The Effectiveness of Private and Public Blockchain Frameworks for Predicting Hypotension in Edge Computing Systems

Ms. Dharani D[1*], Dr. K. Anitha Kumari[2]
{dharani0609@gmail.com[1], kak.it@psgtech.ac.in[2]}

Assistant Professor, Department of IT, PSG College of Technology, Tamil Nadu, India[1],Associate Professor, Department of IT, PSG College of Technology, Tamil Nadu, India[2]

Abstract. The Smart Health care system plays a most predominant role in the current research for the integration of IoT devices with Edge Computing. Blockchain technology is used to ensure immutability of the recorded transaction. It is used to create a decentralized edge computing marketplace, without a single control point. Ethereum Framework is a distributed public Blockchain network uses consensus algorithms such as Proof of Work (PoW) and Proof of State (PoS) to reach consensus about the current state, thus ensuring immutability of data. It is used for developing open-source decentralized applications for public network communities. Certain data in healthcare information system is sensitive and it might not be revealed even to the co-peers. Integration of private Blockchain is essential for limiting the accessibility of records in certain sensitive domains like healthcare. Hyperledger Sawtooth is an enterprise, private and open source Blockchain platform to create distributed networks for enterprises. It uses Proof of Elapsed Time (PoET) as internal consensus mechanism. Both Ethereum and Sawtooth are identified and implemented with a decentralized application. Though the private and public blockchain frameworks have specific potential benefits, their working mechanisms differ from each other depending on various parameters. The system aimed at evaluating the working efficiency of private and public Blockchain networks upon implementing the predictive analysis of hypotension using Mean Arterial Pressure in Edge computing system. The system also integrates Homomorphic Encryption schemes to ensure authenticity of the patient's test report.

Keywords: Private and public Blockchain, Hypotension, Low Mean Arterial Pressure, Edge Computing.

1 Introduction

Blockchain is a decentralized network which uses Distributed Ledger Technology (DLT) to maintain the transactions with timestamp. It ensures non repudiation among the network entities. One cannot deny the transaction that he/she had performed. Once the transaction is performed it cannot be modified. When a network entity is trying to alter the previous transaction it will be recorded as a new transaction. Thus it ensures immutability. Group of transactions forms a block in Blockchain Network. The first block in a network is called as Genesis block. The next transaction to be added to block is determined based on consensus mechanism. As the network doesn't rely upon any centralized authorities to manage transactions, it guarantees decentralization. The feasibility of exploiting the

ICCAP 2021, December 07-08, Chennai, India

DOI 10.4108/eai.7-12-2021.2314550

blockchainfunctionalities are made possible through various cryptographic mechanisms. Blockchain as storage it provides strong security to the data. Blockchain networks can be of various types namely, private, public, consortium and hybrid. Only authorized entities are allowed to join the permissioned Private Blockchain network. Public network includes participants without permission as anyone in the internet can join and perform the transaction. Certain enterprise application needs the combinations of both private and public blockchain networks. Thus integration of both the mechanisms is done to work for a specific organization. Consortium blockchain is similar to hybrid as it combines both private and public networks but it works for federated organizations.

By deploying Blockchain technology at the edge, the system becomes decentralized, this implies there will be no need for a central administrator and enable sharing of medical data in a secure way. In addition, fully homomorphic encryption schemes are used in predictive analysis to enhance security of the proposed system (Bos, J.W., et al 2014). Blockchain network is designed in such a way that metadata is shared with endorsed peers in a safe and consistent way that would eliminate the cost and burden associated with data compromise. As a result of it, many research articles are proposed on "Blockchain for healthcare". Kubendiran, M et al (2019) proposed better security structure for E-Health Systems using Blockchain. The proposal that uses Blockchain for healthcare information systems is tremendously increased for the past decade (Katuwal et. al 2018). A study has been done on the Google Scholar website for searching for a keyword "Blockchain for healthcare" and the number of relevant results retrieved for past ten years are monitored and analyzed. The report is shown in the Figure 1.

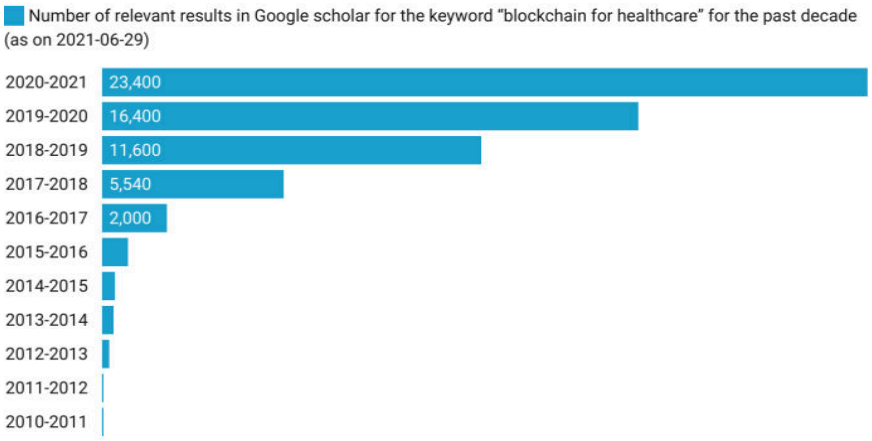

Figure 1. Growth of Research in "Blockchain for healthcare"

In the field of medicine, blood pressure is the mechanism of pushing the blood against the arteries with each heartbeat. A blood pressure impression is denoted as two numbers. The former numeral is the value of the pressure in the arteries when the heart beats and is denoted by the term systolic pressure. The subsequent number measures the pressure in the arteries when the heart takes a break in between the heart beats and it is represented by the term diastolic pressure. Optimal blood pressure is less than 120/80 [systolic/diastolic]. Hypotension is the state of low blood pressure [less than 90/60]. Hypotension can lead to dizziness and faintness (Davies, et al 2020).

In digital world, protecting the medical data is highly important as it holds huge amounts of personal health information which are to be maintained confidential. Edge Computing is a process of performing the computations either near to the source of the data or in the place where it is generated. The former approach of IoT (Internet of Things) data analysis is done through the cloud platform which resulted in different limitations such as data confidentiality and security (Cao, et al 2020). Moreover, Performance of the system always relies on the internet connection. This trend motivates to use the edge analysis where the processing happens at the gateway and cloud platform is used for storing the post analysis data (Dharani D et.al 2020). For deploying data either with hybrid or consortium blockchain networks, the analysis for implementing private and public blockchain network is essential.

2 Related Works

Research in health sector is imperative for improving human wellbeing and health care. To achieve secure data analysis, strong encryption scheme can be identified and applied to the personal health data. The encrypted personal health data is shared among the network peers hence ensuring privacy and security.

In this system, the idea is to implement the project in edge computing to widen the cloud platform utilization and to disseminate it at the edge of the peer to peer network. But it faces security challenges in decentralized administration. Combining Blockchain and edge computing to develop a system facilitates consistent access and control of the network, storage, and processing disseminated at the edges, hence providing the processing near the end in a secure mode (Wang, X., et al 2020).

Now-a-days, many research works are done in the area of security, edge computing and Blockchain. Mohammed Forouzanfar et al (February 2020) proposed such a system to integrate Edge computing with Blockchain technologies. A lot of security mechanisms to protect the data, mechanisms to integrating edge computing and Blockchain have been developed. Lots of paper has been established in these areas.

Al-Mashhadi, M. H. &Khalf, A. A. (2019) proposed efficient hybrid Homomorphic Encryption technique. They apply this technique on image encryption for a secure transmission of personal images in permissionless cloud. This technique is based in the block pixel Literature survey. The proposed method is un-changeable and proficient in terms of safety and time when judge against other schemes. In this scheme, when the images are transferred over the permissionless cloud, the hybrid cryptographic techniques are applied. The hybrid cryptographic techniques are applied for reducing the execution time and to expand the strength of cryptosystem (Forouzanfar, M., et al September, 2015).

Bing Chen (March 2018) proposed the edge computing technique. Due to the volatile increase of Internet of Things, numerous data is produced at the edge of the network. The conventional centralized computing model has turn out to be ineffective because of the bandwidth and asset constraints.

Edge computing is a novel computing approach that permits storing and processing data at the edge of the network and offers intellectual computations near the origin of the data by integrating cloud. This method focuses the data protection and privacy aspects and issues in the field of edge computing. Zhang, J., et al (28 March 2018) proposed ways to implement and guarantee data Security and preserve privacy in Edge Computing structure. In addition, the data protection mechanisms, such as encryption, access management, integrity auditing and

endorsement have been bringing up. The extremely active edge computing environment also makes the system susceptible. The general solutions for this dilemma offer potential benefits to both the edge devices and providers but in addition, it also brings up computational and communicational overheads (Pustokhina et al 2020).

Chuanwen Luo et al (February 2020) proposed Architecture for the amalgamation of Edge with Blockchain Technology. The IoT device is associated to an edge server which controls and manages the devices. Many such connections happen at its edge and form a network. The edge server provides certification authority to the IoT devices. With this architecture, the servers can rapidly process the data. Despite the fact that, having a lot of layered Blockchain architectures developed for IoT sensors, Edge processing Servers and Cloud management amplifies the density and complexity of the computation by a large.

Baraka William Nyamtiga, et. al (25 July 2019) proposed Blockchain integrated Storage mechanism in Edge environment. Here, issues on anonymity, adaptability and integrity to attain practical, secure decentralized data storage have been investigated. Smart devices uses several communication mechanisms to process the system. Here a permissioned Blockchain is imposed. Maintaining data in edge nearest to owners and consumers lifts up the systems' availability, decreases the communication latency and durability. Locking and unlocking states increases delay in fetching data.

Zixiao Shen et. al (April, 2015) proposed a new method to monitor blood pressure constantly based on selected parameters. These parameters were used to handle the values of Systolic Blood Pressure (SDP), Diastolic Blood Pressure (DBP) and Mean Arterial Pressure. The proposed method uses multiple linear regression analysis. This method is of great value as this can be used in wearable devices so that it can monitor the blood pressure continuously.

H.S.Jennathet. al (July, 2020) proposed a system for healthcare data management that uses Hyperledgersawtooth framework to digitalize the medical data. The system integrates two different blockchain architectures. One for Access tracking and the other for Audit trails. It also implements traditional database system MySQL to handle the same data for comparing with the blockchain storage. System functions based on Proof of Concept (PoC) consensus in which the data management is less scalable and entity permission management is not trouble-free.

These surveys are done to understand the different aspects in the relevant research fields and designed the proposed model by considering the various limitations.

3 Proposed System Design

Edge computing is implemented above cloud computing, as edge is decentralized, preferred more than cloud computing in distant spots, where there is no or partial connectivity to a centralized locality. The proposed system involves collection of data from Blood Pressure monitor then retrieves data from Edge. Later, homomorphic encryption is applied and analysis is done on the encrypted data. Then the data is pushed on to Cloud server. System is integrated with Blockchain and a web application design.

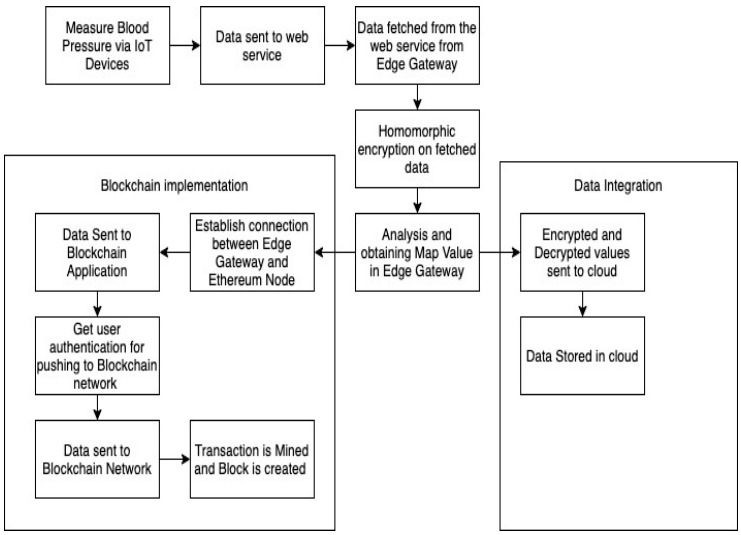

Figure 2. System Architecture

Figure 2 explains the process flow of the system. Dataset [systolic and diastolic pressure] is collected from BP meter. The data is sent to the edge gateway via Bluetooth. Further, the data is retrieved from edge gateway through web scrapping. Homomorphic Encryption Scheme is applied and analysis is performed if a person is prone to hypotension. If Mean Arterial Pressure was greater than 50 gm/dl, then the patient is prone to hypotension. Patient's data is stored in Blockchain for the requirement of immutable records. Contracts are written for writing patient's record into Blockchain and getting patient's record with different views according to the user [patient, researcher]. Front-end is developed using React JS and the front-end and Blockchain is connected through web3.js.

This satisfies the project requirements, as Homomorphic Encryption Scheme ensures security in predictive analysis, Edge Computing systems ensure remote accessibility and Blockchain ensures immutability of record transaction and React JS offers user interface. The smart contract deployments and analysis is done in EthereumBlockchain Platform which is a public Blockchain network and its metrics are measured. In order to provide limited access to various sensitive data present in the application the private Blockchain technologies are generally used (KA Kumari et. al 2020). By considering the impact and sensitivity of healthcare data, the HyperledgerSawtooth, a private decentralized network is also chosen and tested the working of the system against the same application. Thus, the overall system examines the working efficiency of both private and public Blockchain platforms interms of different parameters for predicting the hypotension in Edge computing systems.

4 System Implementation

The work process of the proposed framework incorporates the various stages. The data are gathered in real time using IoT devices. These data are retrieved from the webpage of Edge Gateway where data is retrieved for computation and analysis.The Enhanced Homomorphic Cryptosystem is a completely homomorphic open key encryption plot. It utilizes expansion, increase, blended expansion, and blended duplication over the whole

numbers. The private key will haphazardly be produced for every encryption procedure. A similar plain book doesn't produce the equivalent cipher text, to keep the interloper from breaking the cipher text considerably after it has a solid perception. Thus, homomorphic analysis of hypotension is done.

Blockchain is a relentlessly emergent ledger. It maintains eternal evidence of all the communications took place in a protected, sequential and undeniable way. Blockchain uses various cryptographic techniques to keep data in the blocks secure. A transaction can happen only after the completion of previous transaction. A Blockchain is nothing but the sequence of blocks which holds information. The pictorial representation of the Blockchain model has been described in Figure 3. Each block records recent transactions and it goes into Blockchain as a fixed catalog. After the completion of each block, new block is mined.

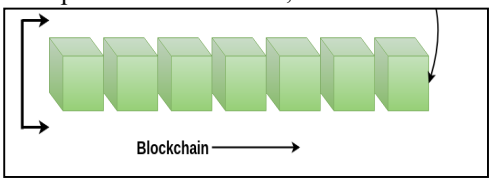

Figure 3. Blockchain Model

Selection of Blockchain as a solution to certain application is a peer reviewed process. It depends on the various parameters (Zhou et.al 2020). If the application no longer requires the transactions to be maintained or if there are no multiple entities present in the network then there is no need for Blockchain. When a system continuously rely upon Trusted Third party monitoring then there is no use for integrating Blockchain. The flow chart is shown in the Figure 4.

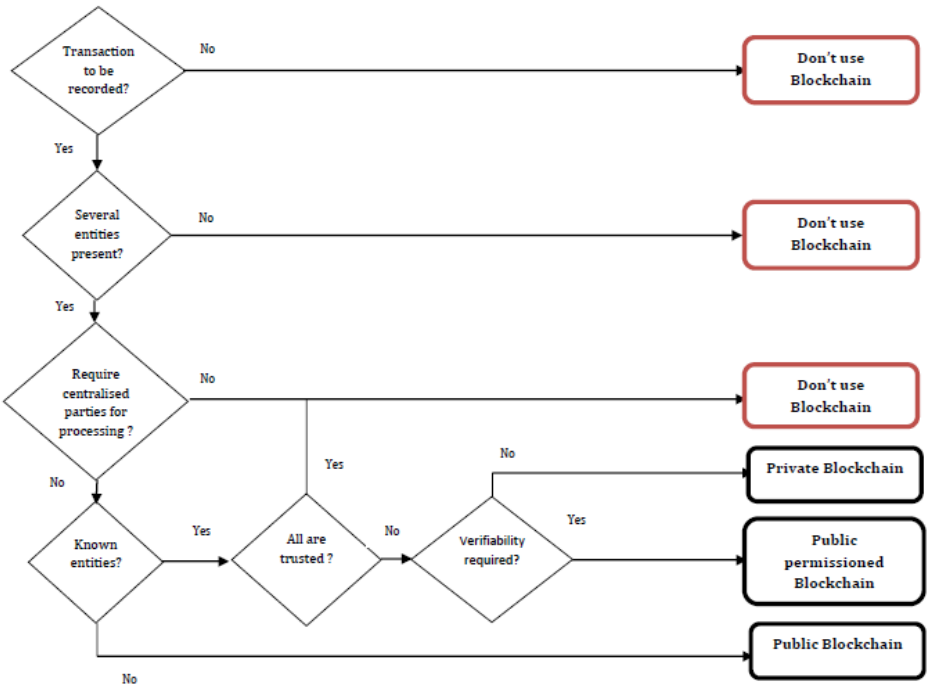

Figure 4. Selecting Blockchain based on constraints

4.1 Implementation of EthereumBlockchain

Ethereum framework is a public blockchain platform that let developers to run and deploy decentralized distributed applications over the network without having to administering the network. Each and every participant in the network is sole responsible for decision making and administering the network. Ether (ETH) is a crypto currency of the Ethereum network. Ether is a peer-to-peer currency. It act as the payment mode for the resource utilization. For any transaction done in a network, transaction fee to be paid and which is of Ethers. In an Ethereum environment, to run and execute any transaction, it consumes Gas. It is termed as execution fee. Upon successful execution, certain amount of Gas is consumed by the network. Gas is generally bought by network peers using Ethers. The smart contracts are piece of code to process any business logic such as transfer of money or assets. These codes are converted to byte code and which are executed by Ethereum Virtual Machine (EVM). EVM understands the smart contracts written in Solidity Language. Once if the smart contract is written and executed, it is stored into EVM in the form of byte code hence ensures the immutability. A Decentralized Application is a combination of front end and smart contracts written as shown in Eqn (1). It is deployed on to the decentralized network.

DApp = frontend + smart contract backend (1)

A sample smart contract is shown in Table 1 which shows the code for EdgeHealthCare.sol that contains code for modules View data and View All data.

Table 1. Smart contract – EdgeHealthCare.sol

```
pragma solidity ^0.5.16;
import "./Set.sol";
import "./PatientData.sol";
contract EdgeHealthCare {
Set.DataresearcherSet;
PatientData[] private patientData;
PatientData[] private nullData;
   mapping(address => bool) rSet;
   mapping(address=>PatientData[]) patientSpecificData;
   constructor() public {}
   function addData(
uint  _encSysPressure, uint  _encDiaPressure,
uint  _encMap, uint  _sysPressure,
uint  _diaPressure, uint  _map,
      string memory  _result
   ) public {
PatientDatanewPatient = new PatientData

(msg.sender,_encSysPressure,_encDiaPressure,_encMap,_sysPressure,_diaPressure,
_map, _result);
patientData.push(newPatient);

patientSpecificData[msg.sender].push(newPatient);
   }
   function registerResearcher() external returns(bool){
rSet[msg.sender] = true;
      return rSet[msg.sender];
   }
   function returnAllData() external view  returns
   (PatientData[]memory){
      if(rSet[msg.sender])
         return patientData;
      else
         return patientData;
   }
   function getPatientData() external view returns
   (PatientData[] memory){
      return patientSpecificData[msg.sender];
   }
   function display() external returns(string memory){
      return "Hello Solidity";
   }
}
```

Patient's data are added to blocks in ethereum which includes parameters of encrypted and decrypted values of patient blood pressure and output of prediction.

React JS is an open source component based frontend User Interface library. JavaScript is used for the application development owing to the Web3.js API with a wide community support. Web3.js is an Ethereum - JavaScript API with a collection of libraries facilitating the communication between a JavaScript application and an Ethereum node using HTTP, IPC or Web Socket.

Ganache is a Test RPC providing a Blockchain emulator with connection with an Ethereum Node. The transactions are processed internally and reduce the Overhead required for running an Ethereum Node. New Blockchain network (workspace) is to be created by specifying the number of accounts and default balance in Ganache set up in the Cloud Server. Public and Private keys for the specified number of accounts are generated. The Blockchain network is set to accept RPC Connections in the specified IP Address. Truffle Box provides a framework to build the Blockchain application with a specified language. The React Box version of Truffle is used to build React JS applications. The application is accessed via the Edge gateway. Wright, K., et al (03 June 2019) proposed smart contracts for Edge Computing. The Smart contracts are stored in the contracts folder. The configurations for running the blockchain application are specified in truffle-configure.js. This file contains configuration for migrating contracts to the Blockchain network. Host IP, Port and network_id are specified in this file. The IP Address of the host from where the RPC connections are accepted is specified and other parameters of the Blockchain network are set.

4.1.1. Deployment

The API calls to the deployed contracts are developed using JavaScript and Web3.js API. A contract instance is created with the address of a smart contract and the methods of the contracts are called from the instance in the javascript application. Once the network is set up in the Cloud and the contracts are stored in the Edge Gateway, the following processes are carried out.The contracts are compiled with the truffle terminal command 'truffle compile'. The contracts are compiled and the ABI generated are stored for reference of the application.The contracts are migrated to the specified Blockchain network (Cloud) with the command 'truffle migrates'. This process requires some gas for migration.The contracts are deployed in the network using 'truffle deploy'.Metamask extension is added to Chrome. It is a Blockchain wallet for Ethereum networks. The wallet is connected to the Blockchain network and the addresses from Ganache are set up using private keys.The react app is started using 'npm run start'. The application then sets up a connection with the Blockchain network and is ready to be used by the user.

The frontend metamask authentication page can be viewed through localhost. Metamask requires password of the Ganache Workspace password to log in and view transactions. The Edge Ganache Network along with user Address displays buttons for scan data, view data, and view all data. These are the functions created in application and it is accessed through Ganache Network. For execution of every transaction it requires transaction ethers to be paid and the same is displayed in the Home page of Edge Ganache Network.

4.2 Implementation of Hyperledger SawtoothBlockchain

The objective of Blockchain is to allow digital information to be distributed and recorded, but not altered. This is where Blockchain plays a vital role. It is used to secure the data and prevent manipulation of data. The Hyperledger is an open source enterprise private blockchain framework to make the data decentralized (Xu, X., et al 2020). There are numerous tools and sub projects available in Hyperledger that differs based on its functionality. Hyperledger is not

supporting any cryptocurrency. Its main focus is to deploy industry oriented blockchain applications.

The private blockchain approach is established in Hyperledger using the channels. Confidentiality of the data is maintained using cryptographic functions even inside the channel. The transactions inside network are triggered using chaincode. As a result of fit, the state change happens. These changes are documented in the ledger. There are three major types of participating peers in the network such as Endorser, Orderer and committing peers. They validate the transactions, orders into block and commit the transaction in a ledger respectively. Generally, consensus mechanism in Hyperledger is the combination of these three consecutive mechanisms (Tanwar et al. 2020).

HyperledgerSawtooth is a Hyperledger sub-project used for developing Blockchain-based solutions that are aimed for use within private enterprises. It is a Blockchain-as-a-service platform that is capable of running personalized smart contracts. The HyperledgerSawtooth was developed by the Linux Foundation in collaboration with IBM, Intel and SAP. The design concept of HyperledgerSawtooth intends to uphold the conception of truly distributed ledgers, thus making the smart contracts more secure and suitable for healthcare. Once the analysis of the encrypted data has been successfully done, the results obtained are securely stored in the ledger.

In HyperledgerSawtooth, blocks are authorized by approved nodes. The validation process verifies transaction permissions to allow the entity to deliver blocks. These blocks are then sent to the transaction scheduler. The communication between the validators of a sawtooth network is made possible by network layer. It performs activities for interconnecting REST API, transaction processors and clients.

As sawtooth doesn't possess block level restrictions, it aids in increasing the performance of transactions. It also put off double spending but still allows multiple transactions. Sawtooth includes Proof of Elapsed Time (PoET) consensus mechanism that follows a lottery mechanism. The architectural overview is shown in Figure 5.

The client can send as many requests as possible and it is not essential to wait for the reply from the other end. Clients interact to validators through REST API which uses JSON standards to deal the requests. Validator validates the signature of a transaction placed by a client. The validated transactions then passed on to transaction processors. Transaction processors are responsible to deal with actual logic with the help of transaction handlers. It determines whether to accept or deny the transactions. Consensus is made through consensus engine and it allows language independent mechanisms.

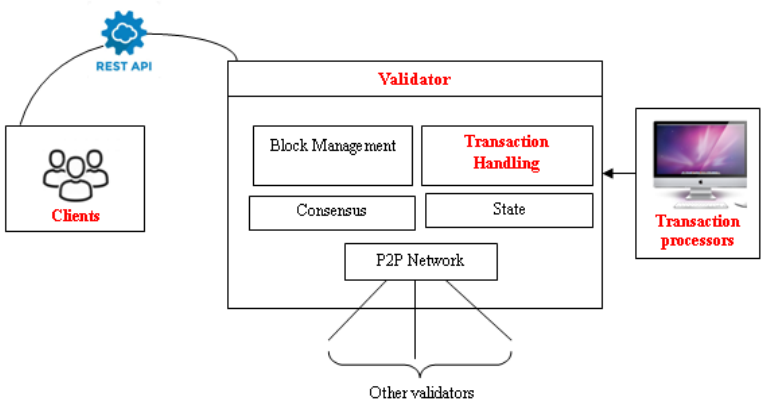

Figure 5. Architecture of Hyperledger Sawtooth

4.2.1. Deployment

The installation of the dependencies made through Ubuntu version 18.04. For the deployment of our application Sawtooth 1.0 version is installed which then compiled in to the local server as a private network. Different entities are added to the network and they were executed in parallel. The entities here are of stake holders who directly involves into the network transactions. The network peers such as of healthcare providers, patients and researcher are added to the configured network along with the validators. Any patients who wish to be admitted in a healthcare clinic should add themselves to the network. The sample query to add a patient to network is shown in Table 2. The access control mechanisms are integrated to the system so as to provide restrictions on handling the sensitive data. Thus ensures implementing the private permissioned network.

Table 2. Query to add patient to Network

```
asyncregisterPatient(ptx, patientID, patientName, address, diseaseType) {
return await
commonFunctions.registerPatient(ptx, patientID, patientName, address, diseaseType);
})
```

To start with the sawtooth environment, the file docker-compose.yml is used. The yml file is used to configure the application's services. After starting the Docker composer, it initializes multi containers as a single service. On running the command 'node index.js' the transaction processor is connected to the sawtooth Validator node and it is set up to get values from the client. The request is sent from the client to the transaction processor and the status of the transaction is reflected in the console log until the status becomes committed then the transaction processor validates the request sent by the client. The data is processed and maintained in the private decentralized network in the form of Hash values.

5 Result Analysis

Empirical results of Blockchain implementations are measured using various benchmarking tools available. The tools are intended to measure various parameters such as

throughput, Latency, Scalability, Fault tolerance, transaction data size, transaction fee, resource consumption and success rate and so on. The identified tools are listed in Table 3.

Table 3. Blockchain Benchmark Tools

Benchmarking Tool	Framework supported
Blockbench	Ethereum, Parity, Hyperledger fabric and Quorum
Hyperledger Caliper	Hyperledger components and Ethereum

Ethereum is an open source public blockchain framework that provides tools for creating DApps. It is different from Hyperledger framework such that it is a private network where only the authorized peers can join the network and participate in mining process. The working efficiency of blockchain network depends on the parameters such as Transaction per Second, scalability and computational heaviness. When the transaction speed is high, it will be possible to send data from one peer to another faster. Simply by changing some parameters one cannot achieve a better transaction speed. Generally, the Bitcoin network calculates number of transactions allowed per block given below. See Eq. (2).

$$\text{No. of transactions per block} = \frac{\text{Block size in Bytes}}{\text{Average Transaction size in Bytes}} \quad (2)$$

Here, Block size parameter is directly proportional to the number of transactions took place per second. Increase in the size of the block would increase the TPS (Transactions per Second). The other way is to regulate the value of Block generation time by fine-tuning the complexity of the puzzle. The Block generation time is inversely proportional to Transactions per Second. Decreasing the block generation time would increase the TPS (Transactions per Second). On an average, Bitcoin blockchain achieves 5 transactions per second.

Ethereum transactions depend on the digital currency called ETH and Gas. Gas is a transaction fee to be paid for running any contract in the network. As per the studies, Ethereum achieves 20 transactions per second in an average. The computational cost of Ethereum transactions for the application in terms of Gas used (gwei) is monitored and values are shown in Figure 6.

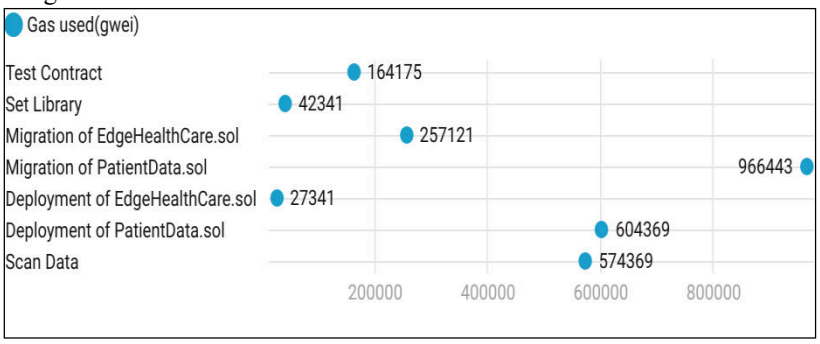

Figure 6. Gas used for Ethereum transactions

Hyperledger framework does not possess cryptocurrency mechanisms. Hence, the transaction evaluation purely depends on the transaction time per second. The intention of the Hyperledger private network is to create enterprise blockchain network. Upon Executing the Application in both Ethereum and Hyperledger we estimated the Number of Transactions executed in ten minutes in the native machine and the result is depicted in Figure 7 and Figure 8 respectively.

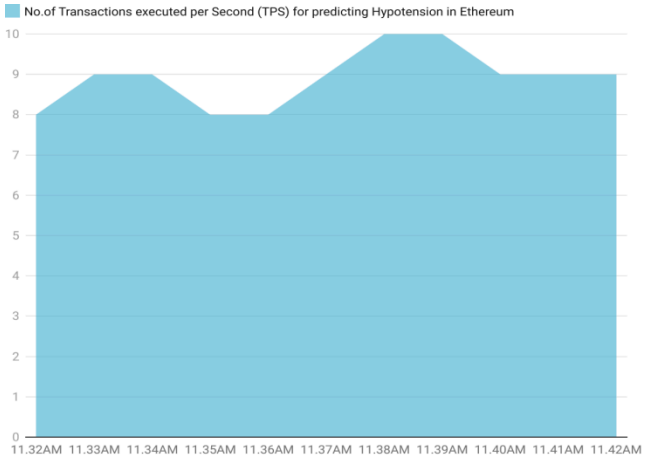

Figure 7. Transactions executed per second in Ethereum

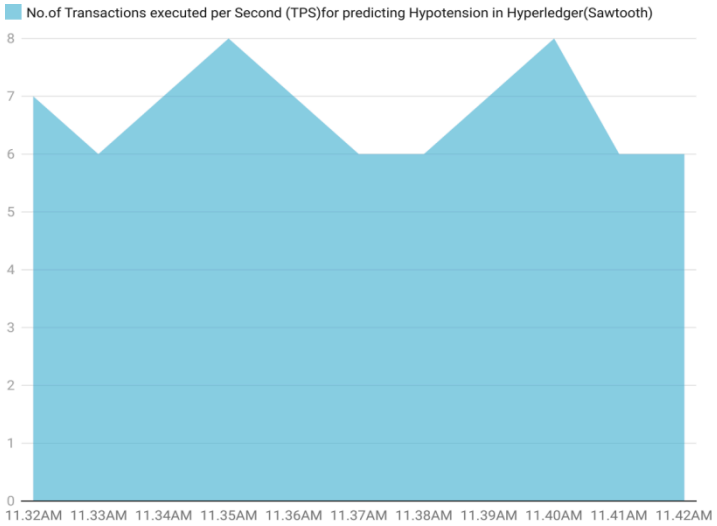

Figure 8. Transactions executed per second in Hyperledger sawtooth

Thus, the working efficiency of various blockchain networks such as Ethereum and HyperledgerSawtooth is analyzed for the healthcare application of predicting Hypotension which also incorporates Homomorphic Encryption schemes to secure the patient information. The Framework Parameter Comparison is shown in Table 4. Also, implementation results are compared against various parameters.

Table 4. Framework comparison

Framework	Network Type	Consensus Algorithms
Bitcoin	Public	Proof of Work (PoW)
Ethereum	Public	Proof of Stake (PoS)
Hyperledger (Sawtooth)	Private	Proof of Elapsed Time (PoET)

6 Conclusion and Future Enhancements

Dataset [systolic and diastolic pressure] is collected from BP meter. The data is sent to the edge gateway via Bluetooth. Further, the data is retrieved from edge gateway through web scraping. Homomorphic Encryption Scheme is applied and analysis is performed if a person is prone to hypotension. If Mean Arterial Pressure was greater than 50 gm/dl, then the patient is prone to hypotension. Patient's data is stored in Blockchain for the requirement of immutable records. Smart contracts are written for storing a patient's record in a Blockchain Network and getting patient records with different views according to the user [patient, researcher]. A decentralized public and private Blockchain network with a web application is developed using these contracts with Javascript and react JS. Web3 Library is used in this application to establish a connection with the Ethereum node. This application thus provides an enhanced layer of security and immutability of patient data.

This satisfies the project requirements, as Homomorphic Encryption Scheme ensures security in predictive analysis, Edge Computing systems ensure remote accessibility and Blockchain ensures immutability of record transaction and React JS offers user interface. The various parameters to be considered before choosing blockchain for the application are analyzed.

Future enhancements include increasing the number of transactions mined per block in Ethereum with Proof of Stake algorithm rather than Proof of Work algorithm thereby improving efficiency of Blockchain network. The throughput of sawtooth implementation is to be addressed. Upon solving scalability and throughput issues in current systems, implementation of hybrid and consortium blockchain for an application shall be focused.

References

[1] Al-Mashhadi, M. H. &Khalf, A. A. (2019). Hybrid Homomorphic Cryptosystem for Secure Transfer of Color Image on Public Cloud. IJCSNS International Journal of Computer Science and Network Security (pp.49-54)

[2] Bing Chen (March 2018). Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. IEEE Access, vol. 6 (pp-2-29).

[3] Bos, J.W., Lauter, K. E., &Naehrig, M. (2014). Private Predictive Analysis on Encrypted Medical Data. Journal of biomedical informatics, 50 (pp. 234-43).

[4] Forouzanfar, M., Ahmad, S., Batkin, I., Dajani, R. H., Groza Z. V &Bolic, M. (February 2020) Edge Computing Integrated with Blockchain Technologies. Research gate Complexity and Approximation (pp.268-288).

[5] Forouzanfar, M., Ahmad, S., Batkin, I., Dajani, R. H., Groza, Z. V., &Bolic, M. (September, 2015). Model-Based Mean Arterial Pressure Estimation Using Simultaneous Electrocardiogram and Oscillometric Blood Pressure Measurements. IEEE Transactions on Instrumentation and Measurement (pp.2-9).

[6] Kubendiran, M., Singh, S., Sangaiah, A. K. (2019). Enhanced Security Framework for E-Health Systems using Blockchain. J. Inf. Process. Syst. 15, 239–250.

[7] Li, J., Li, R., Chen, Z., Deng, G., Wang, H., Mavromoustakis, C., Song, H., and Ming, Z., (December 10, 2017). Design of Continuous Blood Pressure Measurement System Based on Pulse Wave and ECG Signals. IEEE Journal of Translational Engineering in Health and Medicine (pp.5-24).

[8] Nyamtiga, W. B., Rathore, S., Sung, Y., Sicato, S. C. J., & Park H. J. (25 July 2019). Blockchain-Based Secure Storage Management with Edge Computing for IoT. Electronics. 8. 828 (pp-2-20).

[9] Shen, Z., Miao, F., Meng, Q., & Li, Y. (April, 2015). Cuffless and Continuous Blood Pressure Estimation based on Multiple Linear Regression. 5th International Conference on Information Science and Technology [ICIST] (pp.1-5).
[10] Wright, K., Martinez, M., Chadha, U., Krishnamachari, B. (03 June 2019). SmartEdge: A Smart Contract for Edge Computing. 2018 IEEE International Conference on Internet of Things (iThings) & IEEE Green Computing and Communications 18735147.
[11] Xu, L. L. C., Li, D., & Wu, W. (February 2020). EdgeComputing Integrated with Blockchain Technologies", Du DZ., Wang J. (eds) Complexity and Approximation vol 12000. Springer, Cham (pp.1-17).
[12] Zhang, J., Chen, B., Zhao, Y., Cheng, X., Hu, F., (28 March 2018). Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. IEEE Access vol. 6 18209 – 18237
[13] Jennath, H. S., Anoop, V. S., &Asharaf, S. (2020). Blockchain for Healthcare: Securing Patient Data and Enabling Trusted Articial Intelligence. International Journal of Interactive Multimedia & Artificial Intelligence, 6(3).
[14] Fan, C., Ghaemi, S., Khazaei, H., &Musilek, P. (2020). Performance evaluation of blockchain systems: A systematic survey. IEEE Access, 8, 126927-126950.
[15] Satamraju, K. P. (2020). Proof of concept of scalable integration of internet of things and blockchain in healthcare. Sensors, 20(5), 1389.
[16] Kumari, K. A., Padmashani, R., Varsha, R., &Upadhayay, V. (2020). Securing Internet of Medical Things (IoMT) using private blockchain network. In Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm (pp. 305-326). Springer, Cham.
[17] Dharani, D., Kumari, K. A., Aishwarya, S., Sangavi, G. M., &Lavanya, N. A Robust Blockchain Framework for Healthcare Information System.
[18] Katuwal, G. J., Pandey, S., Hennessey, M., &Lamichhane, B. (2018). Applications of blockchain in healthcare: current landscape & challenges. arXiv preprint arXiv:1812.02776.
[19] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.
[20] Zhou, Q., Huang, H., Zheng, Z., &Bian, J. (2020). Solutions to scalability of blockchain: A survey. IEEE Access, 8, 16440-16455.
[21] Xu, X., Sun, G., Luo, L., Cao, H., Yu, H., &Vasilakos, A. V. (2021). Latency performance modeling and analysis for hyperledger fabric blockchain network. Information Processing & Management, 58(1), 102436.
[22] Davies, S. J., Vistisen, S. T., Jian, Z., Hatib, F., &Scheeren, T. W. (2020). Ability of an arterial waveform analysis–derived hypotension prediction index to predict future hypotensive events in surgical patients. Anesthesia& Analgesia, 130(2), 352-359.
[23] Cao, B., Wang, X., Zhang, W., Song, H., &Lv, Z. (2020). A many-objective optimization model of industrial internet of things based on private blockchain. IEEE Network, 34(5), 78-83.
[24] C. Amuthadevi, D. S. Vijayan, Varatharajan Ramachandran, "Development of air quality monitoring (AQM) models using different machine learning approaches", Journal of Ambient Intelligence and Humanized Computing, https://doi.org/10.1007/s12652-020-02724-2
[25] Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. IEEE Access, 8, 107112-107123.