International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Confidential Health Care Data Exchange Between Multiple Entities in Cloud using Block Chain

A.Vijaya Kumar, S. Satya Bhargavi, P.Madhu Priya, K.Shanmukh

Abstract: ***Data in the cloud is leading to the more interest for cyber attackers. These days' attackers are concentrating more on Health care data. Through data mining performed on health care data Industries are making Business out of it. These changes are affecting the treatment process for many people so careful data processing is required. Breaking these data security leads to many consequences for health care organizations. After braking security computation of private data can be performed. By data storing and running of computation on a sensitive data can be possible by decentralization through peer to peer network. Instead of using the centralized architecture by decentralization the attacks can be reduced. Different security algorithms have been considered. For decentralization we are using block chain technology. Privacy, security and integrity can be achieved by this block chain technology. Many solutions have been discussed to assure the privacy and security for Health care organizations somehow failed to address this problem. Many cryptographic functions can be used for attaining privacy of data. Pseudonymity is the main concept we can use to preserve the health care means preserving data by disclosing true identity legally.***

Keywords . Block chain, Decentralization, Healthcare data in cloud, Pseudonymity

I. INTRODUCTION

Day to Day cyber Attacks has been increasing on health care data. Decentralization [1] of cloud data can reduce the cyber-attacks. Decentralization can be implemented by peer to peer network. Few solutions has been designed to solve this problem by decentralizing of data but somehow privacy is not maintained throughout the data. So, the in which we are going to discussing is mainly maintaining the concept of block chain. Few cryptographic functions are utilized to encrypt the data. We have to analyse on the few other concepts like data processing procedures and cost efficiency for implementing privacy of data. Changes to the health care data may affects to the patient's treatment process.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
S.SatyaBhargavi*, Department of CSE ,Koneru Lakshmaiah Education Foundation, A.P, India. Email:surineedi.bhargavi@gmail.com
P.MadhuPriya, Department of CSE, Koneru Lakshmaiah Education Foundation, A.P, India. Emil:madhupakalapati2@gmail.com
K.Shanmukh, Department of CSE, Koneru Lakshmaiah Education Foundation, A.P, India. Email:shanmukh111999@gmail.com
A.VijayaKumar, Department of CSE, Assistant professor at Koneru Lakshmaiah Education Foundation, A.P, India. Email:vijay.cse@kluniversity.in

Privacy access and authorization of data must be maintained. Patients data must be electronic Health Record(EHR) [2]. The data in this record must be encrypted for providing security and privacy. Because treatment of the patients is completely considering the data which may raises due to some concerns like security and privacy. Authorized persons may only have access to store data in cloud and retrieve from the records. Data loss and data theft are the consequences due to lack of security.

Countries like USA, UK are experiencing more data loss. As data of patients are directly entering into the Electronic health Record without encryption so the privacy of data is lost.

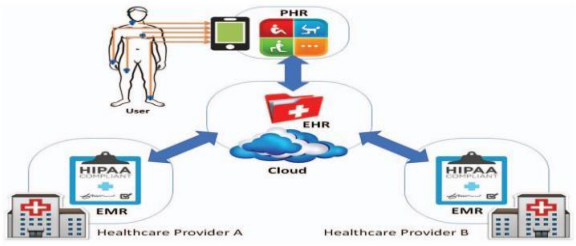


Fig 1 Health care by cloud provider

Rather than entering data into Records of organization if we are providing the cloud platform to store data. Data will be preserved using block chain. But the system is responsible for data loss in the system. Encryption keys will maintain data privacy and control data sharing through other systems. Even if the attackers stoles the data from our system it does not make any sense to understand because it's already encrypted. Encrypted and pseudonymous data can be identified by using these encrypted keys.

Specialized concept of these system is patient can secure his/her health care data by themselves. Sensitive health care data using block chain concept to provide accountability, privacy, security. Health care systems are lacking in the concept of pseudonymity. We achieve such results by some cryptographic functions. Accountability, Integrity, Security, Pseudonymity, privacy can be performed with the increasing an computational power of emerging technology in EHR system.

This concepts are implemented on the different constraints like transaction cost and execution cost. We have implemented this by utilizing java implementation on input and output generation algorithm. Elliptic curve cryptography(ECC) [3] is used for this generation.

Results from this system are compared with Electronic Health Record. Based on the result it would be decided to accept our platform or not.

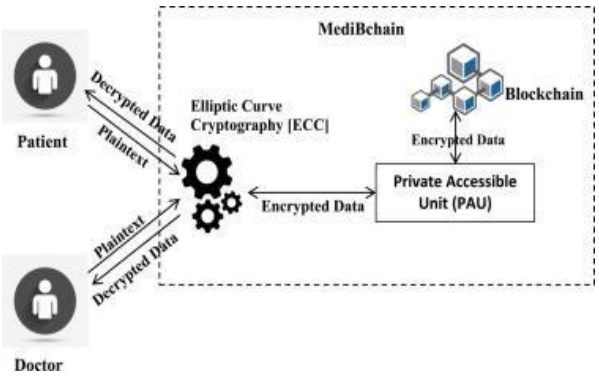


Fig 2 Elliptic curve cryptography for health care Data

Some frameworks are proposed in health care system. Few models are designed for health care data mostly in rural areas for health care data. As the technology is increasing day by day patients data is stored in the cloud as a single entity. Patients are also encouraging the doctors to share their data in cloud to get the service remotely.

Collecting of data and for retrieving data for treatment are the main constraints for data securing. Data collection layer, data management layer and data service layer are the main layers mentioned in the block chain technology.

Controllability and traceability are the two main concepts required for the user to believe and to store data by the patients. This concept can be implemented by multi party computation and Indicator centric scheme. Elements in that particular system are: Registration purpose, Relationship between patient and security provider, Final summary provision, where Registrar Contract maps the verified and identified strings for all the participants in their Ethereum addresses, The system consists of two nodes one will be used to store data and another will be used to maintain the logs of patients record history.

This technology is famous in bitcoin currency also.

Block chain concept means it helps to secure data in the form of block sequentially. It must ensure continuity and immutability for the previous block chain technology. Integrity of the data can be maintained in this chaining concept.

BLOCK CHAIN

Block chain is structure of blocks connected through the network. By maintaining the hash value of the associated previous block, the sequence of the blocks can be maintained in the network. Mining is also utilized by that crypto currencies can be gained. Blockchain [3] is distributed in means of all require nodes for ensuring the integrity. For that block chain technology will cost a lot for this challenge to maintain the block. Time Stamps of the data entered into the bocks are stored to ensure the logs must be saved for the interaction purpose.

Decentralization of data must be maintained to reduce the cost, storage maintenance can be done by the coders but the code written by the programmers will be more complicated. But it provides accuracy and reliability provides data from being tampered and protects data from frauds.

Security principles for this block chain concept:

1. Pseudonymity: Ensuring that true identity of the person is hidden for the legal activities through the dynamic key we can identify the person. Data can also be not understandable even though it is stolen.
2. Privacy: Only authorized person who are having credentials can access the data but they can also cannot access others private raw data.
3. Integrity: The private will be stored by the authorized persons only.
4. Accountability: With the block id only each block can be accessible. The authorized can be able to access the blocks.
5. Security: Parties will maintain parties will maintain secured environment with the encrypted data.

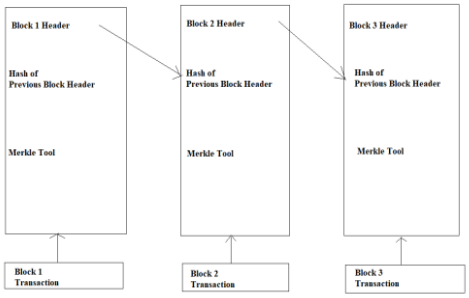


Fig 3 Chain of Blocks

Block chain name states that it would maintain the sequence of blocks which will contain the transactions records in it. It is connected to all the blocks presented in the network. So that it would be difficult to tamper with one record. As the hacker need to change not only the single record but also all the records present inside it.Block chain concept is having some additional characteristics which would be helpful to provide more and more security.

Through cryptology [4] the blocks of data present will be more secured. The participant will have own private key generated to access the blocks. The digital signature would be generated along with the time stamps. If the data in block is changed the digital signature assigned to it will also be changed. So, the authorized person will get the details of data changed in it.

As all the technologies which are mentioned previously are having centralized location so that there will be chance of trusted third party but while we consider block chain technology there will be a peer to peer communication and sync with end user will be maintained. One drawback in the block chain technology is the updating cannot be done in a single system. The computational power and time are used the most for each and every instance of block. Even if we alter the small amount of block there will be chance for using the more computational power. For small block chain there might be a chance for tampering. So for large amount of data block chaining plays a crucial role.

At a glance, Transaction data can be secured by using some of the desirable features. However, there are other conditions and requirements to consider when you want to use a block chain for business.

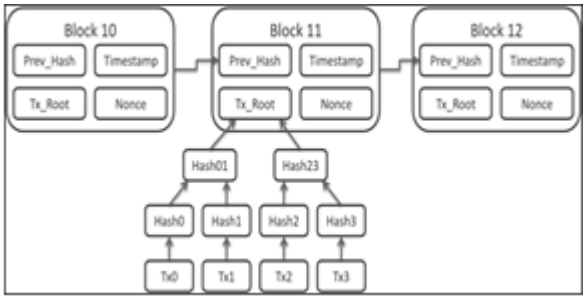


Fig 4 Block chain by hash function

To get the actual plain data the blocks maintained in the block chain has to be decrypted with the keys. As we perform encryption decryption is also be isolated in the same way.

All outputs generated from the blocks are independent of each other. To analyze the output generated in the system we have to compare the data with 5 to 30 kilobytes of data. Eliptic curve cryptography is utilized for the decryption of blocks.

II. LITERATURE SURVEY

Cloud Computing [6] is used to reduced the cost of present problem which will be used to deliver IT resources required by the users. The tier over the internet the data centers are available for most of the users. Large clouds, during present days. Multiple functions will be utilized to divide the data by using the centralized server. If the connections to the user are relative to it, by the designation an edge server. Cloud computing metaphor is the group of networking elements providing service need not be addressed individually or managed by users instead the entire hardware and software managing can be thought as an cloud amorphous. Clouds may be limited to single organization like enterprise clouds or be available to many organizations like public cloud, private cloud etc.

Cloud computing relies on sharing of resources to achieve best economic scale and coherence .The availability of high –capacity networks ,low-cost computers and storages devices as well as the spreading can be done the hardware virtualization, service- orientation architecture and In cloud computing utility and automation can leads to the growth. Present everyone is utilizing the linux operating system rather than Microsoft windows and the data should be grouped together to identify the intrusions and identifying firewall for protecting the data in cloud platform.

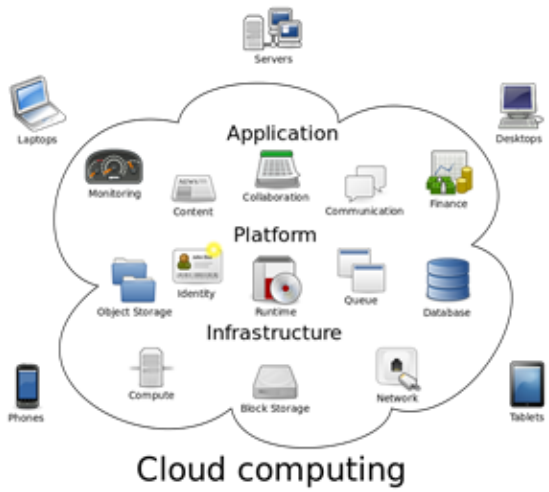


Fig 1.1 Cloud environment

1.1 Multi-Party Encryption:

The list of blocks which are connected is called as the block chain [5], that are connected using cryptography. Each block consists of hash value of the previous associated block at a time stamp.

The modification of data is resistant and through sync maintained in block chain. It is “an open, distributed systems that can maintain an transactions between two parties efficiently are in a verifiable and finalized format. Distributed systems in block chain is typically managed to be a end-to-end networking collectively addressing to an protocol for inter-node communication and validation for new blocks can be performed.

The recorded can be altered only when it maintain retroactivity without changing the data in its consequent blocks. Even the blocks remain unchanged block chain is the most secured design while compared with the remaining technologies and provide more fault tolerance. Decentralization referred to be claimed with a block chain.

Block chain was inverted by a person named Satoshi to serve as public transaction ledger of the bit coin. The invention bit coin made the first digital currency to solve the double spending problem without any need of an trusted authority or central server. The bit coin design has inspiration other application

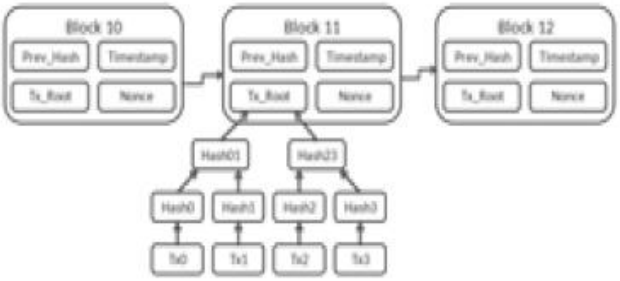


Fig 1.2 Block chain by hash function

Health care data in cloud based on block chain environment. Protecting the health care data stored in cloud environment from the cyber attacks and maintaining the security for the data stored in cloud data centers

Security and privacy: Only registered parties will be able to interact with the systems. Even though we are the registered persons of the system we cannot be able to see the plain text which will be entered by the other parties.

Integrity: Only the authorized persons can access the private data in the system.

Accountability: Each block being identified by corresponding block-id. Only authenticated parties will interact with them and get communicated.

The paper review the block chain technology in which it enhances the Elliptic Curve Cryptography (ECC).Block chain will hold the required data of the users. Each transaction identifiers will make the users to access the data further.

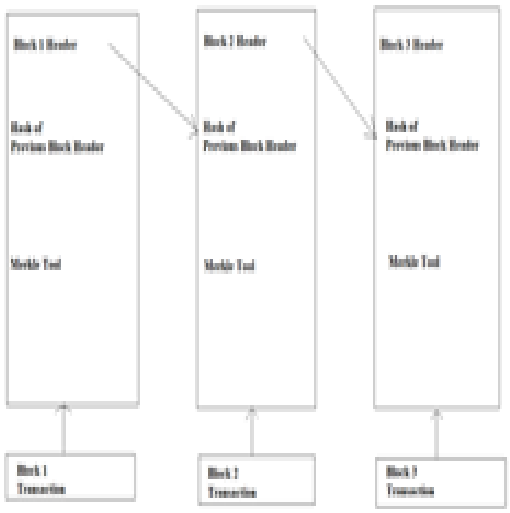


Fig 1.3 Block chain by using hash function and Merkle Root

Elliptic Curve Cryptography (ECC) is an public key cryptography which will follows the asymmetric key format structure. The small key would be required for the encryption. Trapdoor function will be utilized along with it to provide even more security.

Elliptic curves are of applicable for key agreement and digital signatures and pseudo- random generators and other tasks. Directly indirectly which can be used for encryption by combining the keys agreement with an symmetric encryption scheme. They may use in several integer factorization algorithms based on elliptic curves that have applications in cryptography such as Lenstra elliptic curve factorization

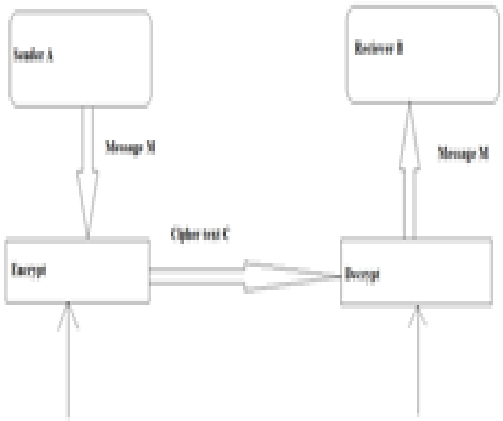


Fig 1.4 Elliptic Curve Cryptography

1.2 Risk Sourcing in Health Care Industry:

Health care information system [6] is utilized to the both logical and physical diverging purposes of the blocks in a network to provide information to the patients/doctors. Using the speediest routers health care information system are connected to the health care records/Electronic health records to get the data. For administrative purpose and managing purpose health care records are connected to the separate networks. Other software tools which will be connected to another software like Telephone management tool in the separate subnets using routers for management of health care records Based on the user requirements level up or level down type storage and infrastructure will be provided for the users. Typically cloud provides the infrastructures [9] are classified into three developed models as public, private, hybrid clouds etc.

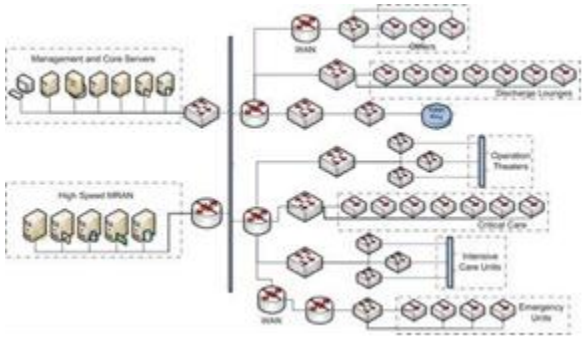


Fig 1.5 Network connection of Blocks

Many applications will be secured using the hybrid cloud architecture and it would be shared through the internet. The hybrid Cloud Architecture will be used to connect with the many systems which will be more used for the software architecture. Private cloud will be used within the organization for the personal plugged in computers within it can be connected to many devices. Both the configurations of Public and private network would be the hybrid network.. The virtual machines which have the physical resources network will be used as the firewall for the resources in the private network. By using the hybrid cloud the resources can be automatically delivered to the client. Three major delivery models of cloud computing are : Software- as-a-Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) . The SaaS can further classified into application-SaaS, Security-SaaS, and networking-SaaS. The SaaS is a‘pay-as-you-go’ service, offered an low-cost alternative to software which will be used as the software just through the subscription for required amount of time rather than using licenced software’s in our personal computer. The acquisition of software and management of the software can be reducd through this Saas. Multiple concurrent users can be used at the time Saas based application.

Many Information security service officers are trying to provide security for saas a based application. Even the back end services will also be provided to the developer who will be trying to incorporate his own application in this Saas. While looking at the stack, Saas will be the above layer while compared with the Iaas and os. At present developers who are required to develop their own application need to maintain the software development life cycle for gathering requirements, Designing, Developing and Testing, Deploying and maintaining of the application.

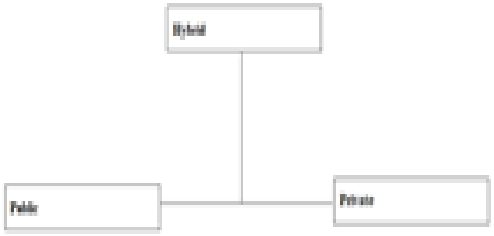


Fig 1.6 Types of clouds

1.3 Private Utility Trade off in Health Care Recommender System:

The benefits of health information systems and health recommender systems [7] are of undeniable—for the users, professionals, and societies as a whole . As the complex systems like health care data centers the privacy must be investigated to which data must be secured and which data must be along the system by the recommendation of the doctors. If the authorized persons or the patients does not want to share the data then even more secured algorithms are also considered as meaning less. The privacy of data is taken as the major constraint then only the user can recommend the algorithm even for the other systems. Because of the user attitude while considering even the health care data is not required to be more secured while compared with the other constraints the health care is also not been shared within the systems

1.3.1. Benefits of Health Care Information System

The health care data is becoming social benefit for many countries they are analysing data and making few other treatment through that data even they are using for the social purpose also. Mostly the benefits of using the more health care data is doctors may be able to identify the risks which are affecting for the most of the population and how the diseases are effecting the people and doctor may be able to identify the diseases which are wide spread throughout the world Their own health by using this digital process it can be identified This digitalized

data can be used even for the patients what is the exact status of their diseases whether it can be cured or not they will be able to get an idea, what is the aid required to cure the particular diseases by using this previous data. Even the quality of education is also increased day by day the patients does not want to disclose their personal diseases through the online sources and what might be the drugs they are using, what is the exact behind that diseases they didn't want to disclose. Empirical evidence makes most of the patients would be able to access their own personal health. For assuring confidentiality, integrity there are lot many concerns and break downs for it .

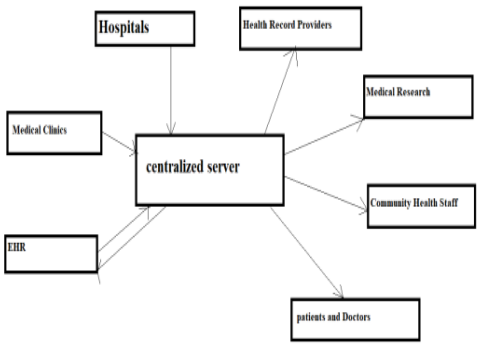


Fig 1.7 Health Recommendation System using Centralized server

III. THEORETICAL ANALYSIS

To provide environment for confidential data exchange between multiple entities in cloud using block chain.

Some of the issues mentioned in literature survey can be mentioned by the other Technologies also but through block chaining technology we will able to get the proper Output even though it lacks in other technologies. Through the distributed process we will Be able to analyse effectively. Ethereum is the platform using for distribution purpose. It is Used to access block chain.

As the "Privacy Friendly platform for health care data in cloud based on block chain environment" paper described about transaction cost and execution cost of the health care.

Data management cloud computing systems. Experimental evaluation platform cloud systems runs well in block chain environment. But the members of health care industries states that are explore the interoperability between different entries. Diagnostic centre, Hospital, doctors, Patients of health care systems. Another process for handling this type of issues key distribution technologies or key theft loss management.

By using SHA Algorithm we are implementing cryptography.

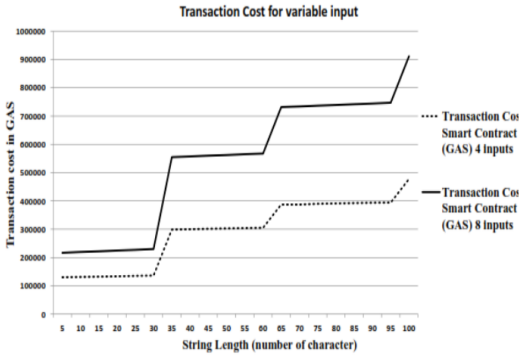


Fig 2.1 Transaction cost vs String Length

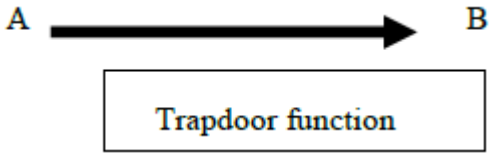
IV. EXPERIMENTAL ANALYSIS

Here we experimentally used cryptographic tool RSA which will be useful for providing cryptographic data for the users.

3.1 Analysing using SHA Algorithm:

By using the trapdoor function we can protect our data more. Where trapdoor function means we can compute data in only direction from another direction it would be difficult to compute without having the specific information.

If we consider message A can be generated by using Key B and trapdoor function.



Trapdoor function

SHA(Secure Hash Algorithm)

a) Obtain the orginal message by giving its message digest.

b) Find 2 messages which produces same digest

For hashing = digital finger print

Each block has the digital finger print of the previous block also.

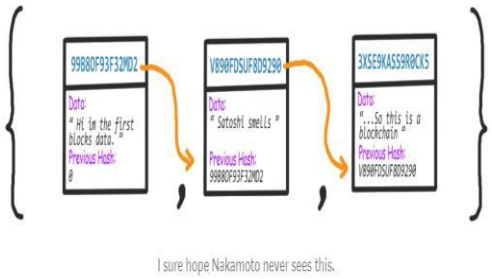


Fig 3.1 Connection of hashed blocks

1) Firstly we are creating new block which will store the required hash value of the previous block.

2) We will be able to calculate the hash value of each block in block chain.

3) We create some blocks and print the hashes in the working order.

The digital signature and required previous block hash value will be stored.

4) The chain of blocks will be calculated and compared with the previous blocks whether we are obtaining the actual result.

5) We used to calculate the difficulty of the blocks by comparing.

Protocol:

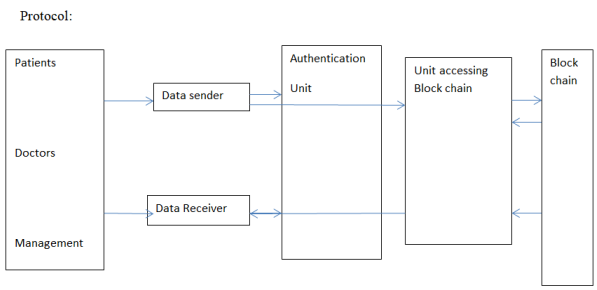


Fig 3.2 Protocol for inserting data

In our protocol data sender and data receiver that means patients, Doctors and management who are the authorized persons can be able to access the authentication unit.

Authentication unit:

When Id and PWd is entered by the user if the user is authorized person which can be declared by entering accessible credentials. Then only user will be able to communicate with the unit which is accessing block chain.

If the user is new to the system and does not have credentials like Id and Pwd then authentication unit will only once for every user..

The data which is been already encrypted by using RSA algorithm is sent to the accessing unit of block chain. Ud

Unit accessing with block chain:

This is the private unit in the system where the authorized persons can only access the system. It will have the interaction with the block chain.

The Encrypted Data Ud will be send to the Block chain so that by using hashing technique it will generate new Uid and supplies back to the receiver.

3.2 Data Sending Protocol:

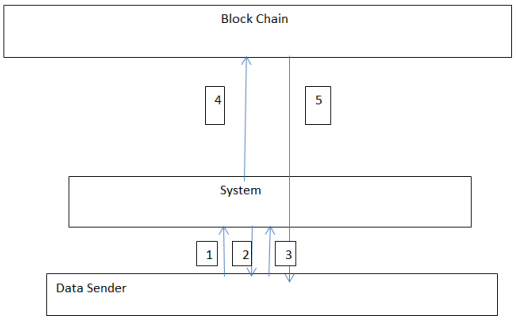


Fig 3.3 Protocol for retrieving data

1)Id and password which is generated from the authentication unit will be entered to the system .

2)Confirmation message will be sent from the system to the sender that either the entered credentials are already registered and authorized credentials.

3)So, the encrypted data will be able to sent to the system from sender. Encrypted message is Ud.

4)The encrypted message will be sent from the system to the block chain. By this it will generate a unique id Uid x where x is considered as name of the sender

5)The unique id will be again given to the sender for further access to the data.

3.3 Data Receiving Protocol:

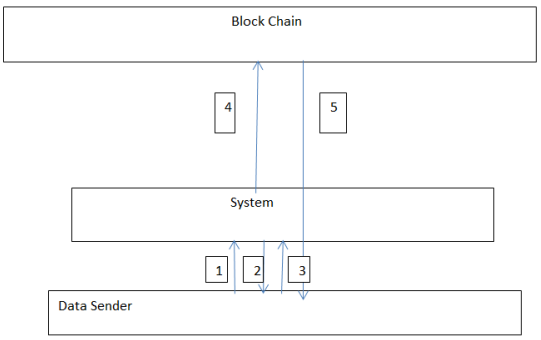


Fig 3.4 Protocol for retrieving data

1) Id and password which is generated from the authentication unit will be entered to the system

2)Confirmation message will be sent from the system to the sender that either the entered credentials are already registered and authorized credentials.

3)The Uid X which is generated by block chain while the sender enters the data must be given to the system.

4)System sends the Uid x to the block chain and access the data by hashing.

5)After hashing the data will be send back to the receiver.

This algorithm will be used for Enter the encrypted data into the block chain by using the hashing function.

It will check for the authorized person and can enter the multiple streams of data. For example while we consider patient wants to enter details of multiple diseases separately into the different blocks this can be done by using the above mentioned algorithm.

3.4 Generation of Uid x for each block of data Entered:

//Block id can be generated

//flag can be returned from the above mentioned algorithm

While flag do

If flag<- 1 do X=block.Number(); Hi=block.BlockHash();

Return Hi;

Else

End

End

Return null;

Pseudonomity:

In this algorithm the true identity of the person who is going to enter the data or access the data is not disclosed to anyone. That is kept secretly by not disclosing the true identity of a person for the legal purpose.

Privacy:

Privacy can be provided to the users as we are sending the encrypted data into the bock chain network and not even trusted third party is present in the system.

Even if the unauthorized person access the blocks of data. It does not provides the meaning full outcome and So that the attacks would be reduced. Database Manipulation, Loss of data

Are the threads which are mainly found in the aspects of security. But in this there would be no chance of Cyber security attacks.

3.5Terms Used in Protocol

Id: Username generated for the users.

Pwd: Password genereated for authorized users. Uid:

The data encrypted by using the SHA algorithm as mentioned above.

Uidx: It is the key generated by the block chain technology using hashing.

3.6Verified authorized user

If any contractor T wants to enter the data and W be the person who wants to address the data

If T && W € Hashing then

If T!= W then

Return false;

Else

//Data Uploading //

Struct Data <- enter data

Data[] data; Flag <- 0;

While Data[i]!=’/0’ do

//inserting data until end

If W sends the address of sender then

Data <- data; Flag <- 1; Return flag;

Else

Return flag;

End

End

This algorithm will be used for Enter the encrypted data into the block chain by using the hashing function.

It will check for the authorized person and can enter the multiple streams of data. For example while we consider patient wants to enter details of multiple diseases separately into the different blocks this can be done by using the above mentioned algorithm.

V. RESULTS

```
Microsoft Windows [Version 10.0.17134.1069]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\mylaptop>cd

C:\Users\mylaptop>cd C:\javaklu

C:\javaklu>javac NoobChain.java

C:\javaklu>java NoobChain
Trying to Mine block 1...
Block Mined!!! : 00000cd74d39200128cd3f53b14cca3ff59c8d7d1b8dd466d4df60fb1c13134e
Trying to Mine block 2...
Block Mined!!! : 00000bad2c26bce8418b8e84cc7d1f73f7be15b1b6cb04a39dc26547103ffcd2
Trying to Mine block 3...
Block Mined!!! : 00000dcc22cb2eeb9fc084a4902a65b945041b8bbccc27c32db587f857035f0f

Blockchain is Valid: true
```

Fig 4.1 shows hash value generated blocks

```
The block chain:
[
  {
    "hash": "00000cd74d39200128cd3f53b14cca3ff59c8d7d1b8dd466d4df60fb1c13134e",
    "previousHash": "0",
    "data": "Hi im the first block",
    "timeStamp": 1574232940561,
    "nonce": 55846
  },
  {
    "hash": "00000bad2c26bce8418b8e84cc7d1f73f7be15b1b6cb04a39dc26547103ffcd2",
    "previousHash": "00000cd74d39200128cd3f53b14cca3ff59c8d7d1b8dd466d4df60fb1c13134e",
    "data": "Yo im the second block",
    "timeStamp": 1574232940881,
    "nonce": 399908
  },
  {
    "hash": "00000dcc22cb2eeb9fc084a4902a65b945041b8bbccc27c32db587f857035f0f",
    "previousHash": "00000bad2c26bce8418b8e84cc7d1f73f7be15b1b6cb04a39dc26547103ffcd2",
    "data": "Hey im the third block",
    "timeStamp": 1574232942237,
    "nonce": 1712032
  }
]
```

Fig 4.2 shows the chain of blocks

4.1 Discussion of results:

If anyone wants to break the security of blocks chain system.

Time advantage will be there for block chain in your network.

No one can create longer block chain.

VI. APPLICATIONS

In polling system during voting. Diagnostic centre data which is stored in cloud and how to provide security from data loss and theft.Provides access for authorized persons like doctors who can access data from cloud platform.

For example while we consider polling system As we can say world becomes more digital and technology was more widespread, blockchain technology can make elections voting system more accessible. Online voting system is to be more secured while we consider the statements released by government.

Cyber security experts have strong concern whether the block chain technology is required to preserve election data. Depending upon the architecture of the block chain technology we can say who will be the authorized person and controls it, validation, exploring of data is done by whom. Block chain is end to end solution for online voting system.Fundamental characteristics of block chain technology are immutability, accountability and security while we consider online voting system.

Time stamps of voting are maintaining securely by encrypting and locking. By using distributed ledger technology which does not maintain centralized data access so that there will be no database deletion like issues arises.Validation mechanism will be used to protect integrity of the data being locked into blocks. The authentication and identification methods are used to prevent fraud voters. The digitalization and automation make voting cheaper and easier.But many of experts addressed that blockchain system must be public, decentralized and permission less in the same way how like bitcoin, Ethernum and Litecoin. By this decentralization no trusted third party is required to potentially corrupt voting system. This block chain is open for all anyone can read the data and add the blocks into the network.The block chain technology must be able to ensure the issues using encryption, cyber security software, security and authentication.For improving confidentiality, fewer nodes must be faster and efficient than permission less system. It helps to mitigate concerns then block chain is energy intensive and not scalable.Immense success of block chain technology has spread through all the financial aspects but has left over the centres. Block chain technology can solve healthcare problems. But it take double time to solve the problem of heath care centers.Block chain works on the principle of peer to peer distributed ledger technology.

2 main components of block chain technology used are:

1. Distributed Network
2. Shared ledger
3. Digital transaction

Critical information of health care centre is scattered across multiple system cannot be accessed whenever its required to access. It becomes inadequate to exchange information.

If we consider that health care information is stored in the form bits and bytes but it can be accessed through all the persons so that it can be corrupted by everyone who is accessing the data.

Through block chain technology central administrator concept would be eliminated throughout the system by cryptography.

VII. CONCLUSION AND FUTURE SCOPE

We have discussed concepts of privacy and security and privacy requirements for health care information data management systems and mentioned why such attributes needed for the health care data centers. We have explored the interoperability between different entities like doctor's data, patient's data and diagnostic center data.

Main concerns we discussed are pseudonomity, privacy and security. In further we want to discuss this on multiple entities.By reducing the execution time and evaluation time of the system. Addressed the different issues like data loss/ Theft mechanism without using the centralized system which means the trusted third party is not included in the system.

ACKNOWLEDGEMENT

We thank KLEF for providing excellent research environments and the department of CSE for extending hand in continuing our re-search work

REFERNCES

1. Abdullah Al Omar, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," Science Direct, 2019.
2. Roman Beck, "Blockchain-the gateway to trust-free cryptographic transactions," ECIS Research paper.
3. "certicorn.corn," [Online]. Available: https://www.certicom.com/content/dam/certicom/images/pdfs/WP-enhancedSecurity_login.pdf.
4. Chuan Zhao, "Secure Multi-Party Computation: Theory, Practice and Applications," Science Direct, 2018.
5. Q. Z. G. N. Liqun Qi, "How entangled a multi party secure system can be?".
6. "Dialogic," [Online]. Available: https://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf.
7. HINA ABRAR1, "Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry," IEEE, 2017.
8. M. Z. Andr´e Calero Valdez, "The Users' Perspective on the Privacy-Utility Trade-offs in Health Recommender Systems," Science Direct, 2018.
9. "TEC," [Online]. Available: http://tec.gov.in/pdf/Studypaper/White%20Paper%20on%20Cloud%20computing.pdf.
10. U. P. R. Nikunj Domadiyaa, "Privacy preserving distributed association rule mining approach on vertical partitioed health care data," Science Direct, 2018

AUTHORS PROFILE

S.SatyaBhargavi is a student of the Computer Science and Engineering Department at the Koneru Lakshmaiah Education Foundation situated at Vaddeswarm, Guntur District.

P.Madhupriya is a student of the Computer Science and Engineering Department at the Koneru Lakshmaiah Education Foundation Situated at Vaddeswarm, Guntur District.

K.Shanmukh is a student of the Computer Science and Engineering Department at the Koneru Lakshmaiah Education Foundation Situated at Vaddeswarm, Guntur District.

Mr.A.VijayaKumar is functioning as an Asst. Professor in Computer Science and Engineering Department at the Koneru Lakshmaiah Education Foundation situated at Vaddeswaram, Guntur District.