An Overview on use of Blockchain Technology and Fog Computing for Securing Health Care System

PROF.KALAM NARREN
Department of Computer Engineering
JSPM's
Rajarshi Shahu College of Engineering Tathawade,
Pune, India.
mickey.neha2911@gmail.com

PROF.V.VINAY KRISHNA
Department of Information Technology
JSPM's
Rajarshi Shahu College of Engineering Tathawade,
Pune, India.
ramjoshi.comp@gmail.com

ABSTRACT

The recent need of user centric electronic record for maintaining patient's health information with different parameters recorded in the hospital during the treatment and also provisioning them as an when required for the further treatment, care or billing purpose. To maintain these records on the decentralized platform which initiate and empower usage with enormous speed along with transparent and secure environment can be achieved through blockchain based system. The use of distributed system which offers ledger facility for storing the records in a secure manner along with interoperability for supporting applications. Blockchain technology reduced the dependence on a centralized authority to verify information integrity and ownership, as well as arbitrate transactions and exchange of digital resources, while enabling secure and undisclosed transactions along with agreements directly between interacting nodes. It has key properties such as immutability, decentralization and transparency that could address urgent health care issues like incomplete peer-to-peer files, and also there is difficulty for accessing information on patient's health. An efficient and effective health care system requires interoperability, which allows software applications and technology platforms to communicate securely and seamlessly, exchange data, and use the exchanged data across health organizations and application vendors. Healthcare nowadays undergo many issues like fragmented data, delayed communications, and disparate workflow tools caused by the lack of interoperability therefore a system which offers the possibility of allowing access to complete and recognized longitudinal medical records with manipulations that are stored in fragmented systems in a secure and Pseudo-anonymous way is suggested In this paper we carried out the literature study as well as system overview of blockchain technology along with fog computing environment which process the massive data in distributed environment. Our partial experimental analysis shows the gaps of current systems and predicts the future research plans.

Keywords—Blockchain, healthcare system, Fog Computing

I. INTRODUCTION

In the current era the various agents of healthcare system are expecting the fast and efficient usage of information for that they are ready to adopt the new technologies for seamless transactions. In the business domain various transactions are happening for day to day operations like order processing, payments to each other among various participants or users. Therefore, each user involved needs to maintain the records of these transactions in separate ledger which leads to more chances of human errors and they have to rely on the third-party intermediaries to verify it which leads to delay in the process. hence if a shared ledger is used then common view of truth will be available for all the users involved in the transactions.

A blockchain technology as the name suggest each transaction as and when occurs it will be kept inside block whereas these blocks has the feature such as the blocks are connected to each other and transactions are kept inside such chain of the blocks which is not reversible. It provides a mechanism to various agents involved in the transactions to compromise and trust over the digital footprints available in the ledger and remove the dependency of trusted third party. The various agents involved in the healthcare systems such as hospitals, doctors, pharmacists, laboratories etc. and the processes involved like claim settlement and payment systems has to interact with the existing data and each operation is checked and recorded like audit log

on the distributed ledger. There is a need to enforce the privacy various access policies are in place as per the role of the agent to achieve security using permission-based access control rules.

A blockchain system has the property called secure and distributed one as it functions on the basis of common system of record which is shared among the vendors or agents which are participating for the business as a member in the network with proper access permissions hence the information can be kept confidential as per the role of the participating agent. The validation will be taken from the participating agents and transactions are only committed which are validated by the members and no one in the system has rights to delete these validated records.

Figure 1: Blockchain

A blockchain system can be visualized as a practically trustable cryptographic database where censorious medical information could be recorded. To better understand blockchain technology it's a network of users or participants involved in the trading will keep on validating the transactions at the regular interval by recording their consensus or agree on the terms of the involved transactions through sharing the true state of the data inside the distributed ledgers which can be used for trading various digital assets of different kinds by enforcing the rules over the network for taking the regular consensus. Blockchain is nothing but the distributed ledger mainly comprises of chain of blocks of transaction data here the record of the transactions are stored block by block as per mentioned timestamp which is main attribute. These blocks are chained through the fingerprint or hash value of the preceding block and forming a distributed database.

The atomic transactions are carried out using distributed ledger where the main attributes will be checked and validated without any requirement of any intermediary. The important parameters are timestamp and certainty that a certain transaction took place, here the use of pre-existing blockchain can be deployed to prove that status at that timestamp by embedding the hash of previous block in the subsequent block in the chain. This can act as the proof-of-work done to maintain and extend the blockchain. During verification the proof will help also they maintain the private information with an immutable link. The system is maintained by a computer network that is accessible to anyone 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. Therefore, 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 attack or information loss with respect to centralized systems. 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 grit 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 periphery server nodes. These fog nodes manage various applications and services to store and 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 we employ blockchain systems. This work we illustrate approach of blockchain applications in various environment data processing methods.

II. LITERATURE SURVEY

According to Zhao, Huawei, et al. [1] efficient key management scheme for health blockchain. It is a consensus that blockchain has great potential application values in the field of healthcare. However, prevention of privacy cover must be solved before the popularity of healthcare restrictions, because blockage over health blocks is involved in a large number of private health data. Here, on the basis of the features of health blockchain, the authors use a body sensor network to design a lightweight backup and efficient recovery scheme for keys of health blockchain.

Amofa, Sandro, et al.[2].A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data. A blockchain-supported architectural framework for secure control of personal data in a health information exchange by pairing user-generated acceptable use policies with smart contracts. The policy is made at the hospital's registered hospitals which determine permissible actions on their personal Health Information. These policies are stored in the system and consulted with the help of smart contracts to make sure when data can be shared or otherwise. Processing nodes, smart contracts and security monitors of participating health institutions cooperate to ensure patient data security is protected from unauthorized access and computations.

The authors Wang, Shuai, et al.[3] presented the System Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. The framework of parallel health care systems (PHSs) based on the artificial systems computational experiments parallel execution (ACP) approach. Emerging blocks technology with, by a composition Consortium blockchain patients, hospitals, healthcare bureaus, and comprehensive health care services for healthcare communities Sharing, medical record review and supervision auditability.

In the paper based on Blockchain-based Personal Health Data Sharing System Using Cloud Storage. Zheng, Xiaochen, et al. [4] had specified a conceptual design for sharing personal continuous dynamic health data using blockchain technology supplemented by cloud storage to share the health-related information in a secure and transparent manner. Personal Health Data Sharing System To enable, based on blockchain and cloud storage technology Users are sharing their personal health data easily and securely.

According to Xia, Qi, et al.[5] in the paper titled as "A system that addresses the issue of medical data sharing among medical big data custodians in a trust-less environment". MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. System Blockchain-based and provides data emergence, auditing and control for shared medical data in the cloud Store in big data establishments. In MeDShare, data transitions and sharing from one entity to the other, along with all actions performed on the MeDShare system, are recorded in a tamper-proof manner. The action of the data series is constantly being checked from the technology mentioned in the paper and later Violations are addressed according to cancellation of access Data.

As per the Neudecker, Till et.al[6] presentation in the paper titled "The System Timing analysis for inferring the topology of the bitcoin peer-to-peer network". A timing analysis method that targets flooding P2P networks and shows its theoretical and practical feasibility. A recognition in Real-world Bit coin Network proves the possibility of notification Cooperative network actively involved with important Accuracy and memories potentially enable attacks on the network. A timing analysis method for inferring a flooding network's topology using information obtained by observing the flooding process.

In the paper based on "Fog Computing as a Defensive Approach Against Distributed Denial of Service (DDoS)" Paharia, Bhumika et.al[7] had proposed an architecture for security of cloud from DDoS attack with the help on additional layer in the architecture termed as Filter Fog here. There is a device Proposed here to enhance the traditional architecture Cloud Computing can be seen as an attempt to secure it Protect the information stored in the cloud. A fog computing is used as a defensive approach from the day-to-day increasing security threats particularly DDoS attacks in cloud computing. Here an architecture has been proposed to obstruct the malicious traffic generated by the DDoS attack from user to the cloud by utilizing the benefits of fog computing.

According to Naidu, Vishal, et al.[8]A Fully Observable Supply Chain Management System Using Block Chain and IOT. The decentralization of this data across different levels ranging from raw material manufacturer to the retailer will lead to a more flexible and transparent system. This feature will turn on results in a system where the data flows faster than traditional Centralized Approach to Supply Chain Management. Using This will help reduce the error rate caused by this system Various stages of supply chain will improve Customer support with full capacity Supply Chain Reprint and Traversal to Provide Spot Face Supplies Inconsistencies at different levels of the tree.

System to Zhao, Huawei, et al [9]. Blockchain is great that's comprehensive Potential app prices for the health service sector, However the above blocks of health blockchain contains great. The number of private health data and it needs to be solved Privacy Protection Problems Before Popularity Health blockchain. System Body Sensor Network, To Build Lightweight Backups and to Build Key Efficient Recovery Planning for Health Inhibitors. The development of electronic techniques, body senor networks (BSNs) emerge to servile the health of the human.

As per Chen, Zhonglin, et al [10] presented paper on " a Security Authentication Scheme of 5G Ultra-Dense Network Based on Block Chain." In this paper authors mentioned about the security authentication scheme of 5G UDN based on the block chaining technologies. An APG-PBFT algorithm based on the block chaining technology with Byzantine Fault Tolerance (PBFT) consensus algorithm is proposed. Mobile Security Authentication Scheme for UC access to UCE, which mainly addresses the problem of how to make reliable access points as APG.

Sr. No	Paper Name	Author Name	Proposed System	Gap
1	Efficient key management scheme for health blockchain	Zhao, Huawei, et al	Various consensus algorithm has been used for key management	Much resource dependency for node creation
2	A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data	Amofa, Sandro, et al	Health care data sharing using blockchain approach	Much expensive than traditional approaches.
3	Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach	Wang, Shuai, et al.	Distributed health care data sharing approach in blockchain	Not used any pure consensus P2P verification algorithm which generate data inconsistency.
4	Blockchain-based Personal Health Data Sharing System Using Cloud Storage	Zheng, Xiaochen, et al.	Blockchain based mining approach for healthcare in cloud environment	High time complexity during data transmission in data stream.
5	MeDShare: Trust-less medical data sharing among cloud service providers via blockchain.	Xia, Qi, et al.	Massive data sharing approach via blockchain using encryption algorithm	High network overhead.
6	Timing analysis for inferring the topology of the bitcoin peer-to-peer network	Neudecker, Till, Philipp Andelfinger, and Hannes Hartenstein.	P2P environment has proposed in bitcoin network	It can work only in GPU's environment.
7	Fog Computing as a Defensive Approach Against Distributed Denial of Service (DDoS): A Proposed Architecture	Paharia, Bhumika, and Kriti Bhushan.	Machine Learning base attack defensive scheme using fog computing	Strong hardware configuration required, much expensive
8	A Fully Observable Supply Chain Management System Using Block Chain and IOT.	Naidu, Vishal, et al.	Supply chain management using IoT and Blockchain in traditional transaction management system.	Traditional approach, system did not used pure blockchain base consensus in P2P environment
9	Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys.	Zhao, Huawei, et al.	Auto data recovery from disk failure using secure blockchain approach.	Key management issues
10	A Security Authentication Scheme of 5G Ultra-Dense Network Based on Block Chain	Chen, Zhonglin, et al.	Authentication approach using consensus algorithm for various network authentication	Applicable in user access control only, not for MAC authentication

III. SYSTEM OVERVIEW

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 also carried out data integrity, confidentiality as well as eliminate the inconsistency for end user.

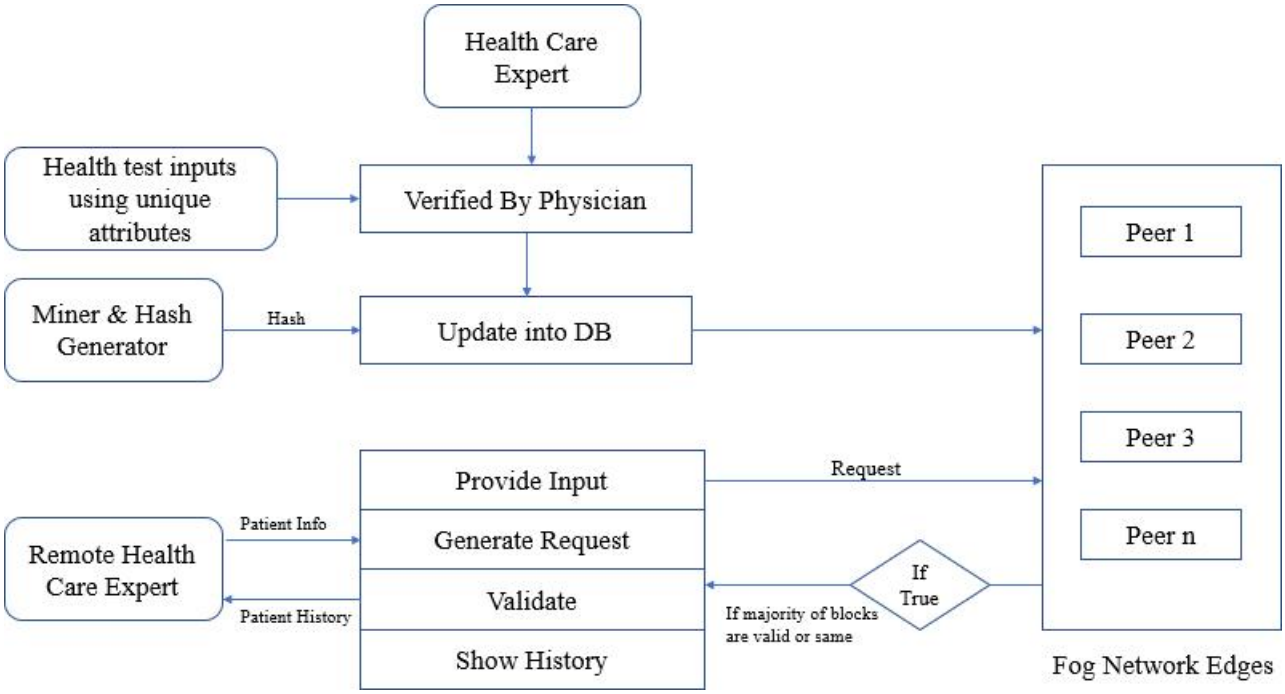

Figure 2: System overview

System highlights the implementation of health care data storage using block chain. In the system the patient if changes the city and then refers to the doctor of the other city then through fog networks the new doctor can get the complete history of that patient and for maintaining the secure data we use the blockchain technology.

In this data is processed in multiple servers so the transactions are processed in sequencing fog network. This illuminates the quality of service issue and time limits. This is a middleware system in which the processing environment in which the load will be balanced using threads. The request generated will be parallels saved on all nodes in a Blockchain manner. 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. If any chain is invalid then it will recover or update the current server blockchain. 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.

IV. CONCLUSION

From the additional technical side, abundant analysis is required to pinpoint the foremost sensible style method in making associate degree practical system exploitation the Blockchain technology whereas equalization important security and confidentiality considerations in attention. whether or not to make a redistributed application leverage associate degree existing Blockchain, extra analysis on secure and economical package apply for applying the Blockchain technology in attention additionally required to teach package engineers and domain consultants on the potential and also limitations of this new technology. Likewise, validation and testing approaches to measure the efficaciousness of Blockchain-based health care architectures compared to existing systems are vital (e.g., via performance metrics associated with time and value of computations or assessment metrics associated with its feasibility). In some cases, a replacement Blockchain network is also additional appropriate than the present Blockchains; thus, associate degree other direction is also investigation extensions of

an existing Blockchain or making a attention Blockchain that completely provides health-related services.. To implement the proposed system with various data nodes will the interesting in future work. The large part of research is targeting on revealing and improving limitations of Blockchain from privacy and security perspectives, but many of the proposed solutions lack concrete evaluation on their effectiveness. The other Blockchain scalability related challenges including throughput and latency have been left unstudied.

REFERENCES

[1] Zhao, Huawei, et al. "Efficient key management scheme for health blockchain." CAAI Transactions on Intelligence Technology 3.2 (2018): 114-118.

[2] Amofa, Sandro, et al. "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data." 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, 2018.

[3] Wang, Shuai, et al. "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach." IEEE Transactions on Computational Social Systems 99 (2018): 1-9.

[4] Zheng, Xiaochen, et al. "Blockchain-based Personal Health Data Sharing System Using Cloud Storage." 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, 2018.

[5] Xia, Qi, et al. "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain." IEEE Access 5 (2017): 14757-14767.

[6] Neudecker, Till, Philipp Andelfinger, and Hannes Hartenstein. "Timing analysis for inferring the topology of the bitcoin peer-to-peer network." Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016 Intl IEEE Conferences. IEEE, 2016.

[7] Paharia, Bhumika, and Kriti Bhushan. "Fog Computing as a Defensive Approach Against Distributed Denial of Service (DDoS): A Proposed Architecture." 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2018

[8] Naidu, Vishal, et al. "A Fully Observable Supply Chain Management System Using Block Chain and IOT." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.

[9] Zhao, Huawei, et al. "Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys." Autonomous Decentralized System (ISADS), 2017 IEEE 13th International Symposium on. IEEE, 2017.

[10] Chen, Zhonglin, et al. "A Security Authentication Scheme of 5G Ultra-Dense Network Based on Block Chain." IEEE Access 6 (2018): 55372-55379.

[11] Kshetri, Nir, and Jeffrey Voas. "Blockchain-enabled e-voting." IEEE Software 35.4 (2018): 95-99.