International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

High Dimensional Health Care Privacy Approach using Blockchain Technology for Health Insurance Company

Aditya Sunil Kolte[1], Yash Jitendra Lodha[2], Ankita Ishwarchandra Patil[3], Shreya Mohan[4]

[1-4]*Student, Padmabhooshan Vasantdada Patil Institute of Technology, Maharashtra, India*

Abstract - *A huge amount of data, generated by different applications in computer networks, is growing exponentially based on non-stop operational states. Such applications are generating a huge amount of information that is harmful for predictable data processing and analytics functionality, which is perfectly handled by the cloud before the explosive growth of Big Data. Blockchain technology reduces the dependency on a centralized authority to certify integrity and ownership of information. It also mediates transactions and exchange of digital assets, while enabling secure and partially anonymous transactions along with agreements directly between the interacting parties. It addresses issues in healthcare, such as incomplete records and difficulty in accessing the patients' own health information because of its key properties like immutability, decentralization, and transparency. An efficient system that stores healthcare information requires its software apps and technology platforms to communicate securely and use the exchanged data across health organizations and other users. Unfortunately, healthcare currently suffers from fragmented data, slowed down communications, and dissimilar workflow tools caused by the lack of interoperability. Blockchain helps to access complete and tamper-aware medical records that are stored in fragmented systems in a secure and pseudo-anonymous manner. Fog computing or fog networking, also known as fogging, is pushing the frontiers of computing applications, data, and services away from centralized cloud to the logical stream of the network edge.*

Key Words: Blockchain, Fog Computing, Machine Learning, Big Data, Secure and Pseudo Transaction, Cryptographic Database

INTRODUCTION

Fog computing is pushing frontiers of computing applications, data, and services away from centralized cloud to the logical stream of the network edge. A Blockchain system is considered a virtually incorruptible cryptographic database where critical medical information could be stored. This system is maintained by a network of computers which is accessible to the one running the software. Blockchain works as a pseudo-anonymous system that has still privacy issues since all transactions are exposed to the public, even though it is tamper-proof in the sense of data integrity. The main control in accessing the records of all patients' healthcare across multiple health institutions and devices, needs to be carefully designed. Blockchain itself is not designed as a large-scale storage system. In the domain of healthcare, a decentralized storage solution would be a great addition considering the weakness of blockchain in this perspective.

Problem Statement

To design and implement a system for health care data, where users' information can be stored in single Blockchain without any Trusted Third Party (TTP) in fog computing environment.

Motivation

1. We observe in that the vision of Blockchain Technology is decentralized cooperation between distributed agents.
2. We notice that the decentralized architecture provides the automatic data recovery from different attacks.
3. Large data storage at the required of decentralized data storage as well as information system
4. The different attack issues in centralized database architectures.
5. There are no automatic attack recovery in central data architectures

METHODOLOGIES/ALGORITHM DETAILS

Algorithms

1. **Hash Generation (Apply SHA 256 from SHA family)**

Input : Genesis block, Previous hash, data d,

Output : Generated hash H according to given data

Step 1 : Input data as d

Step 2 : Apply SHA 256 from SHA family

Step 3 : CurrentHash= SHA256(d)

Step 4 : Return CurrentHash

2. Protocol for Peer Verification

Input : User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain],

Output : Recover if any chain is invalid else execute current query

Step 1 : User generate the any transaction DDL, DML or DCL query

Step 2 : Get current server blockchain

Cchain ← Cnode[Chain]

Step 3 : For each

Nodes Chain [Nodeid, Chain] $\sum\_(i=1)\hat{}n\ (Get\ Chain)$

End for

Step 4 :Foreach (read I into NodeChain)

if(!equals NodeChain[i] with (Cchain)) Flag=1

else continue commit query

Step 5 : if (Flag==1)

Count = SimilarlyNodesBlockchain ()

Step 6 : Calculate the majority of server

Recover invalid blockchain from specific node

Step 7: End if

End for

End for

3. Mining Algorithm for valid hash creation

Input : Hash Validation Policy P[], Current Hash Values hash_Val

Output : Valid hash

Step 1 : System generate the hash_Val for ith transaction using Algorithm 1

Step 2 : if (hash_Val.valid with P[])

Valid hash

Flag =1

Else

Flag=0

Mine again randomly

Step 3 : Return valid hash when flag=1

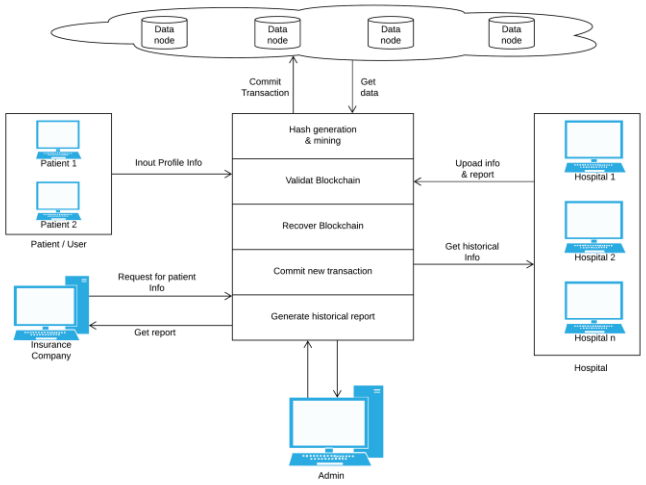

Fig -1: System Architecture

The central outline of the proposed algorithm is the implementation of health care data storage using block chain. System creates the trustworthy communication between multiple parties without using any third party interface. We use the Hash generation algorithm and the Hash will be generated for the given string. Before executing any transaction, we use peer to peer verification to validate the data.

OUTCOME

1. The patient can access any of their data from the specified portal on the Internet.
2. Patient description is shown immediately.
3. Once a transaction is completed, it will immediately reflect in all the nodes.
4. When a record of any node shows invalid data, it will automatically recover by using the other nodes.

APPLICATION

1. Peer to peer communication transaction applications.
2. Bitcoin transaction applications.
3. Zebpay transaction application
4. Bittrex app

CONCLUSION

From the technical view, more research is needed to identify the most practical design procedure in building an interoperable ecosystem, using the Blockchain technology, while balancing critical security and confidentiality concerns in healthcare. Whether to create a decentralized application leveraging an existing Blockchain, additional research on secure and efficient software practice for applying the Blockchain technology in healthcare is also required to educate software and IT domain engineers and domain experts on the potential, limitations and expansion of this new technology.

ACKNOWLEDGEMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. Snehal Javeri from Computer Department of Padmabhooshan Vasantdada Patil Institute of Technology for her valuable suggestions and guidance throughout our course of study and timely help given to us in completion.

REFERENCES

[1] Gupta A, Patel J, Gupta M, Gupta H., (2017), Issues and Effectiveness of Blockchain Technology on Digital Voting. International Journal of Engineering and Manufacturing Science, Vol. 7, No. 1

[2] Navya A., Roopini R., SaiNiranjan A. S. et. Al, Electronic voting machine based on Blockchain technology and Aadhar verification, International Journal of Advance Research, Ideas and Innovations in Technology, (Volume 4, Issue 2)

[3] Hardwick, Freya Sheer, Raja Naeem Akram, and Konstantinos Markantonakis. "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy." arXiv preprint arXiv:1805.10258 (2018).

[4] Meter, Christian. "Design of Distributed Voting Systems." arXiv preprint arXiv:1702.02566 (2017).

[5] Panja, Somnath, and Bimal Kumar Roy. "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain."