Measurement: Sensors 25 (2023) 100630

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

A real time secured medical management system based on blockchain and internet of things

Sharda Tiwari [a,*], Namrata Dhanda [a], Harsh Dev [b]

[a] Department of Computer Science & Engineering, Amity University, Lucknow, Uttar Pradesh, India
[b] Department of Computer Science & Engineering, Pranveer Singh Institute of Technology, Kanpur, India

ARTICLE INFO

Keywords:
IoT
Blockchain
Health
Medical
Sensor

ABSTRACT

Nowadays Electronic Health Care System is growing to a large extent. As data retrieve from IoT devices, that data is needed to store in a database as the different patients have different data. Due to a lack of intrinsic security safeguards, the Internet of Things is prone to privacy and security breaches. The information gathered from IoT devices is mostly saved in a database This data is very important for a particular patient. If this data is altered by any intruder, then the doctor cannot find the actual problem of the patient and also cannot give the patient proper treatment, as a result, it causes great harm to the patient. As a result, a security mechanism for the data contained in the database is required. Blockchain technology will help a lot in this situation. We make an IoT-based prototype that uses Blockchain technology to get rid of this anonymous data access, in the common word patient's data are private through this system.

1. Introduction

Data security is one of the most concerning things for every people nowadays [1]. Even if the data is less significant, no one wants to share it with others. This data security is a burning question for a critical patient. If the intruder has access to the data, he can harm the patient in any way he wants. That is something that no one should do. If an intruder alters the patient's data, the doctor will be unable to provide correct therapy. Here's why that matters in terms of security. Let's assume that an intruder attempts to edit important information data. As soon as they edit the information from the id, the block's hash will change. The next block in the chain will still contain the old hash, and the hacker would need to update that block to cover their tracks. However, doing so would change that block's hash. And the next, and so on [2]. He has to change that way one by one every blocks hash.

Critical patients are unable to see doctors frequently, which is a difficulty for them; thus, if a distance patient monitoring system is available, it will be quite beneficial to them. Also, the aged people of our country are unable to go to the hospital to show their illness, so this system will be much helpful to them [3].

Blockchain has made an enormous change in the security system. In previous days we used the only database to store any kind of patient data and other important things that were confidential to them, this data was not secure anymore. By hacking the database, an attacker might quickly gain access to the data and other reports. That was the source of the patient's insecurity. As a result, blockchain technology has arrived.

Blockchain technology has recently acquired a lot of traction in the health industry due to its importance in resolving the interoperability and security issues with Electronic Health Record (EHR) systems [3]. With its decentralized (no central authority) and trustworthy character, blockchain has shown significant potential in a variety of e-health systems, including the open interchange of electronic medical data records and shared data management among diverse healthcare systems [4]. People have been more interested in eHealth. In terms of Medical science, it is a new technology. The internet is used to give medical services and patient information. This term does not just refer to the technical element; it also has a broader meaning. There have been several efforts in this industry to address this type of security risk. Patients' sufferings have been reduced as a result of blockchain technology; they no longer need to retest their physical conditions if they visit a new doctor since they can share their protected data with the safest platform utilizing blockchain technology.

2. Literature review

Blockchain technology is a collection of blocks that are connected in

* Corresponding author.
E-mail addresses: sharda26tiwari@yahoo.com (S. Tiwari), ndhanda@lko.amity.edu (N. Dhanda), drharshdev@gmail.com (H. Dev).

https://doi.org/10.1016/j.measen.2022.100630
Received 30 September 2022; Received in revised form 26 November 2022; Accepted 6 December 2022
Available online 15 December 2022

an immutable and decentralized network. In IoT, blockchain works without the help of a centralized database. Blockchain is such a technology in which data are stored block by block, whenever new blocks are created, they are added at the end of the chain in a linear procedure. The blockchain network must verify the validity of a transaction after it has been certified. By giving proof of the transaction by a computer, the transaction is linked to the blockchain as a block. Each block on the blockchain network has a distinct hash. A hash is developed using an algorithm and is crucial for cryptocurrency blockchain management. In case of manipulating any information of a block, instantly it changes the block's hash value. However, this causes a change in the hash of the after block also. This is a going process, so by changing or deleting any data all other block hash changes automatically. To change a single block on the blockchain, an intruder will have to change every single block after that. It will take an immense amount of computational power to recalculate all those hashes. So, no one can change a single thing in the blockchain network without notice.

In a blockchain system, there exist two variants of nodes: the first one is that wants to add new blocks in the network and the other is that receives these new blocks to create a chain of blocks. Blockchain consists of blocks and blocks have block headers. And each block header has its unique hash, previous block's hash, Merkle root, nonce, timestamp [5]. Fig. 1 shows a complete idea of the block header.

Blocks in blockchain are connected one by one in a linear manner, it looks like a chain of blocks that's why it is named blockchain. All transactions in a single block are converted into a hash, that's called the hash of the block which is unique. As the blockchain is a chain of blocks, the previous block's hash is also stored in the current block [6–8]. Changing a single transaction in a block without the consent of miners, changes the hash of the block. So, the whole system breaks down.

2.1. The Pow Algorithm for mining new blocks

Proof of work is used for mining transactions. In a block, there is no possibility to update any data. It may, however, be possible to generate all of the block hashes and reassemble the chain in some fashion. Using a transaction mining approach will need, if not impossible, a very high-performance processor. In our circumstance, we use this method to test processing power before mining transactions. The sender must mine a transaction after it has been completed When a node creates a new block, the receiving nodes perform a hash function on the block contents and a nonce, which is known as mining. In cryptography, a nonce is an arbitrary number that can only be used once in a cryptographic communication [9]. It's usually a randomized or quasi-random number used in an identification scheme to prevent prior interactions from being utilized in replay attacks [10]. The specified value must be higher than the hash value calculated. If this requirement isn't satisfied, the nonce is raised, and the hash function is redone using the new nonce. The freshly produced block now contains its proof of work, which will be verified by other nodes in the network when a miner completes its duty. However, mining is not a straightforward operation since computers must execute complicated programs to solve difficult mathematical expressions. Fig. 2 depicts the Pow algorithm.

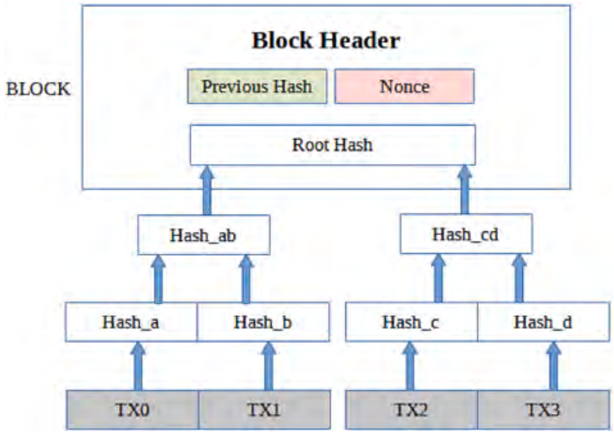


Fig. 1. The block header.

2.2. Internet of things (IoT)

The Internet of Things (IoT) is a compact network of sensors and other devices to communicate with one another through the internet. Internet of Medical Things (IoMT) is a part of an IoT program that collects and analyzes data for testing and monitoring [11]. It has been deemed Smart Healthcare because it is the infrastructure that allows for the creation of a digitized healthcare system that connects accessible patient resources and healthcare services. Remote patient monitoring is now thinkable only for the advancement of IoT. These health monitoring kits can be from wearable sensors to various sophisticated devices. A recent statistic shows that there exists around one-third of IoT devices in the health sector and the analysts predict that it will be increased within 2025, which is the sign of becoming digitalization of our health sector [12]. The tide of development in this sector not only makes our life comfortable but also increases our average life expectancy. But with time IoMT solutions are facing difficulties in security and privacy fragility.

For security purposes, an emerging technology blockchain has been adopted which is quite new to people. Fig. 3 depicts the data sharing procedure through the Internet of Things, nowadays patient health data can be easily shared among doctors, pharmacies, and other third parties with the cooperation of cloud computing.

In [13] the authors have used blockchain for empowering cloud eHealth. They have built the system for radiation oncology for mainly cancer patients. The prototype is built on Hyperledger Fabric – an open-source implementation of the permissioned blockchain technology. Data is uploaded to the cloud here, but there is no IoT implementation in this prototype, thus all patient data must be manually submitted. Their architecture consists of a user interface and a backend that is composed of membership service and certification authority, the network of nodes, a load balancer to redirect a user to any of the trusted nodes in the network, separate cloud-based storage for patient's data, and certificates.

In [14] the authors have proposed a secure Electronic Health Record (EHR) sharing of mobile cloud-based e-Health systems using blockchain, they are employing Ethereum Blockchain platform for building e-Health system, their prototype is mainly mobile-based patient monitoring

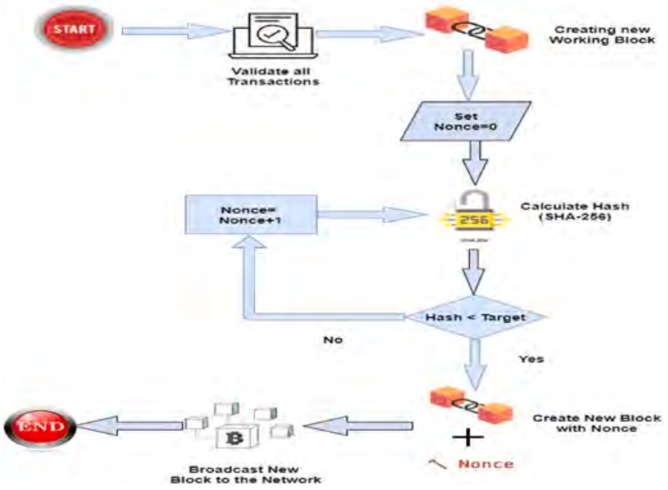

START
Validate all Transactions
Creating new Working Block
Set Nonce=0
Nonce= Nonce+1
256
Calculate Hash (SHA-256)
Hash < Target
No
Yes
Create New Block with Nonce
+
Nonce
B
Broadcast New Block to the Network
END

Fig. 2. The pow algorithm.

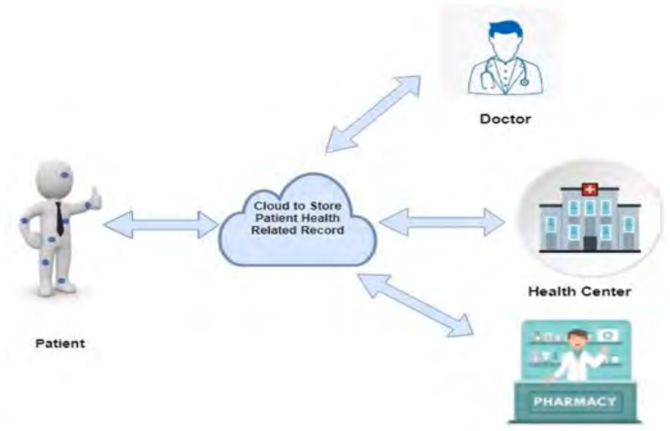


Fig. 3. Internet of things (IoT).

which is different from us. Also, they have used AWS system for cloud system that is very impressive, but if they have used private blockchain their security system would become more secure than the present one.

In [15] the authors have done quite similar work comparing the above two. They have built a prototype of e-Health data access management using blockchain, especially Ethereum blockchain. Ethereum is mainly a public blockchain that is used for data access management. They have also used solidity language for Smart contracts programming and IPFS as a database for file storage. To complete their data collection, they have used many sensors and Raspberry pi.

2.3. Proposed Methodology

The traditional method with IoT technology is to store all data on the cloud. The security of this cloud data is currently a source of worry. Users should be aware of who has access to their cloud data. We want to store patient data on the cloud as well, but with robust security procedures in place. Some data is both influential and sensitive, and it should be securely stored in the cloud, with patients having appropriate control over who may access it. As a result, the security of this data on the cloud must be maintained. We employ well-known blockchain technology for this aspect of security. There are a variety of blockchain systems available; we chose Ethereum because of its excellent security standards. The following are some of the most important reasons to use Ethereum technology:

1. Ethereum is a big established network that has been put to the test over many years with numerous activities and significant value. As a result, it is safe and secure.
2. The key reason we choose Ethereum for our system is that it has many functionalities, is excellent for employing smart contracts, and can safely store data in a decentralized way.
3. It is extremely popular and has a strong community, which is continually looking for new methods to improve the technology.

With all of these benefits in mind, we created an Ethereum-based smart contract for patient-doctor communication. This smart contract allows doctors to simply keep track of their patients. The entire process may be broken down into numerous sections. We'll go through each of these items one by one in this section.

Fig. 4 depicts a visual representation of the central concept of our system, which is divided into two parts: IoT and blockchain. Sensors capture patient data, which is encrypted securely and saved in the cloud. The cloud address is then added to the blockchain. As a result, the system is far more secure than existing IoT medical solutions. Neither storing all the sensor values in the blockchain, we store the cloud address in the blockchain. That makes the system more cost-efficient. This is the main novelty of our work. The proposed methodology's flow diagram is also shown in Fig. 5. By following this diagram anyone can have a clear view of our proposed system (see Fig. 6).

2.4. Steps in our system

In this section, we'll lay out our blockchain section step by step so that everyone understands how the system works. The actions that have been proposed are listed below.

- **Step 1:** Create an Ethereum account for each patient/user.
- **Step 2:** Create own blockchain.
- **Step 3:** Deploy IoT nodes on surroundings.
- **Step 4:** Encryption of sensor value.
- **Step 5:** Data Store on cloud database of Master Node.
- **Step 6:** Data preprocessing.
- **Step 7:** Upload cloud address to a certain block.

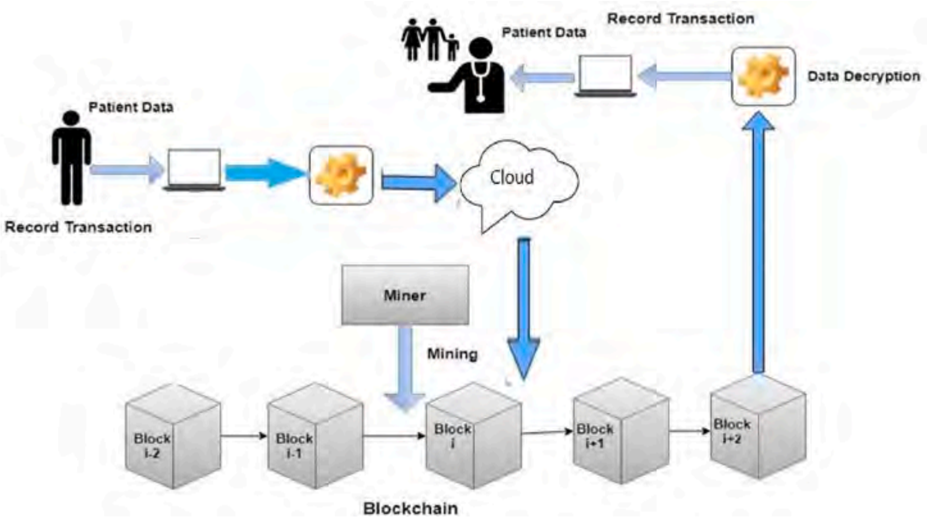


Fig. 4. The overview of blockchain-based e-health system.

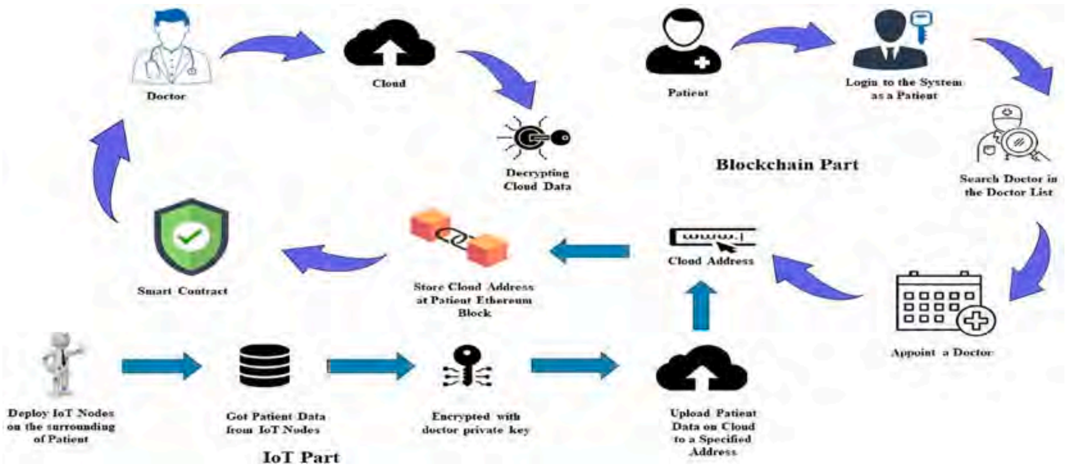

Doctor
Cloud
Decrypting Cloud Data
Patient
Login to the System as a Patient
Blockchain Part
Search Doctor in the Doctor List
Smart Contract
Store Cloud Address at Patient Ethereum Block
Cloud Address
Appoint a Doctor
Deploy IoT Nodes on the surrounding of Patient
Got Patient Data from IoT Nodes
Encrypted with doctor private key
Upload Patient Data on Cloud to a Specified Address
IoT Part

Fig. 5. The flow diagram of Proposed Methodology.

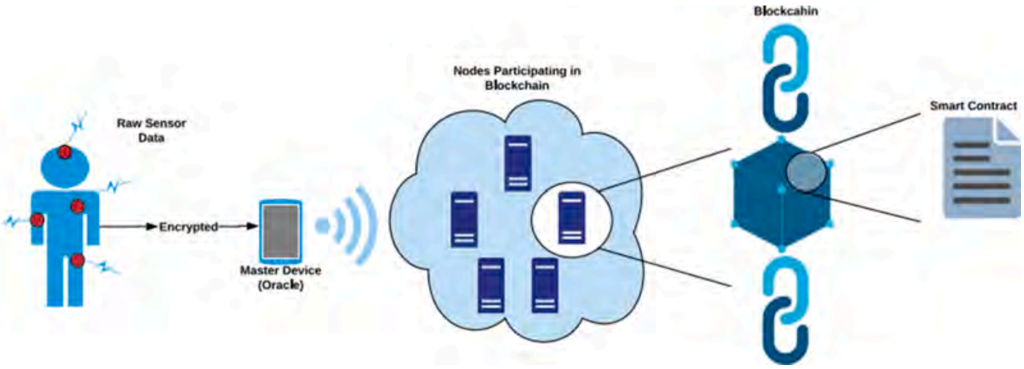


Fig. 6. System architecture.

- **Step 8:** Appoint a doctor.
- **Step 9:** Doctor decrypt the encrypted with his private key;
- **Step 10:** Doctor gives advice and suggestions on the patient block.
- **Step 11:** After a certain time, access power is over;

2.5. System model representation

In this work a system paradigm has been that allows for remote patient monitoring while remaining secure against data breaches. Because essential patient data may be readily altered by anybody, we want to provide a safe and trustworthy platform for patients. The following are the steps used to construct the platform:

2.5.1. Data collected from IoT nodes

The IoT nodes capture the patient's sensible data. They are made up of a variety of sensors (temperature sensor (LM35), heartbeat measurement sensor, etc.) and medical equipment that are placed around the patients. We gather data from these nodes regularly. To collect data from the patient's surroundings, we employ a variety of sensors (temperature sensor (LM35), heartbeat measurement sensor), with Raspberry Pi acting as a Master node. This master node retrieves data from sensors. The data is then preprocessed at this node, and any garbage and superfluous data is cleaned out of the data [16].

After that, the data is encrypted using an asymmetric encryption approach with the doctor's public key and the stored encrypted value in the cloud. Only the patient and appointed doctors have access to his or her data.

2.5.2. Create a blockchain for each patient in the ethereum network

As we all know, each change to a block's content in the blockchain network affects all blocks before it. So, if we construct a single blockchain for all of the patients in the same Ethereum network, and if each patient updates his data on his block, every prior node in the chain would be affected. As the number of patients is growing by the day, this might become prohibitively expensive. As a result, we've recently built a separate blockchain for each patient solely. By generating a new Ethereum account for each patient in the Ethereum network as a prototype, we have shown this technique. The patient has only the right to his block [18,19]. No one can access his info without his permission. Only the appointed doctors can access this block with the doctor's private key.

When patients do not require data from IoT nodes, we may directly upload patient personal information into the MySQL database. He may simply enter the information that he wants to convey to his doctor. This data is immediately uploaded to the database after entering values or information on the website. To read-write, both patients and doctors must meet the essential prerequisites. Store Patients' Cloud Address to Blockchain.

After entering accurate information on our website, the patient must upload his cloud address to his block. Those blocks are sequentially stored on a blockchain network. The entire system then transforms into a compact, secure E-Health system. Patients must log in to their accounts and input the cloud address when they need to upload data to the blockchain. He also has to meet the requirements for his block's read-write authority. The smart contract is developed in the Solidity programming language on the remix ide online and then published on the Ethereum blockchain network [17]. Cloud addresses are primarily saved for each patient on their own Ethereum blockchain. The proposed model not only saves all the data of patients because of the high cost of the gas fee; therefore, we simply store the cloud address of the IoT data. Only the owner of this block has access to it; otherwise, the transaction on the Ethereum.

2.5.3. Give permission to doctor to access the block

Another feature allows a patient to give a trusted doctor access to this block data. If the doctor has a valid Ethereum account and the patient's permission, he can read and write to the block. Furthermore, the patient specifies a time window for further protection, and the doctor is required to access this block during that time frame. The doctor uses his private key to decode. The value of the cloud address and extract the necessary information. Then he provides pertinent advice to the patient by modifying the block's advice variables. The patient then gets this advice on the website's advice page.

2.6. Smart contract

Data security of IoT nodes is our first concern, so we use asymmetric data encryption techniques for ensuring security that makes the system quite secure from attacks. But we deployed our system in Ethereum blockchain to make it safer because cloud data can also be manipulated in any way. These data are stored in the cloud for remote access to the doctor and should be secure from intruder attacks as this data is controversial for critical patients. In this case, patients can permit one doctor to access the cloud data through the smart contract. We make a smart contract that ensures a secure permission checking and gives only the desired doctors access to the cloud data of the particular patient. The pseudocode of the smart contract is described underneath to give a clear idea.

Pseudo Code 1: Pseudocode for Smart Contract.

```
#Patient
Do:
    Collect sensors data and various patient data
    Encrypt all data
    Store data in the cloud
    Save cloud address in the block
    Set an expiry time
End Do

#Doctor
Do:
    If expiredTime < currentTime:
        Get block data
        Get cloud address
        Get the encrypted data from the cloud
        Decrypt this data
        Give Advice
    End If
End Do
```

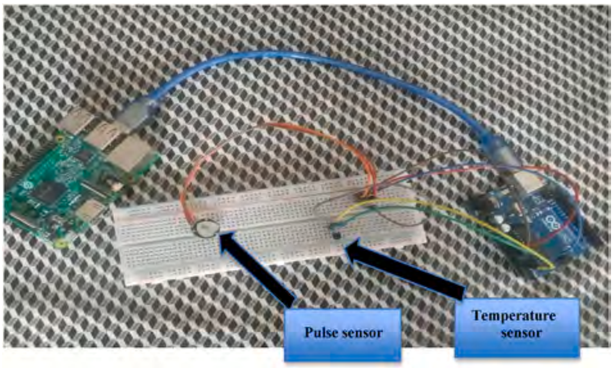


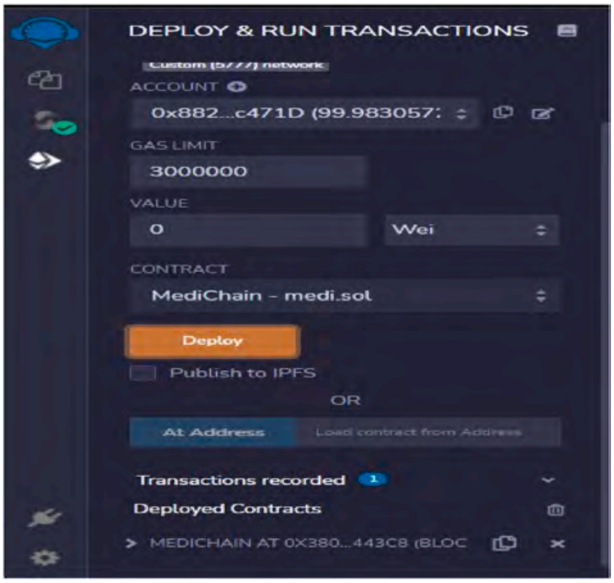
Fig. 7. Circuit setup.

The doctor can only access the patient secured information by his/her private key. The private key decrypts the encrypted data in the cloud. The doctor then gives advice to the patients and this data can be seen by patients only by logging into his/her account on the website. The doctor is allowed to access certain patient blocks only for some time interval after an appointment has proceeded.

2.7. Experimental setup and analysis

Demonstrate the predicted results of IoT nodes using a Raspberry Pi, Arduino Uno, LM35 sensor, pulse sensor to detect temperature and measure heartbeat at a regular interval. We will also compare real-time temperature, heartbeat, and sensor values. The hardware components are combined with the raspberry pi and Arduino Uno to make a beneficial health monitoring tool that can be a blessing for remote critical patients. Software components are also needed to build an ideal system.

In order to measure health metrics, the system employs a variety of hardware components. All the sensors that are connected with the master node, make the system more functional. The proposed system



DEPLOY & RUN TRANSACTIONS

Custom (5777) network

ACCOUNT

0x882...c471D (99.983057:

GAS LIMIT

3000000

VALUE

0 Wei

CONTRACT

MediChain - medi.sol

> MEDICHAIN AT 0X380...443C8 (BLOC

Fig. 8. Deploying smart contract by remix IDE

makes use of the biological sensors listed below.

2.7.1. *Temperature sensor*

In this work, we employ an LM75 temperature sensor. It is inserted into the user's finger to determine the user's body temperature. The output range of the LM75 sensor is −40 °C–110 °C.

2.7.2. *Heartbeat sensor*

A pulse sensor is used to measure the heartbeat. Every minute, it takes a continuous reading of the user's heartbeat. It has a +5 V or +3.3 V operational voltage and a 4 mA current consumption.

Fig. 7 depicts the hardware connection design for the health monitoring system presented in this work. The complete hardware system is built on a breadboard, which is used to link the sensors. For capturing analog sensor data, the breadboard is attached to an Arduino Uno instead of an analog to digital converter, and the entire system is controlled by a Raspberry Pi. Using a USB cable, the Arduino is connected to the Raspberry Pi through serial communication. The Arduino analog PIN A1 is linked to the temperature sensor output pin. The Arduino analog pins are mainly used to connect the other analog output sensors. The heartbeat sensor, for example, is attached to analog pin A0. The VCC and GND pins of the Arduino are linked to the VCC and GND pins on the breadboard. After getting values from the sensor, it is mandatory to store them somewhere such that the doctors can access them. From this, the blockchain and IoT part start to ensure a secure and interrupt less data transfer.

2.7.3. *Software and framework*

Different software and frameworks are used in our system to connect the sensor part with the blockchain and IoT part.

- First, to get value from sensors, code is implemented in Arduino software.
- Then there is a serial communication with the raspberry pi and Arduino ide.
- After that python code is developed for sending encrypted values in the cloud firebase.
- For creating a smart contract Remix IDE is used.

2.7.4. *Remix IDE*

The smart contract developed in remix ide using solidity language. As it is easy to code in remix ide, also easy to compile and connect with Meta Mask effortlessly, we choose remix ide. Fig. 8 gives a clear idea of deploying smart contracts in remix ide (see Fig. 9).

2.8. *Results and discussion*

Several experiments are used to evaluate the study and examine its performance. During the projects, the patients' body temperature and heartbeat were measured. The system is put through a series of testing.

Table 1
Comparison between Measured temperature and Actual temperature.

Users	Temperature using LM75, F	Temperature using Thermometer, F	Average Accuracy
User1	95.4	97.4	**98.24%**
User2	101.3	100.6	
User3	98.3	99.2	
User4	94.3	98.0	
User5	93.9	95.9	

Table 2
Comparison between Measured heartbeat and Actual heartbeat.

Users	Heartbeat using Pulse Sensor (bpm)	Normal Heartbeat (bpm)	Average Accuracy
User1	75	77	**97.23%**
User2	80	83	
User3	91	93	
User4	83	85	
User5	93	96	

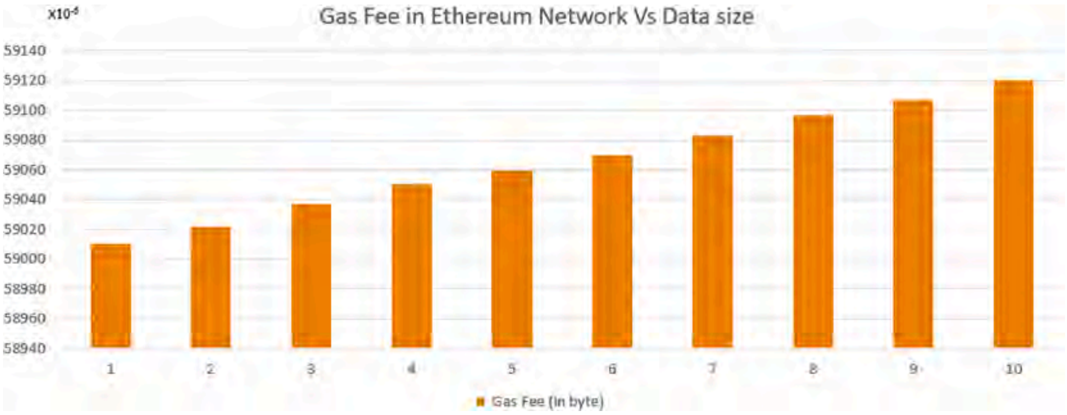


Fig. 9. Gas used during the transaction in Ethereum.

Table 3
Comparison table among the proposed method and the existing methods.

Properties	Type			
	[5]	[17]	[20]	Proposed System
Remote Patient Monitoring	N	N	Y	Y
Remote Patient Disease Detection	N	N	N	N
Use of Sensors	Y	N	Y	Y
User Authentication Advice	N	N	N	Y
Store Data in Blockchain	Y	Y	Y	Y
Use of Cryptographic Function	N	Y	N	Y
Use of IPFS File System	Y	N	Y	N

The health metrics of the patients are displayed in the evaluation of the research's quality.

The patient's body temperature is measured using the LM35 body temperature sensor, as shown in the second column of Table 1. The table compares the temperature calculated by our system to the real temperature of various users as determined by the thermometer. The average accuracy is calculated by utilizing (1).

$$A_v = \frac{1}{n}\sum_{n}\left(\frac{Ts}{Tt}\right) \times 100\% \tag{1}$$

^{A}v = Average accuracy.

N = Number of users
^{T}s = Temperature measured by the system
^{T}t = Temperature measured manually by the thermometer

Also, the heartbeat of the patient is measured using the pulse sensor, as shown in the second column of Table 2. The table compares the heartbeat calculated by our system to the real heartbeat of various users. The average accuracy is calculated by utilizing (1).

2.8.1. *Performance comparison among the proposed method and the existing method*

The proposed system has gained the faith of patients who were the victim of data extortion by many fraud people. Instead of following the conventional procedure, we use blockchain for the sake of data security and transparency. Any type of illegal attempt is contrabanded in this architecture. So, the system is considered one of the safest platforms compared with the remaining e-health platforms.

In this part, we compare our system architecture to those of existing healthcare systems. The comparison is based on the key characteristics of various healthcare systems. The 'Y' symbol denotes a positive aspect, indicating that the related system contains the attribute; on the other side, the 'N' sign denotes a negative aspect. The comparison is shown in Table 3.

2.8.2. *Consumed gas for every transaction*

Every transaction on the Ethereum network requires a gas cost. To put it another way, gas is a sort of cash that may be used to conduct any transaction. Because the Ethereum network's gas charge is so high, we don't store all types of patient data there. As a result, we choose to keep only the individual cloud addresses in Ethereum, which incurs a little gas fee. Our system, on the other hand, becomes more efficient than any other system [21–23]. The graph between the gas fee and the input size in bytes is shown in Fig. 4.5. In this graph, we can visualize that when the size of data increases, the gas fee automatically increases. So, the size of data stored in blockchain must be as small as possible.

2.8.3. *Conclusion*

In the health sector, IoT security is getting a lot of recognition these days. Due to high energy consumption and transmission overhead, existing security technologies are not necessarily suitable for IoT. Hence, to overcome this challenge, we have proposed a blockchain technology that is highly recommended for privacy purposes. This initiative is primarily intended for patients' remote care, as well as the priority protection of sensitive patients' records. To maintain data security, we have implemented the Ethereum blockchain which is considered one of the most effective techniques which are used for data security. We have also used asymmetric cryptography for hashing technique that makes the block transaction safer than other systems.

In the future new sensors, like accelerometer sensor, can be added to the system to measure the accurate position of the patients; additional features could be added to the developed website to advance the functionalities of e-health systems.

CRediT authorship contribution statement

Namrata Dhanda: Data curation, Resources, Software. **Harsh Dev:** Supervision, Visualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

References

[1] K. Fan, S. Wang, Y. Ren, H. Li, Y. Yang, MedBlock: efficient and secure medical data sharing via blockchain, J. Med. Syst. 42 (8) (2018).

[2] V. Gupta, N. Marriwala, M. Gupta, A GUI based application for low intensity object classification & count using SVM approach, in: 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 299–302, https://doi.org/10.1109/ISPCC53510.2021.9609470.

[3] S. Al-Sarawi, M. Anbar, R. Abdullah, A.B.A. Hawari, Internet of things market analysis forecasts, 2020–2030, in: Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), July 2020, pp. 449–453. London, UK, 27–28, ([CrossRef]).

[4] G.J. Joyia, R.M. Liaqat, A. Farooq, S. Rehman, Internet of medical things (IOMT): applications, benefits and future challenges in healthcare domain, J. Commun. 12 (2017) 240–247 ([CrossRef]).

[5] T.M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, P. Fraga-Lamas, Enabling the internet of mobile crowdsourcing health things: a mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care, Sensors 19 (2019) 3319 ([CrossRef]).

[6] C. Li, X. Hu, L. Zhang, The IoT-based heart disease monitoring system for pervasive healthcare service, Procedia Comput. Sci. 112 (2017) 2328–2334 ([CrossRef]).

[7] D. Villegas, A. Martínez, C. Quesada-López, M. Jenkins, IoT for cancer treatment: a mapping study, in: Proceedings of the 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020, pp. 1–6. Seville, Spain, 24–27 June, ([CrossRef]).

[8] J.H. Kim, 6G and internet of things: a survey, J. Manag. Anal 8 (2021) 316–332 [CrossRef] 8. Di Renzo, M.; Zappone, A.; Debbah, M.; Alouini, M.-S.; Yuen, C.; de Rosny, J.; Tretyakov, S. Smart Radio Environments Empowered by Reconfigurable Intelligent Surfaces: How It Works, State of Research, and The Road Ahead. IEEE J. Sel. Areas Commun. 2020, 38, 2450–2525. [CrossRef].

[9] S. Razdan, S. Sharma, Internet of medical things (IoMT): overview, emerging technologies, and case studies, IETE Tech. Rev. (2021) 1–14 ([CrossRef]).

[10] J. Zhu, D.S. Chan, M.S. Prabhu, P. Natarajan, H. Hu, F. Bonomi, Improving web sites performance using edge servers in fog computing architecture, in: Proceedings of the 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, March 2013, pp. 320–323. San Francisco, CA, USA, 25–28, ([CrossRef]).

[11] Y. Flaumenhaft, O. Ben-Assuli, Personal health records, global policy and regulation review, Health Pol. 122 (2017) 815–826 [CrossRef] 12. Directorate-General for Health and Food Safety. eHealth: Digital Health and Care. Available online: https://health.ec.europa.eu/ehealth-digital-health-and-care_en. (Accessed 15 June 2022).

[12] M.H. Van Velthoven, C. Cordon, G. Challagalla, Digitization of healthcare organizations: the digital health landscape and information theory, Int. J. Med. Inf. 124 (2019) 49–57 ([CrossRef]).

[13] N. Kahani, K. Elgazzar, J.R. Cordy, Authentication and access control in E-health systems in the cloud, in: Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE

International Conference on Intelligent Data and Security (IDS), April 2016, pp. 13–23. New York, NY, USA, 9–10, ([CrossRef]).

[14] D. Ferraiolo, R. Chandramouli, R. Kuhn, V. Hu, Extensible access control markup language (XACML) and next generation access control (NGAC), in: Proceedings of the 2016 ACM International Workshop on Attribute Based Access, 11 March 2016, pp. 13–24. New Orleans, LA, USA, ([CrossRef]).

[15] C. Ge, Z. Liu, L. Fang, A blockchain based decentralized data security mechanism for the Internet of Things, J. Parallel Distr. Comput. 141 (2020) 1–9.

[16] Góngora Alonso Susel, Jon Arambarri, Miguel López-Coronado, Isabel de la Torre Díez, 'Proposing new blockchain challenges in eHealth, J. Med. Syst. 43 (2019). Article number: 64.

[17] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Blockchain for secure ehrs sharing of mobile cloud based e-health systems, IEEE Access 7 (2019) 66792–66806.

[18] D. Vujiıciťc, D. Jagodiťc, S. Randiťc, Blockchain technology, bitcoin, and Ethereum: a brief overview, in: 2018 17th International Symposium Infoteh–Jahorina (Infoteh), IEEE, 2018, March, pp. 1–6.

[19] Ethereum blockchain. https://ethereum.org/en/developers/docs/smartcontracts. (Accessed 13 March 2022).

[20] S. Salonikias, M. Khair, T. Mastoras, I. Mavridis, Blockchain-based access control in a globalized healthcare provisioning ecosystem, Electronics 11 (2022) 2652, https://doi.org/10.3390/electronics11172652.

[21] C. Cachin, Architecture of the Hyperledger Blockchain Fabric, 2016. (Accessed 16 March 2022).

[22] N. Rifi, E. Rachkidi, N. Agoulmine, N.C. Taher, Towards using blockchain technology for eHealth data access management, in: 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME), IEEE, 2017, October, pp. 1–4.

[23] Remix IDE. https://remix- ide.readthedocs.io/en/latest/#:~:text=Remix%20IDE%20is%20an%20open,for %20learning%20and%20teaching%20Ethereum. (Accessed 20 March 2022).