International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Enhancing the Health Care Data Security through Blockchain

Neha Sharma, R. B. Joshi

Abstract:*As the Internet technology is improving, large amount of data is generated. To deal with this huge amount of data many applications try to store the data on cloud networks. So before storing the data, security of data should be taken into consideration. Many classical existing approaches have already provided ACID properties with transaction management for consistent data provision. Some multi cloud environment systems also support to provide a consistent streaming data to end users even in high network. The blockchain is an important technique that provide the security for transactional dataset. Bitcoin is the most popular example to illustrate the strategy of blockchain execution. In this research we propose healthcare data security using blockchain and fog computing. The reason behind to use fog computing during the execution is to process the large-scale data which is generated from various sources. This work is categorized into various sections such as: insurance Company, thenthe patient registration as well as hospital registration, for each patient having a unique identification number as well as hospital also. When a particular patient communicates with Hospital as well as makes any future transaction with desired Hospital, it will store all records into the blockchain. The data has been stored according to the classical blockchain miner. SHA-256 has been used for hash generation and mining algorithm applied for validating the current hash according to given policy. The consensus algorithm used to validate the proof of work as well as to validate the current blockchain into peer to peer network. The fog computing is important to reduce the time complexity when system generate the large-scale data. According to various experimental analysis the system will provide drastic security to Private data as well as provide minimum time complexity.*

Index Terms: Blockchain, Fog Computing, Consensus, Time Complexity.

I. INTRODUCTION

Fog computing that is known as edge network, and is pushing borderland of computing functions, information, and supply away from centralized cloud to the probable flow of the network edge. The Fog network system works to build discipline, composition and functionality in the Internet grid rather than functioning primarily through network entrance. We can illuminate the cloud computing infrastructure as a highly visualized IT infrastructure that provides hierarchical networking facilities through nearby server nodes. These fog nodes manage various applications andservices to storeand process information close to end users. Sometimes, fog computing often uses the term "perimeter calculation". Fog and the fringes involve pushing the functioning and intellectual abilities to the closeness of where the information originates. In both structures, the information is sent by the same sources or physical resources. All these systems carry out a physical work in this world as electrical circuits, or detecting the operations around them. To achieve the security using decentralized architecture blockchain systems has been implied. A blockchain system can be visualized as a practically trustable cryptographic database where censorious medical information could be recorded. The system is maintained by a computer network that is accessible to registered users running the software. The blockchain functions as an undefined system that still has privacy problem, as all operations are exposed to all, even though it is tamper-proof in the sense of data incorruptibility. Access authority of the patient's various health records through multiple health institutions and devices must be carefully drafted. Blockchain itself is not drafted as the extensive storage system. In the theory of health care, a decentralized storage solution would greatly complement the weakness of the blockchain in frame of reference. The blockchain network as a decentralized system is more flexible as there is no single point of attack or information loss with respect to centralized systems.

A. *Background of System*

Decentralization: To guarantee strength and adaptability and to wipe out many-to-one traffic streams we need a decentralized framework. Utilizing such decentralized frameworks, we can likewise take out the single purpose of disappointment or data postpone issues. In our model, we are utilizing an overlay decentralized system.

Authentication of data: User's System or cloud administrations store unpreserved information that should be moved to blockchain systems. During transmission, the information could be changed or lost. The protection of such off base altered information builds the weight to the framework and can cause the loss of the patient (demise). Along these lines, to guarantee that information isn't adjusted, we utilize a lightweight advanced mark [2] plot. On the recipient side, information is confirmed with the client's advanced mark, and whenever got effectively, it sends a receipt of information to the patient.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Neha Sharma*, M.E. (II Year), Computer Engineering Department, JSPM's Rajarshi Shahu College of Engineering, Tathawade, Pune-411033.mickey.neha2911@gmail.com
Dr. Ram B. Joshi, Head, Information Technology Department, JSPM's Rajarshi Shahu College of Engineering, Tathawade, Pune-411033.ramjoshi.comp@gmail.com

Adaptability: Solving Proof of Work (PoW) is computationally escalated; in any case, IoT gadgets are asset confined. Likewise, the IoT system contains numerous hubs and blockchain scales inadequately as the quantity of hubs in the system increments.

We dispense with the idea of PoW in our overlay system and separation our overlay arranges into a few bunches rather than a solitary chain of squares, and in this way a solitary blockchain isn't in charge all things considered. Rather we spread the hubs more than a few groups. Our model depends on the circulated nature and other extra security properties to the system.

Data Storage: Storing IoT huge information over blockchain isn't reasonable and in this manner, we use cloud servers to store scrambled information squares. The information is protected over the cloud because of extra cryptographic security like the advanced signature and exclusive requirement encryptions which will be examined later. In any case, it might cause an issue about confided to outsiders. For this reason, we store all exchanges in various squares and make a consolidated hash of each square utilizing Merkle Tree and move it to the dispersed system. Along these lines, any adjustments in cloud information can be effectively perceivable. Doing the capacity as such likewise saves the decentralization over certain degrees.

Anonymity of users: Medical information of a patient may contain touchy data, and in this manner, information must be anonymized over the system. For obscurity, we are utilizing lightweight Ring structure [2] alongside advanced marks. Ring mark enable an endorser to sign information namelessly, that is the mark is blended with different gatherings (named ring), and nobody (aside from real underwriter) knows which part marked the message.

Security of data: Medical gadgets or wellbeing information must be precise and can't be changed by programmers. To spare the information from programmers, we are utilizing a twofold encryption plot. Here twofold encryption does not allude to scrambling similar information utilizing two keys yet rather encryption of the information and again encryption of key which was utilized to encode information. We scramble the information utilizing lightweight ARX calculations and after that encode the key utilizing the open key of the beneficiary. Likewise, we are utilizing the Diffie Hellman key trade strategy to move the open keys and in this way getting the keys is practically incomprehensible for an aggressor.

II. LITERATURE SURVEY

According to “A survey on Security and Privacy issues of Blockchain Technology”, 2018[1] we get a comprehensive survey on Blockchain Technology with its structure and consensus algorithm.

Pazaitis et al., 2017 [2] It explores the potential of blockchain's technology by allowing a new value system that will better support the dynamics of social exchange. The study of the system begins with a discussion on the evolution of perceptions of value in the history of economic thought. Beginning with a vision of value as a mechanism that defines meaningful action in a given context, the system combines the pricing system with the establishment of capitalism and the industrial economy. System, then discuss its relevance to the information economy, exposed as the techno-economic context of the shared economy, and identify new ways to create value that better reflect the social relationships of sharing. Through the illustrative case of Backfeed, a new system of values is envisaged, consisting of three layers: (a) value production, (b) Value Registration and (c) updating the value. In this context, the system addresses the solutions presented by Backfeed and demonstrates a conceptual economic model of decentralized cooperation based on blockchain. The system concludes that blockchain technologyhas the potential to enable the creation of common property-based ecosystems in a shared economy.

On the governance of OI and BT platforms, (“Blockchain Governance”, 2017) [3] writes that at the heart of the problem, as always, lies the governance challenge, namely who dictates and enforces the rules as well as who do system hold accountable when things not working in proper manner. What developers don't understand is that the public wants to put confidence in the institutions that operate the "conventional" platforms, especially when they are exploited by real people, so that they can be held accountable. For example, Airbnb was built on a notion that people are organized, but soon enough trust problems arose like bad consumer experience, fraud, vandalism, etc. Soon Airbnb has evolved from a technology company and a standard platform of rules and authority. As long as the challenges of blockchain governance are not considered, BT's transformer potential will not be realized.

The paper“Blockchain and Open Innovation”, 2017 [4], In recent years, a new technology has been developed – blockchain – which is expected to replace many existing digital platforms. The first came to light at the end of the years 2000 as the architecture for Bitcoin, the most famous virtual currency. But, as with the Internet, the web and other important technologies, blockchain (BT) technology has now transcended its original goal. It has the potential to revolutionize the financial industry and transform many aspects of the digital economy. Open Innovation (OI) and IP industry (IP) will also be affected, so here the system addresses issues regarding BT's adoption in OI to be discussed in this document.

According to Potts et al., 2017 [5] Smart City's agenda for the integration of ICT and IoT, the IT infrastructure to improve the efficiency and adaptability of the city's government has been the implementation of urban development policy for more than a decade. A smart city has more data, compiled with new and better technologies, offering better quality urban services. BT could change the Smart City agenda by changing transaction costs with implications for infrastructure and resource coordination and by encouraging OI as outlined in the previous section. As the city's smart city crypto uses data computing, and is coordinated by distributed rather than centralized systems. The crypto-urban data infrastructure can enable civil society to execute local public goods and facilitate economic and social entrepreneurship in the IO.

Lember, 2017 [6] In fact, the various technologies associated with the "smart city" such as electronic sensors or urban control rooms and urban labs, as well as emerging technologies such as the chain of blocks, 21 that allow the Provision of point-to-point services are increasingly at the centre of how citizens engage in the delivery of public services as part of the user/Citizen IO Program-innovation, Technology and living Labs for Accelerate technological Innovations in the public sector. All of these approaches aim to put the user's experience at the centre of Public sector innovation processes, however, these experimental units and methods are still far from becoming an organic part of the public sector and their change.

W. Liu,T. Mundie, S.S. Zhu, U. Krieger 2017 [7], we get description of Blockchain architecture to store medical records securely.

According to “Issues and Effectiveness of Blockchain Technology on Digital voting”,2017 [8] explains the various blockchain applications.

Johansen, 2016 [9], Because of the novelty of the underlying concepts and technologies, the system provides a new overview of recent developments and literature related to this book and strives to explore related concepts in the literature. Through the exploration of concepts, the immersion system in the use of blockchain as a technological platform for a future ecosystem of applications and software and to look at the theoretical characteristics of technology as a basis of this role. As a result, the system improves the understanding of technology in other contexts throughout the literature and explores current contributions to literature. This study has implications for investigators and practitioners. For researchers, the system seeks to open up research lines on BT's empowerment as a platform-centric technology for ecosystems to thrive as OI. For practitioners, the system shows that it is crucial to continue to develop the technology, as research indicates that the system has not yet reached the tipping point of technology.

According to Glaser &Bezzenberger, 2015 [10] After the theoretical introduction, this system aims to deepen the theoretical grounding in order to give a brief summary of the preliminary research and to highlight the potential areas for future research. In addition, the system seeks to establish a common understanding of the theory in the field of OI with respect to BT. In the field of OI research, BT is still considered an innovative innovation and has not yet been part of the Mainstream OI research. This is further supported by the general landscape, whose main focus has been on blockchain as a cryptographic economic system, e.g. Bitcoin. The system also considers the amount of literature in the region as an important factor in evaluating the maturity of the concepts. System to find that the Bitcoin concept with 24 500 results was explored similar to blockchain with 17 500 results in Google 3 academic. which increased by 10 in just a year of 2016 compared to the first search engines of (Johansen, 2016). There is still a gap to understand the BT in OI. This system tries to give a new perspective on BT by examining current BT research and combining this with other OI concepts such as blockchain as a platform, ecosystems, innovations and characteristics Technological

III. PROPOSED METHODOLOGY

System highlights the implementation of health care data storage using blockchain. The system creates trustworthy communication between multiple parties without using any third-party interface. The three different modules have been illustrated in the system along with architecture, first insurance company admin creates the profile for patients as well as hospital and database. When any patient want to use the health care related services, they can communicate with respective hospital. Similarly, hospital assists the patient and store whole transaction data into the blockchain. For future all three entities should access this historical data anytime, anywhere concurrently. The system also has the ability to eliminate runtime differential privacy-based attacks and proposed consensus algorithm provides the runtime block validation that will provide flexibility to the system.This illuminates the quality of service issue and time limits. This is a middleware system in which the processing environment will balance the load using threads. The request generated will be parallelly saved on all nodes in a Block chain manner.

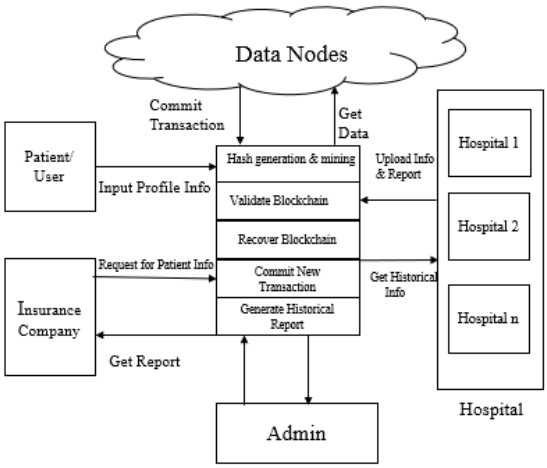


Fig. (a): Proposed System Architecture

Hashgeneration algorithm is applied and the generated hash for the given string is available before executing any transaction, we use peer to peer verification to validate the data. If any chain is invalid then it will recover or update the current server block chain. This will validate till the all nodes are verified and commit the query. Mining algorithm is used for checking the hash generated for the query till the valid hash is generated.Basically, this system carried out a block chain strategy to implement in peer-to-peer environment. The SHA-256 algorithm has used to generate has scored and mining algorithm for fear verification. During the execution system uses consensus algorithm to evaluate whole blockchain with a different pair. Basically, system validates each block when end user generates any data manipulation request, before execution of such a request system validation on blockchain using consensus algorithm. The voting-based majority technique measures trust for each node, and according to highest majority of different pianos system recovers the data losses from different blocks.

This technique ability to eliminate various kind of attacks like collision attack, SQL injection attack, man in the middle attack, session hijacking etc. Moreover, system executes in fog environment which illustrate the data processing environment install hardware network, the different locks parallelly communicate with all data nodes as well as user request simultaneously. This approach also reduces the time complexity for data processing.

IV. ALGORITHMS AND PSEUDOCODE

Algorithm 1: Hash Generation
Input: Genesis block, Previous hash, data d
Output: Generated hash H according to given information
Step 1: Input data as d
Step 2: Apply SHA 256 from SHA family
Step 3:Current Hash= SHA256(d)
Step 4:ReturnCurrent Hash

Pseudocode: Protocol for Peer Verification
Input: User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodeChain[Nodeid] [chain],
Output: Recover if any chain is invalid else execute current query
Step 1: User generate any transaction DDL, DML or DCL query
Step 2: Get current server blockchain
Cchain←Cnode[Chain]
Step 3: For each

$$NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$$

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 = SimilarNodesBlockchain()
Step 6:Calculate the majority of server
Recover invalid blockchain from specific node
Step 7: End if
End for
End for

Mining Pseudocode 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_Valvalidate with P[])
Valid hash
Flag =1
Else
Flag=0
Mine again randomly
Step 3: Return valid hash when flag=1

V. RESULTS AND DISSCUSSION

For the system performance evaluation, the system calculates the matrices for accuracy. The system is executed on java 3-tier architecture framework with INTEL 2.8 GHz I3 processor and 4 GB RAM with distributed environment. The below figure (b) shows the time required for consensus algorithm to validate the blockchain in 4 nodes. X axis shows the size of blockchain and Y shows the time required in milliseconds for validation.

Table. (b):Time required (in milliseconds) for completetransactionwith different records blockchain using four data nodes in P2P Network

Blockchain Size	Validate	Insert	Retrieval
200	120	150	170
400	120	302	330
600	320	435	501
800	470	560	640
1000	630	720	820

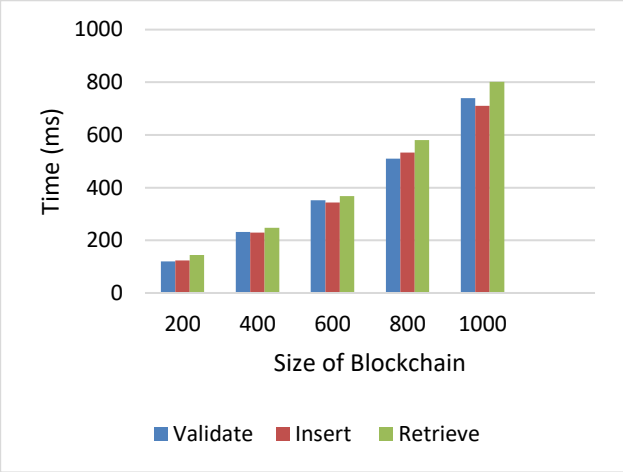


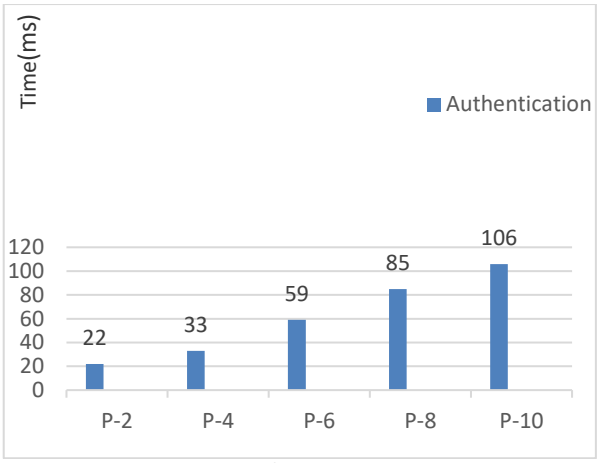
Fig. (b):Time required (in milliseconds) for complete transaction with different record blockchain using four data nodes in P2P Network

In another test case we evaluate the proposed system with smart contract validation by consensus algorithm in different number of peer to peer node.

Table (c): Time required for smart contract validation with different no. of P2P network in blockchain.

Peer Size	Time (ms)
2	22
4	33

6	59
8	85
10	106



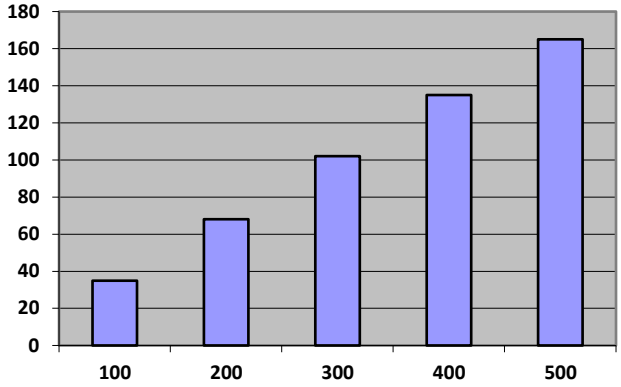
Size of Blockchain

Fig. (c): Time required for smart contract validation with different no. of P2P network in blockchain.

The number of variation taken by algorithm from propose SHA value are evaluated in the third test case. Basically this has been done to evaluate the propose hash string is valid or not according to given mining policy. In many times when system generates SHA code for given transactional data its never fulfill the mining policy. To fulfill the propose mining policy according to given scenario mining to generate the multiple variation on given string. The below figure (d) shows the time required to generate the valid SHA string for specific transaction.

Table. (d): Time required for mining for number of transactions in milliseconds.

Size of blockchain	Time (ms)
20	35
40	68
60	102
80	136
100	175



No. of Transactions

Fig. (d): Time required for mining for number of transactions in milliseconds

VI. CONCLUSION

In this system blockchain technology is usedfor database management with fog computing. From past decades there is very high ratio of data generation like crypto currency, healthcare, data warehousing etc. This system also points on data leakage issues in distributed environment, proposed hash generation techniques and mining algorithm eliminate the collusion as well as Man in the Middle (MiM) attack using the Consensus algorithm. The system is having an ability to defend the unknown attacks and also generating platform runtime blockchain validation. Multiple fog nodes reduce the time complexity of proposed system. To implement the proposed system with various data nodes will be interesting in future work.

REFERENCES

1. A. P. Joshi, M. Han, Y. Wang ," A Survey on Security and Privacy Issues of Blockchain Technology", Mathematical Foundations of Computing doi:10.3934/mfc.2018007 c
American Institute of Mathematical Sciences Volume 1, Number 2, May 2018.
2. Pazaitis, A., De Filippi, P. and Kostakis, V. ,"Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed. Working Papers in Technology Governance and Economic".
http://technologygovernance.eu/files/main/2017012509590909.pdf.
3. Allen, D. " Blockchain Innovation Commons", 2017.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2919170
4. "Blockchain and Open Innovation", 2017. Blockchain and open innovation: What does the future hold? (2017).
https://www.uktech.news/news/blockchain-and-openinnovation-what-does-the-future-hold-20161017.
5. Potts, J., Rennie, E., &Goldenfein, J, " A City Is a Data Pool: Blockchains and the Crypto-City",2017.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2982885.
6. Lember, V, " The Increasing Role of Digital Technologies in Co-production", 2017.
https://www.researchgate.net/profile/Veiko_Lember/publication/319504628_The_Increasing_Role_of_Digital_Technologies_in_Co-production_and_Cocreation/links/59afd7240f7e9bf3c72922e1/The-Increasing-Role-of-Digital-Technologies-in-Coproduction-and-Co-creation.pdf
7. W. Liu, T. Mundie , S.S. Zhu, U. Krieger, "Advanced Block-Chain Architecture for e-Health Systems", 2017. 19th International Conference on E-health Networking, Application & Services (HealthCom): The 2nd IEEE International Workshop on Emerging Technologies for Pervasive Healthcare and Applications (ETPHA 2017).

8. Aayushi Gupta1, Jyotirmay Patel, Mansi Gupta, Harshit Gupta, "Issues and Effectiveness of Blockchain Technology on Digital Voting",
International Journal of Engineering and Manufacturing Science. ISSN 2249-3115 Vol. 7, No. 1 (2017) © Research India Publications; http://www.ripublication.com .
9. Davidson, S., De Filippi, P., & Potts, J. (2016). Disrupting Governance: New Institutional Economics of Distributed Ledger Technology. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811995.
10. Glaser, F., &Bezzenberger, L. (2015). Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems. In European Conference on Information Systems (pp. 1–18). https://doi.org/10.18151/7217326

AUTHORS PROFILE

Neha Sharma, M.E. (II Year), Computer Engineering Department, JSPM's RajarshiShahu College of Engineering, Tathawade, Pune-411033, Mail ID: mickey.neha2911@gmail.com

Dr. Ram B. Joshi, Associate Professor IT, Head, Information Technology Department JSPM's RajarshiShahu College of Engineering, Tathawade, Pune-411033
Mail ID: ramjoshi.comp@gmail.com