Journal of Integrated
SCIENCE & TECHNOLOGY

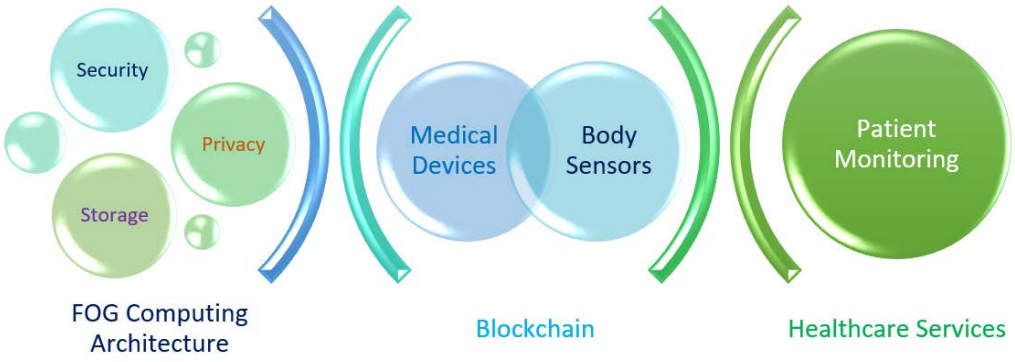
A review on FOG supported architecture in healthcare using blockchain

Charu Awasthi,[1*] Satya Prakash Awasthi,[1] Prashant Kumar Mishra[2]

[1]Department of Computer Engineering, Poornima University, Jaipur, India. [2]Department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur, India

Received on: 28-Jul-2023, Accepted and Published on: 14-Sep-2023

ABSTRACT



Medical expenses are on the rise due to population growth and the prevalence of chronic diseases, which has led to the widespread adoption of technical solutions. A blockchain-based framework offers a decentralized network for tracking these records, enabling rapid adoption while maintaining transparency and security. The implementation of this distributed framework includes a ledger for securely storing records and supporting applications through interoperability. Blockchain technology eliminates the need for a centralized authority to verify information integrity and ownership, as well as mediate transactions and the exchange of digital assets. It also enables secure and confidential transactions and agreements among interacting nodes.Our study investigates both blockchain technology and the fog computing framework for distributed data processing, with cloud-based approaches used to store and process data generated by these solutions. The result is the fog computing model, which brings computational power and storage closer to data sources as a solution to this challenge. Managing medical data within the fog remains a complex task, requiring careful consideration of factors such as accessibility, performance, interoperability, and data protection. This article discusses a Fog Computing-based software architecture designed to simplify the management of medical records, addressing these issues effectively.

Keywords: Blockchain, Distributed framework, medical records, Fog computing model, Data protection

INTRODUCTION

In the present period, different health system agents expect knowledge to be rapidly and efficiently used so that they can implement emerging technology for smooth transactions. Different transactions take place in the business domain daily, including order collection and transfers between different participants or users. Each consumer must therefore keep a separate record of these transactions which leads to more chances of human error and must rely on intermediaries from third parties to verify that this results in delayed procedure.[1] Therefore, when a shared ledger is used, all users participating in transactions have a similar view of the facts. A blockchain technology as the name suggests that any transaction is held within the block as it happens, whereas other blocks have a feature like the blocks are linked and transactions remain inside such a non-reversible chain of blocks. It offers a framework for various transactional agents to compromise and trust the digital footprints in the directory and eliminate the dependence on a trustworthy third party.[2] Data are collected and logged as an auditor's log on the distributed directory for the different agers associated with the medical systems such as clinics, physicians, pharmacists, laboratories etc. and processes such as claim payment systems and payment schemes. Different access policies must be applied in accordance with the role of the agent to ensure security with the application of permission-based access control laws.

A blockchain system is called protected and distributed, based on the common record system exchanged between the suppliers or agents involved for the firm as a network member with appropriate access permissions According to the position of the agent involved,

*Corresponding Author: Charu Awasthi Poornima University, Jaipur, India.
Tel: +91-8506949789. Email: charuawasthi@gmail.com

Cite as: *J. Integr. Sci. Technol., 2024, 12(1), 721.*
URN:NBN:sciencein.jist.2024.v12.721

 ISSN: 2321-4635
http://pubs.thesciencein.org/jist

the details may therefore be kept confidential.[3] The certification is by the participating officers, and only validated transactions are committed by the members and none of the participants have the right to remove the validated records.

The Blockchain works as an undefined mechanism with a data protection problem, since all operations are open to all, while the data incorruptibility is tamper-proof. The access authority of the different health records of the patient must therefore be carefully established via numerous health facilities and devices. As an extensive storage system, the Blockchain itself is not created. The blockchain's vulnerability is complemented by a decentralized storage solution in health theory.[4] The blockchain network as a decentralized system is more flexible, because in comparison with centralized systems there is no point attack or data loss. Fog computing known as the Edge Network pushes limits on machine functions, data and provides the future flow from the centralized cloud of the network edge. Fog network framework is aimed at establishing discipline, composition, and accessibility not only through network entry, but also through the Internet. A highly visualized IT infrastructure providing hierarchic connectivity via peripheral server nodes would illumine the infrastructure of cloud computing. These fog nodes monitor different applications and utilities for the collection and processing of data near end users. The expression "perimeter estimate" is often used for Fog Computing. Fog and the fringes must bring operational and analytical abilities closer to the source of information. Knowledge from the same sources or physical resources is transmitted from both systems. All these devices operate physically or detect operations in this environment as electrical circuits.[5] We use blockchain systems to achieve protection by decentralization. This paper illustrates the approach of blockchain implementations in different processing methods in the environment.

LITERATURE REVIEW

A robust strategy for overseeing the health of blockchain systems holds significant promise in the field of healthcare technology.[6] Nevertheless, it is imperative to address data security concerns prior to imposing any healthcare-related constraints, as numerous confidential health records are intertwined with the healthcare blockchain. In this context, the authors have employed a body sensor network to create a streamlined and effective backup and recovery solution for health blockchain keys, tailored to the unique attributes of the healthcare blockchain.

A framework enabling secure sharing of personal health information within a blockchain-based system has been reported by Amofa, Sandro and al.[7] This technological platform leverages blockchain to ensure the secure management of personal data when sharing health information through the integration of smart contracts with appropriate user policies. These policies are established within registered hospitals, defining permissible actions concerning personal health information. These policies are then stored within the system to facilitate data exchange through smart contracts. Collaborating health institutions work in tandem to safeguard patient data confidentiality, employing processing nodes, smart contracts, and security monitors to prevent unauthorized access and unauthorized computation.

Wang, Shuai et al.[8] proposed the ACP Approach-based System Blockchain-Powered Parallel Healthcare Systems. The parallel health care systems architecture (PHS) is focused on the parallel execution (PEA) approach of artificial systems. Emergent technology blocks with a consortium of blockchain patients, hospitals, and health providers for the healthcare community. Sharing and auditing of medical records and oversight.

The document, centered on a cloud storage system utilizing Blockchain for the sharing of Personal Health Data, introduces a conceptual framework by Zheng, Xiaochen, et al.[9] This framework outlines the use of blockchain technology to facilitate the secure and transparent exchange of health-related information. It provides a system for users to conveniently and safely share their personal health data by merging blockchain and cloud storage technology.

In its article related to system that addresses the issue of sharing of medical data among big data custodians in an environment without trusts, by Xia, Qi et.al.[10] reported about the MeDShare: Confidential sharing of medical data between providers of cloud services. System Blockchain-based data creation, control, and auditing in the cloud store for large data stores can be adopted for shared medical data. In MeDShare, data transfers from one person to another are registered in a tamper-resistant manner for all activities conducted on the MeDShare System. The effects of the data series on using the technologies and subsequently violations can be dealt with by canceling access data.

Till and al[11] presented the work on System timing analysis to infer the topology of the Bitcoin peer-to-peer network in accordance with Neudecker's study. A timing analysis approach that aims to achieve the theoretical and the practical feasibility for flooding P2P networks. A recognition of Real-world Bit coin Network demonstrates the probability of a co-operative network notification actively engaged in critical accuracy and the potential for network attack memories. A tool for timing analysis to determine the topology of a flood network by the observation of the flooding mechanism.

The DDoS attack safety architecture was proposed by the Paharia, Bhumika et.al.[12] with the aid of an additional layer of the Filter Fog architecture. A system for improving traditional architecture is proposed. The protection of cloud information can be regarded as cloud computing. Fog computing is used to defend itself against increasing security threats, particularly DDoS-based cloud-based attacks. The benefits of fog computing are blocked here from malicious traffic generated by the DDoS attack from the user to the cloud.

Vishal Naidu et.al.[13] reported the result of a more open and transparent structure by decentralizing data across layers, from raw material manufacturers to retailers. This feature enables data to flow more quickly than the conventional Centralized Supply Chain Management approach. This would help to reduce the system's error rate. Distinct phases of the supply chain would enhance full customer service Supply chain repression and crossover supply of spot faces Inconsistencies on various stages.

Zhao Huawei et al.[14] emphasize the tremendous potential of blockchain in healthcare applications, highlighting its capabilities. However, they also acknowledge significant challenges within the blockchain space, particularly related to the quantity and resolution

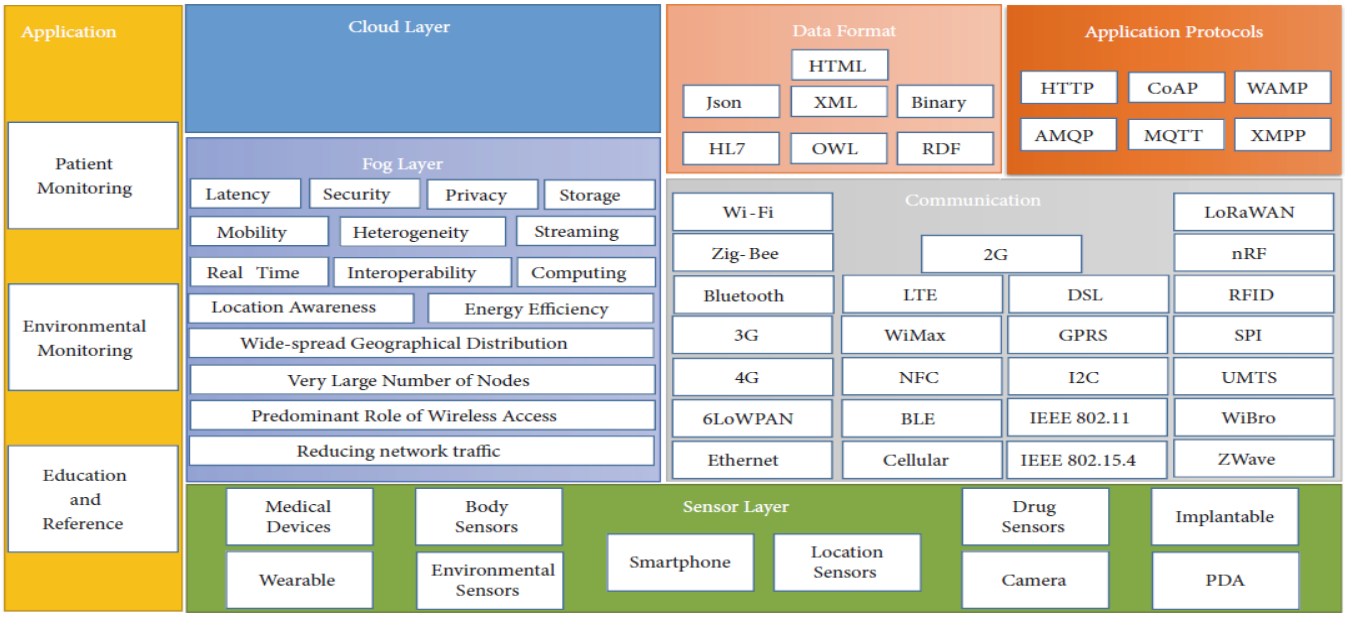


Figure 1. Collected details of FOG computing in Healthcare

of private health data, which need to be addressed to ensure privacy before the widespread adoption of healthcare blockchain. They propose the use of a Body Sensor Network system to create lightweight backups for health data and establish an efficient recovery plan. This involves leveraging electronic techniques to develop Corporate Sensor Networks (BSNs) for the betterment of human well-being.

In another study, Chen, Zhonglin et al.[15] present a paper titled "A Security Authentication Scheme for 5G Ultra-Dense Networks Based on Blockchain." The authors delve into the integration of blockchain technology for security authentication in 5G Ultra-Dense Networks (UDN). They introduce an algorithm called APG-PBFT, based on the Byzantine Fault Tolerance (PBFT) consensus algorithm within blockchain technology. This algorithm is designed to enhance the trustworthiness of access points within the UC access to UCE mobile security authentication system, addressing the challenge of ensuring reliable APG access points.

Table1. Gap analysis

Sr. No	Author Name	Proposed System	Gap
1	Zhao, et al	Different algorithms of consensus were used for key management	A lot of node resource dependence
2	Amofa, et al	Sharing of health care information by blockchain	Beyond conventional methods, more costly.
3	Wang, et al.	Distributed approach to health care data exchange in the Blockchain based cloud mining approach.	No pure P2P checking algorithm used that generates inconsistency in results.
4	Zheng, et al.	Massive data sharing approach with encryption algorithms via blockchain	Data transfer in data stream is highly complicated.
5	Xia, et al.	Massive data sharing approach with encryption algorithms using blockchain	Overhead high network.
6	Neudecker et. al.	In the bitcoin network the P2P environment was proposed	It can only function in the world of GPU.
7	Paharia, et.al.	Defences target machine learning foundation with fog computing	Strong hardware setup required, very costly
8	Naidu, et al.	In the conventional transaction management scheme, Supply chain management using IOT and Blockchain.	The framework did not use pure blockchain basic consensus in the P2P environment as a traditional approach
9	Zhao, et al.	Auto disk failure data recovery using safe blockchain method.	Issues with Key management
10	Chen, et al.	Authentication strategy uses consensus algorithms to authenticate different networks	In use only, not for MAC authentication, for user access control

FOG ENABLED ARCHITECTURE WITH CLOUD

In prior studies, the Fog Computing Model was employed within the healthcare domain. Our research introduces a novel assessment of our work in this context. The paper explores various categories of medical applications developed using Fog computing and the range of diseases these solutions address. Additionally, it delves into the specific attributes adopted by Fog computing, the factors driving its adoption in the market, and the pertinent issues that require attention to enhance its effectiveness. Furthermore, the paper discusses the sensors employed in these solutions, the prevailing architectural styles, and offers details about prototypes used in the assessed projects, including their styles and configurations. The analytical findings are succinctly presented in Figure 1.

The review showed that the handling of medical information contained in the Fog Layer remains an open issue. For such methods, security and privacy are essential features. Stocking capability is another problem because, compared with cloud, Fog has limited space. So, this constraint must be addressed in the Fog-based storage strategies. Moreover, the papers reviewed also mention the performance of information handling in applications as the main explanation for the use of fog computing in the health area. The research also confirms that there is no alternative to Fog's lack of health data management strategy that is supported by an infrastructure that provides more secure storage repositories.[16] Most studies deal with solutions that take advantage of Fog's processing power. A new algorithm is proposed for the complex planning of such vehicle network tasks. The new algorithm provides knowledge to be divided into blocks and computing resources. Based on service scale, completion time and capability, a fog resource service delegation and allocation architecture are suggested. The study does not, however, offer solutions for improving storage in Fog. Given the challenges of the existing solutions, we have suggested improving the management of medicines' infrastructure on software architecture issues related to availability, performance, interoperability, and privacy. Our proposal varies from those analyzed in the literature to enhance the storage and usage of Blockchain to ensure necessary protection for these data in the Fog Layer.

BLOCKCHAIN OVERVIEW WITH CLOUD

Blockchain is a Blockchain decentered directory which stores transaction data between peer-in-pair networks. It is spread out and unchanging. In 2008 Satoshi Nakamoto established the initial concept of Blockchain's work.[17] The base of Bitcoin crypto currencies operation was Nakamoto's in this post. The Blockchain database structure is shown in Figure 2. The Blockchain is comprised of a sequence of chained blocks. The 'Transactions' are included in each box, several actions generated by the network participants. This is validated by networked computers solving the right to construct a new block with mathematical problems.

Another key concept for Blockchain is digital wallets, which are applications that can send, obtain, and store the history of a participant's transactions.

The transaction is first sent through the network when a transaction is sent from Package A to package B. Then it is confirmed and placed in a block by a miner. The block is then sent to all of its supportive network nodes. The current block in Blockchain can be linked to this block. The transaction finally comes to Wallet B. Figure 3 shows the activities. A public-key

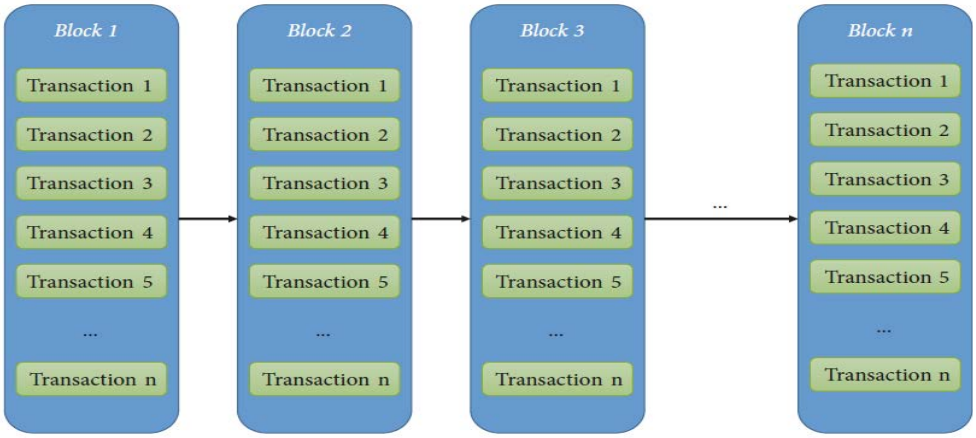


Figure 2. Block chain Architecture

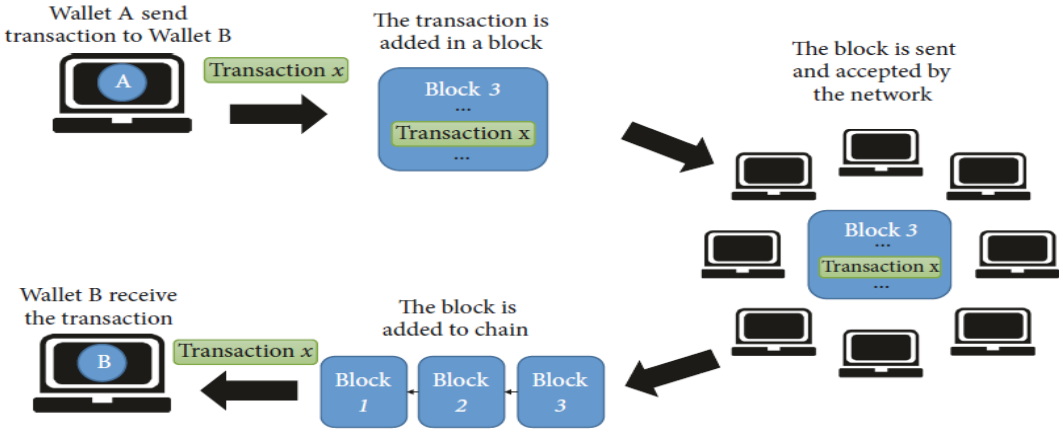


Figure 3. Working in a block chain

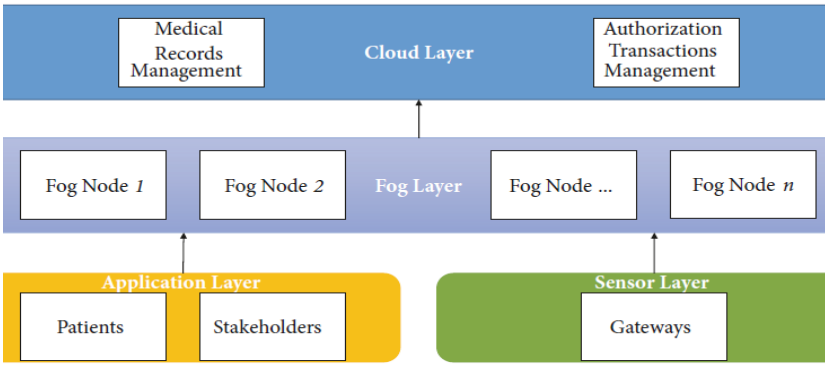


Figure 4. Layered Architecture

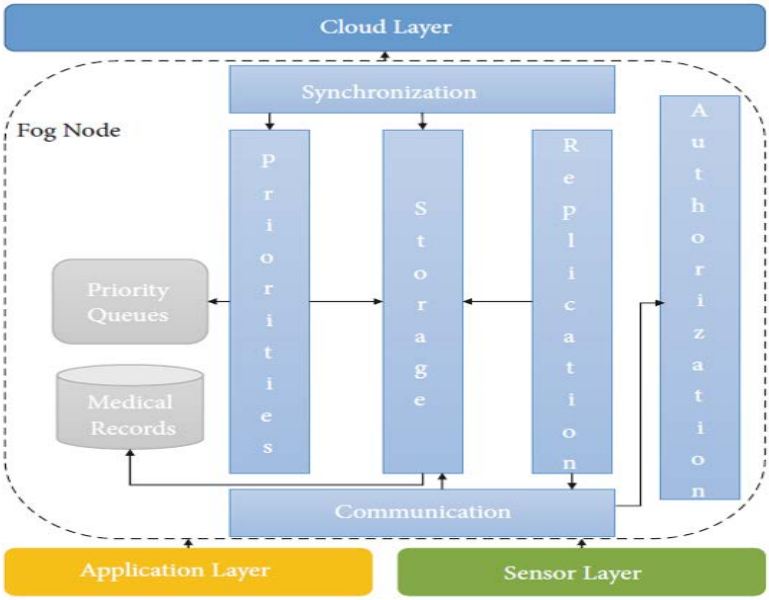


Figure 5. Fog node Architecture

encryption and digital signatures system is used to differentiate managed accounts in digital wallets and to ensure transaction permission. The source node is used to allow data to be sent to each transaction and to ensure its integrity, crystallization techniques are used.

Figure 4 depicts the proposed architecture's layered view. This point of view will contribute to the approach defined [18] in relation to the attributes of changeability and portability. The layers mentioned in Section 2's state-of-the-art review and Figure 1's technical view were used to create this view. It is thus composed of four layers, which are as follows:

• Sensor Layer: oversees monitoring patients using measuring devices.

• Application Layer: oversees entering, manipulating, and controlling patient data records; and

• Fog Layer: oversees managing and storing sub-packages of medical data that are closer to applications.

• Device Layer: This layer collects data from the sensor layer and the application layer systems.

• Cloud Layer: oversees storing a complete set of patient records, data usage information, and authorization records for accessing patients. It also validates the dataset's accessibility.

In the green section of Figure 1, several types of devices are discovered to communicate with the sensor layer. These devices track patients and collect medical data. In terms of the application layer, applications that change medical record data are available and are used by patients, physicians, nurses, family members, emergency services, hospitals, and others.

A fog node is used to verify these operations as a blockchain miner (transactions). Data is also obtained from stakeholders and portals. The NFR4 is supplied with a representative state transfer interface (REST), using the POST, GET, PUT and DELETE operations. The cloud layer synchronizes the data and sub-sets of permissions. Cloud modules include medical information management and licensing transactions. The first is a software variable which allows the entire range of patient information to be stored in a relationship database. This module also guarantees the reception and access to the most latest information from the Fog layer. The REST Gui is also available, allowing access to data management.

The software feature for the whole data set of patient care and the validated data access permission set for the Fog Nodes is a software module, Authorization Transaction Management module. This section is used as a database of Blockchain to store transactions for proprietary applications. Also included are the NFR2 specifications. Figure 5 illustrates the second view of the architecture breakdown. The Fog layer is more complicated in the image and the decomposition of the Fog knot can therefore be imagined. For each module, there are six sub-modules as shown:

• Communication: is in charge of capturing Fog Node-related applications. It also features a REST interface for medical data exchange with the sensor layer and layer of the system. This interface also allows transactions to be transmitted into the Fog Layer through the sensor layer and application layer. Finally, the Bit Torrent protocol provides an interface between the Fog Node and other modules of Fog Layer.

• Authorization: part of the software for patient registration. It also validates stakeholder and gateway authorizations for handling patient registrations. This module is therefore used for carrying out miner validations. This confirms whether a request may modify a sub-set of data. The NFR2 norm complies with the Fog Node part.

• Storage: is a patient subset of connection database storage program variable. The NFR1 and NFR3 specifications are therefore included in this submodule.

• Reproduction: part of a program which reproduces a new fog node sub-set from a nearby fog node. This sub module provides the availability of data-by-data redundancy as a fault tolerance technique. Finally, the NFR1 condition is defined in this submodule.

• Priorities: The Fog node data priority program portion handling. This part includes details on the criticality of the data when last saved. First, the data from the Fog Layer to be saved on the layer will be released which is the bulk of the data available.

• Syncing: a cloud-coated portion of data software to sync fog-coated data.

• Synchronized Data: From time to time, this submodule sends data to the cloud to keep it current.

• Data synchronization: It also searches for information not contained in the Appliance Layer Fog Node.

In addition, synchronization openly uses priority data to free the storage space in the Fog Node. At the end of the day, the data used by the applications is searched and the data is provided more efficiently.

Analysis of Study

In the proposed study, a framework for health data is designed and implemented, where users can save all information into a fog computer environment in a single blockchain without Trusted Third Party (TTP) systems as shown in figure 6. The system also provides data privacy, confidentiality and eliminates end-user inconsistency. The system emphasizes the integration of block chain storage of healthcare data. In the patient system if he switches the city and then calls the physician of the other city the new physician can get his full history across fog networks and use the blockchain technology to preserve the safe data.

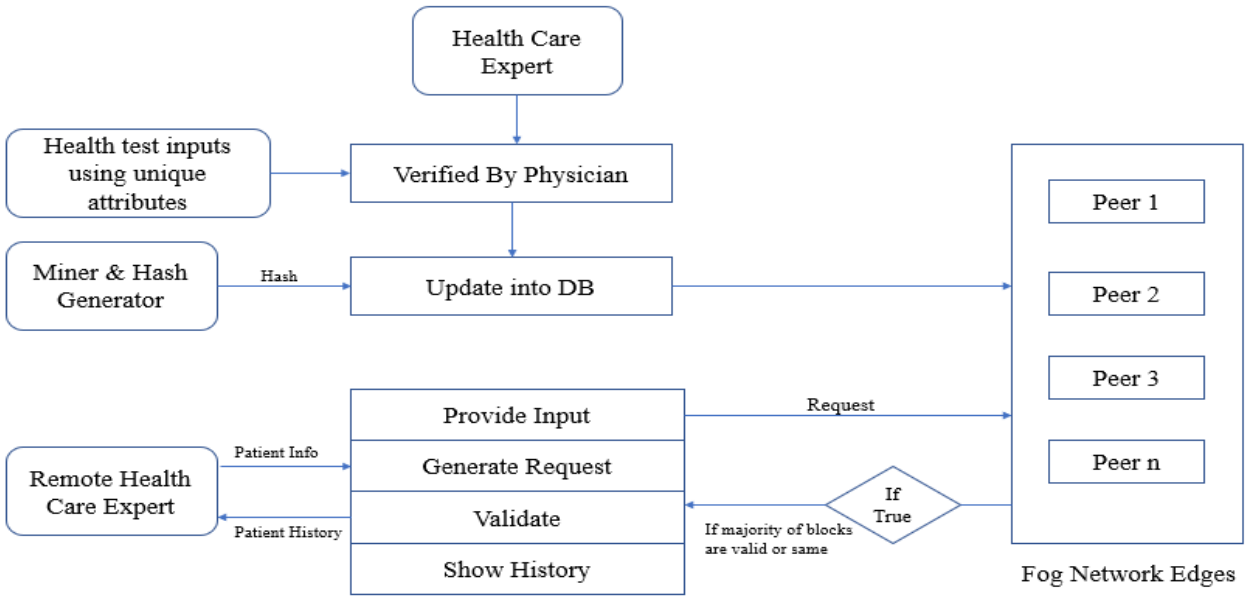


Figure 6. Overview of Architecture

In this data the transactions are stored in a sequencing fog network on multiple servers. This sheds light on the efficiency and time limits of the service. This is a middleware framework in which the load is threaded in a processing environment. The created request is stored in Blockchain parallels for all nodes. The Hash algorithm and the Hash for the given string will be produced. We use peer checks to verify the data before performing any transaction. If a chain is null, the current blockchain server will be retrieved or modified. This will be validated until the query is verified and committed by all nodes. A mining algorithm is applied until the valid hash is created to validate the hash produced for the query.

An abundance of research is expected from the additional technical to identify the most sensitive style method for making use of Blockchain technology by associate graduates, thus equalizing important security and confidentiality considerations. Whether or not you are applying for an established Blockchain degree of redistributed application leverage, extra research on the safe and economic package is to apply the Blockchain technology additionally in the interest of teaching the potential of this emerging technology to package engineers and domain consultants. In addition, validation and tests approaches in comparison with current structures are critical to the efficiency of Blockchain-based health architectures (e.g., via performance metrics associated with time and value of computations or assessment metrics associated with its feasibility).[19] In certain instances, a Blockchain substitute network is often additionally relevant than the current Blockchains; thus, an associate degree is also investigation expansions to an existing Blockchain or a Blockchain service that offers health services fully. In the future, it is interesting to incorporate the proposed system with various data nodes. The focus of the research is the revelation and improvement of Blockchain's shortcomings from the perspective of privacy and security, but most of the solutions suggested are not thoroughly valued.[20] The

other problems of Blockchain scalability including performance and latency were left unknown.

CONCLUSION

A software solution to manage medical records is discussed in this article. The Computing Model is focused on Fog, which offers accessibility and efficiency information closer to applications and appliances.[21] The use of a Blockchain infrastructure can also achieve anonymity. This approach also tackles the need to interoperate with the REST pattern in the contact module. The study also demonstrated unique features of the software architecture which researchers, engineers and programmers use to develop a method for the management of medical records. The solution makes the patient the data controller whose medical data are monitored by control systems. The patient can use his medical history more effectively and he can use the prescribed practices to exchange data stored between nodes.[22]

The use of Blockchain in the architectural framework permits Fog Node to disperse approval processes, remove a single failure point with the cloud computing paradigm from a traditional authentication model, and allow each Fog node to function independently.

CONFLICT OF INTEREST

Authors do not have any conflict of interest for this article.

REFERENCES

1 1. C. Guo, P. Tian, K.K.R. Choo. Enabling Privacy-Assured Fog-Based Data Aggregation in E-Healthcare Systems. *IEEE Trans. Ind. Informatics* **2021**, 17 (3), 1948–1957.

2. A. Banerjee, B.K. Mohanta, S.S. Panda, D. Jena, S. Sobhanayak. A Secure IoT-Fog Enabled Smart Decision Making system using Machine Learning for Intensive Care unit. In *2020 International Conference on Artificial Intelligence and Signal Processing, AISP 2020*; **2020**; pp 1–6,.

3. T. Almehmadi, S. Alshehri, S. Tahir. A Secure Fog-Cloud Based Architecture for MIoT. In *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*; **2019**; pp 1–6,.

4. V. Dave, N. Joshi. Fog computing enabled Ambient Assisted Healthcare systems. In *2019 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics, DISCOVER 2019 - Proceedings*; **2019**; pp 1–7,.

5. E. Badidi, K. Moumane. Enhancing the Processing of Healthcare Data Streams using Fog Computing. In *Proceedings - IEEE Symposium on Computers and Communications*; **2019**; Vol. 2019-June, pp 1113–1118,

6. H. Zhao, P. Bai, Y. Peng, R. Xu. Efficient key management scheme for health blockchain. *CAAI Trans. Intell. Technol.* **2018**, 3 (2), 114–118.

7. S. Amofa, E.B. Sifah, K.O.B. Obour Agyekum, et al. A blockchain-based architecture framework for secure sharing of personal health data. In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services, Healthcom 2018*; IEEE, **2018**.

8. S. Wang, J. Wang, X. Wang, et al. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *IEEE Trans. Comput. Soc. Syst.* **2018**, 5 (4), 942–950.

9. X. Zheng, R.R. Mukkamala, R. Vatrapu, J. Ordieres-Mere. Blockchain-based personal health data sharing system using cloud storage. In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services, Healthcom 2018*; IEEE, **2018**.

10. Q. Xia, E.B. Sifah, K.O. Asamoah, et al. MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. *IEEE Access* **2017**, 5, 14757–14767.

11. T. Neudecker, P. Andelfinger, H. Hartenstein. Timing Analysis for Inferring the Topology of the Bitcoin Peer-to-Peer Network. In *Proceedings - 13th IEEE International Conference on Ubiquitous Intelligence and Computing, 13th IEEE International Conference on Advanced and Trusted Computing, 16th IEEE International Conference on Scalable Computing and Communications, IEEE International Conference on Cloud and Big Data Computing, IEEE International Conference on Internet of People and IEEE Smart World Congress and Workshops, UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld 2016*; IEEE, **2017**; pp 358–367.

12. B. Paharia, K. Bhushan. Fog Computing as a Defensive Approach Against Distributed Denial of Service (DDoS): A Proposed Architecture. In *2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018*; IEEE, **2018**.

13. V. Naidu, K. Mudliar, A. Naik, P. Bhavathankar. A Fully Observable Supply Chain Management System Using Block Chain and IOT. In *2018 3rd International Conference for Convergence in Technology, I2CT 2018*; IEEE, **2018**.

14. H. Zhao, Y. Zhang, Y. Peng, R. Xu. Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys. In *Proceedings - 2017 IEEE 13th International Symposium on Autonomous Decentralized Systems, ISADS 2017*; IEEE, **2017**; pp 229–234.

15. Z. Chen, S. Chen, H. Xu, B. Hu. A security authentication scheme of 5G ultra-dense network based on block chain. *IEEE Access* **2018**, 6, 55372–55379.

16. N. Kshetri, J. Voas. Blockchain-Enabled E-Voting. *IEEE Softw.* **2018**, 35 (4), 95–99.

17. J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, A. Akutsu. The Blockchain-Based Digital Content Distribution System. In *Proceedings - 2015 IEEE 5th International Conference on Big Data and Cloud Computing, BDCloud 2015*; IEEE, **2015**; Vol. BDCloud '15, pp 187–190.

18. P. Clements, D. Garlan, R. Little, R. Nord, J. Stafford. Documenting software architectures: Views and beyond, 2nd ed.; Addison-Wesley, United States, **2003**.

19. C. Awasthi, M. Nawal, P.K. Mishra. Security Concerns of Fog Computing in Field of Healthcare using Blockchain: A Review. In *Proceedings - International Conference on Communication, Information and Computing Technology, ICCICT 2021*; IEEE, **2021**; pp 1–5.

20. C. Awasthi, I. Sehgal, P.K. Pal, P.K. Mishra. Software-Defined Network (SDN) for Cloud-Based Internet of Things. In *Transforming Management with AI, Big-Data, and IoT*; Springer International Publishing, Cham, **2022**; pp 185–213.

21. O. Cheikhrouhou, K. Mershad, F. Jamil, et al. A lightweight blockchain and fog-enabled secure remote patient monitoring system. *Internet of Things (Netherlands)* **2023**, 22, 100691.

22. M.J. Baucas, P. Spachos, K.N. Plataniotis. Federated Learning and Blockchain-Enabled Fog-IoT Platform for Wearables in Predictive Healthcare. *IEEE Trans. Comput. Soc. Syst.* **2023**, 1–10.