A Hybrid Framework based on IoT and Blockchain Network to Store the Patient Health Data

[1]Sharda Tiwari, [2]Dr. Namrata Dhanda and [3]Dr. Harsh Dev, [4]Digesh Pandey

[1,2]Department of Computer Science & Engineering, Amity University Uttar Pradesh
[3]Department of Computer Science & Engineering, Pranveer Singh Institute of Technology, Kanpur
[1]shardatiwari87@gmail.com, [2]ndhanda@lko.amity.edu, [3]drharshdev@gmail.com,
[4]digeshpandey001@gmail.com

Article Info
Page Number: 330 - 339
Publication Issue:
Vol 71 No. 2 (2022)

Abstract

Healthcare industry constantly faces many issues such as patient data access, drug storage log, medical records, or logs these are only a few of the many problems hospitals and other medical institutions must deal with. Healthcare industry must balance patient care with information privacy, security. The healthcare industry faces major issues like, putting the patient at the center, privacy and access, completeness of medical information, cost, supply chain management, drug records. Medical record keeping has evolved into a science of itself, even though the traditional method of storing data over a centralized database can be harmful as mentioned in the sections above, it can be prone to hacking or even a single point failure. Another issue with storing medical data in these databases is that, when these databases need an update in software all the servers are temporally down until the updates are finished. This small window can lead to be very lethal as healthcare is a 24/7 work. Blockchain technology and cryptocurrencies are being touted as the "solution" to problems in many different, disparate sectors throughout multiple industries. In this paper the goal is to identify blockchain technology applications in healthcare industry by conduction a systematic literature based on which a framework will be proposed. The promise of blockchain extends into the healthcare industry allowing a transformation of the current system and its use of information technology.

Article History
Article Received*: 30 December 2021*
Revised*: 06 February 2022*
Accepted*: 20 March 2022*
Publication*: 25 April 2022*

Keywords: IoT, Healthcare, Blockchain, Hospital, Security.

1. Introduction

Now a days receiving the healthcare service from various hospitals and clinic have become very common due to the predominant increase of specialization in the healthcare services. And also due to people knowing to different cities and countries that might be a need for them to receive the medical attention, doctors with the patient's medical history can make precise diagnostics as well as provide proper treatment for them at the right time. The major problem faced by the healthcare service provider is sharing the clinical data and ensuring data security data integrity, confidentiality of the data as well as maintaining the privacy of the patient at the same time. Coming to electronic health records. The blockchain technology enables a variety of applications in the healthcare industry. Its main applications are in the areas of health management, patient safety, and medical device data. To enable the widespread adoption of this technology, it must be a trusted and secure platform that allows data to be shared among multiple stakeholders. Blockchain technology is becoming a popular solution in these areas. However, there are several challenges that still need to be overcome.

EMR: An Electronic medical record or EMR is a digital copy of a patient's medical history. It is a file containing the key information such as diagnosis, prognosis, lab investigation reports and so on. Improving electronic medical records is a very crucial element in improving the overall healthcare intelligence [2]. Healthcare systems around the globe are struggling with the problem of data siloes, both the patients and their healthcare providers have an incomplete record of their medical history. Implementing blockchain technology with EMR can provide the necessary solution to this issue and provide a seamless interoperability of healthcare data [3, 4]. However, permissionless or public blockchain are not suitable for such uses as any anonymous person who is a part of the network can have access to the data. This is mitigated by the usage of permissioned or private blockchain network [5] which limits the exposure of the medical data to the outside or unwanted people. Another aspect of implementing blockchain is a patient controlled or patient driven care, this means that the patient has control over who can access or view their own medical data [6]. Patient data is often surrounded by various laws for privacy in many countries. Data on blockchain is visible to everyone on the network. This can be mitigated by using a private blockchain system rather than a public blockchain. In a private blockchain network the participants need permission to join and access the data whereas a public blockchain network is open to everyone who has access to internet such type of network can possess many security concerns regarding privacy. This can revolutionize the healthcare industry which currently revolves around institution-based care. This gives the patient the opportunity to make better decision regarding their own healthcare treatment. Blockchain enables the patient to have control over the access protocols and can decide whom to give access with the help of a program called as Smart contracts, which are cleverly written lines of code. These codes are executed when a predefined set of conditions are met. These are self-executing lines of code. As the data in these EMRs are secured using cryptographic hash functions. It is economically viable to verify the integrity of the transaction on the blockchain [7]. Blockchain technology has gained momentum in the past few years, yet it still has a long way to go with regards to implementation in Electronic Medical Records. However there have been few implementations of this technology in EMRs. The paper [8] designed an architecture which utilizes a smart app on a smart phone and enables the patient to have access and control over their own data. It utilizes the blockchain as a storage system for the data, but this paper does not mention any use of private blockchain network. As mentioned above using a private blockchain network limits the access to a limited people. A prototype "Med-Rec" [9] design provides a proof of-concept system, which utilizes the decentralization feature of this technology to contribute to a secure, interoperable EMR system. This prototype uses Ethereum smart contracts, the Med-Rec provides patients with comprehensive record review of their medical record. This system prioritizes open APIs and network structure transparency. However, this prototype does not store medical records. It only stores a hash of the record on a blockchain. Another prototype called Med Share [10] was introduced which is a safe and secured blockchain system for medical data exchange among different untrusted parties. Med-Share could be used to share medical data and maintain electronic health records among cloud service providers, hospitals, and healthcare research entities, with greater data provenance, personalized audit control, and minimal possible threats to data security and privacy. The main challenge faced by Med-Rec is the mining incentives, in exchange for sustaining and securing the network via Proof of Work consensus protocol, the miner get access to aggregate, anonymized data. Health Chain [11] which is a patient-centered blockchain framework. It was designed to boost the patient involvement and regulated. This system disseminated the data in a secure and interoperable environment. This is a permissioned blockchain system. Hospitals, Research institutions and Government agencies have the authority to manipulate the blockchain within a private network. Together these form a consortium network which manage the Health Chain network. The benefit of using blockchain with EMRs is that there is only single true version of the records with both, the patient, and the healthcare providers.

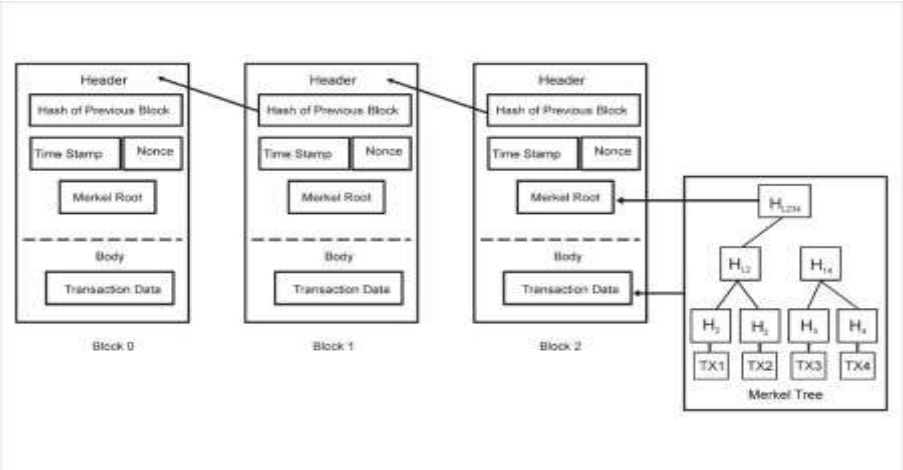
In order to create a secure and reliable IoT platform for healthcare, it is necessary to have an infrastructure for storing all the required data. Blockchain technology can solve this problem. It can also be used for secure remote patient monitoring and compliance with HIPAA and other regulations. In this article, we will discuss

what makes blockchain such a good option for healthcare. Also, we will cover how healthcare IoT solutions use smart contracts to ensure data security. IoT devices can be used to reduce medical errors. They also provide more detailed information and improve patient care. These devices help healthcare professionals analyze emergency situations remotely, including identifying problems and alerting them before arriving [12]. They also help healthcare providers provide real-time health information to patients and physicians. In some cases, healthcare IoT can help prevent pandemics by providing accurate data on patient conditions. For example, a patient's blood pressure can be automatically measured, and they can receive preventive health care from the wearables that they have. The Internet of Things has great potential in numerous domains, including healthcare. Mettler and others have discussed its application to the smart city and drug supply chain. These researchers also show how blockchain is used in drug supply chains. By using this technology for data management, patients can be empowered and prevent counterfeiting. The authors conclude that blockchain can be used for healthcare IoT applications. They highlight some of the challenges associated with developing these systems

1.1 Blockchain

It is a decentralized distributed ledger on a peer-to-peer network. That consists of a list of chronologically arranged block. Its 1st block is called genesis block, and block beforeany given block is called as the parent block each block basically consists of two parts header and body [13]. Header consists of version which specified the block validation rules. Hash of the previous block ensures that if any changes made in the previous block, then the changes will do current block header. Time stamp is creation of time of the block. Markle root is obtained by hash of all the transaction in that block. 4-bit unique number which is used only once in the communication.

Figure 1: Blockchain Blocks Generation



1.2 Core Component of Blockchain

First is the node or peer it is basically a device or a computer in blockchain network. that contains the copy of all the transaction is exchange of informationbetween the two blockchain address. Block is a group of transaction, if anyone wants to add new block into the blockchain then certain block verification process needs to be done by specific most [14]. And those are done by miner consensus is an agreement reached by all the peersin the blockchain network an any transaction in the network

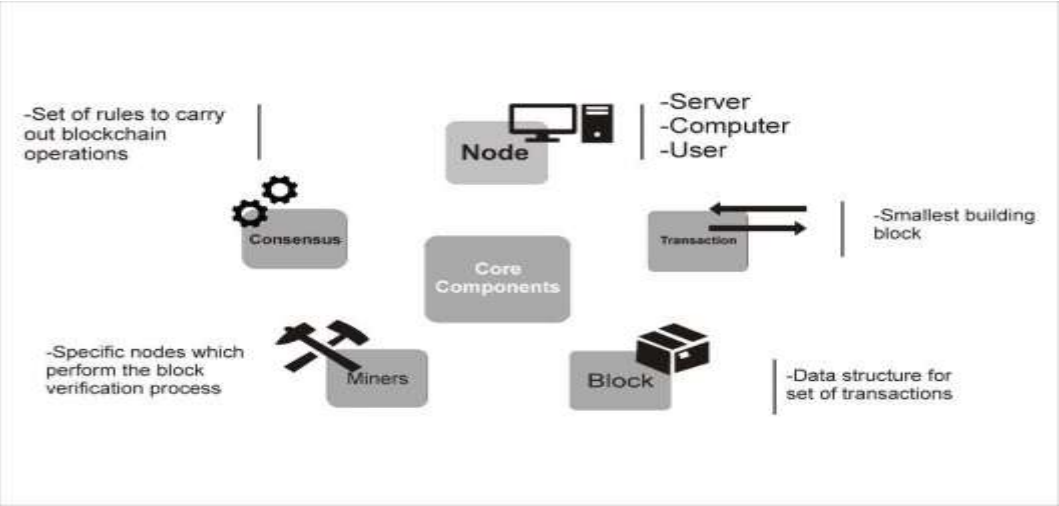


Figure 2: Blockchain Network Core Component

1.3 Types of Blockchain

Public Blockchain (permissionless)- It is also called permissionless blockchain, everyone can access the public blockchain and participant in the transaction. Public blockchain is fully decentralized. their fore no central authority and all the peers in the network has equal authority. Ex- Bitcoin, Litecoin, Ethereum
Private Blockchain (permissioned)-It is also called permissioned blockchain, Restriction on who can join the network and who can participate in the transaction. It is used by companies for internal uses. It is centralized in nature i.e., organization have full authority over the network Hyperledger fabric

2. Proposed Blockchain Framework for healthcare

Blockchain and Hyperledger fabric: Blockchain stored data cryptographically secure which solves the problem related to security of data. And fabric provides CA, & MSP component the provides secure identities for the user which are connected to the network that solves the problem of authentication and authorization. Fabric is permissioned blockchain, so the data remain confidential for the outside world. It comes with a distributed nature so availability will be solved [15]. Blockchain records are immutable, so data integrity problem has been solved. Scalability has been solved because several peers and usually can be applied here in the network. All the modules are pluggable. We can use the different database as well as the fabricSDK is available in different programming language like GO, JAVA, JAVA script, Type Script.

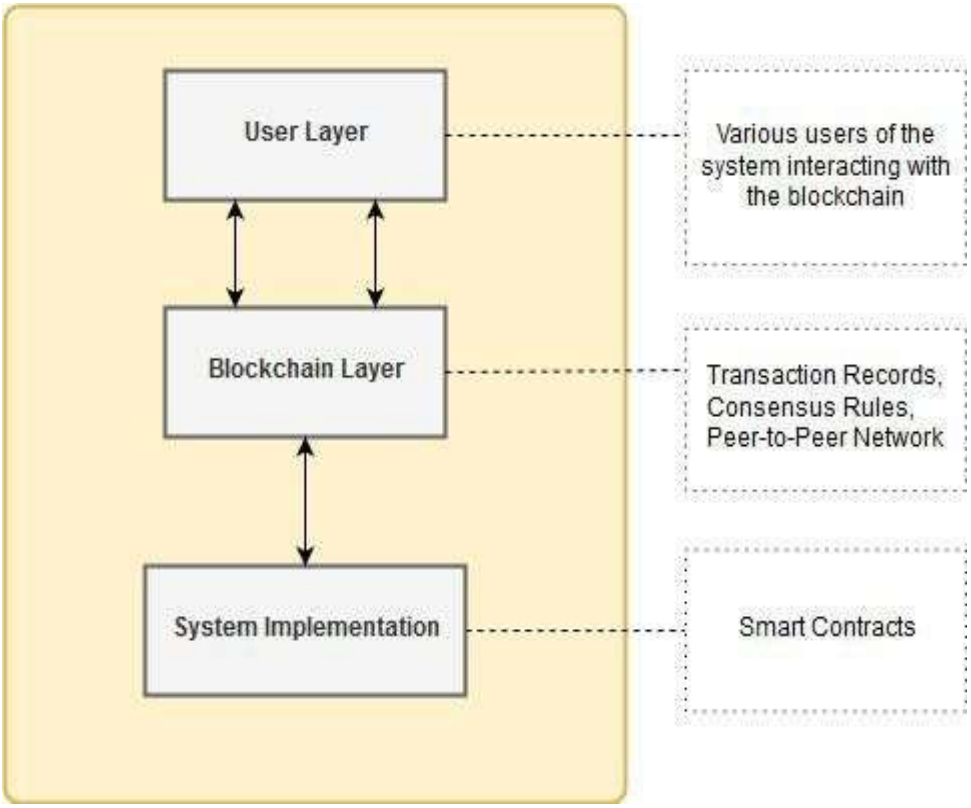


Figure 3: Proposed Blockchain Framework for healthcare

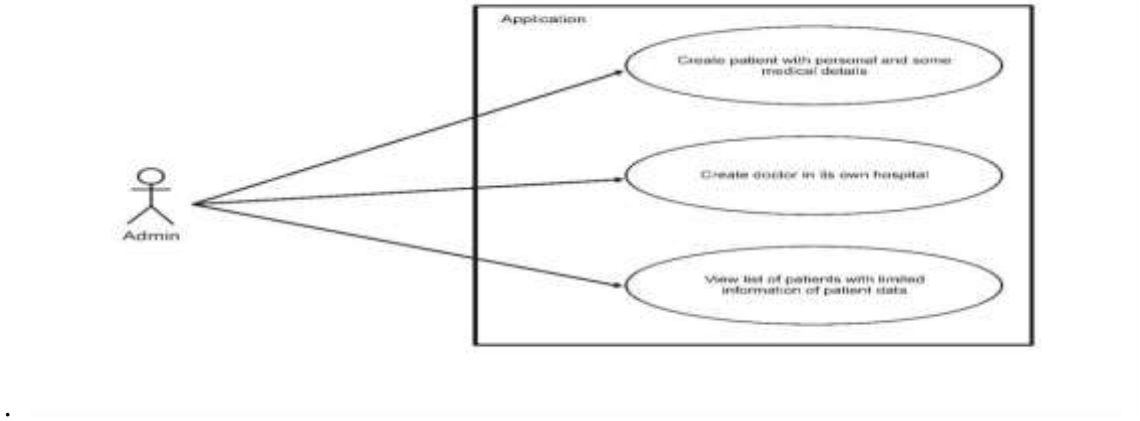
The sharing of data among different medical devices and healthcare providers plays a crucial role in an IoT network. However, one of the major issues in secure data sharing is data fragmentation. Data fragmentation may lead to a gap in information across healthcare providers, who are associated with a single patient. Insufficient information may hamper the treatment process. Blockchain technology is used to solve the problem of data fragmentation and helps the healthcare centers to establish a connection among the data repositories that are present in the network. This further ensures secure and protective sharing of sensitive medical information and increases transparency between the doctors and patients. Blockchain technology also promotes collaboration among healthcare providers and organizations to do qualitative research. The secure transmission in blockchain technology can be due to three factors. First, it contains an immutable "ledger" that can be accessed and controlled by people. It ensures that once a record is stored in the ledger, it cannot be modified. Further, each transaction in the ledger must follow certain predefined rules. Second, blockchain is a distributed technology and operates simultaneously from multiple devices, computers, etc. Third, blockchain follows the agreement rules and data exchange policies with a smart contract mechanism. The smart contract manages identity and sets out permissions to access different electronic medical reports (EMRs) that are stored in the blockchain [11]. It means doctors are only allowed to go through those EMRs to which they have been permitted.

2.1 Blockchain For EHR System

Organization in fabric component are hospitals in the real world. Hospitals are same interest connected to the same channel, if new hospital wants to connect or maintain some another form of data so they will form a new channel, the new hospital will be connected on the existing channel only after approving the hospitals which are configured in the channel configuration. The patient data will be treated asa asset in the fabric. All the data stored in blockchain database, fabric framework provides gate history API which is used to retrieve patient data and will be showed to the doctors. So that take the proper understanding of the patient's

conditions.

Use Case for Admin: Admin use case are really simple .it will create only patient with personaland medical details and create doctors and view the list of patients with limited information off patient data



.

Figure 4: Admin Use Case

Use Case for Patient: Patient can view only self-details all fields can be able to edit personal details. Also the patient will be able to view list of doctors are available in all hospitals. can be able to give permission to a doctor as well as revoke the permission of that doctor. View the history of its own data.

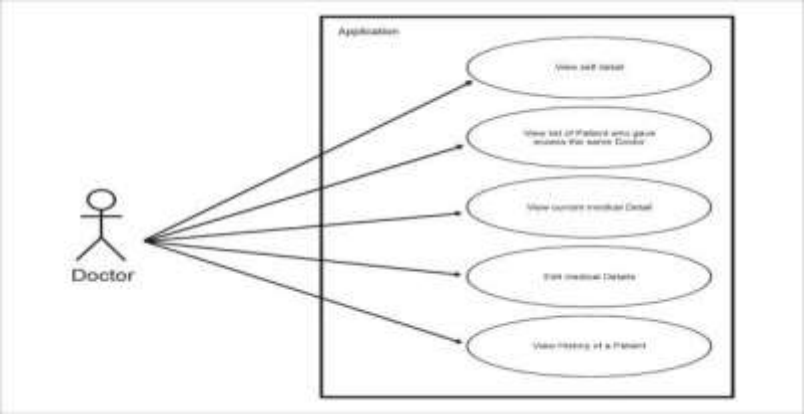


Figure 5: Patient Use Case

Use Case for Doctor: Doctor can view self-details as well as the list of patients who gave access for the same doctor. Doctor can be able to view and edit medical details of the patients also be able to view medical history of patients.

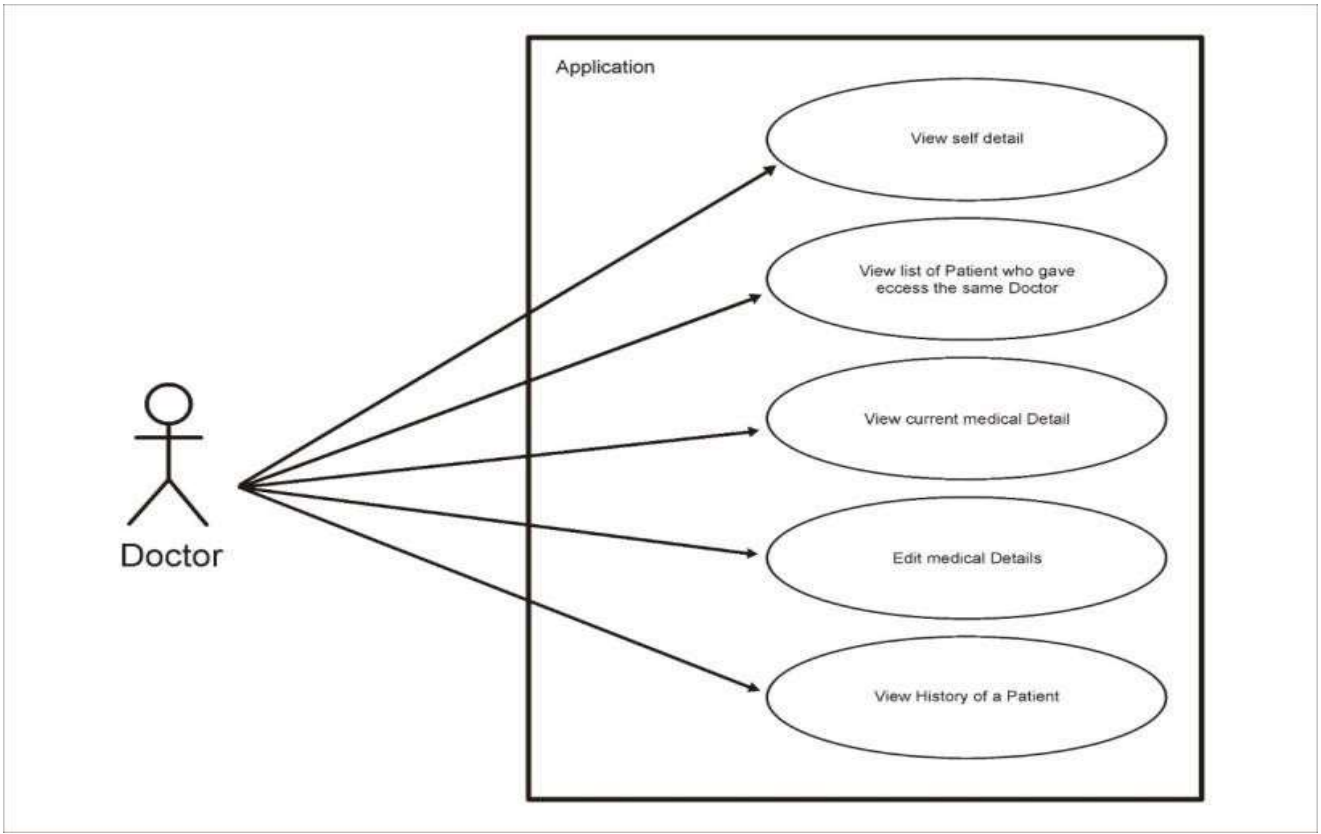


Figure 6: Doctor Use Case

3. **Architecture of Hyperledger Fabric:** Network has been established by the blockchain operator and all the peers in the organization are docker running container fabric SDK has been used to connect this network. SDK is written in Java script and use node JS server is used to handle the backend nodes. The user interface is developed in Angular JS. Redis is the key value paid database which is used for to store doctor's credential mainly username and password. In the network order organization initiates the blockchain .it create the first block in the blockchain which is genesis block other two organization (Hospital 1 and Hospital 2) comes together and form a channel named hospital channel ,it is only channel in this network.it is connected to hospital channel configuration .Hospital 3 is an additional organization ,so if hospital 3 wants to connect these channel ,hospital 1 and hospital 2 given approval .every hospital peers on each peers one ledger and one smart contract . the ledger is a combination of world state and transaction law in world state. We use couch DB and 3 smartcontract its main business logic for admin, patient and doctor which is deployed on every peer.

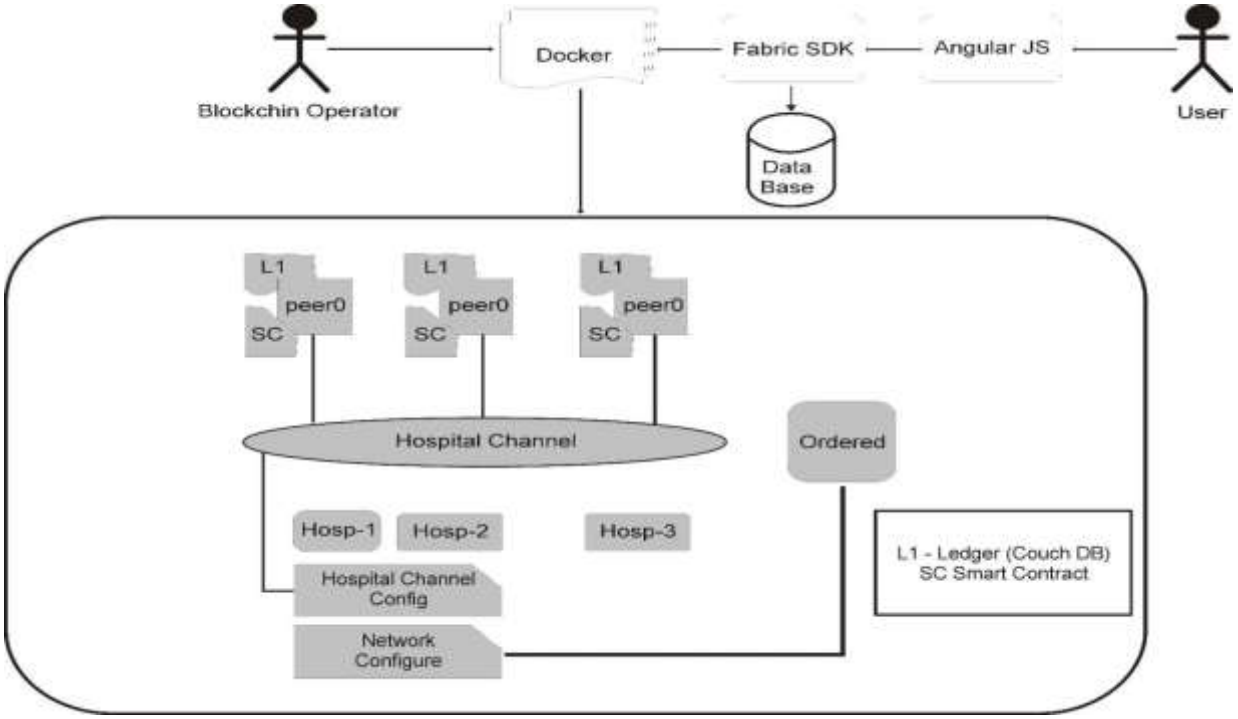


Figure 7: Network System Architecture

4. Algorithm: Smart Contract for Patient Records

Algorithm has five functions that are to define roles, add, view, update and deleterecords.

Algorithm 1 Smart Contract for Patient Records

Define User Assign Roles:

function Define Roles (New Role, New Account)add new role and account in
roles mapping
end function

Add Patient record

Add Data:

function Add Patient Record (*contains variables toadd data*)
if (msg.sender = = doctor) **then**
add data to particular patient‟s recordelse Abort session
end if
end function

Retrieve Data:

View Patient record

function View Patient Record (patient id)**if** (msg.sender = = doctor || patient) **then if** (patient id) = = true **then**
retrieve data from specified patient (id)return (patient record)
to the account that requested the retrieveoperation
else Abort sessionend if
end if
end function

Update Patient record

function Update Patient Record (contains variablesto update data)

if (msg.sender = = doctor) then
if (id = = patient id && name = = patient name)then
update data to particular patient‟s recordreturn success
else return failend if
else Abort sessionend if
end function
Delete patient data
function Delete Patient Record (patient id)if(msg.sender = = doctor) then
if (id = = patient id) then
delete particular patient‟s recordreturn success
else return failend if
else Abort sessionend if
end function

5. Conclusion

There are five major parts to the Blockchain Healthcare IoT system. First, it involves the use of smart contracts to secure patient data. Then, there is the layer 2 or core layer, which contains representative nodes of all the medical parties. The third layer is the higher layer, where processing takes place. Ultimately, the end result is a decentralized and secure system. One of the most compelling use cases for Blockchain Healthcare IoT is remote patient monitoring (RPM). This technology can also be used in the development of wearable healthcare IoT devices that monitor vital signs. However, these systems still face several challenges. One of these challenges is data ownership. Healthcare data is often shared without the patient's consent, and the data stored in them can be stolen if not protected. In addition to this issue, blockchain does not provide a standardized platform to facilitate the exchange of data among healthcare institutions. In addition, if two remote patient monitoring applications use different blockchain platforms, they may not be compatible with each other. Second, healthcare IoT and Blockchain technologies are expected to improve the efficiency of health care facilities. These technologies will improve the network's scalability and support low-end devices. While it is expected that the combination of Blockchain and IoT will improve the quality of healthcare, it is important to note that implementing Blockchain in this industry will likely not be a walk in the park. However, the benefits of Blockchain and IoT are immense and can improve the health care sector.

This framework is only for data storage for enhancing the ability of the system. We include machine learning for quick decision. In this framework permissioned blockchain is uses to store data and data produced by this system is reliable data so this can be also used by any external agency. It may be a government agency, insurance company or defense sector or any other private company. The proposed framework data is reliable secure and save so that any organization or research person can use this data on based on own requirement.

References

[1]. Oikonomou, F.P.; Pelekoudas; Ribeiro, J.; Mantas, G.; Bastos, J.M.C.S.; Rodriguez, J. A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems. In Proceedings of the 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 7–10 September 2021. [**Google Scholar**]

[2]. Oikonomou, F.P.; Mantas, G.; Cox, P.; Bashashi, F.; Gil-Castineira, F.; Gonzalez, J. A Blockchain-based Architecture for Secure IoT-based Health Monitoring Systems. In Proceedings of the IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Porto, Portugal, 25–27 October 2021; pp. 1–6. [**Google Scholar**] [**CrossRef**]

[3]. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2020**, *23*, e4049. [**Google Scholar**] [**CrossRef**]

[4]. Gope, P.; Hwang, T. BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. *IEEE Sensors J.* **2015**, *16*, 1368–1376. [**Google Scholar**] [**CrossRef**]

[5]. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Appl. Sci.* **2019**, *9*, 1736. [**Google Scholar**] [**CrossRef**]

[6]. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of Threats to the Internet of Things. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1636–1675. [**Google Scholar**] [**CrossRef**]

[7]. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [**Google Scholar**] [**CrossRef**]

[8]. Seliem, M.; Elgazzar, K. BIoMT: Blockchain for the internet of medical things. In Proceedings of the 2019 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom, Sochi, Russia, 3–6 June 2019. [**Google Scholar**]

[9]. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [**Google Scholar**] [**CrossRef**]

[10]. Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet Things J.* **2015**, *2*, 515–526. [**Google Scholar**] [**CrossRef**]

[11]. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [**Google Scholar**] [**CrossRef**]

[12]. Alkurdi, F.; Elgendi, I.; Munasinghe, K.S.; Sharma, D.; Jamalipour, A. Blockchain in IoT Security: A Survey. In Proceedings of the 28th International Telecommunication Networks and Application Conference (ITNAC 2018), Sydney, NWS, Australia, 21–23 November 2018; pp. 1–4. [**Google Scholar**] [**CrossRef**]

[13]. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and Iot Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [**Google Scholar**] [**CrossRef**]

[14]. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [**Google Scholar**] [**CrossRef**]

[15]. Y.2060: Overview of the Internet of Things, Telecommunication Standardization Sector of ITU ITU-T Recommendation Database. Available online: **https://www.itu.int/rec/T-REC-Y.2060-201206-I** (accessed on 30 January 2022).