Securing IOT Driven Remote Helathcare Data Through Blockchain

Sarthak Gupta[1], Virain Malhotra[2], Dr Shailendra Narayan Singh[3]
CSE Department, ASET, Amity University Uttar Pradesh, India [1, 2] and Associate Professor
CSE Department, ASET, Amity University Uttar Pradesh, India[3]
guptasarthak03@gmail.com [1], virain.malhotra3@gmail.com[2], Snsingh36@amity.edu[3]

***Abstract* - Blockchain is the latest technology which is used in cryptocurrencies such as bitcoin and ether. Blockchain is the decentralized distributed ledger which is based on the peer to peer network method. As the blockchain is mainly developed for implementation in the virtual cryptocurrency such as bitcoin, so its main purpose is clear that is security. Even though the health care industry is leading in majority of fields whether it is technology, equipments, researches, medicines etc We have even reached to remote locations through IOT devices and but one major thing is still lacking that is security of the data Huge amount of data is being generated everyday from patient's medical checkups, treatments, symptoms etc which near to be dealt with care as they are very crucial and can be tempered by hackers which can lead to serious problems. Therefore such critical data must need to be secured with blockchain as it makes it very difficult to tamper with data. This paper deals with the implementation of the blockchain to solve the above mentioned problems.**

***Keywords*— Etherium, Smart contracts, Blockchain, IoT, IPFS.**

I. INTRODUCTION

Presently there is a huge advancement in the technology. There is advancement in various fields such as agriculture, space, automobiles etc. But the most important advancement has been made in the field of Healthcare. The new technologies such as IoT have helped in covering and monitoring the health of remote population. People who don't have access to doctors due to lack of availability of doctors in such areas can get their health checkups on regular basis with the help of IoT and also get recommendations and prescription based on the data retrieved during the checkups. All this is possible while the patients don't have any means to contact the doctor face to face. All the data respective to the patient collected during the checkups or during the treatment which includes BP level, pulse rate, ECG etc is stored on the website. Both patient and doctors can access those data to monitor and analysis the patient medical history and recovery.
But along with the advancement in the technology and huge amount of data being generated there comes the threat of tampering of data which can be fatal especially in the case of healthcare. As the data can be misused this can harm the patients' health. Hackers can also modify the data which will result in the distortion of the treatment going on. Since the security of the data is very essential in the healthcare applications therefore the data must be dealt with care and must be prevented from any kind of data tampering with the most secured technology such as blockchain.
Blockchain is the decentralized distributed ledger which is based on the peer to peer network method. As the blockchain is mainly developed for implementation in the virtual cryptocurrency such as bitcoin, so its main purpose is clear that is security. To hack or corrupt the data secured by the blockchain one need to change entire chain of blocks, which requires huge computational power and therefore is very difficult to do. This paper deals with the implementation of the blockchain in securing the healthcare data and preventing it from data manipulations by hackers.

II. PROPOSED MODEL

Looking at the problem of insecurity of data in the above existing system, the proposed system introduces the concept of blockchain. Blockchain is the decentralized distributed ledger which is based on the peer to peer network method. It is a global online database that anyone, anywhere with an internet connection can use. Unlike traditional databases which are maintained and third party, the blockchain doesn't belong to anyone. Blockchain stores information permanently across a network of personal computers, this not only decentralized the network but distributes it too.[4] Every new block which is added in the blockchain is shared with the other blocks with the timestamp and thus each block in the blockchain contains the information of the other blocks. This makes the blockchain hack proof and difficult to tamper with.

a. Integration of IOT with Blockchain

IOT is making huge advancement in wireless communication, sensor based technology a and if we combine it with the technologies like Big data and Artificial Intelligence it makes the system more intelligent while not exceeding the cost. But taking into the consideration the limited maintenance cost and management cost there is restricted privacy of data and also insecure exchange of data among the personal computers. There comes concept of Blockchain into play.[7]

Blockchain which is based on the distributed ledger technology can be implemented to IOT networks which themselves are distributed in nature. Therefore these networks

can be secured and shielded from any kind of data tampering at any point.[8]

b. Blockchain in Healthcare

Remote healthcare monitoring and analysis requires cloud storage for resilience and easy access of the data retrieved. Even though cloud is the best platform for privacy and sharing of data among various subjects involved in healthcare monitoring analysis such as patients, doctors, data analyst etc, it does not supports interoperability among the above mentioned stakeholders and also it does not guarantee the integrity and authenticity of medical data.[1]

So to mitigate the above flaws, blockchain technology can be incorporated in this model which ensures and enhance integrity, consistency and also authenticity of the medical records stored.[6] High security and confidentiality of medical data is the first and foremost thing of concern for the patients and all this data should be accessed by only an authorised person. This concern is placated with the help of this technology – Blockchain

Fig 2: Digital signature formation

And once we add the concept of Artificial Intelligence into the concept of securing medical data in blockchain it will eventually become smarter and more secured by automatically realising that this data is of concern and to be secured and which one needs to be discarded.[9]

c. Technologies used and Softwares

1. Ethereum: Ethereum is a distributed computing platform which is based on blockchain and is open source and public. It also features smart contract functionality.[2] It is actually modified version of Nakamoto consensus rough state transition which is based on transaction. Example Cryptocurrency like ether is generated by this blockchain platform. It is written in Go, C++ and Rust.[10]
2. DApps:- These apps which are similar to normal apps from the user point of view are seemingly so only from the front end which is the code written in HTML or CSS. But the difference comes in the backend of the DApps which are distributed peer to peer network and not like backend of normal apps which have server in the backend. Since the applications are distributed peer to peer network these are very helpful in medical apps.
3. Smart Contracts:- Smart Contracts are brain of blockchain so are most important component to be deployed along with blockchain to IoT devices. Specifically, Smart contracts can be considered as scripts and are written in the form of conditional statements and if true actions will be triggered else not.[3]

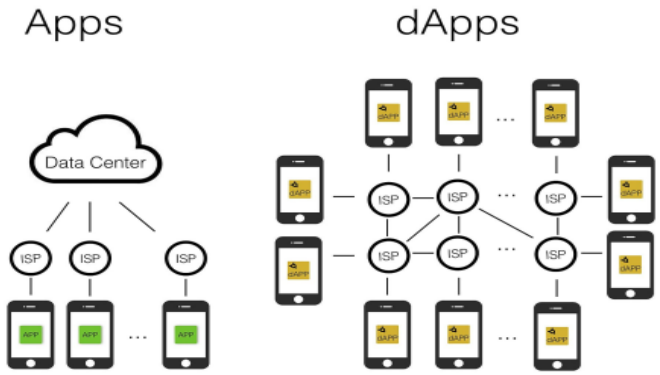


Fig 1: Comparison between Apps & dApps

4. Python:- Python is a high-level general purpose programming language. It is utilized in both machine learning and blockchain applications because of its scalability, portability, robustness, powerful design etc. Python is also very easy to implement as compared to the other programming languages. It is well equipped with the huge amount of inbuilt libraries which can be directly implemented in the AI and Blockchain through a GSM module.

III. WORKING

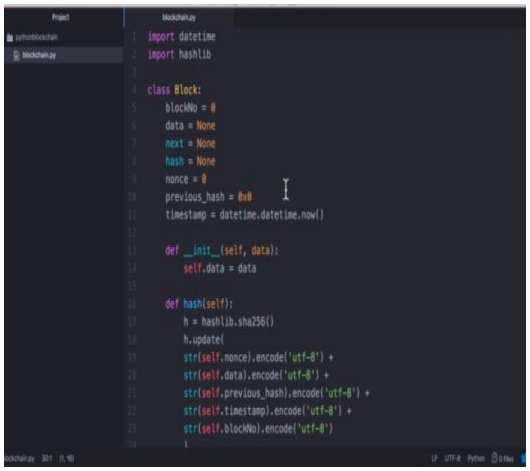
First of all the IoT devices containing sensors will be provided to each patient and the sensors installed in them will continuously monitor the health of the patient carrying that device. The reports of the monitored data will be sent to the doctor on his mobile device and also to the server through a GSM module.

Fig 3: Patient's health data

Moreover the data could also be viewed on a website (as shown in fig 2). And also any abrupt change in the normal behaviour in the patient's health will also be reported with a warning notification to the doctor. But with so much of data stored on the cloud there is a need to secure that humongous amount of data and prevent it from tampering. This virtue is done with help of Blockchain.

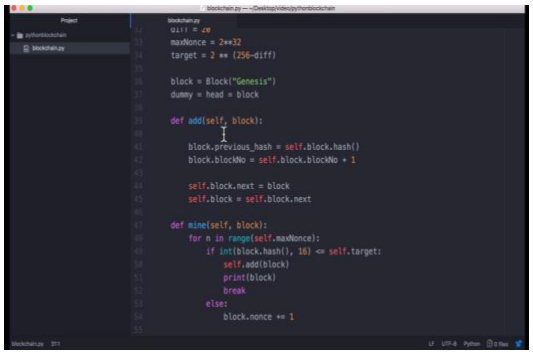
For this, first of all we will have to write a code for the blocks in programming language like python. Here we will create a

class Block with a Block number, data, a pointer to the next block and a hash function of the block. Most importantly a block has the hash function of the previous block which makes a blockchain immutable. There is also a timestamp related to a block this time stamp helps in synchronization of the blockchain.[5]



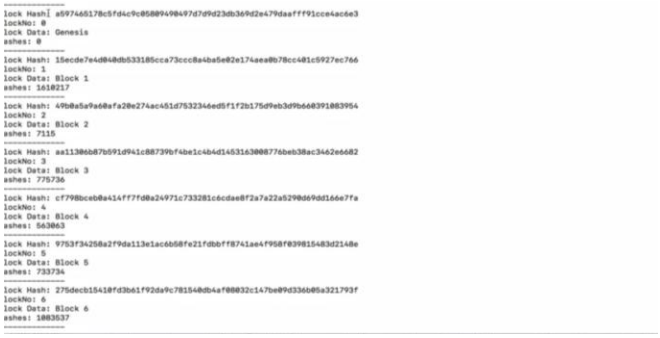
```
import datetime
import hashlib

class Block:
    blockNo = 0
    data = None
    next = None
    hash = None
    nonce = 0
    previous_hash = 0x0
    timestamp = datetime.datetime.now()

    def __init__(self, data):
        self.data = data

    def hash(self):
        h = hashlib.sha256()
        h.update(
        str(self.nonce).encode('utf-8') +
        str(self.data).encode('utf-8') +
        str(self.previous_hash).encode('utf-8') +
        str(self.timestamp).encode('utf-8') +
        str(self.blockNo).encode('utf-8')
        )
```

Fig 4(a): Python source code



```
    maxNonce = 2**32
    target = 2 ** (256-diff)

    block = Block("Genesis")
    dummy = head = block

    def add(self, block):

        block.previous_hash = self.block.hash()
        block.blockNo = self.block.blockNo + 1

        self.block.next = block
        self.block = self.block.next

    def mine(self, block):
        for n in range(self.maxNonce):
            if int(block.hash(), 16) <= self.target:
                self.add(block)
                print(block)
                break
            else:
                block.nonce += 1
```

Fig 4(b): Python source code



```
lock Hash: a97746178c5fd4c9c0580949049d7d9d23db369d2e479daaffff91cce4ac6e3
lockNo: 0
lock Data: Genesis
ashes: 0

lock Hash: 15ecde7e4d04d0db533105cca73ccc8a4ba5e82e174aea0b78cc401c5927ec766
lockNo: 1
lock Data: Block 1
ashes: 1610217

lock Hash: 49b0a5a9a60afa20e274ac451d7532346ed5f1f2b175d9eb3d9b660391083954
lockNo: 2
lock Data: Block 2
ashes: 7115

lock Hash: aa1130bb87b591d941c88739bf4be1c4b4d145316300877 6beb38ac3462e6682
lockNo: 3
lock Data: Block 3
ashes: 775736

lock Hash: cf798bceb0a414ff7fd0a24971c733281c6cdae8f2a7a22a5290d69dd166e7fa
lockNo: 4
lock Data: Block 4
ashes: 563063

lock Hash: 9753f34258a2f9da113e1ac6b58fe21fdbbff8741ae4f958f03981548 3d2148e
lockNo: 5
lock Data: Block 5
ashes: 733734

lock Hash: 275decb15410fd3b61f92da9c781540db4af00032c147be09d336b05a321793f
lockNo: 6
lock Data: Block 6
ashes: 1083637
```

Fig 5: Output

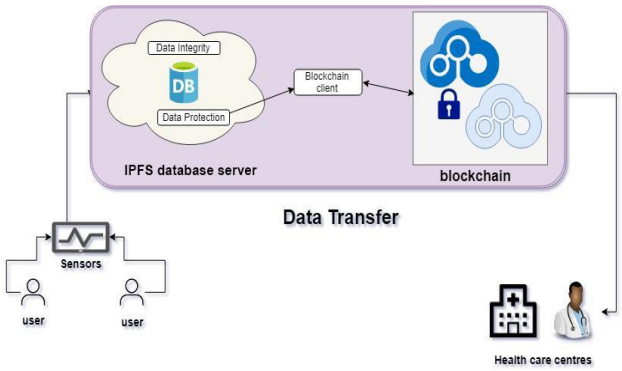


Fig 6: Block Diagram of proposed model

Now once the data of a patient is stored in the form of a string on the block, it gets added to the node along with hash describing the location of the block. Now the smart contract will come into play by connecting it with blockchain which will maintain the privacy and security of the blockchain. The patient – client relation is secured by deploying smart contracts on blockchain. And the data generated by sensors such as Blood Pressure Level, ECG etc. will be sent and stored in off chain database like IPFS through gateways like mobiles and laptops. A hash included in blockchain which will be sent via notification will tell the location and will be sent through client for example clients of Ethereum- geth or PyEth.

Now after the setup is done we will go on to implementation. As we are working on Ethereum environment we are working on the public domain. A patient's health will be detected by sensors and a node is created by Arduino Uno and another node is created at a database IPFS. The patient at a remote location with sensors gets its checkups done and a block will be created with data and hash on it. The patient's block will hold a private key. An authorized doctor will only be able to access that crypt block using its public key and no one else.

Later on, Using smart contracts the data will be stored on an off chain database IPFS and communication between doctor and patient will occur when the doctor will receive the notification about any abrupt change in the normal behaviour or the reports of the patient. That authorized doctor will use his public key to access that information. After a new health report, a new block is added to the previous ledger using the hash of the previous block and a new hash is assigned to the new block. Since a cryptic language is used and a chain of blocks is made which is interconnected, now if hacker will perform some tampering in any one of the blocks, he will have to change the data of in every block because a hash function is linked with each block.

Fig 7: Flowchart of proposed model

Moreover the patient and the doctor will get to know about tampering. So now it becomes very tedious and almost impossible to tamper the data.

Patient ID	Doctor Assigned	Date Repoted	Timestamp	Temperature	Blood pressure	ECG	Hashed History
101	Dr. M	12/2/17	Tmp#1	102 F	85 bpm	value 1	hexa#1
409	Dr. Z	16/3/18	Tmp#2	97 F	110 bpm	value 2	hexa#2

Fig 8: Observed values

IV. CONCLUSION AND FUTURE SCOPE

We used the concept of Cloud computing to conclude our research paper. All the necessary data can be saved on cloud and data analytics can be performed to observe some patterns on health problems based upon region, climate, time, number of patients with similar symptoms etc. Patients who are willing to share their health records and medical data can be given some incentives in cash which will inspire more patients to cooperate and aid in analysis. Further the fees of prescribed doctors can also be paid through in-system online cash service which will also be protected by the blockchain.

Also the authorized family members and guardians can be provided facility through which they can access the website and monitor the patient's condition from the distant location.

REFRENCES

[1] Nabil Rifi , Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher "Towards Using Blockchain Technology For eHealth Data Access Management" 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME) DOI: 10.1109/ICABME.2017.8167555

[2] Michael Coblenz "Obsidian: A Safer Blockchain Programming Language" 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C) DOI: 10.1109/ICSE-C.2017.150

[3] Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, Yasuhiko Miyazaki, Akihito Akutsu, Jay Kishigami, "Blockchain Contract: Securing a Blochain Applied to Smart Contracts" 2016 IEEE International Conference on Consumer Electronics (ICCE) DOI: 10.1109/ICCE.2016.7430693

[4] Madhusudan Singh, Abhiraj Singh, Shiho Kim "Blockchain:A Game Changer For Securing IoT Data" 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) DOI: 10.1109/WF-IoT.2018.8355182

[5] https://www.youtube.com/user/CreatiiveCode

[6] Blockchain: Opportunities for Health Care, August 2016, [Online]Available:deloitte.com/content/dam/Deloitte/us/Documents /publicsector/us-blockchain-opportunities-for-health-care.pdf

[7] Sayed Hadi Hashemi, Faraz Faghri, Paul Rauschy and Roy H Campbell,"World of Empowered IoT Users", 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI),2016

[8] Das, Manik Lal, "Privacy and Security Challenges in Internet of Things," Distributed Computing andInternet Technology.,pp.33-48, 2015.

[9] On Public and Private Blockchains, "https://blog. ethereum.org/2015/08/07/on-public-and-privateblockchains/, "2017

[10] Ethereum Foundation, "Ethereum project," http://www.ethereum.org. Accessed Jan. 3, 2017