Integrating IoT with Health Record Management System using IPFS and Blockchain

Waseem Khan
University of Mumbai
Kharghar, Navi Mumbai
Maharashtra, Pin code-410210

Gargi Kumbhare
University of Mumbai
Kharghar, Navi Mumbai
Maharashtra, Pin code-410210

Pradnya Pugaonkar
University of Mumbai
Kharghar, Navi Mumbai
Maharashtra, Pin code-410210

ABSTRACT
Remote Patient monitoring is the current need of society. As the world has recently faced a pandemic and has realized the importance of RPMS for regular check-ups of patients. Blockchain, being the efficient technology in providing a secure environment for storing the data, can be used at different levels when combined with other technologies.A hybrid system using blockchain and IoT-sensors to detect and record the human vitals and interfacing these data to a website using wireless protocols for real-time monitoring is implemented by combining these two technologies. Using the Interplanetary file system (IPFS),blockchain, and smart contract patient's data is provided with the security it needs. The combination of these technologies will drive the control of the data in the patient's hand as they are the real owners of the data. Thus, improving the quality of healthcare by making it more efficient, reducing costs and cybercrimes against medical data.

Keywords
Blockchain, IoT, Thingspeak, Security, InterPlanetary File System(IPFS), Infura, Smart Contract, Ethereum.

1. INTRODUCTION
Nowadays, technology is a part and parcel of our daily lives for a number of reasons. One such technology is Blockchain. Blockchain is a shared immutable ledger that is used to record transactions, manage assets and develop trust. Blockchain technology was introduced along with Bitcoin by Satoshi Nakamoto[1]. Blockchain in the healthcare sector holds potential solutions to the traditional healthcare problems that already exist around patients' services.The ability to improve the sharing of patients' data makes the systems more intelligent, adaptable and increases the reliability of services offered in the health care sector for better use. For recording vital signs from patients' body IOT (Internet Of Things) devices are used.

IoT is believed to be the most growing paradigm since its discovery due to the impact it has in the field of technology in general. The main goal of IoT is to give computers the ability to smell, hear, and see the environment as humans, to enable them to be more analytical and observant to the world without misinterpreting the human entered data. A combination of IoT and Blockchain capabilities can further refine the use of Blockchain-IoT systems in the healthcare sector.

2. BACKGROUND
Many countries are suffering from a dramatic increase in the number of patients, and it is becoming more difficult for patients to access primary doctors or caregivers [8]. The use of IoT in the medical field is increasing rapidly, many hospitals use Remote Patient Monitoring systems (RPMS) to monitor the vitals of the patients and provide necessary care remotely. This generates a lot of Electronic Medical Records (EMR) and that needs to be kept secure as it is sensitive data. Although the current technologies used to secure this data is not very reliable, and is vulnerable to all sorts of cyber-attacks, tampering of records.

Secondly, the patient is not in charge of the data in any sort of way. This paper focuses on putting forward a different approach for securing these EMR using Blockchain Technology. As Blockchain is immutable and highly secure, tampering with records is close to impossible. This paper talks about the integration of IoT and Blockchain Technology by implementing an Arduino-based RPMS and integrating it with a Private Blockchain network, linked to a smart contract, which drives all the control in the patient's hands as they are the real owners of this data.

3. OBJECTIVE
As Internet of Things (IoT) devices and other remote patient monitoring systems increase in popularity, security concerns about the transfer and logging of data transactions arise. In order to provide security to the data generated by these devices, the proposed system utilizes blockchain-based smart contracts to facilitate secure analysis and management of medical sensors.

Objectives of our proposed system are as follows:

- It is used for measuring automatically or at regular intervals the value of a patient's important physiological parameters such as - Body temperature, BPM, Blood oxygen level(SpO2), ECG.
- It helps patients to monitor their own condition at any time using the IoT device.
- The data generated by the device will be secured using a private blockchain network.
- The control of the medical data is with the true owner of the data i.e. The patient at all times, only the patient can provide access to data to doctors and caregivers.

4. PROPOSED SYSTEM
4.1 IoT
The IOT device proposed is consists of Arduino Uno R3 microcontroller, ESP8266 Wi-Fi module, and 4 medical sensors viz Pulse Sensor, LM35 body temperature sensor,

MAX30102 Blood oxygen sensor and AD8232 ECG sensor as shown in Figure 1.

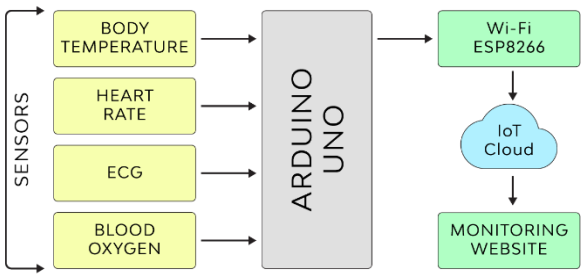

Figure 1: Block diagram of Remote Patient Monitoring System

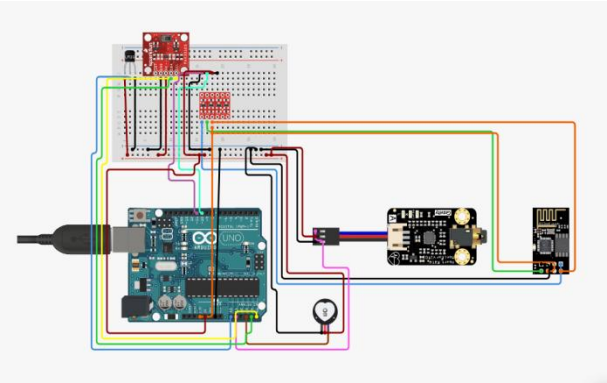

Figure 2: Illustrates the circuit diagram of the RPM device.

The Circuit diagram of the Remote Patient Monitoring(RPM) device shown in Figure 2 illustrates the medical sensors that are connected to the ArduinoUno analog input pins which feed the sensor's output to the Arduino. A bi-directional logic converter is used to connect the ESP8266 Wi-Fi module as it works on a 3V power supply and the entire circuit works on a 5V power supply. The patient's data is processed by the microcontroller and stored on the thingspeakIoT cloud via a Wi-Fi module and is fetched on the website for real-time monitoring.

4.2 Smart Contract

Smart Contracts are known as a piece of code that acts as an intermediate between Dapps and blockchain. Smart contracts are secure from tampering and alternation as they run directly on the blockchain[1]. They are needed to perform any task on the blockchain, the most common language for smart contracts is solidity as the programmers can program it to perform any operation, they want on the blockchain.

The smart contract gets triggered whenever patients perform a transaction (i.e.share reports with the doctors on the website) and it consists of a write and a read function. The write function writes the hash generated by IPFS into the Blockchain and similarly the read function reads the hash from the blockchain when Doctors are required to view the shared data of their patients.

4.3 Blockchain and Website

The website is designed both for patients and doctors, where the patients can log in for real-time monitoring of their vitals and can also provide access to their caregivers to monitor the data. Also, patients can consult numerous doctors available on the website as per their needs by sending external test reports to their preferred doctors.

Authorized doctors can create an account on the website and provide consultations to the patients as per their expertise, but the doctors just have the right to view the report via their dashboard on the website and they cannot save or alter the data as the patient is the rightful owner. The whole system is built using xampp server, Html, JavaScript, CSS, bootstrap for frontend and Php, SQL for the backend.

The reports uploaded by the patients are stored on the InterPlanetary File System (IPFS) which is a peer-to-peer hypermedia protocol designed for data storage. All the files stored on IPFS have a unique hash that is generated using the sha256 algorithm and is used for the identification of that stored file[10].

Even in the breach of the website,the patient's reports will be kept secure as it is stored on a peer-to-peer distributed network rather than directly on the website. The IPFS returns a content Identifier (CID) which is its hash[11]. The hash is unique to the content that it came from, and this hash acts as the key to view or retrieve that data.

Figure 3. shows how this hash is then stored on a local Ethereum blockchain network for that purpose Ganache is used, which is a test Ethereum network provided for development purposes[7]with the help of a smart contract.Ethereum blockchain provides us with timestamping data, which makes tampering of data almost impossible, but to store a file on Ethereum can be very expensive given the amount of processing the Ethereum blockchain has to do and the higher gas fees, whereas the content-based addresses that IPFS returns are 46 bytes in size which is a tiny amount considering the size of files. Soit is cheaper to publish a file on IPFS and store their content-based address on the Ethereum blockchain.

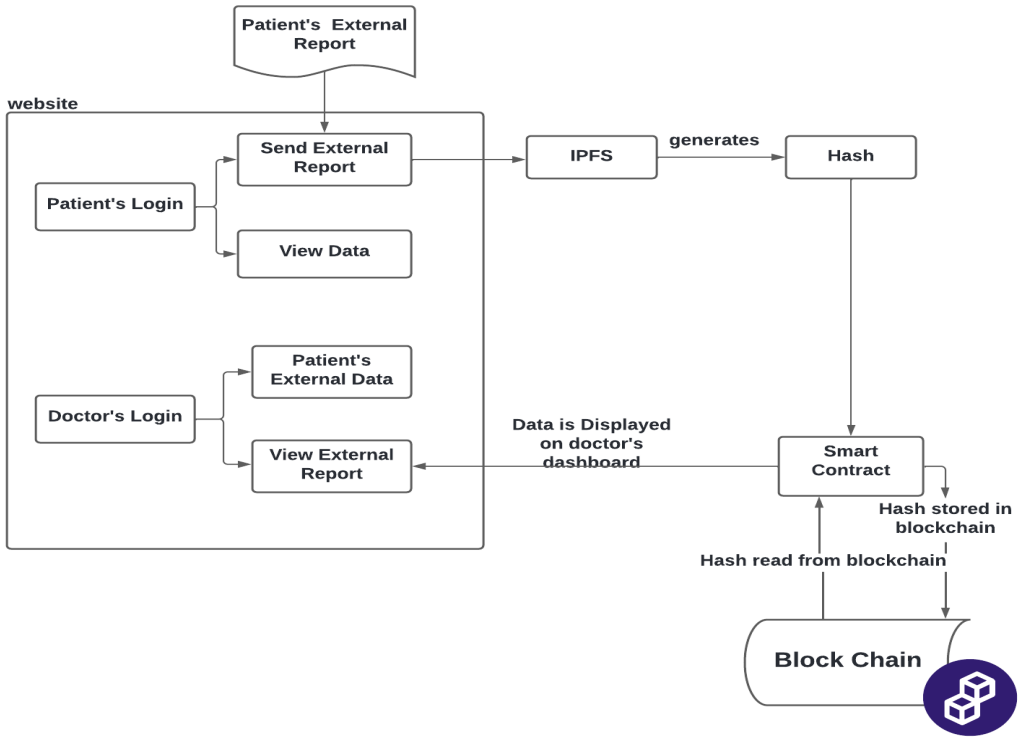

Figure 3: Process flow of the website and Blockchain

5. RESULT

5.1 Performance analysis

5.1.1 IoT Device

The system readings of existing devices are compared with the proposed system's IoT Device for analyzing its efficiency. For Heart rate,Mi Band 3, for body temperature a clinical thermometer and for blood oxygen levelDr. Morepen Pulse Oximeterwas used. Table 5.1.1.1, 5.1.1.2, and 5.1.1.3 show the comparison of readings for Heart rate, Body temperature, and Blood Oxygen Level respectively.

Table 5.1.1.1

Heart Rate			
Mi Band 3	92 bpm	88bpm	89bpm
Our System	88 bpm	87bpm	78bpm

Table 5.1.1.2

Body Temperature			
Clinical thermometer	99°F	98°F	98°F
Our System	97°F	102°F	98°F

Table 5.1.1.3

Blood Oxygen			
Dr. Morepen Pulse Oximeter	99% SpO2	98% SpO2	96% SpO2
Our System	93% SpO2	96% SpO2	94% SpO2

Table 5.1.1.4 Accuracy of all Sensors

Sensors	Accuracy of Our System
Heart Rate	93.6%
Body Temperature	99.3%
Blood Oxygen	96.67%

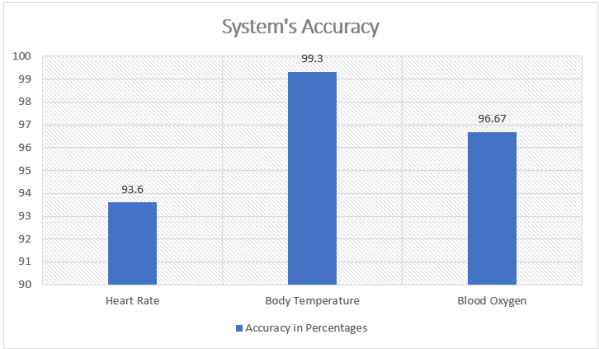

Figure 4: Graphical representation of the accuracy of our system

Table 5.1.1.3 shows the accuracy of the system in comparison with already existing systems in the market.

5.1.2 File Transaction

When the patient performs a transaction a certain gas fee is utilized to write that transaction on the Ethereum blockchain network, which can be calculated as

$$Gas\text{-}fee = Gas\ consumed \times Gas\ Price$$

The Gas consumed for a random transaction is 93159 and its Gas price is 200 Gwei, Sothe gas fee can be calculated as,

$$Gas\text{-}fee = 93{,}195 \times 200 = 18{,}639{,}000\ Gwei$$

To convert the same in etherthe following method is used

$$1\ Ether = 1000{,}000{,}000\ Gwei$$

$$Gas\text{-}fee\ in\ Ether = 18{,}639{,}000/1000{,}000{,}000\ Gwei$$

$$= 0.0018639\ ETH.$$

6. ACKNOWLEDGEMENT

The authors would like to thank Dr. S.M.Patil and Prof. S.N.Mhatre for helping through all the difficulties related to the paper and the project.

7. CONCLUSION

In recent years IoT has had a huge expansion in various fields and has majorly contributed to the medical sector. Blockchain has also grown. This work proposes a novel approach for increasing the efficiency and reliability of IoT in the blockchain. It overcomes the issues faced by the conventional method of storing medical records, as it utilizes the off-chain storage mechanism of IPFS. The patient-centric approach of our system helps in building trust among the users as the patients are in control of the data at all times.

The proposed platform is based on a local blockchain network and addresses inherent challenges such as data security, identity, and scalability, to name a few.

In future this proposed system can help healthcare institutes to completely decentralized their storage mechanism and thus help build trust among the users as well as the governing bodies.In traditional data storage architecture data needs to be replicated at least twice in order to be default pursue fault tolerance. The inherent characteristic feature of IPFS replicates data on its peer nodes for a set number of times, as a result the proposed system is fault tolerant and cost effective at the same time. This will help the said institutes to drastically reduce costs associated with IT infrastructure needs.

8. REFERENCES

[1] Ayesha Shahnaz, Usman Qamar (Computer Science Department, National University of Science and Technology (NUST), Islamabad. 44000, Pakistan), Ayesha Khalid(The Center for Secure Information Technologies(CSIT), ECIT Institute, Queen's University of Belfast, Belfast BT7 1NN, U.K.) "Using Blockchain for Electronic Health Records" October 9, 2019 (IEEE Access)

[2] Yi Chen, Shuai Ding, Handong Zheng, ShanlinYang(School of Management, Hefei University of Technology, Hefei, Anhui, China), Zheng Xu(The Third Research Institute of the Ministry of Public Security, Shanghai, China) " Blockchain-Based Medical Records Secure Storage and Medical Service Framework" 22 November 2018, Springe

[3] Antonio Celesti, Armando Ruggeri, Maria Fazio, Antonino Galletta, Massimo Villari and Agata Romano (2 May 2020) "Blockchain-Based Healthcare Workflow for Tele-Medical Laboratory in Federated Hospital IoT Clouds" Sensors-MDPI

[4] Antonio Fusco, Grazia Dicuonzo, Vittorio Dell'Atti, and Marco Tatullo" Blockchain in Healthcare: Insights on COVID-19", 30 September 2020, International Journal of Environmental Research and Public Health.

[5] Madhusudan Singh (Yonsei Institute of Convergence Technology, South Korea), Abhiraj Singh (Department of Mechanical Engineering IIT-Roorkee, Roorkee, India), Shiho Kim (School of Integrated Technology, Seoul, South Korea) "Blockchain: A Game Changer for Securing IoT Data" (March 07,2018) IEEE Access.

[6] Dash, S., Panda, R., &Padhy, S. . (2021). Blockchain-based intelligent medical IoT healthcare system

[7] Bhabendu Kumar Mohanta, Member, IEEE, Debasish Jena, Member, IEEE, SomulaRamasubbareddy, Mahmoud Daneshmand Senior Life Member, IEEE, and Amir H. Gandomi Senior Member, IEEE "Addressing Security and Privacy Issues of IoT using Blockchain Technology".

[8] Gautam Srivastava∗†, Jorge Crichigno‡, and Shalini Dhar§ " A Light and Secure Healthcare Blockchain for IoT Medical Devices"(2019) IEEE.

[9] Ismail Keshta Ammar Odeh "Security and privacy of electronic health records: Concerns and challenges"(July 2021)Egyptian Informatics Journal.

[10] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, ''HealthSense: A medical use case of Internet of Things and blockchain,'' in Proc. Int. Conf. Intell. Sustain. Syst. (ICISS), Dec. 2017, pp. 486–491.

[11] Shivansh Kumar Aman Kumar Bharti Ruhul Amin "Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions"(17 Dec 2020) Wiley