Blockchain Based Security Solution for Medical Data

Naveen Kumar S, M Dakshayini, Raghavendra R Biradar, Rajashekargouda G S

Abstract: ***Existing health organizations maintain their patients and medical data using centralised management approach. This system is more vulnerable to data breaches which leads to security threats and patients don't have control over their data. According to German cybersecurity company Greenbone Networks, the patient records, 121 millions of medical images and scans from India has been leaked which includes details such as the name of the patient, their date of birth, the national ID, name of the medical institution, their medical history, physician names and other details. According to poneman cost of data breach study, the cost of the data breach for healthcare organizations approximated to be $380 per record. According to 2016 Breach Barometer Report, 27,314,647 patient records were affected. The patient don't have control over their data and data can be misused. Hyperledger fabric framework based Blockchain technology is most desirable solution to prevent data manipulation and data theft .It also facilitates patient to have control over their data. Hyperledger fabric is a permissioned distributed ledger framework and provide high degrees of confidentiality, flexibility, and scalability.***

Keywords: medical data, centralized management approach, blockchain, Hyperledger fabric framework

I. INTRODUCTION

Data is most important assets to all business industries. The electronic document recording become an unchangeable trends with help of information and storage technologies. Which helps the people to store, access and operate the data which is generated in various applications. The communication is impossible without a data source. For any applications or any processes the data is important. The highly sensitive data is affiliated to privacy and it must be properly protected. In health care industries the data is important for patients in organization. In existing healthcare organizations store the patient information, diagnostic reports and medicines data etc using centralised method. In real world the patient personal information is collected by receptionist. The data is stored locally, it is not more secure and data can be leaked anytime. The patient also not have control on their own medical data. The sharing of medical data is time consuming and it is complex process management. Switching from centralised to decentralised system using block chain technology to provide the security and privacy to users.

Revised Manuscript Received on July 29, 2020.

Naveen kumar S, Student, Department of Computer Networks Specialisation, B.M.S College of Engineering, Bengaluru, India.

Dr. M Dakshayini, Professor and Head, Department of Information Science and Engineering, B M S College of Engineering [BMSCE], Bengaluru, Karnataka, India.

Raghavendra Biradar, Student, Department of Computer Networks Specialisation, B.M.S College of Engineering, Bengaluru, India.

Rajashekaragouda G Sankanagoudra, Student, Department of Computer Networks Specialisation, B.M.S College of Engineering, Bengaluru, India.

Health organizations generate sensitive and important data at every stage of medical treatment such as consultation, surgery and diagnosis.

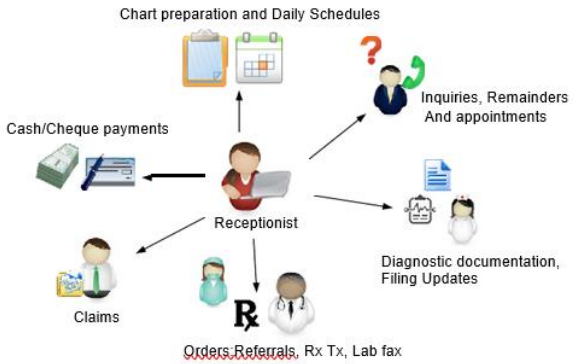

Figure1. Existing centralized healthcare model

Hospital stores medical data such as doctor's prescriptions, X-rays, MRI scans, angiography, radiography, endoscopy and sensitive health information like HIV diagnosis, cancer diagnosis and psychological conditions. Blockchain is the distributed , unchangeable ledger that is stored across blockchain network. It can be used in many applications like healthcare, supply chain, data sharing, insurance etc .Hyperledger Fabric is the permissioned based blockchain network framework and provide the architecture with representation of roles between nodes in infrastructure, execution of chain code , customisable consensus and membership services. Fabric network consists of peer nodes, which is executes the smart contract ,access ledger, endorse the transaction and interact with applications. Orderer nodes which make sure the consistency of blockchain and communication in network. Membership server provider has the certificate authority ,managing the X.509 certificates and authenticate member identity and roles. Hyperledger framework provides the permissioned network, performance, scalability, level of trust, data privacy, unchangeable distributed ledger, protection of digital keys and sensitive data. Hyperledger fabric framework offers to create channels i.e the group of participants can create a separate transaction ledger. In fabric network each participants are known to every other participants in the network. The channel is create between two participants and no other participants have the ledger in that channel. The Hyperledger fabric model consists of following: Shared ledger: Hyperledger fabric has the ledger system and consists of world state and transaction log components. World state component is the database of ledger and describes the ledger states. Transaction log component stores all the transactions in the network. The ledger is combination of both world state and transaction log component.it is levelDB key value store database. Smart contract: In hyperledger fabric the smart contract is written in

chain code and invoke by application.
Chain code is interact with world state component. Using Go, java etc programming languages can be implement chaincode.Membership service provider: it is responsible for issuing certificates to each participants who enters the network. Privacy: In Hyperledger Fabric network the privacy is most important requirement. The data is share in the network depend upon the participants. Consensus : it is the general agreement between participants in the network. Consensus mechanism maintains the integrity and security in blockchain network. It represents good relationship between participants in network. Instead of depending on single organization that store and manage the data access policies i.e single point of power and failure. In real world practice difficult to choose complete trusted entity for data usage. By using consensus mechanism between untrusting parties, the blockchain technology gives assurance the data security , access control over important data , medical data management and trustful data access among the different parties in medical domain.

II. LITERATURE REVIEW

Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte [1] proposed system as a blockchain technology is eliminate the centralized approach and provide security to medical data. This paper provides information as the blockchain technology is the decentralized and distributed ledger can impact on data sharing, billing, research in medical, identity thefts and financial record crimes using smart contracts. This paper also highlights patient controlled model of data maintenance using blockchain. The main approach is to write a smart contract which is executes own set of protocols agreed between two parties. Executing the smart contracts in three steps: Invoking, record creation and validation. This paper also suggests that the blockchain is the best solution for maintaining the health records. According to Rexford Nii Ayitey Sosu, Kester Quist-Aphetsi, Laurent Nana [2] are proposes the cryptographic approach using md5 hash algorithm to validate and verify the health data using blockchain technology. Md5 algorithm is used to verify and authenticate the captured health data for analysis. The medical data is sensitive which can be collected, managed and handled. So the security to medical data is important and it is necessary in health system. Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman [3] proposed system consists MedRec: it is decentralised system to manage record and handle the electronic medical record using blockchain approach. This system provides broad, unchangeable log and easy access to medical data across healthcare sites. MedRec handles the authentication, data sharing, accountability and confidentiality during sharing of sensitive information. The new design system integrates the local data storage, interoperability with providers and making suitable and adaptable. The medical skateholders participate in blockchain network as miners and provide the access for them to aggregate, mining reward of unnamed data, sustaining and secure the system. According to Yiheng Liang [4] present the blockchain technology in healthcare industry as state of art design. In this system the individual identity can be verified and health data is processed through blockchain network. This system is proposed to make easier to verify identity, data access, sharing of medical data and provide the security to health data of patients. This paper is focused on efficiency of verification approach system, scalability process of updating data, resolve the privacy concerns and protection of data.
According to Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher [5] proposed the system has the advantages of blockchain technology for deployment of important and secure medical data storage and exchange. In this paper the main concern is to provide privacy and confidentiality of critical health data to patients and only authorized persons can use this electronic health record. The proposed methodology to building blockchain network solution to various e-data health challenges. In this paper they concentrate on security to data sharing and low computational power. It is unusable and stimulates poor performance to store all medical data on blockchain network. The blockchain can be used as tool to store data and pointer to where data is actually present. In future they will focus on Iot data rates, completion date and resist parameters to achieve minimised performance in an e-health system. According to Jamal N. Al-Karaki, Amjad Gawanmeh, Meryeme Ayachek, Ashraf Mashaleh[6] are proposed the blockchain infrastructure called DASS_CARE for healthcare system using blockchain technology. This infrastructure helps decentralized, accessible, scalable and secure to medical data. The healthcare system is complex system and interconnected with many organization. These organizations has separate information device to manage medical data and patients personal information. The proposed system has many objectives: improving the standard of health system, lower delivery cost and magnifies the medical data management. This framework aim is to enable the secure and reliable sharing of health data between authorized entities, support the healthcare organizations for secure share and store of medical data, patients have control over their own medical records, facilitates the data analysis. So this framework provides services to healthcare providers without compromising security, confidentiality and integrity of medical data. According to Leila Ismail(Member, IEEE), Huned Marewala, and Sherali Zeadally [7] are proposed system with light weight blockchain architecture that uses the HBCM and which is orders transactions, generates the blocks. This method or technology will eliminate the issue of splitting and widespread in bitcoin network. In this paper they introduced the methodology as light weight blockchain architecture for medical data management and it has low interaction, computational overhead. This method uses the scalable and well organised energy consensus protocol instead of energy consumed protocols. This architecture divides the nodes into several clusters and each cluster maintain the individual ledger. Thus it reduces communicational and process delay in the network. They analysed this architecture by examining the threats model that were existing in the bitcoin blockchain network and shows the privacy and security of the architecture. Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu, Danyi Li[8] are proposed the user based medical data sharing by using decentralised ,permissioned blockchain network to protect privacy and identity using membership service provider in network.

This network uses the mobile applications that is required to collect the data from various devices, medical devices ,mobile devices and sync the data to cloud. So for insurance companies and providers can share the data between different entities in the network.

The cloud database has the validation and integrity technology to preserve the integrity and security to medical data. This method uses the tree based batching and data processing to handle the large data sets that uploaded by mobile applications. Thus , this method provides the privacy, integrity, security, scalable and improved performance of the healthcare blockchain network.

III. PROPOSED SYSTEM

Hyperledger network supports distributed ledger technology on permissioned blockchain networks for broad range of industries. It is modular blockchain network provides confidentiality, resilience, security and flexibility. The hyperledger fabric has the characteristics and are shown below:

a) Hyperleder fabric able to create permissioned network
b) It provides the confidentiality to participant data
c) Cryptocurrencies are not required
d) Hyperledger fabric frame work is programmable

The transaction lifecycle of hyperledger fabric network is shown in fig2. The process of transaction lifecycle of hyperledger network is shown below:

1. Application is submitted the transaction proposal to endorsing peer.
2. Endorsement policies control the what combinations of endorser are needed to sign transaction proposal. Endorsers are responsible for execute the smart contract or chain code to energize transaction proposal in network and creating write/read sets.
3. The application receives the signed transaction proposal responses from endorsing peers.
4. The application gives or submit the signed transaction proposal to ordering services.
5. Ordering services creates the bundle of transactions and send them to commiting peers.
6. Committing peers receives the bundle of transaction and it is responsible for validate the transactions, endorsement policies and commit block.

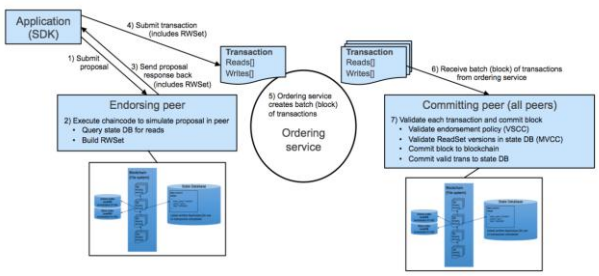

Figure2. Transaction lifecycle of Hyperledger Fabric

The user based patient health data storage and sharing proposed diagram shown in fig.3. The large amount of medical data needs to be managed and processed by using hyperledger based blockchain network. Hyperledger blockchain network has doctor peer, insurance company peer, patient peer in organization. Blockchain network contains many organizations. The patient data is generated by doctor and the patient data is stored in particular organization. These medical data is visible to all participants in organization. Medical data is stored in the database that maintained by the organization.

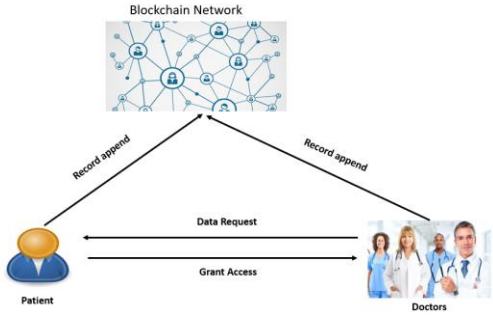

Figure3. User based patient health data storage and sharing network

In hyperledger blockchain network the certificate is issued to each participants and that certificate is generated by Certification authority present in organization. The network provide the certificate at each level of process and ensure the security, authentication and privacy. The participants in the network has the endorsement policies issued by endorsement peer that is present in the network. The each participants contains agreement when the medical data is stored or sharing between participants in the organization or between the organization. Once doctor generates the patient medical data is stored in the network and it is replicated in the each participants ledger. Based on user or patient permission the medical data is append or share in the network. Suppose insurance companies need the medical data, these companies request the patient and once patient approve the request then the data is available to them. If patient is reject the request then the medical data is not shared or not available to them. The participants in the network maintains the consensus mechanisms and provide the security and privacy. The endorsement policies verify the signature of participants and ensures the authorization in the network. The medical data sharing, appending, removing or any process in the network needed patient permission. Hyperledger fabric is a permissioned distributed ledger framework and provide high degrees of confidentiality, flexibility, and scalability.

IV. IMPLEMENTATION

In Hyperledger fabric blockchain environment consists of peer, Certification Authority(CA), Orderer and CouchDB containers. Crypto materials and config files are maintained the all containers in the organization. Containers must have channel information and genesis block access. The participants needs certificates to become valid member in the blockchain network and crypto config files manage those certificates. Crypto tool is generated the cryto config files and configtxgen tool is created genesis block and channel information. Hyperledger fabric network consists of Certification authority and Membership service provider(MSP) is a key component to control or restrict access in the network. Cryptographic methods and protocols validates the certificates authentication of user.

The certificates are generated by Certification Authority and that shows the identities in the network. The membership service provider has the lists of these permissioned identities. MSP can also define characteristics and rules in the blockchain network. The fabric framework based blockchain network can have one or more Membership service provider. The MSP provide the powerful, springiness and interoperability membership operations in the blockchain environment.

Ordering services is a component to give a bundle of communication channel to peers and clients in the network. This service also provide the environment to broadcast the transaction messages in channel.

The Hyperledger Fabric network is created and the channel creation, chaincode is invoked and it is showed in fig below.

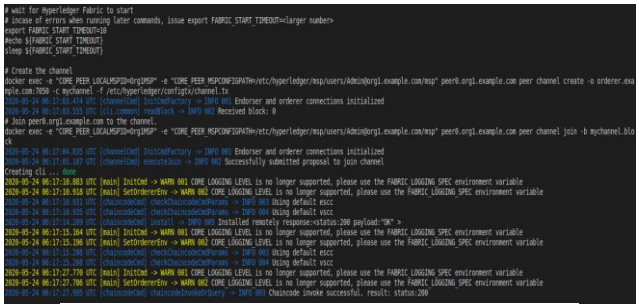

Figure4. Hyperledger fabric-channel creation

The healthcare hyperledger fabric network is run in different containers and these containers are shown below. The neighboring containers don't have visibility to these containers and ensures that visibility control, security, confidentiality to medical data in network. To enable communication between these containers it must have network and containers should attached to it.

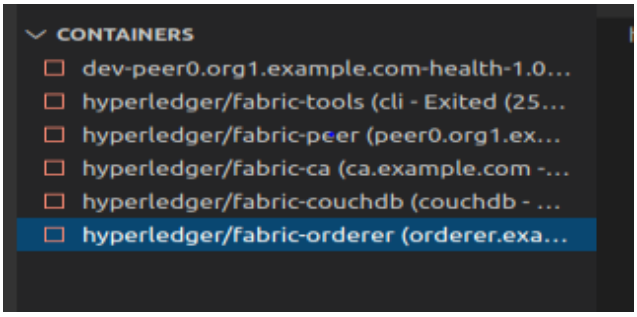

Figure 5. Lists of generated docker containers of healthcare system

Healthcare based Hyperledger fabric network created and it consists of Certification Authority, peer, orderer and couchDb peer of each hospital organizations. The health care hypeledger fabric blockchain network is shown below

```
docker-compose -f docker-compose.yml up -d ca.example.com orderer.example.com peer0.org1.example.com couchdb
Creating network "net_basic" with the default driver
Creating ca.example.com      ... done
Creating orderer.example.com ... done
Creating couchdb             ... done
Creating peer0.org1.example.com ... done
```

Figure6. Hyperledger fabric network

V.RESULTS

The Healthcare hyperledger blockchain network is created and provide the services to patients when they visited the hopsitals and medical data is stored securely based on patient permission. Suppose some health department needs patient medical data stored in hyperledger fabric network then the data is stored or retrieved from ledger only when patient approved permission. This is ensure the security to medical data in blockchain network. The patient will approve the permission based on API using gadgets and API format is given below:

{
"Patient Name": "Bob"
"Patient ID": "1dae76767e72f45e183431fb2bbr87868"
"From": "Hospital 1"
"To": "Hospital2"
"Transfer": " Hospital 1 to hospital2"
}

docker-compose -f docker-compose.yml up -d ca.example.com orderer.example.com peer0.org1.example.com couchdb
Creating network "net_basic" with the default driver
Creating ca.example.com   ... done
Creating orderer.example.com ... done
Creating couchdb   ... done
Creating peer0.org1.example.com ... done

Figure7. Healthcare hyperledger fabric network

The healthcare hyperledger fabric network is present in blockchain and network is shown in fig 4. The network contains the organizations like hospitals, insurance. Each organizations include patients ,doctors, insurance providers. Each are identified by unique ID and ensure the security to storage and sharing medical data. The organisations has the certification authority to ensure the authentication of participants who enter the blockchain network. Suppose data is need to be fetch from ledger doctor or insurance provider needs permission from patient.

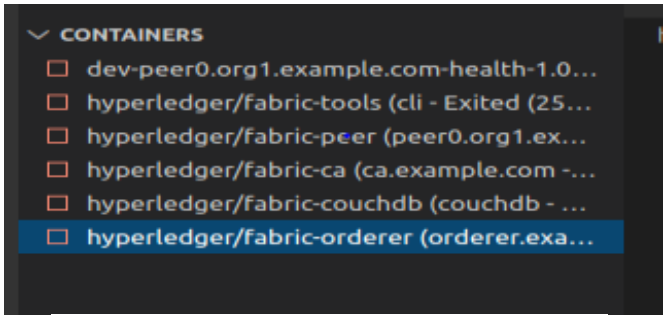

Figure 8. Healthcare hyperledger fabric network containers

The healthcare hyperledger fabric network is run in different containers and these containers are shown in fig 5. The neighboring containers don't have visibility to these containers and ensures that visibility control, security, confidentiality to medical data in network. To enable communication between these containers it must have network and containers should attached to it.

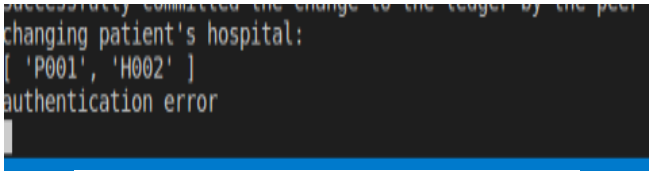

Figure 9. Medical data saving -access denied

The medical data of patient is stored in the ledger of hospital is not sharing or saving in another ledger of hospital and authentication failure is shown in Fig 9.

VI. CONCLUSION

Using Hyperledger fabric framework is able to create permission-based network. The Hyperledger fabric permissioned network used across industries. The Hyperledger fabric network ensures the performance scalability, level of trust. The Data is most important assets to all business industries. Health records are very important and required to safe those data using permissioned blockchain network. The hyperledger fabric framework blockchain network is guaranteed to provide security to medical data in blockchain network. Any one or health department or insurance companies want to add or remove the data from ledger in network needs patient permission then only the data is added or removed from ledger and make sure high security to medical data in blockchain network.

Our approach is to secure the medical record and this architecture is user or patient control based blockchain network. Hyperledger based blockchain network provide the security, flexibility, privacy.

REFERENCES

1. Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte School of Electronics and Communication Engineering REVA University, Bangalore, India. "Health Record Management through Blockchain Technology". In Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019).
2. Rexford Nii Ayitey Sosu, Kester Quist-Aphetsi, Laurent Nana, Ghana Technology University College. "A Decentralized Cryptographic Blockchain Approach for Health Information System". In 2019 International Conference on Computing, Computational Modelling and Applications.
3. Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman Media Lab."MedRec:UsingBlockchainforMedicalDataAccessandPermission Management". In 2016 2nd International Conference on Open and Big Data.
4. Yiheng Liang Department of Computer Science Bridgewater State University. "Identity Verification and Management of Electronic Health Records with Blockchain Technology".
5. Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher COSMO, IBISC Laboratory, University of Evry, France. "Towards Using Blockchain Technology for eHealth Data Access Management". In 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME).
6. Jamal N. Al-Karaki, Amjad Gawanmeh, Meryeme Ayachek, Ashraf Mashaleh ,Department of Information Security Engineering Technology, Abu Dhabi Polytechnic, MBZ city, Abu Dhabi, UAE ."DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain".
7. Leila Ismail(Member, IEEE), Huned Marewala, and Sherali Zeadally ,College of Information Technology, UAE University, Al Ain 15551, UAE. "Lightweight Blockchain for Healthcare". This work was supported by the Emirates Center for Energy and Environment Research of the United Arab Emirates University under Grant 31R101.
8. Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu, Danyi Li, 1 Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China. "Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications".

AUTHORS PROFILE

Naveen kumar S is MTech student , computer networks specialisation at B.M.S college of engineering,Bengaluru. He completed the electronics and communication background in Bachelor's degree.

Dr. M Dakshayini, holding M.E degree with FCD, awarded Ph.D in the area of computer networks in 2010. Presently she is working as Professor and Head in the Department of Information Science and engineering, B M S College of Engineering[BMSCE], Bengaluru, Karnataka, India. She has 24 years of teaching experience, 5 research candidates have been awarded with Ph.D degree under her guidance. She has delivered expert lectures at various Seminars/Workshops. She is BOS/BOE member for various Institutions. She is a member of National Board of Accreditation, India. She has more than 50 International peer reviewed Journal Publications, 26 International conference, 5 national conference Publications and 8 Springer Book chapters to her credit. She has published a patent for the research work.

Raghavendra Biradar is a student, persuing MTech in the field of Computer Networks at B.M.S College of Engineering, Bengaluru. He also completed the Bachelor's Degree in the flied of Computer Science Engineering.

Rajashekaragouda G Sankanagoudra is a final year Mtech Student of Computer Networks branch at B.M.S College of Engineering, Bengaluru.He also had Electronics background in Bachelor's Degree.