Smart Patient Vitals Recording System

J COMPONENT FINAL REPORT

Submitted in the fulfilment for the J Component of

Privacy and Security in IoT (BCT3004)

in
B.Tech. Computer Science and Engineering
(with specialization in IOT)

By

A.N.Loganathan (19BCT0081)
V. Hari (19BCT0080)
Syed Mohammmed Buhari P (19BCT0102)

Under the guidance of

Dr. ANISHA M. LAL

SCOPE

VIT®
UNIVERSITY
(Estd. u/s 3 of UGC Act 1956)
VELLORE ■ CHENNAI
www.vit.ac.in

School of Computer Science and Engineering

Winter Semester 2021-22

Abstract:

This paper will discuss the major aspects that go into designing a system which will be handling medical records and how they can be used along with blockchain and IoT technology. It will look into how these two technologies can go in together and come up with a technology sensing recording product that is safe, secure and most of all smart. With the trends of increasing interest in IoT systems comes the question of security based questions for these machines and how secure the nodes we are using to sense patient details are. In order to give that security we have decided to come up with a IoT sensing technology which will be combining IoT sensors and WSNs to a blockchain backend based on the ethereum blockchain and will make use of smart contracts for security. A conclusion will summarise our findings and challenges along with our approaches. References will be provided for further research and investigation.

Introduction:

Medical Record: To improve our medical service for our patients around the world we must have a readily available standardised medical record history any time anywhere. We must also overcome many of the challenges like record type, storage, medical records and reports, ownership and reading rights, data security, patient's right of knowledge.

Medical records can be or many types like test reports, word documents, images, videos and data. They are important in our medical history. They are different formats which have different formats.

Central storage is important too. It is because many doctors may not have their own or may have a different medical record system. Record formats also perform a great threat to the standardisation of them. Nevertheless formats can mostly be converted from one to another. Another problem is the increasing storage for the records, and all old records must be archived regularly for future use.

HK eHealth. There are few other criteria imposed by ehealth system (eHR) by Hong Kong government [1]. Those include (1) government-led, (2) data privacy and security, (3) not compulsory, (4) open and pre-defined common standards, (5) building block approach. Every record access of patient's record will be recorded and notification will be sent to the corresponding patient. The record data are very restricted, including lab tests, x-ray, etc. Medical doctor's reports may not be there. All authorised medical personnel may read the patient's records if the corresponding patient agrees.

Tokenization. Tokenization is very important in this respect of medical reports sharing. Token will not depend on operating systems and does not include content within. The storage server can examine the validity of the token before sending out the required report(s). The report owner can sign the request token sent by specific viewer with confidence.

Literature Survey/ Related Work:

[1] A comprehensive review on blockchain and Internet of Things in healthcare . Transactions on Emerging Telecommunications Technologies

The applications of IoT in healthcare are classified as follows.

i Smart Healthcare:

Healthcare is human life's most vital component. The Pattern of IoT intervention in healthcare began with the phenomenon of remote patient monitoring. This prodigy has now been reinforced, and different healthcare pieces of equipment are working on IoT-based principles. From providing data analysis, end-to-end connectivity, management of drugs and medicine, and remote medical assistance, IoT applications in healthcare are manifold.

ii Medical alert system:

Medical alert systems are now being used to monitor the patients' safety and security. These can be used as wearables that if a patient becomes motionless for a more considerable period, then alerts can be generated to their families

iii Clinical decision support systems (CDSS):

CDSS systems are being proposed using IoT majorly for chronic diseases. The patients' records can be monitored more smartly and intelligently, leading to a healthcare ecosystem benchmark.

iv Surgical robotics:

Surgical robotics is a new reality these days. Though some limitations are involved, surgical robotics have given more precise results than human doctors. The technology is entirely in the spotlight and is expected to revolutionize the healthcare industry.

v Smart hospital:

Managing hospital infrastructure is a tedious task, especially when managing lengthy paper records. The smart solutions offered by IoT can help the medical staff easily monitor and manage long paper-based records efficiently. The automation can help to optimize the existing systems used in the hospitals, providing a sense of reliability and ease of use by the medical staff.

vi Medical biometric domain:

Biometric systems are based on unique features of individuals such as fingerprint scanner, retina scanner, voice recognition, etc., and are hence used for critical security systems.

vii Telemedicine:

IoT is enhancing the telemedicine industry by providing quality of care to the people involved. Smart medication is now coming in place to remind the patients to take their medicines on time. The adoption of IoT with telemedicine in the healthcare industry is a bit slow now, but it will steadily progress at its pace.

Need and evaluation of blockchain technology and IoT in healthcare :

Leading healthcare organizations are looking for new opportunities to combine the IoT and blockchain technology with machine learning and artificial intelligence (AI) to enhance patient outcomes and streamline daily healthcare procedures. Hence, the word “Internet of Healthcare Things” (IoHT) is the most recent word being used in the health industry that corresponds to a linked device or a platform that can interact with the healthcare IT system. Blockchain and IoHT in the healthcare ecosystem,from monitoring patients to managing assets and tracking inventory, several healthcare companies are making use of IoHT.

[2] Electronic health records in a Blockchain: A systematic review.

Identity:

Information from the individual device will get easily monitored in the blockchain-based IoT systems as unique identifiers are used for each device. Similarly, Blockchain in IoT systems can provide reliable aggregated certification and identity verification.

Decentralization:

The decentralization of IoT systems based on blockchain will eradicate some centralization architectural issues like centrally controlled failure and performance bottlenecks.

Security:

IoT implementations’ operational data would ensure security as every operation used is guarded with cryptography. With blockchain applications, conventional IoT procedures could be redesigned to deal with the healthcare ecosystem.

Immutability:

The unalterable nature of IoT systems based on the blockchain can develop patients' confidence as they monitor and ascertain every transaction with little or no fear of manipulation. Besides, this property shall improvise the traceability of information sent by the IoT sensors.

Reliability:

IoT data in the blockchain can stay unchanged and dispersed over time.

Secure code deployment:

Using the robust-immutable blockchain capacity, code could be safely and reliably inserted through the systems

[3] Blockchain-based distributed patient-centric image management system

In recent years, many researchers have focused on developing a feasible solution for storing and exchanging medical images in the field of health care. Current practices are deployed on cloud-based centralized data centers, which increase maintenance costs, require massive storage space, and raise privacy concerns about sharing information over a network. Therefore, it is important to design a framework to enable sharing and storing of big medical data efficiently within a trustless environment. In the present paper, they propose a novel proof-of-concept design for a distributed patient-centric image management (PCIM) system that is aimed to ensure safety and control of patient private data without using a centralized infrastructure. In this system, they employed an emerging Ethereum blockchain and a distributed file system technology called Interplanetary File System (IPFS). Then, they implemented an Ethereum smart contract called the patient-centric access control protocol to enable a distributed and trustworthy access control policy. IPFS provides the means for decentralized storage of medical images with global accessibility. The PCIM system ensures a high level of data security by applying asymmetric cryptographic techniques. They describe how the PCIM system architecture facilitates the distributed and secured patient-centric data access across multiple entities such as hospitals, patients, and image requestors. Finally, they conducted experiments to test the proposed framework within the Windows environment and deployed a smart contract prototype on an Ethereum testnet blockchain. The experimental results demonstrated that the proposed scheme is feasible.

[4] A privacy-preserving healthcare framework using hyperledger fabric

Electronic health record (EHR) management systems require the adoption of effective technologies when health information is being exchanged. Current management approaches often face risks that may expose medical record storage solutions to common security attack vectors. However, healthcare-oriented blockchain solutions can provide a decentralized, anonymous and secure EHR handling approach. This paper presents PRE HEALTH, a privacy-preserving EHR management solution that uses distributed ledger technology and an Identity Mixer (Idemix). The paper describes a proof-of-concept implementation that uses the Hyperledger Fabric's permissioned blockchain framework. The proposed solution is able to store patient records effectively whilst providing anonymity and unlinkability. Experimental performance evaluation results demonstrate the scheme's efficiency and feasibility for real-world scale deployment.

[5] On the economics of knowledge creation and sharing

This work bridges the technical concepts underlying distributed computing and blockchain technologies with their profound socioeconomic and sociopolitical implications, particularly on academic research and the healthcare industry. Several examples from academia, industry, and healthcare are explored throughout this paper. The limiting factor in contemporary life sciences research is often funding: for example, to purchase expensive laboratory equipment and materials, to hire skilled researchers and technicians, and to acquire and disseminate data through established academic channels. In the case of the U.S. healthcare system, hospitals generate massive amounts of data, only a small minority of which is utilized to inform current and future medical practice. Similarly, corporations too expend large amounts of money to collect, secure and transmit data from one centralized source to another. In all three scenarios, data moves under the traditional paradigm of centralization, in which data is hosted and curated by individuals and organizations and of benefit to only a small subset of people.

[6] Blockchain for health data and its potential use in health it and health care related research.

Bitcoin is based on open-source cryptographic protocols and has proven to be a very safe platform for crypto-currency exchange. While the identities behind some Bitcoin transactions remain unknown, the platform provides transparency as anyone can access the blockchain and see balances and transactions for any Bitcoin address. Lack of data privacy and the absence of robust security make the Bitcoin public blockchain unsuitable for a health blockchain that requires privacy and controlled, auditable access. Additionally, the Bitcoin standard for block size and maximum number of transactions per second present scalability concerns for large-scale and widely used blockchain applications. Private and consortium led blockchains would address the privacy, security and scalability concerns. However, these blockchains would pose different challenges as they run the risk of not being vendor neutral and do not use open standards.

Technical Advantages of a Healthcare Blockchain :

Blockchain technology offers many advantages for health care IT. Blockchain is based on open source software, commodity hardware, and Open API's. These components facilitate faster and easier interoperability between systems and can efficiently scale to handle larger volumes of data and more blockchain users.

The architecture has built-in fault tolerance and disaster recovery, and the data encryption and cryptography technologies are widely used and accepted as industry standards. The health blockchain would be developed as open-source software. Open-source software is peer-reviewed software developed by skillful experts. It is reliable and robust under fast- 7 changing conditions that cannot be matched by closed, proprietary software. Open-source solutions also drive innovations in the applications market. Health providers and individuals would benefit from the wide range of application choices and could select options that matched their specific requirements and needs.

Blockchain would run on widely used and reliable commodity hardware. Commodity hardware provides the greatest amount of useful computation at low cost. The hardware is based on open standards and manufactured by multiple vendors. It is the most cost effective and efficient architecture for health and genomic research. Excess blockchain hardware capacity could be shared with health researchers and facilitate faster discovery of new drugs and treatments. Blockchain technology also addresses the interoperability challenges within the health IT ecosystem.

[7] A privacy-preserving healthcare framework using hyperledger fabric

Electronic health record (EHR) management systems require the adoption of effective technologies when health information is being exchanged. Current management approaches often face risks that may expose medical record storage solutions to common security attack vectors. However, healthcare-oriented blockchain solutions can provide a decentralized, anonymous and secure EHR handling approach. This paper presents PRE HEALTH, a privacy-preserving EHR management solution that uses distributed ledger technology and an Identity Mixer (Idemix). The paper describes a proof-of-concept implementation that uses the Hyperledger Fabric's permissioned blockchain framework. The proposed solution is able to store patient records effectively whilst providing anonymity and unlinkability. Experimental performance evaluation results demonstrate the scheme's efficiency and feasibility for real-world scale deployment.

[8] An Internet of Things-Based System Integrated with Blockchain to Manage Patient Data in the Healthcare Sector

This paper proposes Blockchain based IoT systems to improve the inefficient functionalities of healthcare systems by integrating blockchain with Iot systems. This approach enables traceability and patient centered data.

This paper takes advantage of distributed IoT artifacts contribution and decentralized properties of Blockchain to deliver secure and traceable events on a public Blockchain. And they use Raspberry Pi's as client nodes to synchronize data directly to the blockchain.

The IoT wearable device of this system will be designed to capture the vital signs on a patient's body through sensors embedded within the device. The output results of the IoT wearable device will be communicated on an application interface connected to the public Blockchain. The use of a Blockchain on this system is presented to record all the transactions on a public ledger as the results of having the most improved efficient healthcare records for proper diagnosis to take place on time. However, the patient manages the permission on the public ledger of the system, deciding on who should access the information on the ledger.

This IoT system will be integrated with a public ethereum Blockchain that will also provide an encryption property as an extra feature to protect the privacy of data before storing it on a public Blockchain. Proposes the use of Proof of Authority (PoA) for our consensus mechanism. The nature of PoA improves time efficiency on incoming transactions by mining them into the Blockchain through voting/agreements. Also increases the speed in which transactions will be mined into the Blockchain without any further delay.

The proposed idea is to use Raspberry Pi's to act as client nodes. A BootNode is basically used to assign (peer) new ethereum nodes to the Blockchain network. Not only does the BootNode gives the privileges to the new nodes to be part of the network but it also alerts the already existing nodes about the arrival of newer nodes to the system. Both replicas of the BootNode in our system will monitor and scale the incoming/outgoing requests and the interactions of nodes across the network.

[9] Blockchain-based remote patient monitoring in healthcare 4.0

In this paper, they provided insights to the blockchain-based RPM system for healthcare sector. Also presented the blockchain-based system architecture to overcome the security and privacy issues of traditional systems. And Discussed various research challenges of blockchain in the healthcare sector.

The current traditional system has various holes such as insider attacks, And not getting any updated real time information, Lack of transparency of information stored by doctors and patients. And no digital signed agreement as healthcare providers and caregivers.

Blockchain is a distributed ledger where multiple parties are connected and work together. It maintains the immutable log of transactions which protects data tampering. Blockchain allows doctors and patients to access the updated healthcare data instantly as each participating member of the blockchain is having a copy of the entire blockchain. The authenticity of data in the block of a blockchain can be well-taken care of by the smart contracts and consensus algorithm.

Electronic health records can be maintained. They are decentralized ledgers in EHR means that data cannot be held by any intruder. In a blockchain, each node has an updated copy of the ledger, and each node validates the copy thus the intruder cannot get control all over the ledger. In a Permissioned blockchain, doctors, hospitals, labs are able to access the patient's data after taking permission from the patient.

For maintaining the security of the real-time data, blockchain uses the cryptography algorithms like RSA, SHA, and hash function where every block is connected through a previous block and one unique random number that can be very difficult to guess by an intruder or attacker.

When the information has been received by the doctor who has connected in a blockchain network. They have no rights to access their data without taking permission from the patient. The first doctor can request the patient, if the patient allows accessing their data then a doctor can use their data for further process. A doctor gives a few suggestions for taking medicine, treatment, and others that are required for the patient. The doctor also can share a few diagnosis information to laboratories for a disease diagnosis of the patient. Thus, RPM saves the time of the patient and gets quality care at a very reasonable cost.

[10] Continuous patient monitoring with a patient centric agent: A block architecture

The Internet of Things (IoT) has enabled a variety of services to be provided without the need for human involvement, including continuous remote patient monitoring (RPM). RPM is difficult to implement due to the complexity of RPM topologies, the quantity of data sets created, and the restricted power capacity of devices. We propose a tier-based End to End architecture for continuous patient monitoring in this study, with a patient centric agent (PCA) at its heart. When data pouring from body area sensors needs to be securely stored, the PCA controls a blockchain component. A lightweight communication protocol is included in the PCA-based architecture to ensure data security across multiple segments of a continuous, real-time patient monitoring system. Data is inserted into a database as part of the architecture.

The design comprises storing data in a personal blockchain to allow for data sharing among healthcare experts and integration into electronic health records while maintaining privacy. The blockchain has been modified for RPM, including allowing the PCA to choose a Miner to reduce computational effort, allowing the PCA to manage multiple blockchains for the same patient, and replacing each block with a prefix tree to reduce energy consumption and incorporate secure transaction payments. The PCA-based End to End architecture improves security and privacy in RPM, according to simulation results.

[11] Healthcare blockchain system using smart contracts for secure automated remote patient monitoring

As the use of Internet of Things (IoT) devices and other remote patient monitoring systems grows, security issues concerning data transfer and logging emerge. We suggest using blockchain-based smart contracts to assist secure analysis and management of medical sensors in order to handle the protected health information (PHI) generated by these devices. We designed a system in which the sensors communicate with a smart device that calls smart contracts and records all occurrences on a private blockchain based on the Ethereum protocol. By sending messages to patients and medical experts in real time, this smart contract system would facilitate real-time patient monitoring and medical interventions while also keeping a secure record of who initiated these activities. This would fix a lot of security issues.

This would resolve many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all involved parties in a HIPAA compliant manner.

[12] Secure authentication for remote patient monitoring with wireless medical sensor networks

Wireless medical sensor networks, or WMSNs, are critical for remote healthcare monitoring. Sensor nodes are implanted in the patient's body to capture physiological data and send it across an unsecured channel in remote healthcare monitoring. The health information of a patient is extremely delicate and vital. Any tampering with physiological data will result in incorrect diagnoses and harm to the patient's health. As a result, for accessing real-time health information from patients through an insecure connection, privacy, data security, and user authentication are critical. This paper presents a secure and reliable two-factor based remote user authentication mechanism for healthcare monitoring in this regard. The proof of authentication was done using BAN logic, which ensures that the proposed technique enables mutual authentication and session key agreement.

The informal security verification demonstrates that the created protocol is resistant to a variety of security threats. The suggested method was simulated using the AVISPA tool, and the simulation results show that it is secure against both active and passive attacks. The suggested protocol is efficient in terms of security features, calculation cost, communication cost, and execution time, according to the results of the performance evaluation.

Authentication Remote patient monitoring establishes a reliable and convenient link between the patient at home and the doctor at the clinic. The doctor has access to the patient's status at any time and from any location, and the patient receives adequate therapy from the doctor over an insecure channel. If someone illegally obtains a patient's information, the patient's privacy will be compromised. User authentication is one of the most significant security mechanisms for preventing unauthorised users from accessing real-time data; it secures both session key agreement and mutual authentication between participant entities.

[13] Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals

Many healthcare applications have been developed in recent years to improve the healthcare business. Electronic healthcare research and industry have been transformed by recent advances in information technology and blockchain technology. The human healthcare system has been improved and safeguarded thanks to the development of tiny healthcare sensors for monitoring patient vital signs. The proliferation of portable health devices has improved the quality of health-monitoring status, both at the activity/fitness level for self-health tracking and at the medical level, by providing practitioners with more data and the opportunity for early diagnosis and treatment recommendations. Interaction with and collecting of electronic medical records require data security and comfort while providing personal medical information. Current systems, on the other hand, struggle to achieve these objectives due to their limitations.

The new solutions should be aimed at improving data access, and they should be overseen by the government in terms of privacy and security regulations, to ensure that data for medical purposes is reliable. Blockchain is paving the way for a change in the traditional pharmaceutical sector, with benefits such as data transparency and privacy. In this work, we propose a new infrastructure for monitoring patient vital signs based on blockchain smart contracts. Hyperledger fabric, an enterprise-distributed ledger platform for constructing blockchain-based applications, is used to design and create the suggested system. Patients benefit from this strategy since it offers them with a broad, immutable history log as well as worldwide access to medical information at any time and from anywhere. Libelium e-Health is a service provided by Libelium.

To collect physiological data, the Libelium e-Health toolset is employed. A standard benchmark tool called Hyperledger Caliper is used to evaluate the performance of the proposed and developed system in terms of transaction per second, transaction latency, and resource utilisation.

The proposed approach outperforms the standard health-care system in terms of patient data monitoring.

[14] A smart patient health monitoring system using IoT

Healthcare monitoring systems have become one of the most important systems in recent years, and they have become increasingly technological. Humans are confronting an issue of untimely death owing to numerous illnesses, which is caused by a lack of timely medical care for patients. The main goal was to create a dependable patient monitoring system based on IoT so that healthcare professionals may monitor their patients who are either hospitalised or at home using an IoT-based integrated healthcare system in order to ensure improved patient care. Sensors, a data gathering unit, and a microprocessor were designed for a mobile device-based wireless healthcare monitoring system that can offer real-time online information about a patient's physiological status.

The proposed patient health monitoring system can be extremely useful in emergency situations because it can be tracked, recorded, and saved as a database on a daily basis. In the future, the IoT device will be integrated with cloud computing, allowing the database to be shared across all devices. Intensive care and therapy are provided at hospitals.

[15] Smart healthcare support for remote patient monitoring during covid-19 quarantine

Since the advent of the novel coronavirus (COVID-19) illness pandemic in 2019, social separation and quarantining have become normal procedures around the world. Frequent hospital contact visits are discouraged due to full adoption of the above control procedures. However, some people's physiological vital needs still necessitate routine monitoring in order to live a healthier lifestyle. Contact-based hospital visits are now considered non-obligatory, thanks to recent technological breakthroughs in the areas of Internet of Things (IoT) technology, smart home automation, and healthcare systems. To that purpose, a remote smart home healthcare support system (ShHeS) is proposed for monitoring patients' health and obtaining prescriptions from doctors while at home. Aside from that, doctors can use the system to diagnose illnesses.

Smart home technologies promote healthy living and better healthcare support services for the elderly and handicapped, allowing them to live independently and comfortably at home rather than in nursing homes, hospitals, or other confinement facilities. As part of the smart home automation system, the healthcare module will improve healthcare facilities for patients at home or in remote places outside of hospitals. As a result, there is a decrease in depression caused by loneliness in hospital wards for patients. Doctors may keep an eye on their patients from the comfort of their own offices, give medication, and observe crucial health metrics for remote diagnosis. Furthermore, the rapid advancement of software and hardware innovations in the smart home healthcare system allows patients, particularly the elderly, to benefit.

Methodology

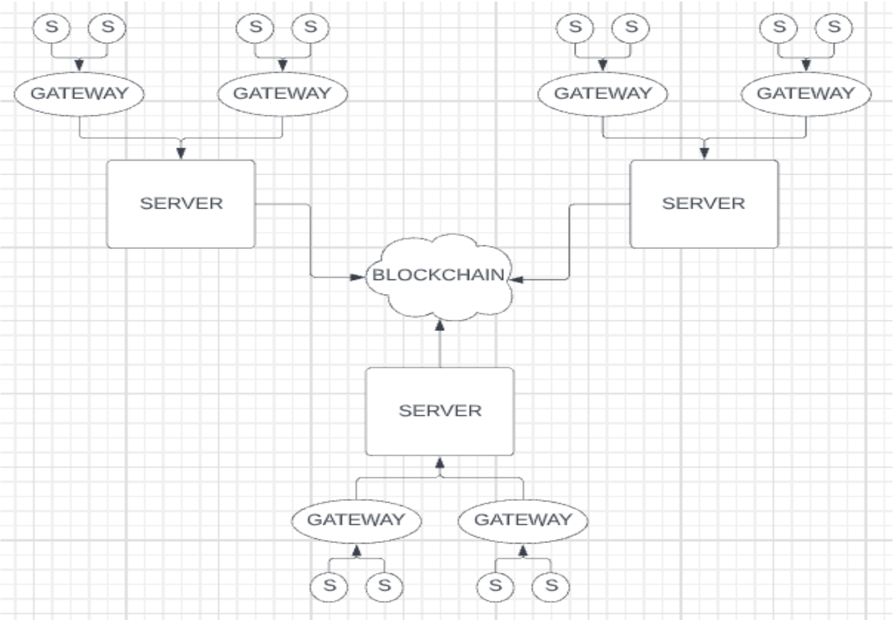
Objective:

IoT sensors collect significant amounts of sensitive patient data, raising privacy and security concerns as well as introducing a plethora of new threats. A significant concern is the need for suitable security procedures. Despite the existence of numerous IoT security standards, such as two-factor authentication and biometrics, blockchain technology can provide an exciting IoT data privacy solution. Limited access and the capacity for sensors to shut down in the event of a compromised environment are among the security protections built into blockchain, lowering the risk of data manipulation.

Modules :

- Frontend React GUI
- NodeRed
- Ganache (Private Blockchain)
- Node Server
- IOT Devices

Overall framework or architecture



Module by module in detail :

Ganache:

- It is a personal Ethereum blockchain which you can use to run tests, execute commands, and inspect state while controlling how the chain operates.
- Here in this project, we use it for Creating a private Ethereum blockchain, in which we store the collected sensor data.

Node-red:

- It is a programming tool for wiring together hardware devices, APIs and online services in new and interesting ways. It provides a browser-based editor that makes it easy to wire together flows that can be deployed to its runtime in a single-click.
- It is built on Node.js. We made a simple flow to Add a new patient, thermometer, pulse oximeter And to update the data periodically.

Node:

- It is an open source, backend javascript runtime environment that handles the server.

React UI:

- A Front-end framework to develop web user interfaces as components.

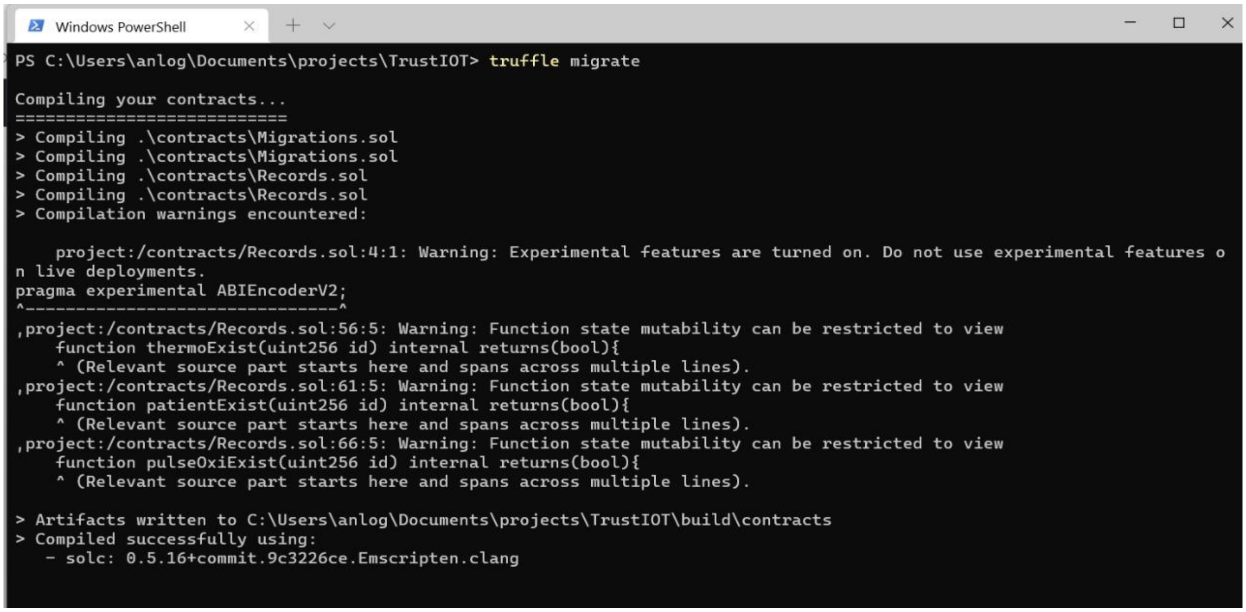
We implemented smart contracts using the Ethereum coding language Solidity. We are not running our operations and smart contracts on the public Ethereum blockchain, but on a separate, private chain using Ethereum’s protocol.

So first we simulate the flows of sensor nodes and its data using Node-red. And then, we send the collected data to the node server to handle the data. Node server pushes the data into the Ethereum private blockchain which can then be retrieved to be displayed in the UI (to doctors, patients).

Experimental Results and Discussion

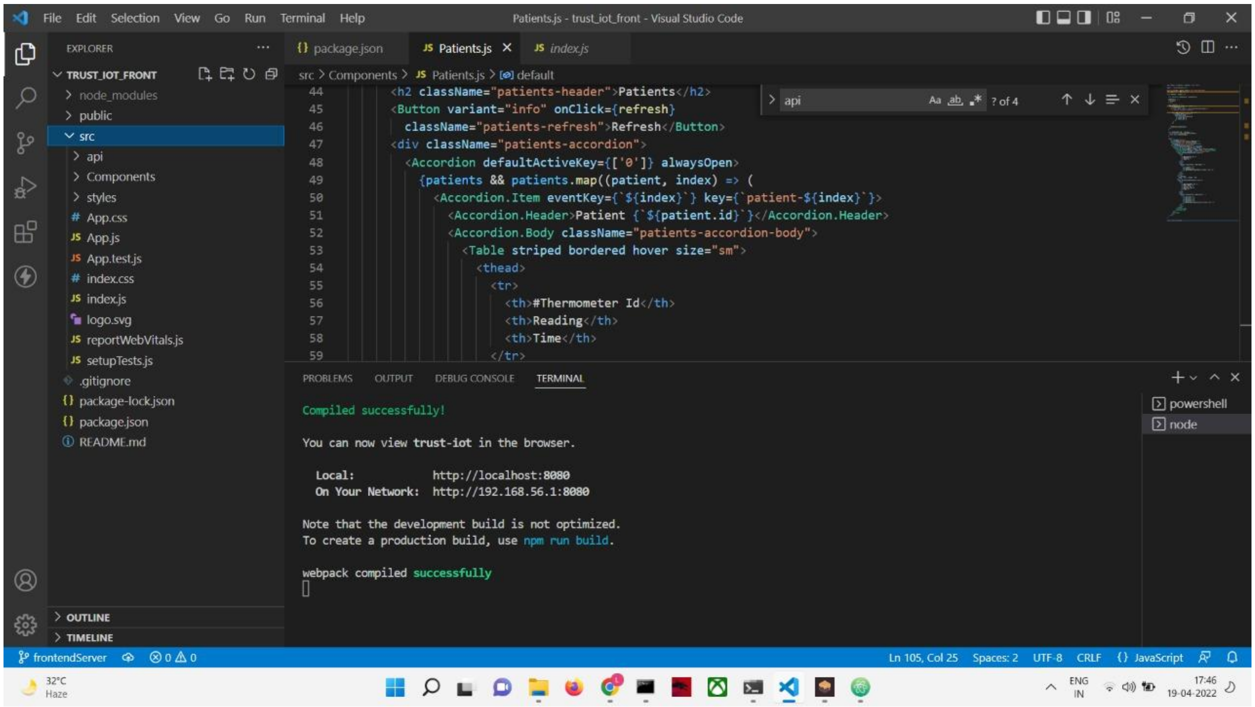
Experimental Results/ Simulation results:

Pushing the smart contract to the private Blockchain and starting the backend server



```
PS C:\Users\anlog\Documents\projects\TrustIOT> truffle migrate

Compiling your contracts...
===========================
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Records.sol
> Compiling .\contracts\Records.sol
> Compilation warnings encountered:

    project:/contracts/Records.sol:4:1: Warning: Experimental features are turned on. Do not use experimental features o
n live deployments.
pragma experimental ABIEncoderV2;
^-------------------------------^
,project:/contracts/Records.sol:56:5: Warning: Function state mutability can be restricted to view
    function thermoExist(uint256 id) internal returns(bool){
    ^ (Relevant source part starts here and spans across multiple lines).
,project:/contracts/Records.sol:61:5: Warning: Function state mutability can be restricted to view
    function patientExist(uint256 id) internal returns(bool){
    ^ (Relevant source part starts here and spans across multiple lines).
,project:/contracts/Records.sol:66:5: Warning: Function state mutability can be restricted to view
    function pulseOxiExist(uint256 id) internal returns(bool){
    ^ (Relevant source part starts here and spans across multiple lines).

> Artifacts written to C:\Users\anlog\Documents\projects\TrustIOT\build\contracts
> Compiled successfully using:
   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang
```

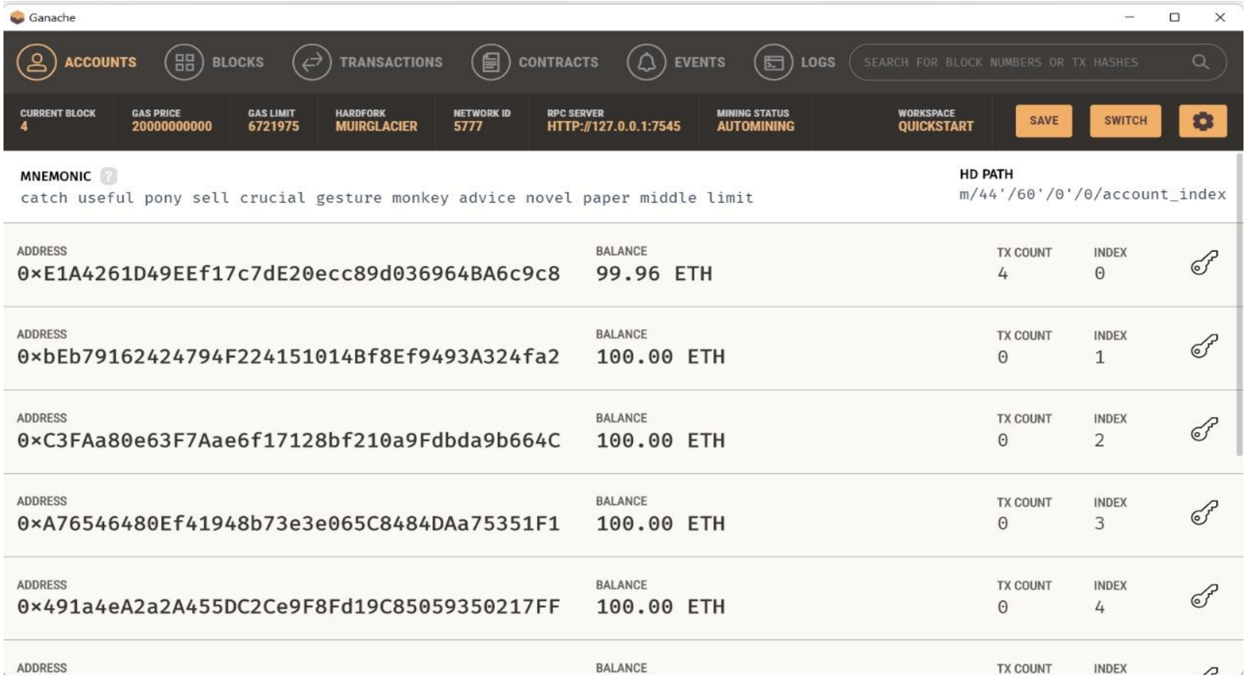
Starting the frontend Server :



```
      <h2 className="patients-header">Patients</h2>
      <Button variant="info" onClick={refresh}
        className="patients-refresh">Refresh</Button>
      <div className="patients-accordion">
        <Accordion defaultActiveKey={['0']} alwaysOpen>
          {patients && patients.map((patient, index) => (
            <Accordion.Item eventKey={`${index}`} key={`patient-${index}`}>
              <Accordion.Header>Patient {`${patient.id}`}</Accordion.Header>
              <Accordion.Body className="patients-accordion-body">
                <Table striped bordered hover size="sm">
                  <thead>
                    <tr>
                      <th>#Thermometer Id</th>
                      <th>Reading</th>
                      <th>Time</th>
                    </tr>
```

```
Compiled successfully!

You can now view trust-iot in the browser.

  Local:            http://localhost:8080
  On Your Network:  http://192.168.56.1:8080

Note that the development build is not optimized.
To create a production build, use npm run build.

webpack compiled successfully
```

Ganache : Virtual Personal Private Blockchain environment



Ganache

ACCOUNTS BLOCKS TRANSACTIONS CONTRACTS EVENTS LOGS

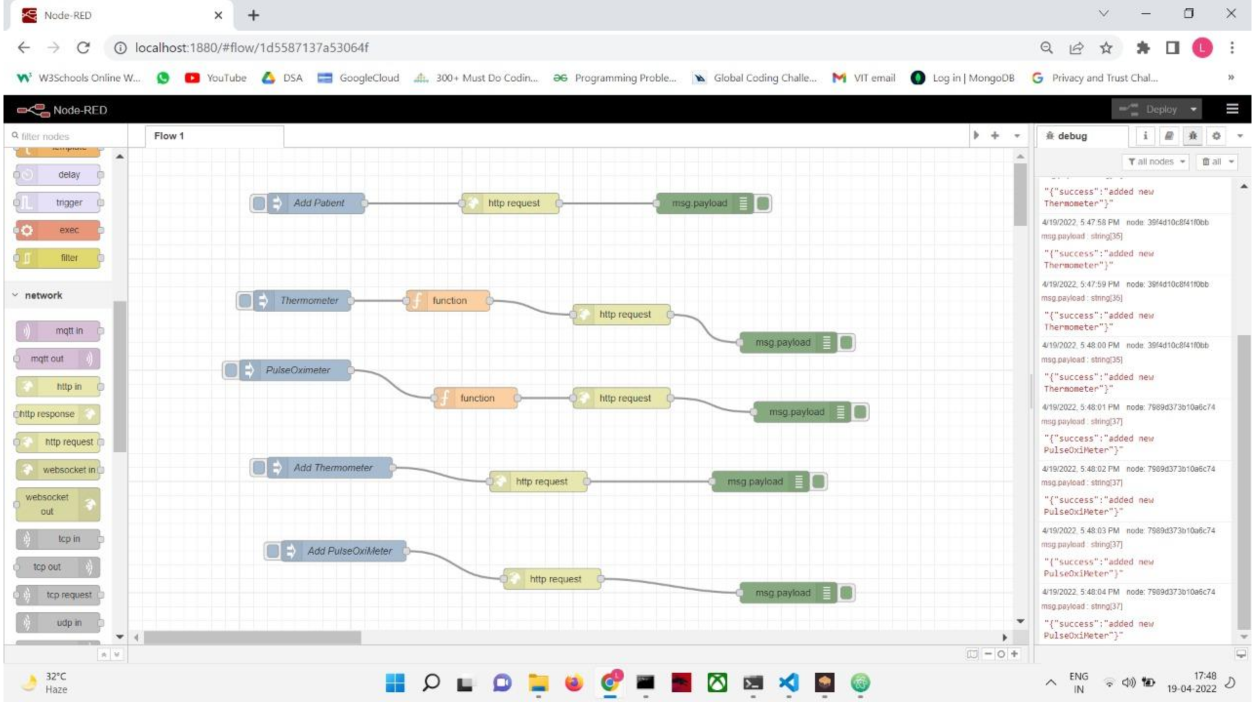
CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
4	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

MNEMONIC
catch useful pony sell crucial gesture monkey advice novel paper middle limit

HD PATH
m/44'/60'/0'/0/account_index

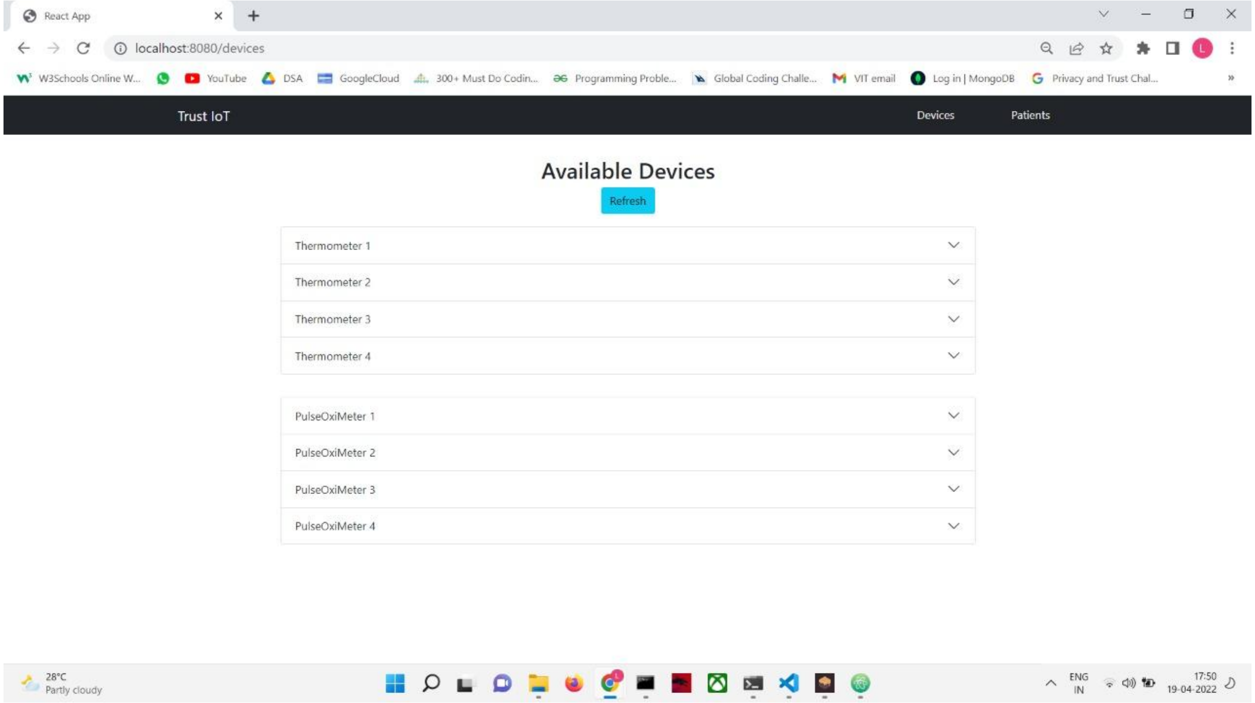
ADDRESS	BALANCE	TX COUNT	INDEX
0×E1A4261D49EEf17c7dE20ecc89d036964BA6c9c8	99.96 ETH	4	0
0×bEb79162424794F224151014Bf8Ef9493A324fa2	100.00 ETH	0	1
0×C3FAa80e63F7Aae6f17128bf210a9Fdbda9b664C	100.00 ETH	0	2
0×A76546480Ef41948b73e3e065C8484DAa75351F1	100.00 ETH	0	3
0×491a4eA2a2A455DC2Ce9F8Fd19C85059350217FF	100.00 ETH	0	4

NodeRed : Simulation of IOT devices in the hospital in node red as flows.



```
"{"success":"added new
Thermometer"}"
4/19/2022, 5:47:58 PM  node: 39f4d10c8f41f0bb
msg.payload : string[35]
"{"success":"added new
Thermometer"}"
4/19/2022, 5:47:59 PM  node: 39f4d10c8f41f0bb
msg.payload : string[35]
"{"success":"added new
Thermometer"}"
4/19/2022, 5:48:00 PM  node: 39f4d10c8f41f0bb
msg.payload : string[35]
"{"success":"added new
Thermometer"}"
4/19/2022, 5:48:01 PM  node: 7989d373b10a6c74
msg.payload : string[37]
"{"success":"added new
PulseOxiMeter"}"
4/19/2022, 5:48:02 PM  node: 7989d373b10a6c74
msg.payload : string[37]
"{"success":"added new
PulseOxiMeter"}"
4/19/2022, 5:48:03 PM  node: 7989d373b10a6c74
msg.payload : string[37]
"{"success":"added new
PulseOxiMeter"}"
4/19/2022, 5:48:04 PM  node: 7989d373b10a6c74
msg.payload : string[37]
"{"success":"added new
PulseOxiMeter"}"
```

Frontend GUI : a reactJS based frontend GUI for viewing real time patient vitals.



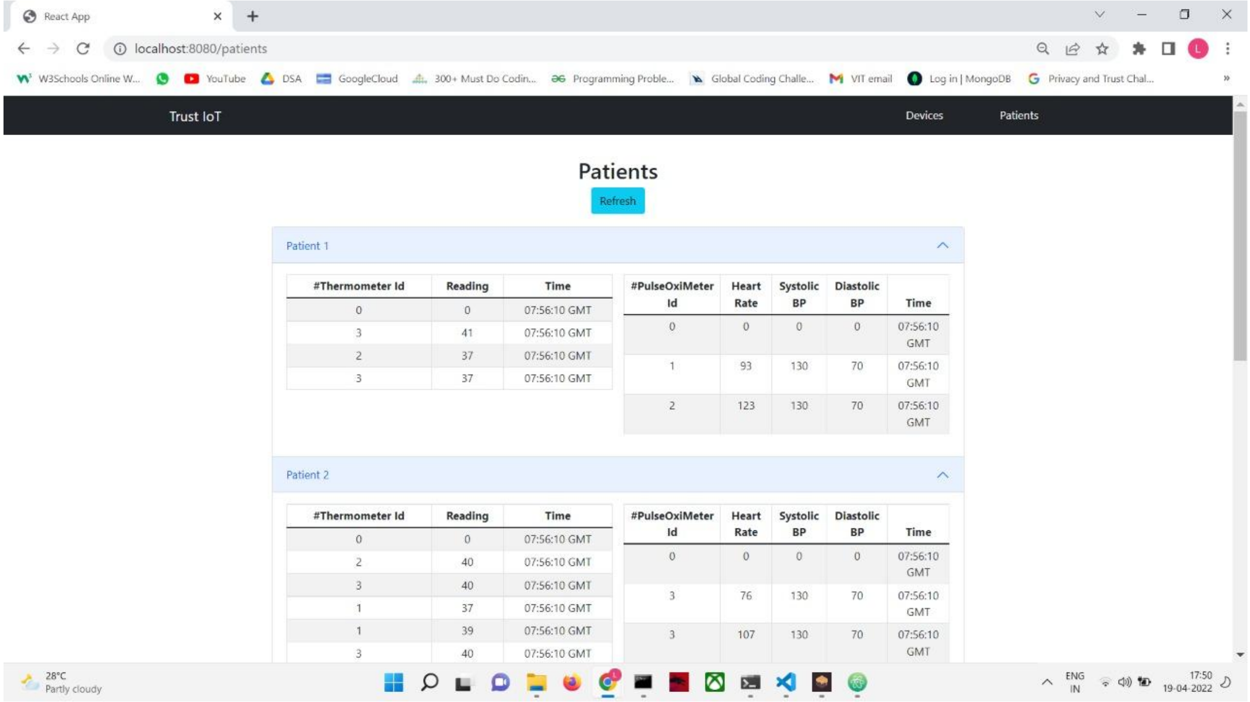
Available Devices

Refresh

- Thermometer 1
- Thermometer 2
- Thermometer 3
- Thermometer 4

- PulseOxiMeter 1
- PulseOxiMeter 2
- PulseOxiMeter 3
- PulseOxiMeter 4

Real Time Patient Vitals :



Patients

Refresh

Patient 1

#Thermometer Id	Reading	Time
0	0	07:56:10 GMT
3	41	07:56:10 GMT
2	37	07:56:10 GMT
3	37	07:56:10 GMT

#PulseOxiMeter Id	Heart Rate	Systolic BP	Diastolic BP	Time
0	0	0	0	07:56:10 GMT
1	93	130	70	07:56:10 GMT
2	123	130	70	07:56:10 GMT

Patient 2

#Thermometer Id	Reading	Time
0	0	07:56:10 GMT
2	40	07:56:10 GMT
3	40	07:56:10 GMT
1	37	07:56:10 GMT
1	39	07:56:10 GMT
3	40	07:56:10 GMT

#PulseOxiMeter Id	Heart Rate	Systolic BP	Diastolic BP	Time
0	0	0	0	07:56:10 GMT
3	76	130	70	07:56:10 GMT
3	107	130	70	07:56:10 GMT

Project Link : https://github.com/LOGANATHANAN/TrustIOT

Conclusion

Objective :

IoT sensors capture large volumes of sensitive patient data, posing privacy and security concerns as well as opening the door to a slew of risks. The requirement for appropriate security mechanisms is a significant concern. Despite the existence of various security rules for IoT applications, such as two-factor authentication and biometrics, blockchain technology can give an intriguing IoT data privacy solution. Blockchain is packed with security features such as limited access and the ability for sensors to shut down in the event of a compromised environment, reducing the danger of data manipulation.

Results Achieved:

We have successfully implemented a Decentralised app or Dapp which fulfils the purpose of creating a backend system of pushing patient vitals details to the blockchain using solidity and web3 modules which communicate with the blockchain from the backend server we've built. The dapp is capable of doing the following actions:

- Communicate with the IoT sensors and get information from them
- Send the information from the IoT sensors to the backend
- Then communicate with the blockchain using solidity and push that patient's records in to the blockchain
- It can add new patients and devices to the blockchain
- It can retrieve sensed information from the blockchain and display it in our frontend

Advantages:

- Blockchain based solution
- Once the collected data gets stored in blockchain, then it takes care of securing the data
- The IoT-sensitive data will remain permanent and cannot be changed due to blockchain infrastructure. The technology encourages traceability and accountability of data.
- Besides trusted transactions on Blockchain, it leads to minimised attacks by preventing the attackers from maliciously infecting IoT devices.
- Blockchain can be used to authenticate and authorise devices within IoT applications.
- With public-key cryptography, the sensitive IoT applications' real identity can be hidden.

Limitations:

- Physical security of the sensor nodes
- Network overhead in blockchain
- Lack of authentication and communication between Iot devices

- Lot of computational power required
- Transmission between the patient’s smart device and the blockchain nodes is over an open channel.

Future Enhancements :

- Authenticate each and every node - It is a way to authorise and allow devices which are only within the network making sure no unauthorised devices are in the network giving false readings
- Develop storage efficient blockchain
- Only authorised users being able to send requests to the main server for adding data

References:

[1] Aashima Sharma;Sanmeet Kaur;Maninder Singh; (2021). *A comprehensive review on blockchain and Internet of Things in healthcare . Transactions on Emerging Telecommunications Technologies, (), –.* doi:10.1002/ett.4333

[2] Mayer, A. H., da Costa, C. A., & Righi, R. D. R. (2020). Electronic health records in a Blockchain: A systematic review. *Health informatics journal*, *26*(2), 1273-1288.

[3] Jabarulla, M. Y., & Lee, H. N. (2020). Blockchain-based distributed patient-centric image management system. *Applied Sciences*, *11*(1), 196.

[4] Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors*, *20*(22), 6587.

[5] Metwally, O. (2017). On the economics of knowledge creation and sharing. *arXiv preprint arXiv:1709.07390*.

[6] Linn, L. A., & Koo, M. B. (2016). Blockchain for health data and its potential use in health it and health care related research. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST* (pp. 1-10). Gaithersburg, MD, USA: NIST.

[7] Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors*, *20*(22), 6587.

[8] Muofhe, M., Dlodlo, N., & Terzoli, A. (2019, October). An Internet of Things-Based System Integrated with Blockchain to Manage Patient Data in the Healthcare Sector. In *2019 Open Innovations (OI)* (pp. 97-103). IEEE.

[9] Hathaliya, J., Sharma, P., Tanwar, S., & Gupta, R. (2019, December). Blockchain-based remote patient monitoring in healthcare 4.0. In *2019 IEEE 9th international conference on advanced computing (IACC)* (pp. 87-91). IEEE.

[10] Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access*, *6*, 32700-32726.

[11] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, *42*(7), 1-7.

[12] Hayajneh, T., Mohd, B. J., Imran, M., Almashaqbeh, G., & Vasilakos, A. V. (2016). Secure authentication for remote patient monitoring with wireless medical sensor networks. *Sensors*, *16*(4), 424.

[13] Jamil, F., Ahmad, S., Iqbal, N., & Kim, D. H. (2020). Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors*, *20*(8), 2195.

[14] Senthamilarasi, C., Rani, J. J., Vidhya, B., & Aritha, H. (2018). A smart patient health monitoring system using IoT. *International Journal of Pure and Applied Mathematics*, *119*(16), 59-70.

[15] Taiwo, O., & Ezugwu, A. E. (2020). Smart healthcare support for remote patient monitoring during covid-19 quarantine. *Informatics in medicine unlocked*, *20*, 100428.