IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 5, May 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105360|

Health Care Privacy Approach using Blockchain Technology

Juweriya Shaikh [1] , Mansi Lagad [2] , Ankita suryavanshi [3] , Prof. R.S Waghole [4]

U.G. Student, Department of Computer Engineering, KJ College of Engineering and Management Research Pune, India[1,2,3]

Associate Professor, Department of Computer Engineering, KJ college of Engineering and Management Research Pune, India[4]

Abstract: A huge amount of data, generated by different applications in computer network, is growing up exponentially based on nonstop operational states. Such applications are generating an avalanche of information that is disruptive for predictable data processing and analytics functionality, which is perfectly handled by the cloud before explosion growth of Big Data. Blockchain technology alleviates the reliance on a centralized authority to certify information integrity and ownership, as well as mediate transactions and exchange of digital assets, while enabling secure and pseudo- anonymous transactions along with agreements directly between interacting parties. It possesses key properties, such as immutability, decentralization, and transparency that potentially address pressing issues in healthcare, such as incomplete records at point of care and difficult access to patients' own health information. An efficient and effective healthcare system requires interoperability, which allows software apps and technology platforms to communicate securely and seamlessly, exchange data, and use the exchanged data across health organizations and app vendors. Unfortunately, healthcare today suffers from siloed and fragmented data, delayed communications, and disparate workflow tools caused by the lack of interoperability. Blockchain offers the opportunity to enable access to longitudinal, complete, and tamper-aware medical records that are stored in fragmented systems in a secure and pseudo-anonymous fashion. 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.

Keywords: Blockchain, Cryptography Decentralized, Distributed Systems, Cloud Storage, Role base Access Control (RBAC).

I. INTRODUCTION

Fog computing or fog networking, also known as fogging, is pushing frontiers of computing applications, data, and services away from centralized cloud to the logical stream of the network edge. A blockchain system can be considered as a virtually incorruptible cryptographic database where critical medical information could be recorded. The system is maintained by a network of computers, that is accessible to anyone running the software. Blockchain operates as a pseudo-anonymous system that has still privacy issue since all transactions are exposed to the public, even though it is tamper-proof in the sense of data-integrity. The access control of heterogeneous patients' healthcare records across multiple health institutions and devices needed to be carefully designed. Blockchain itself is not designed as the large-scale storage system. In the context healthcare, a decentralized storage solution would greatly complement the weakness of blockchain in the perspective.

II. RELATED WORK

Smart Contracts [1] also called crypto-contract, it is a computer program used for transferring / controlling the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy / agreement. These smart contracts are stored on block-chain and BC is an ideal technology to store these contracts due to the ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred / returned or since the transaction actually happened.

Currently CSIRRO team has proposed a new approach to integrate Block on IOT with [2] In its initial endeavor, he uses smart-home technology to understand how IOT can be blocked. Block wheels are especially used to provide access control system for Smart Devices Transactions located on Smart-Home. Introducing BC technology in IOT, this search again provides some additional security features; however, every mainstream BC technology must have a

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105360|

concept that does not include the concept of comprehensive algorithms. Moreover, this technology cannot provide a general form of block-chain solution in case of IOT usage.

According to Ilya Sukhodolski. The Al [3] system presents a prototype of multi-user system for access control over datasets stored in incredible cloud environments. Like other unreliable environments, cloud storage requires the ability to share information securely. Our approach provides access control over data stored in the cloud without the provider's investment. Access Control Mechanism The main tool is the dynamic feature-based encryption scheme, which has dynamic features. Using Blockchain based decentralized badgers; Our systems provide an irrevocable log for accessibility requests for all meaningful security incidents like large financing, access policy assignment, alteration or cancellation. We offer a set of cryptographic protocols that make the secret or secret key of cryptographic operation confidential. The hash code of the sifter text is only transmitted by the block on laser. Our system has been tested on prototype smart contracts and tested on IteriumBlockchan platforms.

According to [4] a basic IoT Blockchain fusion model with four layers which contains different types of IoT devices. Distributed file system is considered in the model to store huge amount of IoT data. Then, a case study for blockchain-based IoT application, a Machine-to-Machine(M2M) autonomous trading system, is proposed on the Ethereum blockchain. We build smart contracts for device registration, data storage, service provision and fair payment, and the proof-of-concept is implemented using two Raspberry Pis to interact with smart contracts. The proposed system verifies that blockchain could improve IoT applications in transparency, traceability and security.

According to [5]Edgence (EDGe + intelligENCE, is proposed to serve as a blockchain-enabled edge-computing platform to intelligently manage massive decentralized applications (dApps) in IoT usecases1. To extend the range of blockchain to IoT-based dApps, Edgence adopts master node technology to connect to a closed blockchain-based system to the real world. A master node contains a full node of the blockchain and a collateral, and is deployed on an edge cloud of mobile edge computing, which is convenient for the master node to use resources of the edge cloud to run IoT dApps

According to [6] introduces HCloud, a trusted JointCloud platform for IoT systems using server less computing model. HCloud allows an IoT server to be implemented with multiple servers less functions and schedules these functions on different clouds based on a schedule policy. The policy is specified by the client and includes the required functionalities, execution resources, latency, price and so on. HCloud collects the status of each cloud and dispatches server less functions to the most suitable cloud based on the schedule policy. By leveraging the blockchain technology, we further enforce that our system can neither fake the cloud status nor wrongly dispatch the target functions.

According to [7] introduce the concept of a decentralized glasified service exchange platform where the solution providers can dynamically offer and request services in an autonomous peer- to-peer fashion. Cost and decision to exchange services are set during operation time based on gasification policies according to business goals. The proposed concept is based on blockchain technology to provide a tokenized economy where the IoT solution providers can implement gasification techniques using smart contracts to maximize profits during service offering and requesting.

According to Vipul Goyalet. Al [8] develops new cryptosystems to share encrypted data properly, which we call key-policy attribute-based encryption (KPABE). In our cryptosystem, Cipher text is labelled with a set of properties and controls that it connects to private key access configurations that a user can decrypt the encryption. We display the utility of our product to share audit log information and broadcast encryption. Our creation supports private key providers, which subscribe to categorized identification-based encryption (HIBE).

Hao Wang et Mate Al [9] They offer a secure electronic health record (EHR) system based on special-based crypt co-occurs and blockchain technology. In our system, we use attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data and to use identity-based signature (IBS) to apply digital signatures. In order to obtain various functions of ABI, IBE and IBS in crypto, we present a new cryptographic primitive, it is called a joint feature-based / identity-based encryption and signature (C-AB / IB-ES). It simplifies system maintenance and does not require the installation of separate cryptographic system for various security requirements. In addition, we use blockconne techniques to ensure the integrity and inspection of medical data. Finally, we offer a demonstration application for medical insurance business.

According to [10] a scheme to generate seed needed for key generation and a scheme to manage the public key using blockchain. First is a random seed generation scheme needed for key generation? In order to prevent the risk of a man-in-the-middle attack and reverse engineering, seeds are generated by using out-of-band communication and hardware variation. Second is a key management system for the IoT using blockchain? The scheme we propose is to distribute the public key on the blockchain network. The public key is used to encrypt a session key that will be used for communication between devices.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105360|

III. PROPOSED SYSTEM AND DESIGN

In the proposed research work to design and implement a system for health care data, where user can store all information in single blockchain without any Trusted Third Party (TTP) in fog computing environment.
The system contains following modules:
The system contains following modules:
Hospital: An entity that communicates with the patient to generate a symmetric data to each medical record**.** An entity that requests medical record locally.
Patient: Patients are responsible for registering themselves into the system, deploying their uploading and submitting the medical records, and responding to data queries from doctors (requests to share medical records).
Insurance Company: Upload Policy details and show patient history.
Distributed Block chain: The Blockchain is the distributed ledger used to represent the current state of delegated access rights in the system. Permissions to interact with the Blockchain are handled by the Root Authority and the Attribute Authorities.

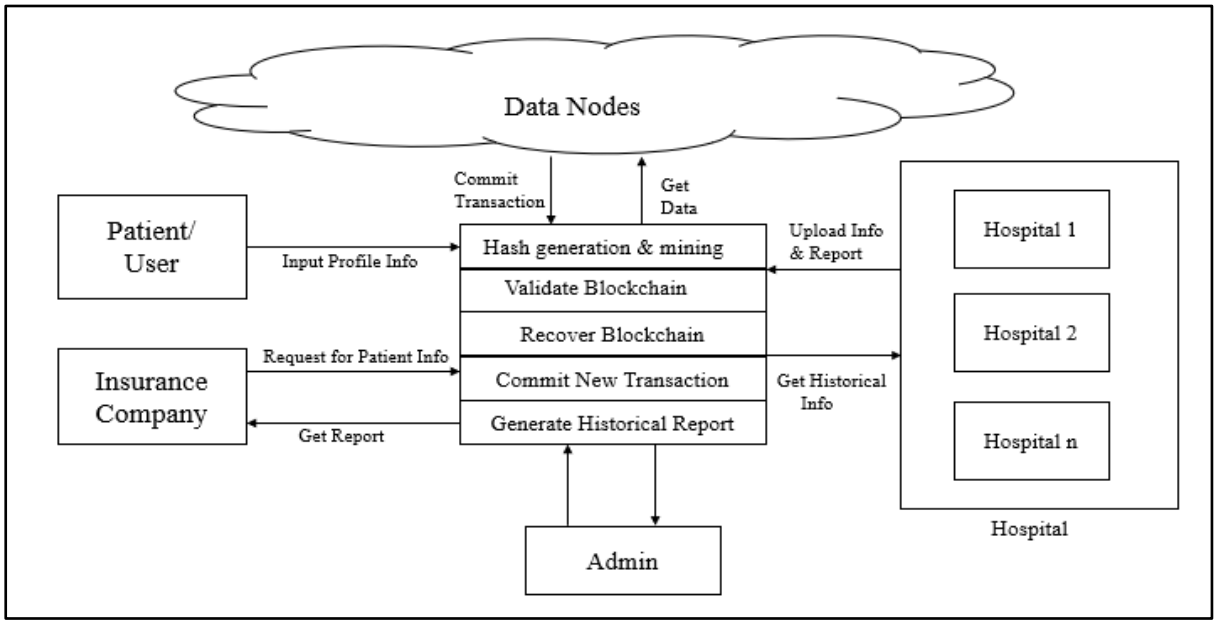

Figure 1: Proposed System Design

Algorithm 1: Protocol for Peer Verification

```
Input : User get IP address
Output : Enable IP address or current query if any connection is valid
Step 1 : User generate the any transaction DDL, DML or DCL query
Step 2 : Get current IP address
  For each (read IP address)
            If (connection(IP) equals(true))
          Flag true
        Else
          Flag false
      End for
Step 4 : if (Flag == true)
      Peer to Peer Verification valid
        Else
            Peer to Peer Verification Invalid
      End if
      End for
```

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105360|

Algorithm 2 : Hash Generation

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 : Current_Hash= SHA256(d)
Step 4 : Return Current_Hash

Algorithm 3 : Mining algorithm

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: Foreach (read I into NodeChain)
If (!.equals NodeChain[i] with (Cchain))
Flag 1
Else Continue Commit query
Step 4: if (Flag == 1)
Count = SimilaryNodesBlockchain()
Step 5: Calculate the majority of server
Recover invalid blockchain from specific node
Step 6: End if
End for

Algorithm 4: Validate Invalidate

-Proof of work-PoW

The PoW system was the first to be used by a running blockchain, originally deployed by Bitcoin. In PoW, nodes (computers that make up the blockchain network) can earn the right to validate a block while simultaneously recording transactions onto the ledger. Strong incentives are typically given to the node that is awarded the status of 'winner'. The winner is granted the authority to validate the block. For reference, the incentive for this winner is currently a bounty of 6.25 bitcoins (at a current market value of $46.3k USD per bitcoin [Aug 17, 2021]). This authority is earned when a user is the first to solve a complex cryptographic problem and, in doing so, obtains the missing key (i.e. 'hash function') to finalise that block. This process is commonly known as mining.

You may have heard that the mining process has been heavily scrutinised for its detrimental effect on the environment. Essentially, it requires enormous levels of computing power to be able to run random inputs into the cryptographic problem and achieve the correct result. When you have multiple mining farms (i.e. networks of mining computers) all competing for the one bounty, there will inevitably be a huge amount of wasted energy. These farms are comprised of large facilities, with rows of very expensive, highly specialised computers that consume HUGE quantities of energy. For reference, Bitcoin produces around 70.35 Mt of CO2 annually, which is comparable to the emissions of developed nations like Greece.

As a result, only large entities with sufficient resources to operate these mining farms have any hope of participating in block validation creating a centralisation of power. For example, only a handful of mining pools in large part currently control the Bitcoin blockchain. Their collective power due to a large controlling interest in the currency creates underlying concerns for everyday crypto enthusiasts. This possibility has been called a 51% attack. It is believed that in a 51% attack, the entity with the majority stake in the blockchain would be able to reverse historic transactions and block new transactions from going through. At the same time, an entity that controls 51% or more of the network would harm the value of their own assets by acting unethically. Nevertheless, the fact that such an instance is possible is cause for concern.

Algorithm 5 : Recovery

With the rapid development of network information technology, network attacks have become more and more common. Network hackers can easily use Trojan horses, worms, and local vulnerabilities to attack devices on the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105360|

network. In the power Internet of Things, attackers usually maliciously delete or tamper with the data (such as collected and summarized data, firewall configuration information, virus database data, and log file) stored in the terminal to interfere with the stable operation of the power Internet of Things. For example, attackers can tamper with the firewall configuration of the device to further implement a distributed denial of service (DDOS) attack. IoT administrators can use data backup and recovery technology to reconstruct the firewall. Then, the IoT environment can be repaired. So, data backup and recovery technology is an important method to ensure the stable operation of the power Internet of Things. Currently, mainstream data recovery solutions mainly include two types: centralized data backup and recovery solution

The blockchain is essentially a distributed database. Blockchain has the characteristics of decentralization and can ensure that the stored data is difficult to tamper with. At the same time, the blockchain's oracle mechanism can ensure that reliable data is provided for the blockchain, and IoT data nodes can accurately and reliably obtain data on the blockchain through smart contracts. Therefore, blockchain technology provides a promising solution to the above problems. However, the storage scalability of the blockchain is poor, and each node needs a complete ledger in the storage system to maintain the decentralization and consistency of the ledger, which puts high storage requirements on each node server. This has caused the storage scalability of the blockchain to become a major bottleneck for the application of blockchain technology to data backup and recovery

New Transaction:

Usually by doing above mentioned algorithms to be in with a chance of selecting, verifying & validating transactions. This saves substantial computing power resources because no mining is required. After this the new transaction is created and blocks are build

IV. RESULTS AND DISCUSSION

The time required for the consensus algorithm to validate the block chain in four nodes is shown in Figure 2. The X axis depicts the transaction of the block chain, while the Y axis depicts the time needed in milliseconds for each of the four nodes

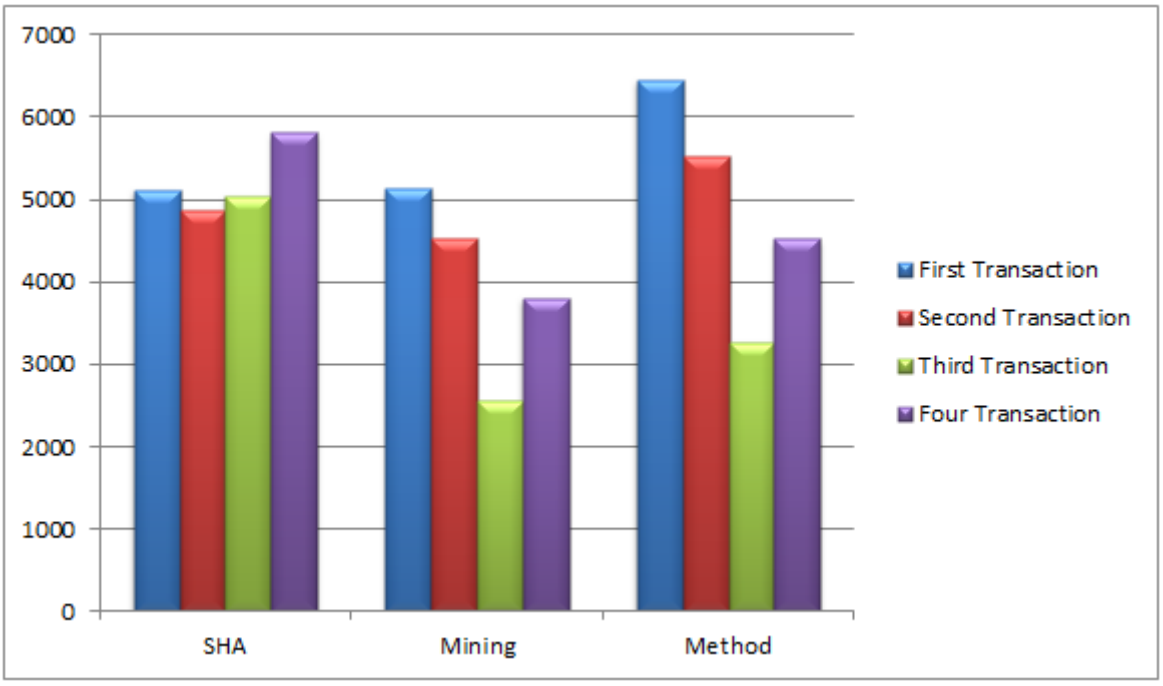

Fig. 2 Time required (in milliseconds) for complete transaction with different records block chain using 4 data nodes in P2P Network

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105360|

V. CONCLUSION

There are many research directions in applying Blockchain technology to the healthcare industry due to the complexity of this domain and the need for more robust and effective information technology systems. An interoperable architecture would undoubtedly play a significant role throughout many healthcare use cases that face similar data sharing and communication challenges. From the more technical aspect, much research is needed to pinpoint the most practical design process in creating 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 needed to educate software engineers and domain experts on the potential and also limitations of this new technology. Likewise, validation and testing approaches to gauge the efficacy of Blockchain-based health care architectures compared to existing systems are also important (e.g., via performance metrics related to time and cost of computations or assessment metrics related to its feasibility).

VI. FUTURE SCOPE

Future research will focus on this overall scalability and speed over time to improve the user experience. Also insurance company will be able to make new transactions

REFERENCES

[1] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, \Privacy-preserving data aggregation computing in cyber-physical social systems," ACM Transactions on Cyber-Physical Systems, vol. 3, no. 1, p. 8, 2019.
[2] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, \Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, vol. 32, no. 6, pp. 144{151, 2019.
[3] J. Li, H. Ye,W.Wang,W. Lou, Y. T. Hou, J. Liu, and R. Lu, Efficient and secure outsourcing of differentially private data publication," in Proc. ESORICS, 2019, pp. 187 206.
[4] Gong, Xinglin, Erwu Liu, and Rui Wang. Blockchain-Based IoT Application Using Smart Contracts: Case Study of M2M Autonomous Trading. 2020 5th International Conference on Computer and Communication Systems (ICCCS). IEEE, 2020.
[5] Xu, Jinliang, et al Edgence: A blockchain-enabled edge-computing platform for intelligent IoT-based dApps. & China Communications 17.4 (2020): 78-87.
[6] Huang, Zheng, Zeyu Mi, and Zhichao Hua. &HCloud: A trusted JointCloud serverless platform for IoT systems with blockchain. & China Communications 17.9 (2020): 1-10.
[7] Gheitanchi, Shahin. & Gamified service exchange platform on blockchain for IoT business agility& 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020.
[8] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, \Enabling efficient and geometric range query with access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870{885, 2019.
[9] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, Privacy preserving attribute- keyword based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116{ 131, 2017.
[10] Choi, Jungyong, et al. "Random Seed Generation For IoT Key Generation and Key Management System Using Blockchain." 2020 International Conference on Information Networking (ICOIN). IEEE, 2020

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details