

# Blockchain Technology In E-Healthcare Applications

**Instructor Name :** Sir Aziz Mehmood Farooqi

**Group Partners :RANA HAMZA ALI 9834**

**FABEHA NAQVI 9876**

**Source Paper:**International Journal of Information Technology (IJIT) – Volume 6 Issue 5, Sep-Oct 2020 ,”Blockchain Technology In E-Healthcare Applications” by Elayaraja P-Software

Engineer-Chennai



**Abstract Introduction**

**Methodology For Security**

**Blockchain- A Distributed Ledger Technology Security analysis Of E-Healthcare Via Blockchain Working Procedure Of Blockchain Technology Important Elements in Blockchain Cyber-Security**

**Distributed Ledger Hash Functions**

**Access Control Model for E-Healthcare Conclusion**

ABSTRACT

E-HEALTHCARE is the promising approach and being considered as the vital and most important approach in the Healthcare sector.Being such an important and promising approach the security and authentication is must for the information being accessed in model.Wireless Sensor Networks (WSN) technology is enabling Internet of Thing (IOT) so while being used in E-Healthcare for Communication so the security ,integrity and authentication is needed.For security needed in E-Healthcare Blockchain Technology (BT) with distributed Ledger proposed and these technologies also proved their worth regarding security purpose.Although many security algorithms , protocols and technologies were proposed for security reasons but for securing sensitive information or data Blockchain Technology is proving itself most promising.

Blockchain Technology (BT) uses Distributed layer for securing Cloud Computing and data stored in Cloud storages and for securing the credibility and integrity of data stored in clouds BT uses security algorithm like Hash Function when security of data is done now the main need is authentication of applications which is done by the Access Control Management of BT.In the end of paper results are shown after examining the performance of Blockchain Technology in source Paper and other reports published internationally.

KEYWORD: Blockchain Technology BT, Distributed Ledger, Hash Function, Access Control.

# INTRODUCTION

Blockchain is a specific type of database work in such way that data stored as blocks in ledgers in decentralized manner and then chained together, to understand this consider that those blocks have some storage capacity and when they get filled by data than they are chained to the previously filled block with data like forming a chain and this goes on when all new data after freshly added block get stored in the block that also chain with the previous one block.Blockchain stores data in decentralized manner in simple words data is stored in various devices ,computers,systems and servers and these devices are hosted by the multiple users within the decentralized cloud of blockchain.Data stored in decentralized manner with the P2P(peer-to-peer) storage access is protected with blockchain technology and various cryptographic algorithms for encryption of data .

Nodes are used for storing data ledgers in decentralized networks .Those nodes are created by the computation of users present on that P2P network with the help of cryptographic computational processes. Blockchain architecture provides properties like Transparency that the all transactions of data is visible to the public network each transaction is assigned its own identity known as hash also known as the transaction receipt all devices on the P2P network have access to these records creating high level of transparency ,Robustness or Durability in blockchain technology is built in which means the data stored across the network cannot be controlled by any single entity, Audibility in blockchain assure that the data block stored in chain cannot be change and edited which cause that the blockchain stays in the chronological order and making it tamper proof, Security in blockchain is the most important property because the transaction records are visible to the network so the data get on the high risk of being misused for encountering this problem blockchain provides two primary security mechanism first is

network structure and the second one is cryptography. Cryptography assure that the sign data was approved by the authorized user and the decentralized structure of network eliminate the chances of attacks because if someone wants to attack the network he has to get control majority of nodes at the same time present on the network.

As discussed in the source paper the scenario of patients sharing their data in the EHR- Electronic Health Record system the main purpose of storing data in EHR is to preserve data and also for the further use of it. EHR stores data on blockchain ,which ensure the security and the availability of data . Security concerns are fulfilled by the confidentiality of EHR are provided by the key management or key agreement schemes for establishing the secure communication channel between doctor and patient for understanding the key agreement between dr and patient consider that the data records stored by the patient are encoded with private key and mentioned on the blockchain which assure its access to the only authorized persons and it has to be noted that the data stored once cannot be change or edited .

When the data is stored on a network it is needed that the stored data is accessible by the authorized users ,and when users demand specific data it gets the desired data from the network for this purpose Blockchain is discussed and proposed as the access control manager for the E-Healthcare Systems.



METHODOLOGY FOR SECURITY

Typical Health care system is ancient now .It depends overall on the physical interactions between consumers. Such as if Doctor has to check patients physically and have access of limited data ,but as per modern studies for better healthcare results one should be examine with overall medical history but because of the hard copy reports cannot be stored for long time use

,patients lose their medical history as they lose their reports .Blockchain solve these issue with the storage of medical data or report which are accessible universally. Because of these issues Blockchain in healthcare is proving its worth and will completely serve healthcare sector in near future.

As Blockchain is taking over the old healthcare system the security of databases is the main concern. For securing healthcare databases Support Vector Machine (SVM) is used. Support Vector Machine (SVM) was invented by the Vapnik & Chervonenkis but at that time algorithm was in early stages and was used for linear classification of data .Later Vapnik, Boser & Guyon suggested using kernel trick for non-linear classification . Svm is the most dominant algorithm for classification of data when data is available with features and class labels we can use SVM. For providing security and accessibility to data to the E-healthcare user based access control is used in blockchain. For this purpose Key management is done in such way that the Unique Id is given to every user in healthcare system which help to create secure ,fast, accessibility and the transparent exchange of medical data Unique Id give mechanism for all users of healthcare system such as patient ,doctors ,labs ,insurance agencies and government to ask for access ,and have the medical record of patients .Blockchain allow the interoperability of medical data of patient which can help patient for universal access of their records and that's also beneficial for insurance matter as well as for the governments for the audit of public health care record and also for examining the health or medical data of specific person. Block chain as a decentralized database can solve all interoperability problems. Blockchain cans also solve all issues and problems in drug traceability process by giving security and drug traceability because data

stored in blockchain is unchangeable and also its time stamped so it can also be used in future for research and verification.Blockchain can provide solution for the easy clinical trials or audits because the blockchain provides the fully integer data so it can be verified for authenticity of information or reports.And it also assure that no one can access data with the authorization.

Block chain provides suitable data structure for storing data that it can be accessed by the authorized person such as it kept accessible to the doctor and the patients.And when patient wants to revoke someone access can be revoked .Patients can share data anonymously

,patients have full control on the data only they can allow someone to access data .

# Blockchain- A Distributed Ledger Technology

Blockchain is a specific type of database work in such way that data stored as blocks in ledgers in decentralized manner and then chained together, to understand this consider that those blocks have some storage capacity and when they get filled by data than they are chained to the previously filled block with data like forming a chain and this goes on when all new data after freshly added block get stored in the block that also chain with the previous one block.

Blockchain stores data in decentralized manner in simple words data is stored in various devices ,computers,systems and servers and these devices are hosted by the multiple users within the decentralized cloud of blockchain.Data stored in decentralized manner with the P2P(peer-to-peer) storage access is protected with blockchain technology and various cryptographic algorithms for encryption of data .

In P2P network users using devices are called nodes that share data on a network which is stored as ledger ,Blockchain is a network in which nodes are considered to be evaluating transactions of data and also validating them,organizing data into blocks and updating their ledger.Block chain distributed model has layers being used for functions layer are.

FABRIC LAYER which is used by nodes to host ledgers and chaincodes,applications and authorized users wanting to interact with these nodes .A node in this layer can host many ledgers and chaincodes exceptions are also there .

APPLICATION LAYER is used for chaincode,Apps and s-contracts.this layer has two categories first is Application layer which is responsible for the applications which are used by users to interact with Blockchain distributed networks.Second one is Execution is sub layer which deals with the smart contracts,actual Rules to be executed and actual Chaincode those get executed .

NETWORK LAYER is used for inter-node communication in Distributed network.Nodes can find each other ,synchronize with each other and can communicate with each other to continue the valid state on Blockchain Distributed Network.

Distributed ledger provides peer to peer network connection ,which allow any peer to create new transaction and allow to read from the shared consistent copy of the database because there is no central server of data.Distributed ledger uses consensus protocol for validation of transactions( could be in any form financial,asset and services).Transactions are done under some rules which are called smart Contracts.Confidentiality of transaction is possible because of digital signatures (private key/public key) to encrypt or sign transactions on the ledgers.Besides its way secure technology but there are some challenges also like some malicious changes were recorder to transaction which were spotted by some peers .Distributed ledgers are extremely beneficial in financial transaction such as Blockchain but it's also

promising in the E-healthcare applications.Distributed ledger Technology DLT decreased so many inefficiencies in operations of E-healthcare because of providing immutable data which is easily accessible universally any time and the security was provided by the decentralized nature of network which cannot easily threatened from malicious activities.

Blockchain technology a type of distributed ledger technology used for recording transactions happen over decentralized network.Concept of decentralized network means there is no such authority which evaluates and follows up transactions instead transaction is distributed across many users or nodes present on the network.This technology allows peers to verify transaction by computing cryptographic hash functions without the need of trusting other peers on the network.Blockchain uses the consensus protocol for verifying the transaction by nodes.Distributed database having consensus protocol provide the trustless fashion which enabled many blockchain-application such as crypto-currency these p2p applications uses p2p network instead of centralized servers.

# Security analysis Of E-Healthcare Via Blockchain

A single blockchain network cannot serve various industries and sectors. That's why various blockchain networks were created but the market is using two types of blockchain networks. Permissionless Blockchain (Public) and Permissioned blockchain (Private).

Permissioned Blockchain Technology is a closed system in which nodes are not free to join network,perform transactions and access data .Permissioned Blockchain is used by the centralized organizations those who want to leverage the power of network for their internal business functions.Such private blockchain runed by several companies only approved peoples and devices can run nodes on the network,execute smart contracts,issuing and reading transactions and validate them.They are free to choose which consensus algo they want to use. Transparency in Permissioned blockchain is not must but condition can vary and depends on the organization.Promised Blockchain is most promising for the healthcare sector as there only defined users and authorized parties are allowed .

## Working Procedure Of Blockchain Technology

Technically Blockchain is chain of data blocks ordered in non trusted distributed Network of peers.Each block assist or refer to the previously joined data block and refer to its hash and the hash of the Previous data block.A block stores the details about the users interacted these interactions are called transactions which are stored in the blocks.Once hash is calculated it generate the block .changing inside the block indicates change in hash of block.so we can say that the hash refer to the change occurred in the block.Each newly added block have the hash of previous block.Thats why attacking this type of network is so difficult because if someone want to get access of network he has to change all the hashes of blocks before.So this hashing function in which when single node announces the completion in hashing function other nodes also verify that .we can say that the information saved by one node is verified by the other node.

## Important Elements in Blockchain Cyber-Security

Distributed Ledger

Distributed Ledger brightens the ways organizations can work ,it can assist organizations in their operations such as in health for health data securing and availability for future use and for governments in passport issuance,land registries etc with the premium security of their data

,because is some malicious attack happen to the network its harder to crack that because all the data stored in DLT is in the form of distributive copies of data and if some one want to crack in to network he has to attack all copies simultaneously for making attack successful.Security having by distributed ledgers allows network extensive transparency.Distributed ledgers allow easy audit trials which removes the fraud possibility.

Hash Functions

Hash functions are most used cryptographic algorithm in blockchain technology.Hash functions are developed to provide integrity to data.In simple words Hash Function is a mathematical function that transform input into a fixed size output.Hash function is collision resistant means it cannot produce single output to two or more inputs.These are some properties of hash functions

,One-Way means it's possible to go from input to output but can't do in reverse this property stops it from the collision, Large space out this means checking as many output as the possible output of hash function,Non-Locality in con local function no similar outputs were produced by the similar inputs.

Blockchain uses hash function for several uses some are Digital Signature are used for data integrity and authentication in blockchain transaction,Proof 0f Work consensus algo define legitimate blocks as one header has less hash value, since consensus algo assure a valid block hash function is required for their collision resistance,BlockchainChains as each block contain hash of previous block this insure that the changing one block without connected block is not possible, hash function improve integrity of blockchain digital ledger.

Hence sometimes cryptographic functions are broken if attack aur flaw found in hash function

,they cant find hash collision.Hash Output Length hash functions are best to find collision in brute force search.These reasons make hash functions important for the security of blockchain.

# Access Control Model for E-Healthcare

Access Control is the core of any sector security.Access control is the solution for authentication and integration hearts to the organization and for this Block chain technology is the m,ost promising technology for the E-healthcare Access Control.Block chain is now entering where technology will be applicable to even decide which type of block chain should be used.As we now in block chain data is decentralized means data is not saved on a single server. Which is distributed across all devices connected to the block chain network. So block chain can be the Network of nodes connected in a peer to peer way where the device is connected as a node and communicates to other nodes. So here the authentication is also required for the purpose of identifying users .For this we will consider the attribute base accessed policy for E-healthcare.

Data authorized users or parties for that data will be these.User is the one who is approved to access the data if the accessibility is associated with cipher information as the data owner chatagraized .E-healthcare Data Owner is the access policy which decentralized its data into various copies of parts by the use of symmetric encryption under various contect keys . Service Provider control data access and deals with the attributes of users .Central Authority the governance entity providing parameters whether public and private and access to the user based on their attributes.

# CONCLUSION

Although Blockchain was associated with the cryptocurrency but with other uses of this technology the use of Blockchain in Healthcare is were radiant.Decentralized network Block chain provides every important necessity of E-Healthcare for moving forward from typical healthcare system to the block chain system which will boost this sector. As Blockchain is taking over the old healthcare system the security of databases is the main concern.For providing security and accessibility to data to the E-healthcare user based access control is used in blockchain.FRom Blockchain E-Healthcare will be served with accessibility and security of data which is nice trade off between Security and Performance and will help to go further to find more good solutions.