International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

A Novel Healthcare-based Block chain (HBC) System for Security Healthcare Data and Privacy Protection

Shyam Mohan J S , S Monisha

Assistant Professor, Computer Science and Engineering, Sri Chandrasekhrendra Saraswathi Viswa Maha Vidhayalaya (SCSVMV), Tamilnadu, India.
Student, Computer Science and Engineering, Sri Chandrasekhrendra Saraswathi Viswa Maha Vidhayalaya(SCSVMV), Tamilnadu,India.

Abstract

Due to the increasing innovations in the healthcare sector and medical field, particularly after the Covid-19 pandemic, a strong security mechanism is needed to secure and protect the data of patients collected from various hospitals. Electronic Health Record systems (EHRs) consist of clinical notes, patient listings, lab results, imaging results, screening tests, etc. Privacy and security are the key concern for the healthcare sector. In this paper, we propose a novel Healthcare Block chain (HBC) for securing the confidential details of the patient data. We have explored the real-time applications in healthcare sectors using HBC and tried to provide a framework for tamper-proof data. The proposed HBC model addresses the problems related to securing patient data. This paper also provides insights into driving forces for technological framework from a theoretical perspective to performance evaluation metrics.

Keywords

Block chain Technology, Data Privacy, Electronic Health Record System, Patients Privacy, Data Protection

1. Introduction

Smart technologies, such as the Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning, Virtual Reality (VR)and Augmented Reality (AR), have revolutionized the engineering and manufacturing sectors, including automotive, computing, and electronics, and aerospace and defense. Healthcare systems were adopted by healthcare providers, like hospitals and general practitioners, are no exception. Over time, they have becoming more powerful and useful [1]. Similarly, EHR systems [2] began to emerge which the integrated stand-alone non-networked systems, including the social media channels, to store patient information and this made the sharing of health data over networked channels, including social media, or between druggist, using EHR systems. Interaction and communication between healthcare providers and patients were also enhanced From 2016 to the present day, we have experienced the Healthcare 4.0 era. This era was came from the concept of Industry4.0, where Hi-tech and Hi-touch systems are being introduced, using technologies like cloud computing, fog and edge computing, big data analytics, AI, and machine learning, to build block chains to support real-time access to patient's clinical data [3]. Healthcare data requires a high level of privacy and security. Privacy refers to persons having the correct rights to allow or disclose personal information to others. This demands consensus among the healthcare providers and regulators, and the creation of agreed policies and procedures. Privacy is the starting point to determining who and whom should be allowed to access personal patient information [4]. In line with this issue, numerous security standards have been developed, such as HIPAA, COBIT, and DISHA, which have been applied to protect patients' health information. Healthcare security is also of paramount importance to healthcare providers to help safeguard the privacy of patient's health information. This includes managing access control of patient information, security of patient data from unauthorized users, the modification and destruction of stored data, etc[5]. The fitness of data stored on HER systems plays a critical role in the success of a healthcare provider [6]. The security of healthcare records is becoming increasingly important for keeping data safe from security breaches and criminal activity. If unauthorized users can gain access to patient data, it can be sold or leaked to the market, with patients' personal information being revealed to anyone with access. This information may include addresses, telephone numbers, full names, etc. The privacy of patients' data is essential in successful healthcare management [7]. In recent years, research relating to block chain and smart ledgers has gained in popularity due to the emergence of crypto currencies, such as Bit coin and Ethereum.

Block chain stores and shares data in a distributed, trusted, and immutable manner, removing intermediaries, and not requiring a centralized dependency for checking transactions [8,9]. Transparency in block chain provides a less complicated method for accessing ledger-based transactions over networks; it connects with different computing powers from multiple nodes in the block chain network, making it extremely powerful concerning calculation speed [10]. The block chain network then uses the SHA-256 algorithm to create a unique hash. All hashes are then linked through a previous hash; this makes an unbreakable network of transactions. If someone attempts to append a transaction, then it would be validated by the network node or by a smart contract, consensus. This immutable ledger, therefore, cannot be modified [11]; it can only be appended to the transaction of blocks.

This paper is organized into the following sections: Section II describes the related work involved. Section III discusses the solutions. Sections IV provide our proposed work and process, Section V discusses about the algorithms we used, Section VI discusses the experimental setup, section VII provides the results of the proposed work followed by conclusion.

2. Related Works

Yup etal. (12) explored the block chain approach for healthcare intelligence concerning the sequestration of druggies. They proposed a data access control for sequestration and designed the healthcare data gateway. Zhang etal. (13) proposed PSN- grounded healthcare to secure the system, designing two protocols for authentication and sharing of healthcare data within a block chain network. Xia etal. (14) designed a block chain- grounded approach for healthcare data sharing using pall- grounded services. They proposed the Med share system for access control, provenance, and security of medical records. Liang etal. (15) designed a mobile- grounded healthcare record sharing system using block chain, proposing a secure stoner-centric approach to give access control and sequestration using a channel conformation scheme. Jiang etal. (16) proposed a medical data exchange system using block chain, accordingly developing out- chain and on- chain verification for the security of the system's storehouse. Li etal. (17) explored data protection systems for healthcare, proposing algorithms for memory operation that help in data operation. Fan etal. (18) proposed block chain- grounded medical information of cases, perfecting agreement mechanisms to achieve enhanced security and sequestration of data within the system. Wang and Song (19) proposed a secure medical record sharing system using an trait- grounded encryption medium. They used smart contracts to insure the integrity and traceability of the health data. Guo etal. (20) presented an trait- grounded hand scheme for multiple druggies in electronic health record operation, using block.

3. Solutions

Secure transmission and preservation of privacy for the patients' tending knowledge area unit the most issues within the e-health application. However, the redistributed essence of the block chain and alternative attributes like fixity and transparency bu ild block chain terribly appropriate for e health. however there area unit still challenges for applying. Currently we have a tendency to discuss the challenges and justify our solutions.

3.1. Knowledge Storage

It isn't sensible and appropriate to store IoT huge knowledge on the block chain ledger. Attributable to this, we have a tendency to don't store the information on the block chain, however solely we have a tendency to store the tips to the information (hash of encrypted data) on block chain to lighten the cupboard space of bloc chain. the information (encrypted data) area unit hold on on Off chain storage

3.2 Security of knowledge

Patients' tending knowledge area unit sensitive. To satisfy the safety of knowledge, we have a tendency to use a bilaterally symmetric key secret writing theme. At first, the information is encrypted by bilaterally symmetric key secret writing so sent to the block chain network. Therefore even in Off-chain Storage, {the information |the knowledge| the knowledge} is hold on within the type of encrypted data.

3.3 Patients' Privacy

The most concern that's self-addressed during this paper is conserving patients' privacy as a result of Patients' tending knowledge is extremely privacy-sensitive. we have a tendency to assume that the medical staffs area unit honest-but-curious. In our system, patients may be stay (pseudo) anonymous. At a similar time, medical workers profiles may be hold on the block chain in order that patients will trust medical workers by supportive medical workers identities. Our projected platform satisfies the subsequent Items:

1)Patients' knowledge Ownership: In our platform, patients area unit the sole owner of their tending knowledge, and solely they'll management that knowledge. As such, the platform acknowledges the medical workers as Service suppliers with granted permissions set and also the patients as tending knowledge homeowners.

2) Fine-grained Access Control: every patient will grant a group of permissions to any desired member of the medical workers for accessing a patient's tending knowledge. Also, the patient will alter or revoke the set of granted access permissions. These permissions area unit firmly hold on block chain ledger as access-control policies, wherever solely the patient will modification or revoke them.

3) Knowledge Transparency and Audit ability: Patients have complete and correct transparency over their collected tending knowledge, and that they will savvy medical workers will access to tending knowledge.

4. Proposed system

In this Project, we are describing security issues for patient health records stored in a Decentralized (data will be maintained at multiple peer or systems) Block chain server. Nowadays patient data can be shared between multiple hospitals, insurances agencies, governments, and labs. Due to sharing of data there will be data security issues raised for the patient as this data can be misused by agency peoples or attackers may steal this data. . To overcome from this problem we are using a Decentralized Block chain server which maintains data as blocks of trees and at each transaction all previous hash code will be verified and if verification successful then data will be considered as intact and if data changes then Block chain server will notify that system is under attack and it gathers data from another working node. Due to this transaction hash code verification and immutable data storage make Block chain secure and trustable in the current market.

5. Proposed method

Our proposed method consists of the following modules:

1. Users

2. Healthcare agents

3. Cloud storage

4. Off chain Server:

5.1 Users:

This are patients who create their medical profiles and give permission access to Healthcare agents and this permission can be controlled by access control program to decide which users allowed to access patient data

5.2Healthcare Agents:

This can be doctors, insurance companies or government users and here government can access patient data to know how many people are suffering from which disease. Insurance companies can access this data to decide to give insurance policy to patients or not and doctors can access this data for treatment.

5.3 Cloud Storage:

Here blockchain encrypted data storage will be consider as cloud storage as we don't have any cloud server so we are storing data in blockchain server i.e. offchain server.

5.4 Off chain server:

We store patients' encrypted data on off-chain storage. For the implementation of off-chain storage, we use The Interplanetary File System (IPFS) that is a peer-topeer distributed file system that seeks to connect all computing devices with the same system of files. It provides a high throughput content-addressed block storage model, with content-addressed hyperlinks. IPFS combines a distributed hash table (or DHT), an incentivized block exchange, and a self-certifying namespace. IPFS has no single point of failure, and nodes do not need to trust each other. In IPFS, we distribute the data and store them on different servers all over the world. Not using the central server is the reason for the advantage of IPFS over conventional cloud storage.

In proposed method, data is obtained from IOT sensors, medical system etc.. The patient will create an account with a specific user id and password in that all the medical records will be uploaded. For example if a patient wants to send the all the medical record to another doctor who is far from them to get suggestions of their health, the patient will give access to them to see all the records. Similarly, if the patient wants to get the insurance then the patient will give access to that company as a proof.

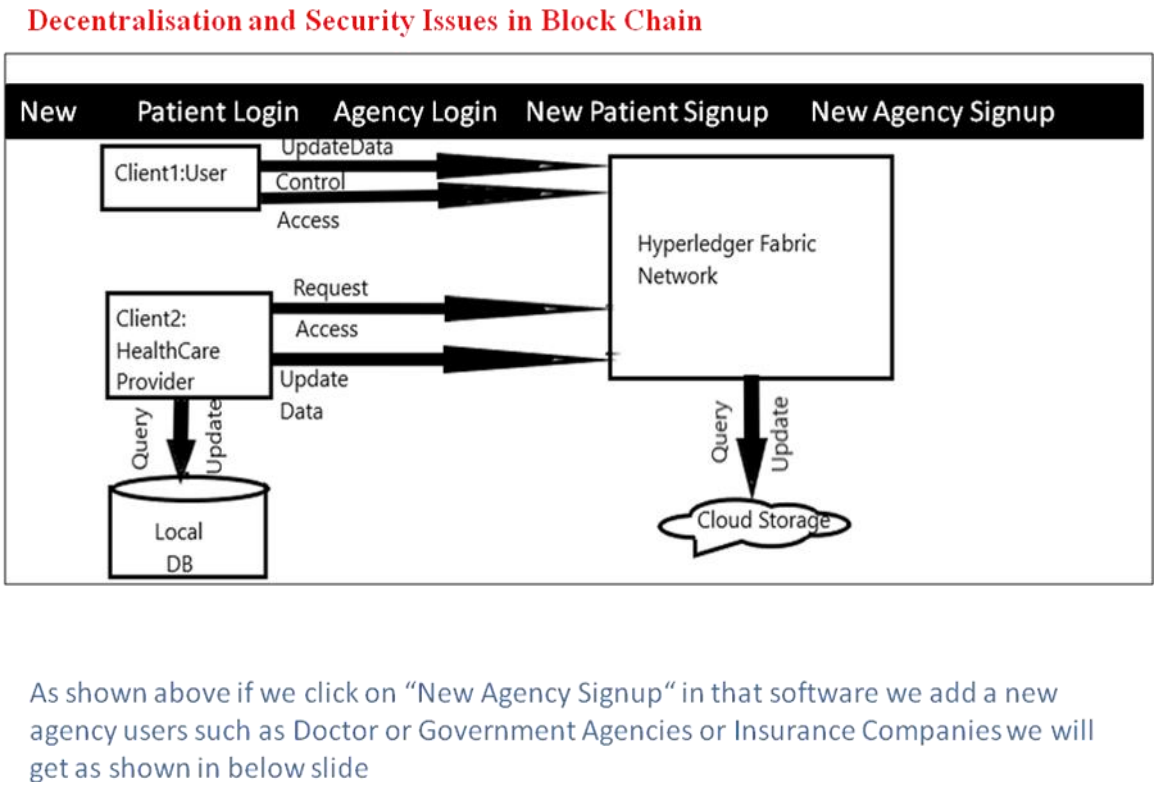

Fig.1 *Decentralization and Security issues in Block chain*

6. Algorithms Used:

1. For patient data security we are using AES encryption and decryption algorithm.

2. Blockchain consensus hashcode algorithm is used to generate hashcode for each record and this patient record and hash code will be store inside RTREE as nodes

3. Before storing new record blockchain consensus algorithm will validate all previous hashcode to check any previous data is changed by hacker or not.

4. If not changes then blockchain will store new record and if changed then blockchain will contact another node from decentralized list of nodes to store new record and mark that machine as attacked.

5. All this execution steps will called as proof of work in blockchain terminology

• To Create Initial Block in Blockchain:

```
def create_genesis_block(self):
        genesis_block = Block(0,[],time.time(),"0")
        genesis_block.hash = genesis.compute_hash()
        self.chain.appen(genesis_block)
```

• To add new block to blockchain:

```
def add_block(self,block,proof):
        previous_hash = self.last_block.hash
        if previous_hash != block.previous_hash: #hashcode verification
        return false if not self.is_valid_proof(block,proof):
        return false block.hash=proof print(" "+str(block.hash)) self.chain.append(block) return True
```

• Proof of work(PoW) compilation:

To check if block_hash is valid hash of block and satisfies the difficulty criteria.

```
def is_valid_proof(self,block,block_hash):
print (" "+str(block_hash == block.compute_hash())+ " "+block.compute_hash+"
"+str(block_hash.startwith('0' * Blockchain.difficulty))) return(block_hash.startswith('0' *
Blockchain.difficulty) and
block_hash == block.compute_hash())
```

7. Experimental Setup

For the testing performance of the proposed framework we have conducted experiments by using the following configurations: Intel Core i7-6498DU CPU @ 2.50GHz 2.60 GHz Processor and 8.00 GB of memory with Windows 64-bit OS (version 10).

7.2 Software Required

Python 3.7

8. Result

This project can be run by the following users

- *Users: These are patients who create their medical profiles and give permission access to Healthcare agents and this permission can be controlled by an access control program to decide which users allowed to access patient data*
- *Healthcare Agents: This can be doctors, insurance companies, or government users and here government can access patient data to know how many people are suffering from which disease. Insurance companies can access this data to decide to give insurance policies to patients or not and doctors can access this data for treatment.*
- *In the proposed Project we are gathering patient data from IoT sensors but we don't have such sensors so we are entering patient's records manually and then share with different users. Cloud Storage: Here Block chain encrypted data storage will be considered as cloud storage as we don't have any cloud server so we are storing data in Block chain server*

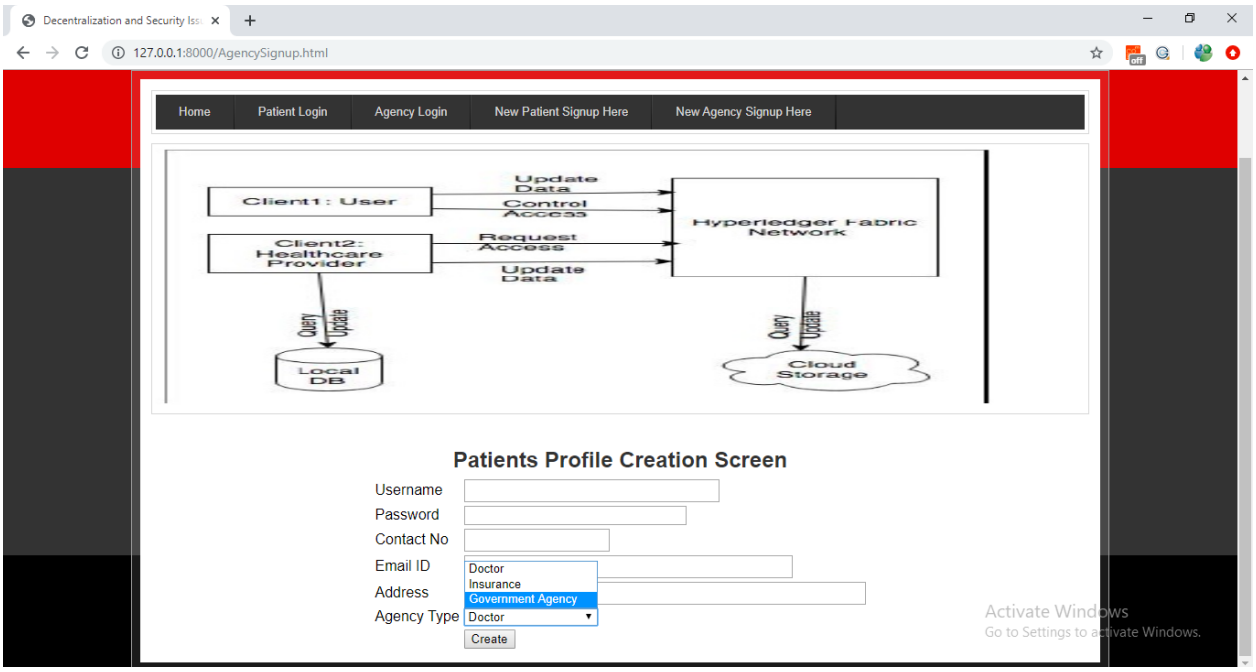

Fig 2. *Patients Profile Creation*

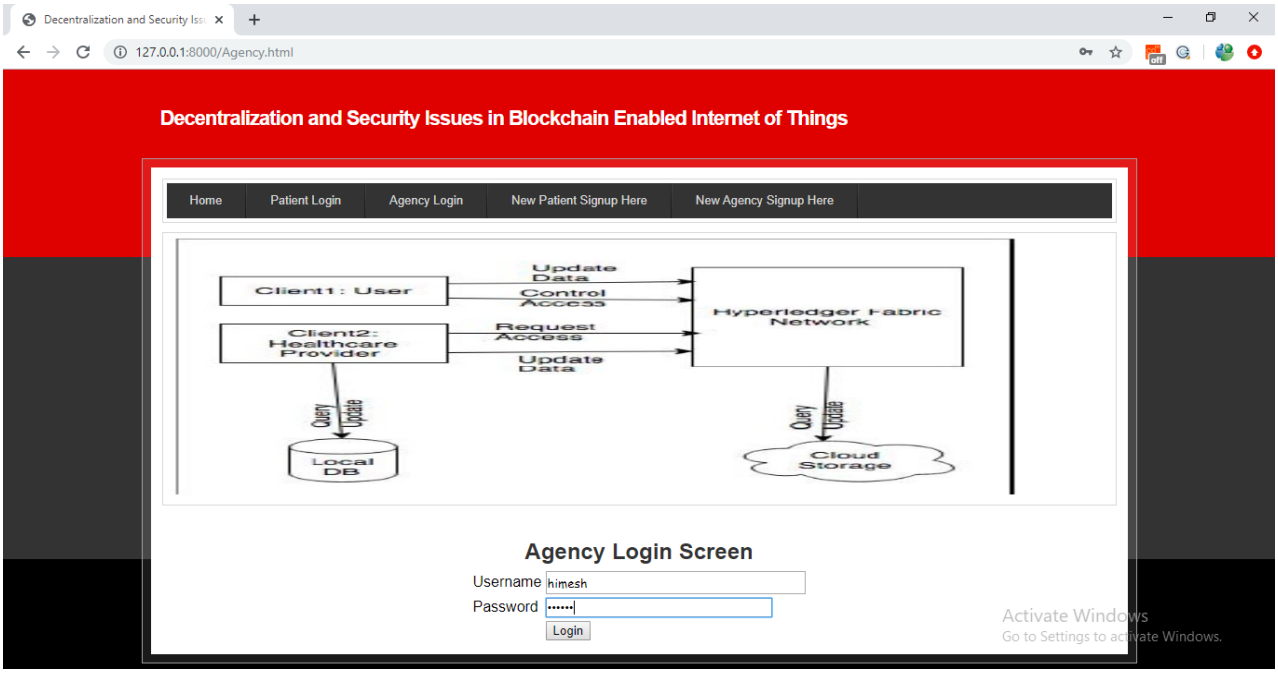

Fig 3. Agency Login

In the above screen doctor, Himesh is login and he has permission to access patient data so he can see all records.

9. Conclusion

In this project, we discussed how to block chain technology can be useful for the healthcare sector and how can it be used for electronic health records. Despite the advancement in the healthcare sector and technological innovation in EHR systems they still faced some issues that were addressed by this novel technology, i.e., block chain. Our proposed framework is a combination of secure record storage along with the granular access rules for those records Also, the framework proposes measures to ensure the system tackles the problem of data storage as it utilizes the off-chain storage mechanism of IPFS. And role-based access also benefits the system as the medical records are only available to trusted and related individuals. This also solves the problem of information asymmetry of the EHR system.

References

[1] Kumari A, Tanwar S, Tyagi S, KumarN. Fog calculating for healthcare4.0 terrain openings and challenges. Comput Electric Eng 2018

[2] Vora J, DevMurari P, Tanwar S, Tyagi S, Kumar N, ObaidatM. Blind autographs grounded securede-healthcare system. In 2018 International conference on computer, information and telecommunication systems (CITS); 2018

[3] Kumari A, Tanwar S, Tyagi S, Kumar N, Parizi RM, Choo K-KR. Fog data analytics a taxonomy and process model. J Netw Comput Appl 2019.

[4] Vora J, Italiya P, Tanwar S, Tyagi S, Kumar N, Obaidat M, et al. Icing sequestration and security ine-health records. In 2018 International conference on computer, information and telecommunication systems (CITS); 2018

[5] Chen L, Lee WK, Chang C-H, Raymond Choo K-K, ZhangN. Blockchain grounded searchable encryption for electronic health record sharing. Fut Gener Comput Syst 2019.

[6] Hathaliya JJ, Tanwar S, Tyagi S, KumarN. Securing electronics healthcare records in healthcare4.0 a biometric- grounded approach. Comput Electric Eng 2019.

[7] Shae Z, Tsai JJ. On the design of a blockchain platform for clinical trial and perfection drug. In 2017 IEEE 37th transnational conference on distributed computing systems (ICDCS); 2017.

[8] Mistry I, Tanwar s, Tyagi S, KumarN. Blockchain for 5g- enabled IoT for artificial robotization a methodical review, results, and challenges. Mech Syst Signal Process 2019.

[9] Kabra N, Bhattacharya P, Tanwar S, TyagiS. Mudrachain blockchain- grounded frame for automated cheque concurrence in fiscal institutions. Fut Gener Comput Syst 2020.

[10] Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat M, et al. Bheem a block chain- grounded frame for securing electronic health records. In 2018 IEEE globe com shops (GC Wkshps); 2018

[11] Alhadhrami Z, Alghfeli S, Alghfeli M, Abella JA, ShuaibK. Introducing block chains for healthcare. In Electrical and calculating technologies and operations (ICECTA), 2017 transnational conference on; 2017

[12] Yue X, Wang H, Jin D, Li M, JiangW. Healthcare data gateways plant healthcare intelligence on block chain with new sequestration threat control. J Med Syst 2016.

[13] Zhang J, Xue N, Huang X. A secure system for pervasive social network- grounded healthcare. IEEE Access 2016.

[14] Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, GuizaniM. Med sharetrust-less medical data sharing among pall service providers via block chain. IEEE Access 2017.

[15] Liang X, Zhao J, Shetty S, Liu J, LiD. Integrating blockchain for data sharing and collaboration in mobile healthcare operations. In Particular, inner, and mobile radio dispatches (PIMRC), 2017 IEEE 28th periodic transnational council on; 2017.

[16] Jiang S, Cao J, Wu H, Yang Y, Ma M, HeJ. Blochie a block chain- grounded platform for healthcare information exchange. In 2018 IEEE International conference on smart computing (SMARTCOMP); 2018.

[17] Li H, Zhu L, Shen M, Gao F, Tao X, LiuS. Block chain- grounded data preservation system for medical data. J Med Syst 2018.

[18] Addict K, Wang S, Ren Y, Li H, YangY. Med block effective and secure medical data participating via block chain. J Med Syst 2018.

[19] Wang H, SongY. Secure pall- grounded EHR system using trait- grounded cryptosystem and block chain. J Med Syst 2018

[20] Guo R, Shi H, Zhao Q, ZhengD. Secure trait- grounded hand scheme with multiple authorities for block chain in electronic health records systems. IEEE Access 2018