International Journal of E-Health and Medical Communications
Volume 11 • Issue 1 • January-March 2020

SeFra:
A Secure Framework to Manage eHealth Records Using Blockchain Technology

Charanya R., Vellore Institute of Technology, Vellore, India

Saravanaguru R.A.K., Vellore Institute of Technology, Vellore, India

Aramudhan M., PKIET, Karaikal, India

ABSTRACT

Electronic health information is an efficient technique for providing health care services to society. Patient health information is stored in the cloud, to allow access of eHealth information from anywhere, and at any time, but the technical problems are security, privacy, etc. Sharing the medical data in a trustless environment is overcome by the proposed framework SeFra. The proposed work provides a secure framework to manage the eHealth record by using blockchain (SeFra). For authentication purposes, a temporal shadow is used and the integrity of health records is ensured by blockchain technology.

KEYWORDS

Ehealth, EHR, Merkle Tree, Sefra, Temporal Shadow

INTRODUCTION

Nowadays, most of the industries are moving through a digital transformation journey and technologies like IoT, cloud, and mobility. Digital transformation is applicable for Healthcare system too, but the only problem is trust and security. Sharing the healthcare data in cross-institute is one of the biggest challenging tasks (Cheong, Shin, & Joeng, 2009). Even healthcare data are shared securely, integrity problem is still unchecked, this is will be overcome by the proposed framework. The patient details are very sensitive information, so it's our responsibility to protect from an unauthorized user. The existing eHealth system facing a lot of privacy and security issues. In the proposed system the sensitive encrypted health is protected over the cloud. In this paper, the authors focus on privacy, integrity, and anonymity. The data privacy means only authorized user can access the healthcare data (Kolodner, Cohn, & Friedman, 2008). The institutional health data is highly confidential and it is an asset to the institution. The anonymity is another way to secure the health record, remove the identical information and share only partial data (Charanya, Aramudhan, Mohan, & Nithya, 2013). Adding privacy in the healthcare system is more important for patient and service provider (Charanya & Aramudhan, 2016). This is achieved by using Blockchain.

DOI: 10.4018/IJEHMC.2020010101

Blockchain technology was first introduced by Satoshi Nakamoto in 2008. It's a new technology used in online cryptocurrency like bitcoin. Blockchain enables trust and transparency due to the peer-to-peer distributed ledger. The Blockchain is a distributed ledger, an endless list of records called blocks. The Cryptography techniques are used to secure the records. By using the hash pointer, each block is linked with the previous block. The two types of blockchain configuration are public and private. Public means its permissionless, anyone can participle in the network, whereas private means its permission, it's available to the known person. For example, an organization performs 15 transactions per second, each transaction receives its own signature, the digital signature is combined by using a tree structure and form single fingerprint. The fingerprint is sent to the next layer such as a service provider. Once validated its stored in the blockchain, then all users can see, then the copy is sent to the organization to store locally. The main disadvantage of the traditional blockchain, speed, scalability, and storage capacity.

The Blockchain is a distributed public ledger, with a set of rules the transactions get appended, achieved by distributed consensus of participants in the system. Participants can keep track of the transaction in a distributed way, where each participant have the copy of transactions (ledger). The Integrity of data is validated by using Blockchain.

Blockchain technology is used in healthcare to solve healthcare security problems. The encrypted health information is hashed and hashed value is stored in a distributed way, shared by multiple parties that secure all the records. The information is stored in the blockchain. Here each record is added to the previous record, never removed. Each record has own timestamp. All the transactions are encrypted and verified by the network. Keyless Signature Infrastructure blockchain deployed by Estonia government, data scales to 10^{12} items of data every second.

The existing work drawback is overcome by our proposed system. According to Provchain, the user has to pay fees to get provenance service and also pay for blockchain network also it's not supporting federated cloud. The BSPP protocol secures the eHealth system also it allows the authorized doctor to access the patient health record and it's not supporting the conjunctive keyword search, also planning to propose specific miner and verification election algorithm. The entire drawback is overcome by the proposed SeFra framework.

The objective of the proposed work is to give rights to the authenticated user to access the health record, also it maintains the integrity of the health record by using blockchain. The mostly researcher are the miners and the rewards are to get the anonymized record, also this framework is work with both blockchain, and cloud service provider is used. It supports the services like a doctor can access the health record and also the doctor can view the patient history details. The time taken to store the encrypted health record and retrieve the record is only a few seconds. The access privilege service is provided by means of a smart contract. The patient billing details are automatically sent to the insurance company. The researchers get the anonymized details as miner reward.

ROAD MAP

This paper is organized as follows: Section I Is Introduction. Section II discussed existing techniques and its drawbacks. Section III discussed Overview of the framework and its functionalities. Section IV Implementation, and result and conclude in Section V.

RELATED WORK

In attribute-based encryption, private key issued by the trusted authority and verified the attributes issued for each user. The user shares data according to a policy written over attributes and issued across different user domains. Limitation in this approach is the trusted authority has to perform a dual role like verify attributes across the different organization and issue private keys to every user. This is overcome by using blockchain. In blockchain, permissions are given based on the ownership of access tokens. Each user is issued with the token. The access rights are associated with the token (Ekblaw, Azaria, Halamka, & Lippman, 2016). Token will track who has certain attributes. Here multiple authorities in a decentralized network and accomplish with same ends. The new approach with new technologies such as steemit, IPFS, Storj, SAFE network, the article ends with two open questions: How feasible the decentralized the IDP using blockchain and to minimize the latency what topology is used to store private data. The homomorphic technique is secure and good, also it hides the user to an SP.

The content distribution is used in the ICN network (Fotiou, & Polyzos, 2016). The HIBE provide content storage, content integrity, and content provenance verification. Here no central authority or trusted authority to generate keys. The user identity is used as a public key and private key generator generate a private key for each identity. The patient wants to share the unique content name (patient record or file) with other users, then provide integrity protection and content provenance verification based on content names. The content integrity protection ensures that content cannot be modified during the transaction. Each piece of information is stored in the content storage node. The owner has the authority to authorize the storage node to store content on behalf by using trust delegation algorithm. The HIBE Delegation Algorithm generate secret keys SKs that correspond to the name of content items, authorized node store and distribute those keys to this node. During content retrieval, the other user sends a query to blockchain to retrieve the information. The query includes the content name of the desired content. Next step, the other user request issues a standard ICN content retrieval request. The drawback of the HIBE, it allows identifier hierarchies with constant –size SP, but when comes to the cost of having SP is larger than the size supported by namecoin which is used. To overcome this problem, either alternative of blockchain or HIBE could be explored in future.

A framework is proposed (Yue, Wang, Jin, Li, & Jiang, 2016) to secure healthcare system. Patient health information is sensitive information, Sharing the health information is one of the important parameters in the healthcare system. The patient health information is the personal assets of the patient and has full control of their health data. The patient has no control to manage the data, it scattered on different systems, which prevent data sharing. In this paper, the patient has full control to share the data easily without any privacy issues, this is achieved by using the proposed Application (Healthcare Data Gateway (HDG)) architecture based on the blockchain. Both patient and practitioners are equipped with HDGs. The HDG manage all type of data by means of a schema. In this approach patient no need to trust the central authority to generate the keys or to authorize the data. Here all the data are stored in the blockchain, the access control model is used to access the data, and indicator-centric schema as storage model. By using this approach, Patient can share the health information to the doctor in a simpler and secure way.

Mobile computing and wireless sensing prompt new concepts based on Pervasive social network-based healthcare. The Pervasive social network user can share the health information securely which is collected by medical sensors. In PSN based healthcare, the important research question is how the health data are shared among PSN nodes. The PSN based Health care system mainly consists of two protocols and the network is split into two (Zhang, Xue, & Huang, 2016). Wireless body area network (WBAN) and PSN Area. The WBAN provides a secure link between mobile and sensor nodes through protocol I IEEE 802.15.6 authentication association protocol and PSN Area provides sharing the health data securely by using blockchain through protocol II. The advantage of the protocol is performance is good even in unbalanced computational load. The Human body Channel (HBC) is established with NSB channels, so difficult to spoof or block the messages also prevents attacks. The limitation is system performance is tested with few experiments.

The Blockchain architecture, decentralized data provenance it provides privacy and availability of the health data (Liang, Shetty, Tosh, Kamhoua, Kwiat, & Njilla, 2017). In this paper, the authors introduced the ProvChain architecture to collect and verify the data provenance into blockchain technology. The three main phases in ProvChain are data collection, data storage, and data validation. Provenance data contain sensitive health information. Hence need to secure the health information also ensure the integrity of the health data. This is achieved by blockchain. The list of a hash of provenance data forms a Merkle tree and Merkle root node stored in the blockchain. The data provenance provides log it maintains the history of the changes in the data, also it maintains who accessed the data or modified the data. Each record contains a timestamp and generates blockchain receipt for validation. The user should pay a fee to get data provenance service given by the cloud provider and cloud provider will pay to the blockchain. Future work plan to develop provchian for the federated cloud provider, so that better provenance service and data security. To validate the blockchain receipt the open source architecture improves better security and flexibility.

Ekblaw et al. (2016) present a prototype is a decentralized patient health record management using blockchain technology. The secure system provides easy access to medical record between providers, also provides treatment sites to the patient. The secure systems give confidentiality, authentication, and integrity. The Sensitive information is stored in the local database, so the doctor can easily access the information and give treatment. The other medical stakeholders like public health authorities, researchers can access the anonymized health information in the blockchain, securing the data via proof of work. The MedRec system solves challenging issues like system interoperability, slow access to medical data, improved data quality and quantity. Also, it allows the researcher to access the anonymized data in the blockchain. The Smart contract in blockchain provides a log, it contains viewing permission and data access retrieval information. If doctor or admin add a new record for the patient, and patient only have rights to sharing of records between providers. Each patient record is uniquely represented in the form of IDs like SSN number or aadhar. Each patient record is mapped with Unique ID via public key cryptography. Future work is more security testing need to be done.

Ekblaw et al. (2017) deal with Transparency and confidentiality are two of the most important aspects of security in the cloud. This framework provides a solution to these issues. It makes the use of the blockchain as a reference or metadata of the actual health data instead of being the actual database to the huge amount of hospital records and data. This system also deals with the hypothetically possible 51% attack. It ensures the performance and speed of the blockchain that forms the backbone of the biomedical applications. However, it does not deal with the most important attribute of security, which is data integrity.

The issues in e-healthcare systems like reliability, security, the efficiency of the mechanisms being involved in the storage of e-health records (Liu, Zhu, Mundie, & Krieger, 2017). It addresses the demand for the privacy of the patient's data. The blockchain here, instead of just acting as the reference to the actual data (off-chain), stores the actual data itself such as billing information, claims, etc. Each of the peers in the system has access to the stored data and each one of them is given a unique identifier for the purpose of verification of their files. The patients themselves can set the access control to their data. They can specify the actual viewing rights by each of the individuals involved in the maintenance of his e-health data. Additional procedure logic embedded in health blockchain alters personalized medication services. The challenge behind this is peers in the system have to be verified by a third-party.

The failings within the Message Authentication Code rule for integrity verification furthermore as that of the primitive encoding strategies (Zikratov, Kuzmin, Akimenko, Niculichev, & Yalansky, 2017). The impotence of hash trees whereas handling an oversized range of knowledge invalidating their integrity has conjointly been referred. The system follows the essential blockchain rule for block creation. It takes within the transactions and mines them into completely different blocks supported a time window. It stores the total file onto the blockchain. For the aim of integrity verification, the file whose integrity has to be verified is fetched from the chain. A previous copy of the hash of the file underneath scrutiny already exists. Hash of the file fetched from the blockchain is found and cross-verified with the already existing hash. However, storage and performance concerns may arise.

The framework strives to ensure availability, privacy, security and access control over the health-related data and their sharing (Dubovitskaya, Xu, Ryu, Schumacher, & Wang, 2017). One major challenge that it deals with is of keeping the medical history of a patient up-to-date. It advocates the promotion of health information exchange ecosystems for the secure, efficient and accurate sharing of patient data across various domains. Pseudonymity provided by the blockchain technology is a potential threat to the privacy of an individual participating in it. The potential applications of blockchain in healthcare according to this paper also includes primary patient care, medical research, and associated health. The system ensures privacy by providing access control mechanisms to the patient over his data. Confidentiality is ensured by the encryption of data by a secret key. Availability is guaranteed by migrating the whole architecture onto a cloud. However, it deals less with the integrity concerns in of data.

The Hashed health record is processed through Merkle tree using keyless signature infrastructure signature and publish results. Keyless Signature Infrastructure verifies the integrity of the data and compares the result which is stored in the blockchain (Buldas, Kroonmaa, & Laanoja, 2013). The main limitation in this technique is a periodic publication of root hashes is witnessed media. The witnessed media are newspapers, public forums and micro-blogging platform (Liang et al., 2017). To eliminate the frequent publication, a frequency of published root hashes has been proposed once per month.

The privacy-preserving machine learning which is adapted in the blockchain. Here anonymized health data is stored in blockchain (Kuo, & Ohno-Machado, 2018). Mainly focus on privacy-preserving and interoperability between institutions. The challenge is scalability and efficiency.

The anonymized and encrypted patient record is stored in the central database and the original record is stored in the institutional database (Wong, Yee, & Nohr, 2018). The data are stored in the central database so that we can access the data from anywhere and any institution.

The drawback of the existing work is mention in Table 1. Most of the existing work is maintained integrity but the novelty of the proposed work is to achieve the authentication, confidentiality, and integrity.

PROPOSED FRAMEWORK SEFRA TO SECURE THE EHEALTH RECORD USING BLOCKCHAIN

The doctor can directly enter the patient record in SeFra healthcare record by giving the doctor unique ID. To maintain the interoperability, HL7 format is incorporated into our framework. The doctor has

Table 1. Pros and cons of existing work

Model	Who, When	Discussion	Open Issues
Attribute	(Yang & Yang, 2017)	Patient able to manage all own data.	Access rights based on attribute only
Hierarchical Based	(Fotiou & Polyzos, 2016)	Provide integrity	Expensive
Healthcare Data Gateway	(Yue et al., 2016)	Simple and easy to use	Protection provide to patient database
Pervasive Social Network	(Zhang et al., 2016)	Share data in simpler and secure way	Performance tested with a few experiments.
Data Provenence Architecture	(Liang et al., 2017)	Provide data privacy, data availability, data integrity, and data consistency	Not developed in Federated cloud
MedRec	(Ekblaw et al., 2016)	provides easy access to medical record	More Security testing need to be done.
Modelchain	(Kuo et al., 2017)	Speed and performance	Security not up to the level
Advanced blockchain architecture	(Liu at al., 2017)	Patient set the access rights.	Peers in the system have to be verified by a third party.

to enter the patient details in HL7 format. Initially, the electronic health records stored in the local database and then health record is encrypted and stored in the cloud.

Figure 1 explains how the data are securely stored in the blockchain by using the proposed work SeFra. The encrypted health information is hashed and stored in the server. Finally, the root value is stored in the blockchain. The patient has rights to set the access privilege in the smart contract. To view the health record, each patient set the access privilege like read, write, etc., in the smart contract.

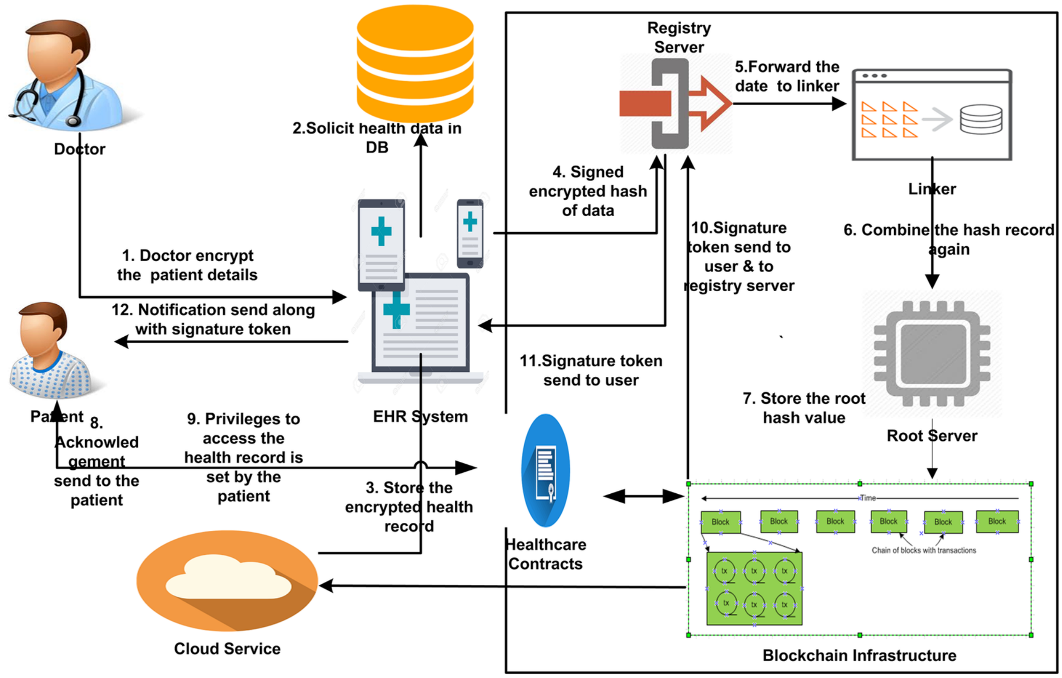
The Hospital can easily use the SeFra healthcare system and add the healthcare record, but difficult to adopt the existing health record. It takes time to integrate the existing record in the system. Each hospital needs to enter the patient history in the system, so it takes time to integrate the health information in the system.

The registry server takes only a hash of data is taken as input. The linked server links all requests into a hash tree and top hash values are retained for each second. The top hash values in a hash tree are linked together form a root value and its stored in the root server. Combining all the artifacts for a particular time can be summarized and published. The path used to move from root value to initial value is defined as signature token.

Hashing

Hash tree aggregation is proposed by Merkle and used for digital timestamping by haber at el. The user information is converted to hash values. The computer programme which takes input from the user and converts it into an alphanumeric string called "hashing." The size of the alphanumeric string is of the same size regardless of the size of the input. Bruce Schneier mentioned any change in the input like changing the single character, adding the punctuation, etc., will have a different output hash but with the same size. Here the SHA 256 algorithm is used to hash the medical record.

Figure 1. Proposed SeFra framework to secure the eHealth system


Doctor
2.Solicit health data in DB
Registry Server
5.Forward the date to linker
Linker
4. Signed encrypted hash of data
10.Signature token send to user & to registry server
6. Combine the hash record again
1. Doctor encrypt the patient details
12. Notification send along with signature token
11.Signature token send to user
7. Store the root hash value
Root Server
Patient
8. Acknowledgement send to the patient
9. Privileges to access the health record is set by the patient
EHR System
3. Store the encrypted health record
Healthcare Contracts
Time
Block
Block
Block
Block
Block
Block
Chain of blocks with transactions
tx
Cloud Service
Blockchain Infrastructure

Hash Tree

It's a one-way hash function, concept comprises with a digital signature for authentication purposes. The Merkle tree is used to maintain the proof of the integrity of the health data without the help of trusted authority. Also, it reduces the Input/output size and proofs are computationally easy. The leaf node of the Merkle tree is hashed and the non-leaf node is also hashed and labeled of its child node. Rehash the hashed child nodes (patient records) and form the parent node. The same process needs to be repeated until the root hash node is reached. It provides secure verification for the patient record.

It converts a list of the document into fixed hash length digest associated with temporal shadow. Instead of timestamping, temporal shadow is used for more security. The temporal shadow considers three timings like time in, time out and in between time. The registry server takes an only hash of data is taken as input. The linker server combines all requests into a hash tree and top hash values are retained for each second. The signature check integrity of the health care data even the user does not monitor.

Verification

The authenticity is done by using a hash of file under test. To verify the authenticity of the digital file by comparing the original signature with the root node. If the process generates the same value, it is identical to the original hash file, then it is an authenticated user, else then it is a forgery or altered version. The storage scale is approximately 2gigabyts per year, scale with time not with a number of items signed. The hash is a one-way function, no mathematical process allows recreating the file from a hash.

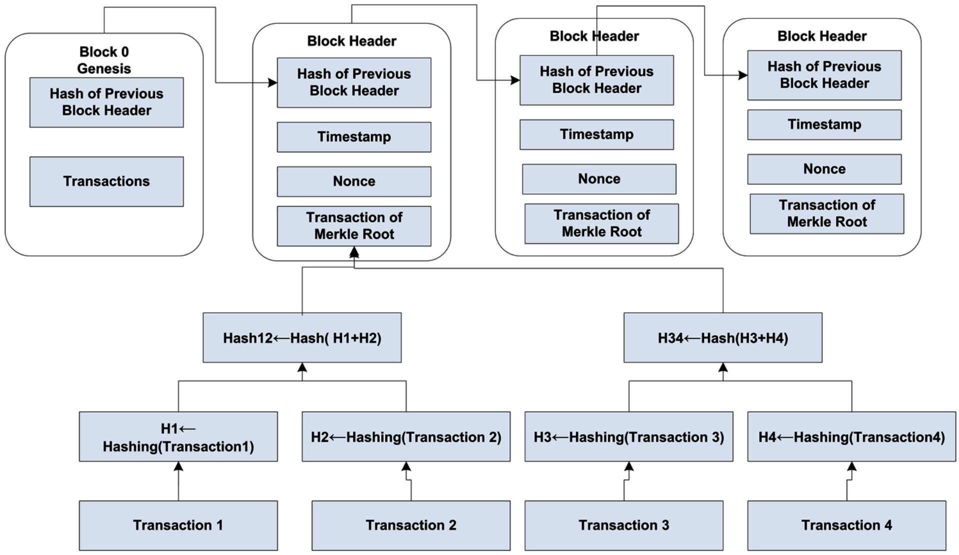
Blockchain

Blockchain technology provides data security and integrity. The following area discussed how blockchain can be applied to the electronic patient record. 1) discussed the structure and overview of the blockchain. 2) Discussed how blockchain technology useful for health care. 3) Mentioned how the records are managed. The Blockchain is like a database and stores each patient transactions as blocks, by using cryptographic signature where each block is linked with the next block (Satoshi Nakamoto, 2008). The linked block forms a chain. Blocks are numbered in ascending order. The blocks are identified by their ids. Block ID is the hash of data. Patient records are replicated in other blocks in the network. This blockchain is used as a ledger, which can be shared by anyone with proper privileges. The permission is given to the preselected user (registered user) to access the data. The Blockchain is based on a distributed peer to peer, public and private key infrastructure. Mainly it supports all medical transactions like physician orders, patient queries, prescriptions, clinical test results, etc. Each block contain records or metadata about actual records, such as patient ID, Provider ID, visit ID, etc. EHR stored in blockchain, then unique patient identifier is created by a digital signature to ensure the identifier are linked. The following components are present in the blockchain.

Block Structure

In Figure 2, Block structure is simple, it contains an index, temporal shadow, hash, data, and previous hash. All Transaction combined and stored in the block. Every ten minutes, combined transactions are verified through mining. The block is hashed to maintain the integrity of the patient record. Here SHA 256 algorithm is used for Hashing techniques. To create a block, the miner should aware of a hash of the previous block and remaining information, like data, temporal shadow, and hash. The first block in the blockchain is called as genesis block. The Block is validated, if the block is valid based on this miner suggestion, then a block is added to the blockchain.

Figure 2. Blockchain structure


Block 0
Genesis
Hash of Previous Block Header
Transactions
Block Header
Hash of Previous Block Header
Timestamp
Nonce
Transaction of Merkle Root
Block Header
Hash of Previous Block Header
Timestamp
Nonce
Transaction of Merkle Root
Block Header
Hash of Previous Block Header
Timestamp
Nonce
Transaction of Merkle Root
Hash12←Hash(H1+H2)
H34←Hash(H3+H4)
H1← Hashing(Transaction1)
H2←Hashing(Transaction 2)
H3←Hashing(Transaction 3)
H4←Hashing(Transaction4)
Transaction 1
Transaction 2
Transaction 3
Transaction 4

Block Header

Each block contains the block header and set of a transaction as its payload. All transactions are represented as leaves in Merkle tree (Nielsen, & Gollmann, 2013). Each header contains the signature and the hash of the header of the previous block. The block header is repeatedly hashed until the condition satisfied. The condition is also specified in the header, i.e. the value of hash digest must be below the target value. The use of temporal shadow is when the block was initiated, and when its added to the blockchain. Nonce value indicates the proof of the work that is used while creating the creating the block (valid block-block always have a certain number of zeros).

Temporal Shadow

It creates a unique digital fingerprint for each file called as a hash. Each patient record keeps tracks by the process of creation time, submission time and waiting time simply call it as time in, time out and in between time. The temporal shadow considered the three timing for generating signature, also to check the integrity. The main aim is to remove the trusted authority. It is referred to as "Proof-of-existence." The system generates the temporal shadow for each hashed record and its included in the hashed file. This is useful for validating the user and also to check the integrity of the health record. The main advantage of the temporal shadow is trust, convenience, and cost. The signature token contains path through hash tree-starting from a root hash value to the signed hash value.

Signature Token

The user sends signed hash of data to user. The registry server receives the hash of health record as input and returns a signature token to the user. It contains reconstructing the path through the Merkle hash tree. It's user responsibility to keep safe the signature token. The signature token contains path through the hash tree from the top root hash to the hash value of the leaf node. By using a signature token, the record can easily fetch by the authenticate user.

Nonce

The nonce is a 32-bit random number and its used once. Miner guesses the nonce value. The value adds to the block of text and then rehashed. The hash of block consists of the previous block+random number + transactions. The hash result is a string that has a certain zeros front. The main aim is to find the target value greater than the hash value.

Merkle Tree Root Value

Its mainly used to verify the integrity of the data. Each patient record is hashed and the final hash value is linked and together with a hash-tree and from a root value. The root hash value is stored in the blockchain.

To Add the Block in the Blockchain

In Blockchain each record is added to the database, never removed from the database, it cryptographically linked to previous records (Nielsen, & Gollmann, 2013). The new transaction or records is added to the network, it will be evaluated by most of the nodes, if the information matches with existing history, then new transaction approved and new block added to the chain. The hash digest of the block header has to recalculate if the data are modified in existing blocks. All the linked blocks needed to be recalculated to satisfy the condition. Every block needs to be recalculated since each block depends on the previous block. The tokens are issued to the creator of a block. The hashed health records were registered in the blockchain. Its server-based signature, different from the ordinary signature.

Genesis Block

This block is the first block in the blockchain, this block is special because of every block point to the previous block. The Genesis block invoked when new blockchain is created.

Mining

In blockchain, the miner calculates the pending transactions (block) and applies into mathematical puzzles. The Miner find the solution and shared with other nodes in the network. If the solution to the puzzle is correct then it is added to the blockchain. Miner the block found in each day remain steady, each block should contain proof of work, so that block considered as valid. Each time proof of work is checked by other nodes. For Block mining SHA256 algorithm is used to hash the previous block header.

The hash is calculated with many zeros is low. To generate the new hash, each round nonce is incremented. To accept the block in the blockchain, Block header hash value must be lower or equal to the target value. The condition is value should start with certain zeros. Nonce range is 0 to 4,294,967,296. If the miner found the correct solution then 25 bitcoins as a reward, but the reward is given after 99 blocks added to the ledger. For a miner, this is the incentive to validate the transaction.

Steps to be Followed to Store the Health Record in the Cloud by Using SeFra Framework

- The Patient’s information is stored locally in hospital database;
- For the security purpose, doctor encrypts the patient health information with the patient public key by using the RSA algorithm;
- The encrypted patient health records are stored in the cloud, to access the information from anywhere, anytime;
- Electronic health record systems convert the list of encrypted patient record into a hash of documents using a SHA 256 algorithm i.e. converted into fixed length associated with time;
- Registry server receives the hash of records and forwards it to the linker;
- Linker server receives the request from the registry server. Hash of records is converted into a hash tree and the top hash value is forwarded to the higher server;
- The signature token is generated from the root hash value to the leaf node. Each transaction is hashed and formed into a Merkle tree and stored in the blockchain;

- EHR System sends a notification to the patient for acknowledgment;
- The Smart contract is maintained in the blockchain, which allows the patient to set the access permission to access the record by whom and what. For e.g. Patient ram allow the family members like parents, brother, sisters to view Ram's overall health information but no write permission is allowed. Nurses are allowed to see the prescription and doctor has to write permission;
- The Generated Signature token is forwarded to the user, registry server, and cloud.

Steps to Retrieve the Electronic Health Record in the Cloud

- Doctor requests to access the patient record by giving the valid patient ID and patient signature token;
- Electronic health record system forwards the request to Blockchain. The access privilege is checked in the smart contract and it allows the authorized user to access the data with the signature token;
- At the next level of authentication, cloud validates the authenticity of the user by sending session key to registered user mobile or Email;
- The authentic user enters the session key to the cloud, which is validated and allowed to access the encrypted health data;
- The encrypted health record is decrypted by using the user-patient private key which is shared by the patient to the doctor.

Steps to Store the Block in the Blockchain

- Transactions are collected and stored into the block;
- Each transaction in the block is verified by miners;
- Mathematical problem solved by the miner called as proof of work;
- The Researcher will get the anonymized record as a reward, the researcher will be the miners who solve the puzzle;
- The miner who solves the puzzle first will get rewarded;
- Finally, miner verified transactions are stored in the blockchain.

Proof of Work

Each block refers to a previous block header. If the hash value is lower than the target value then its considered as a valid block. By using proof of work, the block is added to the previous block and forms a chain, called a blockchain. For eg The hash of SHA 256(SHA-256(hashed Previous header and nonce) < Target Value= 0000….00XXX..X. then the transaction is added to the blockchain is explained in Table 2. In blockchain, miner node is selected from N number of nodes in the network, B_n is the current node. The encoded health record is added to the block. Within the time limit, some nodes act as a miner and solve the puzzle. The miner who solves the puzzles first will get credit to access the anonymized health record and now block is added to the blockchain and distribute the hashed information to all peers.

Cloud Service

Cloud is centralized storage media, it provides sharing of resources over the internet. Cloud reduce the infrastructure cost. In our proposed framework the cloud maintains healthcare database. Access control list maintains the access control information i.e. who should access what information. The Healthcare database contains encrypted health information and its linked with access control list database to authenticate the user.

Table 2. Pseudocode creating a block and adding it to the blockchain

```
Parameter:
$r_{i:}$ Patient record
$B_{i-1:}$ Previous block
$B_{i:}$ Current block
$ts_i$: temporal shadow $E_{id:}$ Ethereum blockchain
BC-Blockchain
Input: Signing nodes N, number of transactions(t1….tn) assigned to node B, Blockchain, Sequence of block $b_{i,}$
Output: Block added in the blockchain

Process
G←Genesis block // first block
For i=0 to n do
$B_i$ ←block($z_{i,}$ temporal shadow $ts_i$, nonce $n_i$,hash of previous block header $z_{n-1,}$ $P_{id,}Ei_d$)
If(miner solve($B_i$<target value) then
BC←addblock($b_i$) $_{//}B_i$ is added in the blockchain
else
Nonce++; //until it get satisfied
End
```

The Benefit of SeFra

The Advantage of having SeFra compared with other blockchain is Security, time, privacy, scalability, reliability, etc.

Confidentiality

The patient health records are encrypted before uploading in the file in the blockchain. Each patient record is encrypted with the public key and each has a digital signature. Each record is appended with temporal shadow and cryptography. Only authenticate user access the health record by providing the proper digital signature.

Authentication

Authentication is an important technique which is implemented in SeFra. It secures the health record with a temporal shadow. An only authorized user can access the health record by giving the signature token. The signature token is a path from the lower level to higher level data, i.e. how the data is moving from the lower level to a higher level.

Integrity

In Distributed ledger, the patient health record is hashed and stored in the blockchain. Each record is appended with a temporal shadow. So, its easily track the who done, on which time duration. Each hashed record is linked with the previous record at a particular time. It is impossible to change the hashed record. If the data changed and all the data linked with the record also change. So, it is easily identified who changed the data.

IMPLEMENTATION

The proposed work SeFra is implemented in the ethereum blockchain, here smart contract is used to set the access privilege and allow the authorized user to access the eHealth record. The smart contract policy script is generated using solidity. The smart contract is the important parameter for security, it executes the scripts in the blockchain. The smart contract contains information about hashed record, ownership, permission of the data. Here the patient record is hashed and its stored in the blockchain. The encoded patient records are stored in the blockchain with a private key, which allows access to a specific individual. The hashed records are linked and form a root hash value. The miner checks the transaction and tries to solve the mathematical problem, once anyone miner solved the puzzle, and its checked with others. If the majority got the same answer, then the first miner will get a reward. In our system, mostly the researcher will act as a miner and the anonymized record is given as rewards. Then block is stored in the blockchain. The access permission is maintained in the smart contract. The smart contract is developed using solidity. The contracts maintained in our proposed work like a patient, insurance contract, and all the contract are linked with tag contract. All the patient details entered in the patient contract and the doctor enters the patient details and access privilege is set by each patient. The only authorized user can access the records. Billing information is sent to the insurance contract. Proof of delivery is applicable to send the surgery receipt to the insurance provider that stored in the blockchain. Finally, all the contracts are tagged with the tag contract.

RESULT

A comparative analysis of the proposed framework SeFra with the (Ora, & Pal, 2015) framework RSA based integrity. This SeFra framework is implemented using Java in ethereum, access control information is maintained by a smart contract. Solidity is used to write policy in the smart contract. Here three attributes have been considered:

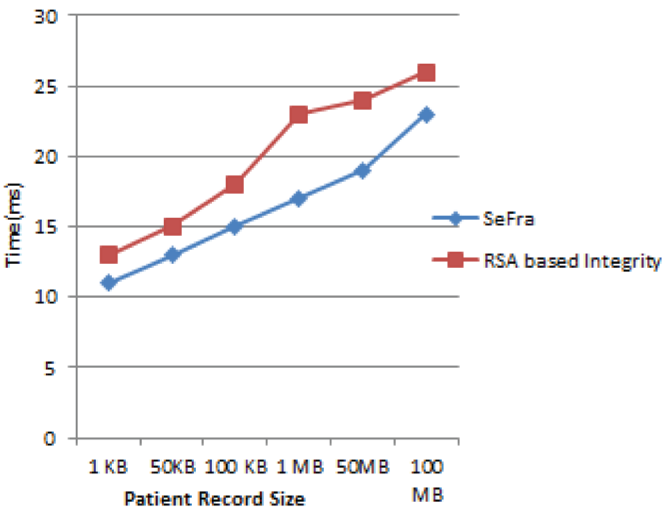
- Time
- Reliability
- Difficulty

Time

For comparing the time that the two algorithms in consideration would be taking for verifying the integrity of files, four test scenarios were taken. The authors considered healthcare-associated files of four different sizes. The authors ran the two algorithms on the different files one by one and found out the trend as shown in the given chart for the four given files in Figure 3.

The nature of the graph obtained is as follows.

Figure 3. Graph depicting the comparison of two algorithms



The x-axis represents file size and time is represented millisecond in the y-axis:

- **SeFra:** The encrypted patient record is hashed and appended with a timestamp. Each patient record is linked with the previous record. It's difficult to change the patient health record and it is difficult to trace. The time taken to verify the integrity of file of any size is independent of it. This is because, only the hash value of each file is stored in the cloud and ultimately blockchain, which has been used to do the cross verification of hashes for integrity;
- **RSA based Integrity:** This method was observed to work fine with files of smaller sizes, but the increase in the size of the file results in an increased number of parts into which it is divided. Each part giving a fixed length homomorphic encrypted output. Thus, to verify the integrity of the whole file, its different encrypted parts have to be accumulated which result in an even larger chunk of data.

Mining Difficulty

Here we consider the mining time with the number of blocks. The mining time is represented in x-axis and number of blocks in y-axis in Figure 4. The graph shows how much time the miner takes to append the block in the blockchain. Again, the SeFra framework is compared with another framework medichain in terms of mining time and a number of blocks. Based on the graph SeFra framework ethereum miner take less time when compared to the medichain is shown in Figure 4.

Security Analysis

Table 3 shows the comparing the existing work with the SeFra. Comparing each patient record is appended with a temporal shadow and hashed values form a Merkle tree. The same procedure will be done until we get the root value of the Merkle tree. The final root value is stored in the blockchain. Here each block is linked with the previous block, if there is any change in one block then automatically all the future block hash values will get change. So, changes reflect the lack of integrity. By using this technique, it provides more security.

Challenges and Opportunities

An important challenge, the patient lost the signature token then it's difficult to access the patient record. It's difficult to recover the signature token. Based on the proposed framework SeFra, security mechanism of distributing blocks in a peer-to-peer network is good with encryption and digital

Figure 4. Graph depicting the comparison of two framework

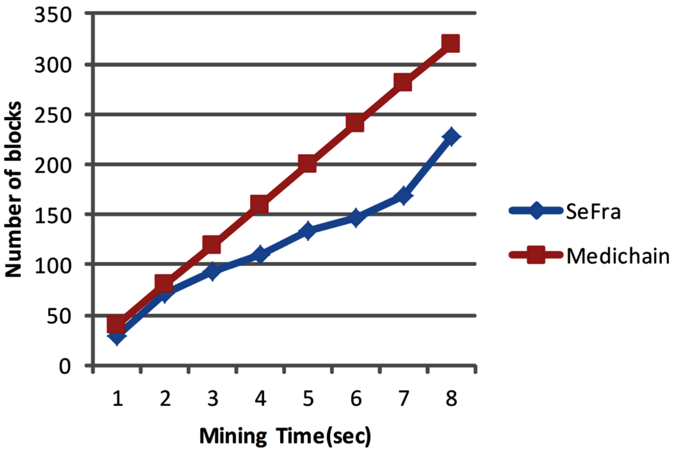


Table 3. Comparison of existing work with SeFra

	Patientory	Medibloc	Medichain	Medrec	SeFra
Blockchain	ETH(Permissioned)	QTUM(Public)	ETH	Permissioned	Permissioned
Launch date	Apr-17	Oct-17	Mar-18	Aug- 2016	April 18
Location	Atlanta, USA	Seoul, South Korea	London, UK	United states	India
Strength	Information Exchange	Improving the data quality and quantity for medical research, information exchange	Improving the data quality and quantity for medical research	Improve the data quality and quantity.	Information exchange, Data quality and quantity for medical research
Private blockchain	Yes	No	Yes	Yes	Yes
Standard	HIPAA	HIPAA	HIPAA	HIPAA	HL7
Consensus protocol	Proof-of-work	Proof-of stake	Proof-of-work	Proof of work	Proof of Work
block time	17sec	Minutes	20 sec	19sec	16sec
Smart Contract	Solidity	Solidity	Solidity	Solidity	Solidity
Patient control	No information	Patient control	Patient and doctor have right to share	Full control	Patient control
Focus	Telemedicine	Patient care, doctor, researcher	Telemedicine, Researcher	Patient care, Research	Patient care, Researcher, Insurance
Open Source	Yes	Yes	Yes	No	No
Security	Authentication, Confidentiality	Authentication, Confidentiality and data sharing	Authentication, Privacy	authentication, confidentiality, accountability and data sharing	Authentication, integrity and confidentiality
Rewards	No	No	No	anonymized data	Anonymized data for research
Future work	Integrate with Public blockchain	Digital image exchange, open source software	Performance Testing, Security Attacks	Open source software, HL7	Open source software, reduce the computation power

signature. The patient health records are connected with each other. It’s difficult that attacker tries to spoof, try to access or try to decrypt. The SeFra framework preserves the integrity of the patient details.

CONCLUSION AND FUTURE WORK

Authentication and Integrity is an important factor for eHealth cloud. In this paper, we constructed a SeFra framework to secure the eHealth system using Blockchain. By using blockchain, secure the electronic health record without thrusted third party. The First security technique is encryption, encrypt the electronic health record with a set of attributes using user public key. The second security technique is hashing, hashing the encrypted electronic health record and forms an enhanced Merkle tree. Finally, the top value is stored in the blockchain. No trusted authority to verify the authenticated user of the blockchain also user do not need to monitor the blockchain.

The future work of the proposed system is mentioned as follows. First, each patient has to maintain the private key to access the health record. It’s the responsibility of the user to maintain the key, if key loses its difficult to access the patient record, also the system never allow to recover private key, this need to be overcome in future work. Second, eHealth system should use it real-time environment like a hospital. Third, more experiments need to be performed to test the performance of the system.

REFERENCES

Buldas, A., Kroonmaa, A., & Laanoja, R. (2013, October). Keyless Signatures' Infrastructure: how to build global distributed hash-trees. In *Proceedings of the Nordic Conference on Secure IT Systems* (pp. 313-320). Springer. doi:10.1007/978-3-642-41488-6_21

Charanya, R., & Aramudhan, M. (2016, February). Survey on Access Control Issues in Cloud Computing. *Proceedings of ICETETS*, 237–240.

Charanya, R., Aramudhan, M., Mohan, K., & Nithya, S. (2013). Levels of security issues in cloud computing. *IACSIT International Journal of Engineering and Technology*, *5*(2), 1912–1920.

Cheong, H. J., Shin, N. Y., & Joeng, Y. B. (2009, February). Improving Korean service delivery system in health care: Focusing on national E-health system. In *Proceedings of the International Conference on eHealth, Telemedicine, and Social Medicine eTELEMED'09* (pp. 263-268). IEEE.

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. *AMIA Symposium*, 650. PMID:29854130

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13, p. 13)

Emmadi, N., & Narumanchi, H. (2017, January). Reinforcing Immutability of Permissioned Blockchains with Keyless Signatures' Infrastructure. In *Proceedings of the 18th International Conference on Distributed Computing and Networking* (p. 46). ACM. doi:10.1145/3007748.3018280

Fotiou, N., & Polyzos, G. C. (2016, April). Decentralized name-based security for content distribution using blockchains. In *Proceedings of the 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 415-420). IEEE. doi:10.1109/INFCOMW.2016.7562112

Kolodner, R. M., Cohn, S. P., & Friedman, C. P. (2008). Health information technology: Strategic initiatives, real progress. *Health Affairs*, *27*(5), w391–w395. doi:10.1377/hlthaff.27.5.w391 PMID:18713825

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220. doi:10.1093/jamia/ocx068 PMID:29016974

Kuo, T. T., & Ohno-Machado, L. (2018). ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017, May). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing* (pp. 468-477). IEEE Press. doi:10.1109/CCGRID.2017.8

Liu, W., Zhu, S. S., Mundie, T., & Krieger, U. (2017, October). Advanced block-chain architecture for e-health systems. In *Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 1-6). IEEE doi:10.1109/HealthCom.2017.8210847

Nakamoto, S. (2008, March). Bitcoin: A peer-to-peer electronic cash system.

H. R. Nielsen, & D. Gollmann (Eds.). (2013). Secure IT Systems. In *Proceedings of the 18th Nordic Conference, NordSec 2013*, Ilulissat, Greenland, October 18-21. Springer.

Ora, P., & Pal, P. R. (2015, September). Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography. In *Proceedings of the 2015 International Conference on Computer, Communication, and Control (IC4)* (pp. 1-6). IEEE. doi:10.1109/IC4.2015.7375655

Wong, M. C., Yee, K. C., & Nohr, C. (2018). Socio-technical consideration for blockchain technology in healthcare: The technological innovation needs clinical transformation to achieve the outcome of improving quality and safety of patient care. *Studies in Health Technology and Informatics*, *247*, 636–640. PMID:29678038

Yang, H., & Yang, B. (2017). A Blockchain-based Approach to the Secure Sharing of Healthcare Data. In *Proceedings of the Norwegian Information Security Conference*.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems*, *40*(10), 218. doi:10.1007/s10916-016-0574-6 PMID:27565509

Zhang, J., Xue, N., & Huang, X. (2016). A secure system for pervasive social network-based healthcare. *IEEE Access*, *4*, 9239–9250. doi:10.1109/ACCESS.2016.2645904

Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., & Yalansky, L. (2017, April). Ensuring data integrity using Blockchain technology. In *Proceedings of the 2017 20th Conference on Open Innovations Association (FRUCT)* (pp. 534-539). IEEE. doi:10.23919/FRUCT.2017.8071359

R. Charanya has been associated with Vellore Institute of Technology (VIT), Vellore, since June 2010 and is presently working as an Assistant Professor in School of Information Technology and Engineering (SITE). She has eleven years of teaching experience. She is doing her Ph.D in Computer Science and Engineering in the field of securing the ehealth system in the cloud using blockchain. Her area of interest includes cloud computing, software engineering, and Blockchain. She published more research papers and conference papers in reputed journals.

R.A.K. Saravanaguru has been associated with Vellore Institute of Technology (VIT), Vellore, since June 2004 and is presently working as Associate Professor in School of Computer Science and Engineering (SCOPE) and Assistant Dean Academics. He has sixteen years of teaching experience. He completed his Ph.D in Computer Science and Engineering in the field of Context aware middleware for vehicular adhoc network. His area of interest includes context aware systems, middleware, web services, VANET, data science and network security.

M. Aramudhan received his B.E in Computer Science and Engineering from the Regional Engg. College, Trichy in 1997. In 2001 he completed his M.E in Computer Science and Engineering from Regional Engg. College, Trichy. He received his Doctor of Philosophy in Computer Science & Engineering at Anna University, Chennai in 2008. He is currently working as an Associate Professor in the Department of Information Technology at Perunthalivar Kamarajar Institute of Engineering and Technology since 2009. His area of interest is Computer Networks, Web Technology, Operating System, Data structure, Programming Languages, DBMS. He published more journals and conference paper in the reputed journal.