographic approaches mainly the usage of SKE and PKE cryptographic primitives. Here the SKE deploys the same secret key for encryption and decryption which is highly impossible in Electronic Health Record and commonly used algorithm in SKE is Advanced Encryption Standard (AES).PKE it has two separate keys one is public and private key encryption. Automatically PKE Schemes alone are inefficient because it is slower in operations and large key size.

3. Background on Block chain Technology

Block chain can be explained as; it is peer- to-peer network which have distributed and shared ledger that was initially used in the financial sector. Here block chain can be distinguished in to two types one is permission- based and other is permission less block chain implementation. Permission less system can identify participants are either pseudonymous or anonymous and every user can append a new block to the ledger. In case of permission-based block chain the identity of a user can be controlled by the identity provider. This identity provider is trusted to maintain access control within the network. Block chain implementation can be explained with the concepts ethereum and hyper ledger.

3.1. Permission Less Block chain Implementation

Ethereum is an implementation of permission less block chain that allows user to create and execute the code of arbitrary algorithmic complexity on ethereum platform. Like virtual machine we have Ethereum virtual Machine(EVM). We have two types of cloud created in EVM which is Externally Owned account (EOA) is controlled by the private key of a user. Other account is CONTRACT account that can be seen as anonymous agent that is present in the Ethereum execution environment and it is controlled by its contract code.

It must be paid for executing a code in ethereum. In Ethereum Consensus can be achieved by the proof –of- work (POW). It is based in mining and finding a nonce input to the algorithm, so that the hash of a new valid block satisfies the requirements and these requirements set the difficulty threshold for the process of finding nonce. Proof-of-stake and proof-of-burn is two virtual mining mechanisms that are alternative to the proof of work.

3.2.Permission-Based Block chain Implementation

In this permission based system user will not have an incentive to cheat their identity because it is revealed to the identity server. Participation in consensus management is restricted to the predefined set of users. Hyper ledger an implementation part of permission-based block chain is an open source block chain that is initiative hosted by the Linux Foundation. Hyper ledger is a modular architecture. That allows plugging in different consensus mechanism. Hyper ledger service could be categorised in to three types; Membership service, Block chain service, and chain code service.

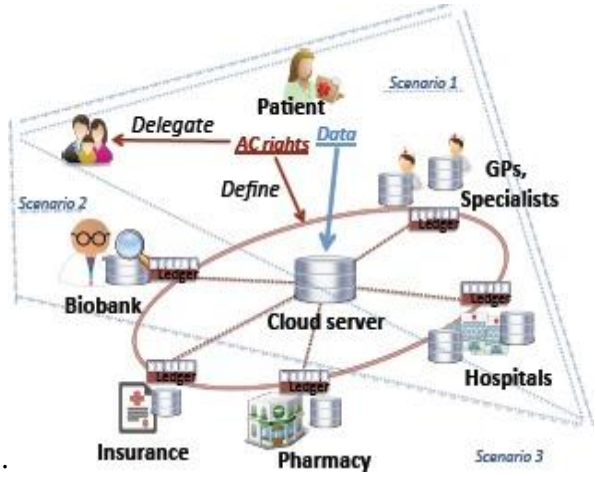
Membership service manages identity, privacy, and confidentiality on the network. When the user is assigned with a username and password that will be used to issue the enrolment certificate to identify the registered user. Block chain services manage the distributed ledger on the peer-to-peer protocol that is used on HTTP/2. Chain code services provide a secure way to execute smart contracts. These smart contracts are implemented by the chain code that is divided in to Logic and Associated world state. Logic is set of rules that is defined how transactions will be executed and how the state will change. State is said to be database that stores the information in the form of keys and values that are arbitrary byte arrays. Ledger manages all this block chain by including cryptographic hash function of the state when appending a block. This also helps in efficient synchronization, will let us know when the node goes off-line and amount of data stored in a node.

4.Block Chain Technology in HealthCare

To provide efficient security to the health care system here the usage of block chain technology has come in to existence. Here three scenarios are explained Primary patient care, Data aggregation for the purpose of research, connecting different healthcare.

4.1. Scenario 1: Primary Patient Care

A patient may visit many hospitals for the treatment where he has to maintain and update all the reports, at times it may lead to the situation where he could not find the required information. When the information is not available he has repeat the same test for the laboratory results. Moreover, health care data are highly sensitive there is no privacy preserving system in clinical practise to maintain access control policy in an efficient manner. So sharing databetween the hospitals and health care providers with security need lots of effort and time consuming too.



.

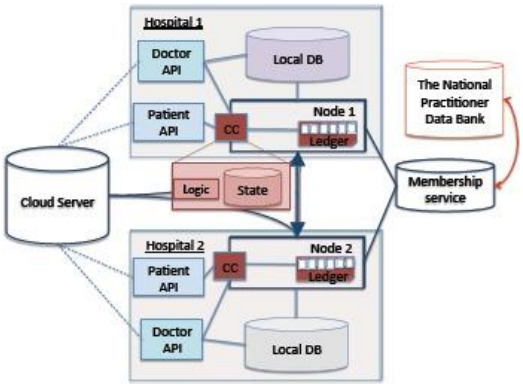
4.2.Scenario 2: Data aggregation for the purpose of research:

It is important that data to be trusted and highly authentic. Shared distributed ledger will provide traceability and guarantee patients privacy and transparency of the data aggregation process. Due to lack of the above mentioned process patients are not willing to participate in data sharing process. So using block chain technology with in a network of researchers, like bio banks, health care institutions will have facility to access the patient's data for the purpose of research.

4.3.Scenario 3: Connecting different Health care.

Using (permission-based) block chain among entities such as insurance companies and Pharmacies will facilitate medication and cost management system for a patient especially in chronic diseases. Providing pharmacies with updated data prescriptions will improve the logistics. Access to the shared distributed ledger would allow the transparency in the whole process of treatment from monitoring if a patient follows the prescribed treatment.it would also be helpful to communicate with the insurance companies and pharmacies to know the cost of treatment and medications.

5.System Architecture



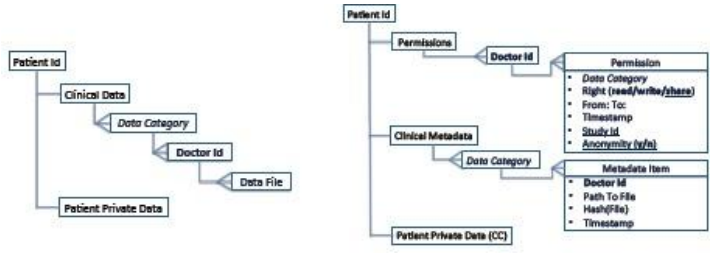
Above shown figure explains about the framework of data management. It consists of Membership service, Database for storing health care data off-chain, Nodes managing consensus, and API's for different users; in the above mentioned diagram we focus on Doctor and patient, and other roles and functionality will be explained depending on their scenario.

Membership service registers user to different roles. These roles define different functionality of the chain code that is available to the user. When registering the user of different doctors, it is important to see that doctor is well qualified in medical filed. To verify the register user we can consult National Practitioner Data Bank. There is also an encryption key pair for every registered user; for signing (SK^{S}_{U}, PK^{S}_{U}), for pairing (SK^{ε}_{U}, PK^{ε}_{U}), for every user (U).

Patient also generates an encryption key pair ($SK^{A\varepsilon S}_{P}$) which is used to encrypt/decrypt the data that is corresponded to the patient. The same key pair generates pseudonymous where only registered users will know whether the ledger stores data related to patient. So with the patient encryption key a patient can share his data with doctor.Patient's data are stored off-chain in the database. A local database management system in the hospital that stores data (Cancer in our use case). Then a cloud based platform stores patient's data organized based on the data category and encrypted with corresponding patient key, $SK^{A\varepsilon S}_{P}$. A registered clinician could access or uploads the data in the cloud repository based on the access control policy defined by the patient and implemented in the chain code Logic.

Each and every node on the network is set with chain code that acts as a validating hyper ledger peer. Nodes receive transactions that are submitted by the users through a role-based *APIs*. The Node, which is selected as a leader, organizes all transactions in a block and initiates the PBFT consensus protocol. There is an implemented chain code logic, based on that transactions are executed. State stores all the collected information about patients in a key-value pair format. A Key – a Patient Id in the system – is a pseudonym of the patient that is generated as a hash of the concatenation of the symmetric key $SK^{A\varepsilon S}_{P}$ and a Uniquely Identifiable Information of the patient (UIIp): H ($SK^{A\in S}_{P}\|UII_{P}$). Combination of SSN (if applicable), date of birth, given names, and a ZIP code of the patient could be used as UII_{P}. A Value is a patient record stored as a byte array. Next we describe the data structure in detail.

6.Data Structure and System Functionality



(a) The structure of the patient's data stored in the cloud. (b) The structure of the patient's metadata stored on the chaincode.

Above shown figure explains how the patient's data and metadata are stored and organised: patients' data are stored off-chain locally (clinician database) and in the cloud as presented in Figure. Here three categories are explained, History and physical exams, Laboratory results, and Delivered radiation doses. In the future, categories are based on

both the semantics and the sensitivity level of the data. Data files related to the patient are uploaded by different clinicians are stored within the corresponding category. Patient optionally stores some private data which is encrypted with the patient public key, PK^SP.

The structure of the patient's metadata consists of the following blocks: Permissions, Clinical Metadata, and Patient Private Data (which is optional). Permission block organises as follows: Each and every Permission corresponds to a Doctor Id, with which a clinician is registered in the system. Every permission specifies the timeframe (i.e. From: To :) during which a clinician has during which a clinician has a right to **read** the patient's data which has fallen into a specific Data Category, and upload them to the cloud repository **(write),** or **share** the patient's data within a framework. For the latter the patient could also use Anonymity tag to specify if the data must be anonym zed before sharing or could be shared as they are. Here the role of timestamp is to make every permission unique and allows a patient to update and access control changes corresponding to the same Doctor Id.

Clinical Metadata is a block that contains information about all uploaded files in the cloud by different clinicians. Metadata items are categorized based on the semantics of the corresponding data files. Every Item contains an Id of the clinician (Doctor Id), and a pointer to the file that is stored in the cloud, Path to the File, the Hash of the Data File, Hash (File), to ensure that nobody try to forge the data stored in the cloud, and the Timestamp of the event is recorded when the Data File was uploaded..

To ensure exact functioning of the developed chain code here the network consists of a Membership service and four Nodes capable of running PBFT consensus protocol. Four nodes is the minimum that is needed to run the PBFT consensus protocol. Here CC is deployed on every node and issued a set of "invoke" transactions and "query" transactions to access the information from that particular State. A patient is able to create a metadata record on the chain code, and add permissions, retrieve his up-to-date metadata record, and, then, his data is stored on the cloud. A user registered with a Doctor role is able to upload, access

7.SHA (Secure Hash Algorithm)

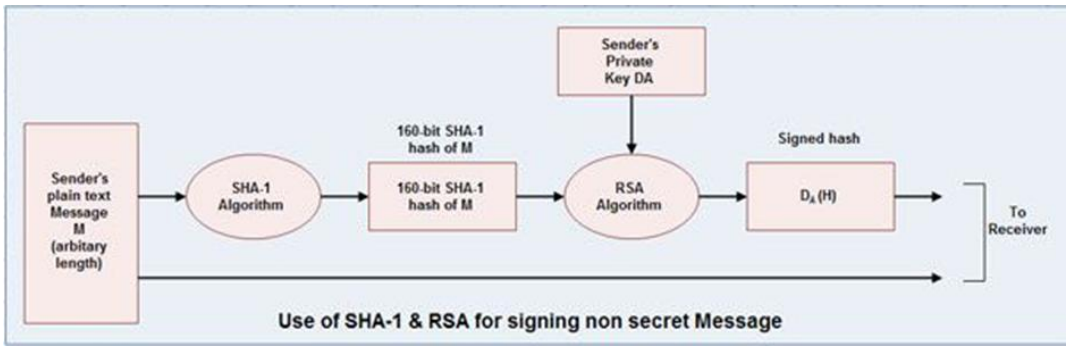
Secure Hash Algorithm (SHA) is a family of cryptographic functions which are designed to keep the data secure. It works by performing data using a hash function and this hash function consist ofbitwise operation, modular addition, and compression function.Security Hash Algorithm (SHA) was developed in 1993 by the National Institute of Standards and Technology (NIST) and National Security Agency (NSA).It was designed as the algorithm to be used for secure hashing in the US Digital Signature Standard. Hashing function is one of the most commonly used encryption methods. A hash is a special mathematical function that performs one-way encryption. SHA-l is a revised version of SHA designed by NIST and was published as a Federal Information Processing Standard (FIPS). SHA-l processes input data in 512-bit blocks. SHA-l generates a 160-bit message digest.

The procedure is used to send a non-secret but signed message from sender to receiver. In such a case following steps are followed:

1. Sender feeds a plaintext message into SHA-l algorithm and obtains a 160-bit SHA-l hash.

2. Sender then signs the hash with his RSA private key and sends both the plaintext message and the signed hash to the receiver.

3. After receiving the message, the receiver computes the SHA-l hash himself and also applies the sender's public key to the signed hash to obtain the original hash H.



8.Conclusion

The proposed work using block chain technology in the medical record can help the health sector in different ways. Block chain is decentralised system. Here in this paper the proposed system uses permissioned-based block chain implementation so that only authorised users can access the data in the system. The architecture of the frame work specifies how data is shared between the patients, doctor (in the long treatment), and insurance companies with effective security, fine-grained access control to each other in the frame. Here the patient and doctor play a major role in sharing data, based on the treatment a patient can change the hospital or region if required. A patient can also share the prescription to pharmacies to get the tablets as soon as possible.

14 References

14.1. Journals

[1] The HIPAA Privacy Rule [Internet] U.S. Department of Health and Human Services. 2017. http://www.hhs.gov/hipaa/

[2] Code of Federal Regulations. Title 21 Food and Drugs. Department of Health and Human Services. Part 50: Protection of human subjects [Internet] https://www.ecfr.gov/

[3] Code of federal regulations. Title 45 Public welfare. Part 46: Protection of human subjects [Internet] US Department of Health and Human Services; 2009. Department of Health and Human Services. Available fromml: https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/ [Google Scholar]

[4] EU Directive. 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the EC. 1995;23(6) [Google Scholar]

[5] An update on Google Health and Google PowerMeter [Internet] Google official blog. 2017. [cited 9 March 2017]. Available fromml: https://googleblog.blogspot.ch/2011/06/update-on-google-health-and-google.html.

[6] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008 [Internet]. Available fromml: https://bitcoin.org/bitcoin.pdf. [Google Scholar]

[7] Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) 2016 Aug;:25–30. [Google Scholar]