IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12314

EHRChain: A Blockchain Based EHR System Using Attribute Based and Homomorphic Cryptosystem

Rajiv M Yadav[1], Feon Jason[2]

Masters Student, School of CS & IT, Jain University, Bengaluru, India[1]

Assistant Professor, School of CS & IT, Jain University, Bengaluru, India[2]

Abstract: The medical industry urgently needs to address issues such as secure storage, reliable sharing, access control and privacy protection. In this article, we propose EHRChain, a blockchain-based EHR system that uses an attribute-based homomorphic cryptosystem to solve the aforementioned problems. First, we designed a medical record storage solution based on blockchain and IPFS technology to achieve secure large-capacity medical data storage and reliable sharing. Second, we proposed an improved cryptographic primitive called SHDPCPC-CP-ABE. Our SHDPCPC-CP-ABE simultaneously realizes the functions of partially concealing ciphertext-based semi-policy and dynamic authority change. In addition, our regime achieves subject neutrality of forensic identification of medical disputes and fine-grained access control to medical data. Third, our system applies an additional homomorphic cryptosystem, the Paillier cryptosystem, with optimized parameters to protect patient privacy during the medical insurance claim process.

Index Terms: Ethereum, Blockchain, EHRchain, Healthcare.

I. INTRODUCTION

A blockchain is a set of blocks linked by cryptographic chains. Blockchain is one of the latest technologies with a stron g foundation in cryptography that allows programs to leverage these capabilities to generate strong security solutions. H ere the data is broken down into chunks and joined by links. Each block has a hash value assigned to it, which is used as the representation of the block. The connection between each block is created by embedding the hash of the previous bl ock into the current block.

A block consists of a data part, a hash, a part and a previous hash, to summarize. The blockchain formed is no longer ke pt in a single machine. Each user of a blockchain (also called a distributed ledger) has their own copy. When someone tr ies to modify the data, the hash is modified, the link is broken, the hash is modified. An attacker must modify and recalc ulate the hashes of subsequent blocks for the attack to succeed.Users govern each block based on their consensus and ca n accept or reject each block. Thus, the blockchain offers security, immutability and transparency. Public, private, and c onsortium blockchains are the three main types of blockchains in use today.

Think of a blockchain as a database A blockchain can be thought of as a distributed database with many users. Each user has access to important information. The basic terms of blockchain are: peer-to-peer network, asymmetric peer-to-peer network, asymmetric encryption, and hashing are all components of peer-to-peer blockchain.

Ciphertext Policy Attribute-Based Encryption (CPABE) is a very powerful asymmetric encryption mechanism, but its complexity and overhead cannot be ignored in the blockchain environment. Additionally, limited devices (such as sensors) often require encrypted data as they are often responsible for sending the sensitive data they collect to more powerful devices (such as storage servers).

This project proposes a new approach to use CP-ABE on very resource constrained sensor nodes in a blockchain environment. The proposed method takes advantage of the cooperation between heterogeneous nodes, making the implementation of CP-ABE feasible in blockchain environments by delegating expensive operations to a set of support nodes. After analysis and experiments, we demonstrate that SHDPCPC-CP-ABE is indistinguishable under a chosen plaintext attack and takes one third of the time of CP-ABE when changing the access policy.Our system outperforms other EHR systems.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12314

II. LITERATURE REVIEW

In , the authors proposed a technique, Ciphertext-policy attribute-based encryption (CP-ABE) for the Electronic Health Record (EHR).

[1] Ramani et al. recommend a blockchain-based secure and effective data access method for the patient and the doctor. The proposed system also sustains the integrity of the system. MeDShare observes objects that receive data for suspicious use from the system. A tamper-proof manner is used to record all the activities offered on the MeDShare system.

[2] Liang, Xueping, et al. recommend a novel user- centric health data access method through a decentralized and permissioned blockchain to preserve privacy through a channel formation scheme.

[3] Wang et al. suggested a safe electronic health record (EHR) scheme using attribute-based cryptography and blockchain technology. [4] Nguyen et al. proposed a new EHRs distributing structure that merges blockchain with a decentralized inter-planetary file system (IPFS) on the mobile cloud. Significantly, the authors created a dependable access control method based on the smart contract to attain safe EHR distribution between various medical providers and patients. The authors concluded that their work presented an efficient solution for dependable information transfers on the mobile cloud, even protecting vital medical data against possible risks.

[5] Ismail et al. suggested a lightweight blockchain framework for healthcare data management, which decreases computing and communication overlaps compared to the Bitcoin network, which divides network contributors into clusters and maintains one copy of the ledger per cluster. Their structure introduces the need for canals, which permit safe and secret transactions within a group of network contributors. Moreover, the authors suggested a solution to prevent the forgery that exists in the Bitcoin network. The authors showed the efficiency of their suggested framework in offering safety and confidentiality to the Bitcoin network by examining various threats. The authors also discuss how their suggested architecture copes with identified threats.

[6] Bodkhe et al. analyzed a variety of solutions using blockchain and also their compatibility with a variety of applications based on Industry 4.0. First, the authors explored current cutting- edge solutions to smart appliances' compatibility with blockchain in different industry 4.0 appliances. The advantages and disadvantages of conventional safety solutions were also explained with regard to their countermeasures. The authors investigated personal healthcare-associated problems inorganizations that can be pursued by blockchain and also its exclusive characteristics, which can be applied to address healthcare challenges. They also reviewed previous work, giving a lot of consideration to the application of blockchain in the healthcare sector. Finally, they discussed the advantages and potential research opportunities for the blockchain-related technology used in the healthcare sector.

[7]Wagh et al. provided a comprehensive overview of blockchain technology. The authors provided a synopsis of blockchain architecture, security in blockchain and its benefits . Furthermore, they explored its application in a new field, namely, the health sector. The authors also discuss how health records in the health information system could be protected using blockchain technology. [8]Ramani et al. suggested blockchain as a shared scheme for healthcare systems. The authors proposed a safe and effective information access method based on blockchain fora patient with a physician in a particular health care setting. Their study of the program's safety demonstrated that it maintains the organization's integrity and can resist well-known attacks . Furthermore, the implementation results illustrate the potential of the system proposed by the authors. Information transfers from one company to another are recorded undamaged on MeDShare, which uses access control mechanisms to efficiently monitor information activities to identify companies involved in breaches of data . [9] Liang et al. suggested an innovative customer-centered medical information distribution system using decentralization with authorized blockchain for defending confidentiality based on channel creation programs and to improve identity management based on a blockchain- supported association service. The mobile appliance created to gather medical information from body sensor nodes also coordinates data for a cloud for distributing information to healthcare providers .

The authors utilized identity-based encryption (IBE) and attribute-based encryption (ABE) to encrypt healthcare information. They also utilized identity-based signatures(IBS) for develop digital signatures. This efficiently facilitates the organization of a scheme that does not require the introduction of various cryptographic schemes for various safety needs. Bach et al. conducted a comparative study of blockchain consensus algorithms, especially Ethereum, which utilizes a consensus protocol known as proof-of-work (PoW). This method allows the decentralized Ethereum networks to come to consensus on the order of transactions and account balances. This prevents customers from "double spending" their money, and also makes sure that the Ethereum chain is extremely hard to overwrite or attack.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12314

III. PROPOSED METHODOLOGY

3.1 SYSTEM ARCHITECTURE

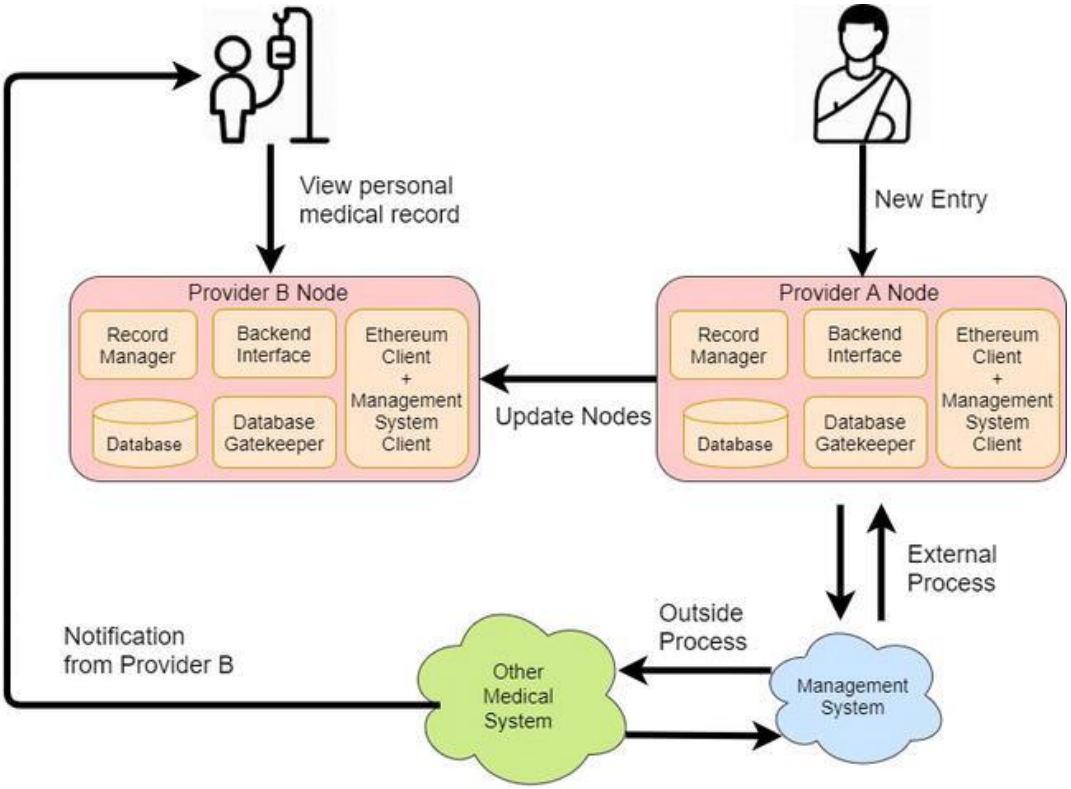


Fig 3.1 System Architecture

3.2 Displays the System's Access Login Design Diagram

Electronic health records (EHR)are regulated by health centers instead of patients, making it difficult to obtain medical advice from various health centers. Thus, patients need to concentrate on restoring the management of their health details and their medical information . The quick evolution of blockchain technology encourages population healthcare, including access to patient information and medical data. The technology offers patients access to extensive, consistent reports with free access to EHRs from treatment websites and providers. In this section, we describe the development of a blockchain security framework for EHR (BSF-EHR) with multiple authorities to meet the need for blockchain in shared EHR systems. This framework protects the privacy of patients and maintains the consistency of EHRs.

The patient visits the doctor. Then doctor treats the patient. After treatment, the doctor uploads the EHR to the server. For future use, the doctor can download the EHR.BSF-HER can be defied as a novel secure electronic health record of patients which could be privately shared by institutions or patients. Using BSF-EHR, the patient is able to manage, download and share his/her EHRs independently. The proposed BSF-EHR framework consists of five parties: the patient, doctor, insurance agent, EHRs server and the data verifier. Similar to the traditional EHR system, the patient visits the doctor. Then the doctor treats that patient. The EHR system server is one of the nodes in a blockchain network. It acts as a miner that collects transactions (EHRs) and organizes them into blocks. Whenever EHRs are created after treatment, all network nodes receive them and verify their validity. Then, the miner node gathers these transactions from the memory pool and begins assembling them into a block. The memory pool is a "waiting area" for transactions that each node maintains for itself. After a transaction is verified by a node, it waits inside the memory pool until it is picked up by a miner and inserted into a block. This new block will then be added to the blockchain. However, before the block can be added to the chain, the information contained in it must be verified by the miner. This happens by creating a so-called "hash". A hash is a 256-bit number that uniquely identifies the data in the block. After block creation, the miner distributes it to all the available nodes in the blockchain network (doctors and patients).

Also, BSF-EHR provides access control for each node based on its own blockchain concept. Through this, the patient can view their own EHR in their own blockchain and no one else can see the details. Additionally, a doctor can view the EHR

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

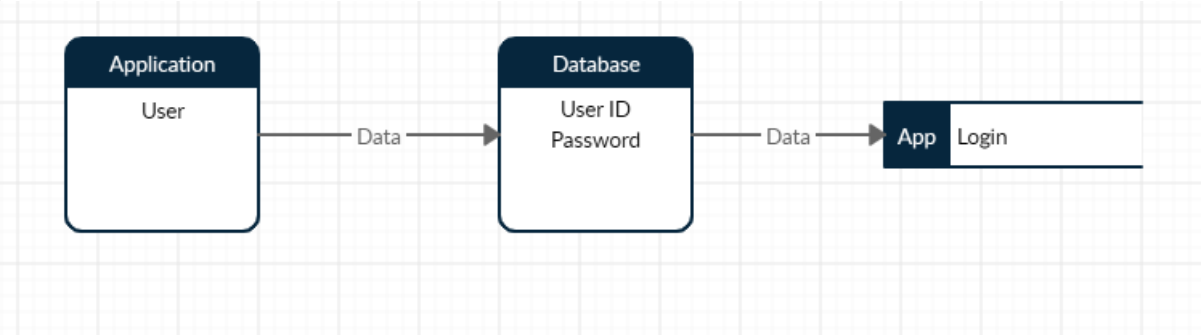
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12314

of patients who have been treated by him/her in their own blockchain. A doctor can view only permission-granted patient blocks in his/her own blockchain. For medical insurance claims, the doctor can share this EHR (copy of own blockchain) with an insurance agent.The insurance agent can view the EHR of patients who claimed in his/her own blockchain and after approval, they can also provide the insurance amount to the patient.Furthermore, the patient can send a data verification request (with a copy of their own blockchain) to the data verifier.Finally, the data verifier checks whether the data are safe or not and provides verification results to the patient.

LEVEL1:

Login:



LEVEL 2:
User:

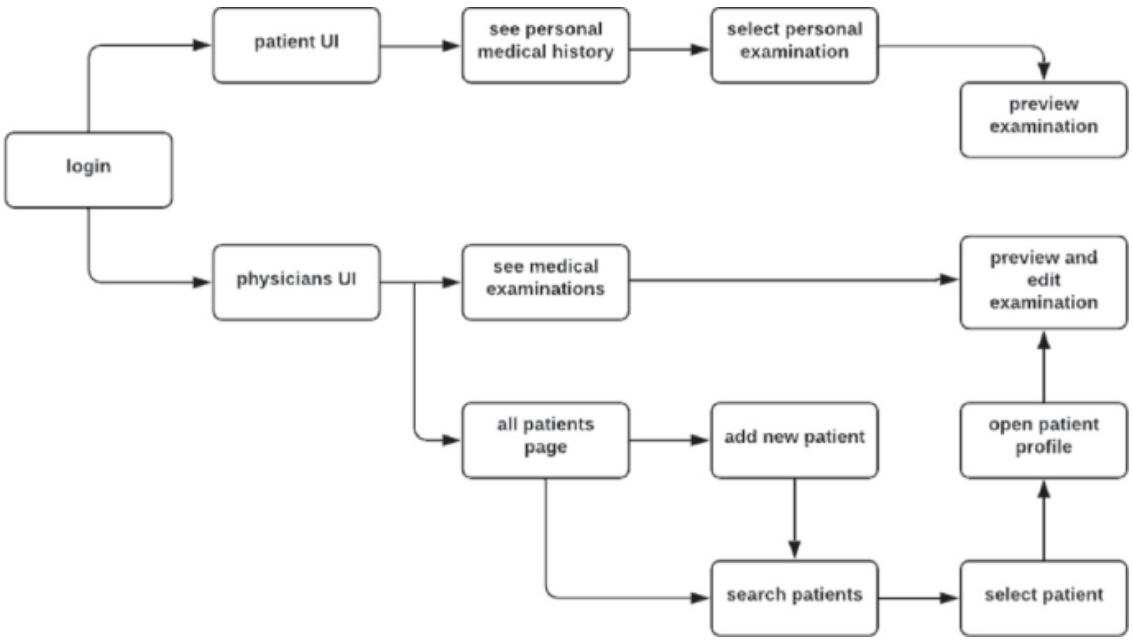


Fig 3.2 The System's Access Login Design Diagram

3.3 Design of EHR

User Interfaces:
This includes the user interface (UI), which allows users to interact with the application, as well as any client-side logic and libraries required to implement the functionality. Testrpc is a Node.js based Ethereum client for testing and development. It uses ethereumjs to simulate full client behavior and make developing Ethereum applications much faster.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

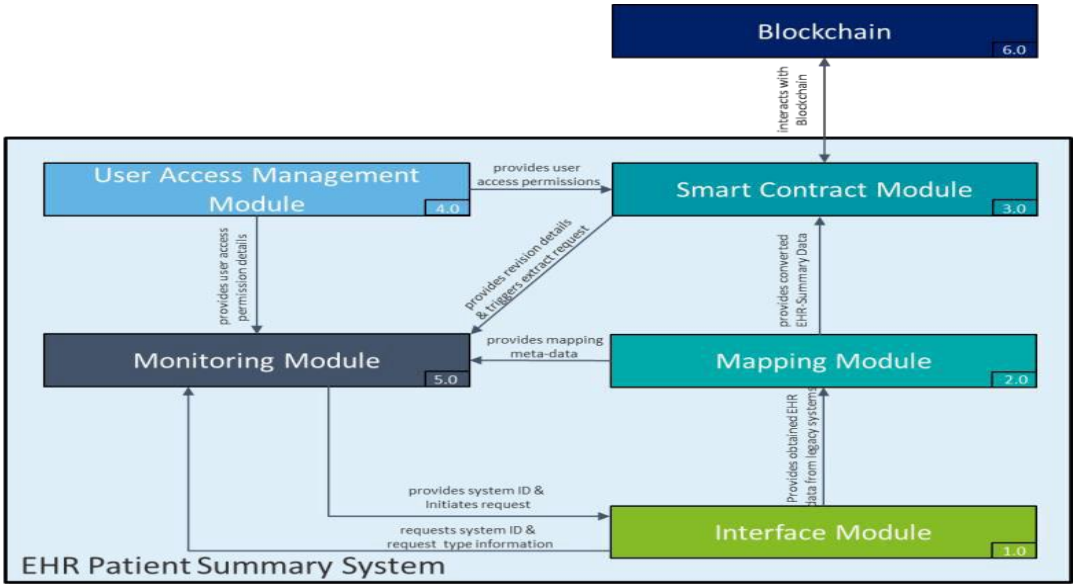
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12314

BlockCreation:
A block is a container data structure. The average size of a block seems to be 1MB (source). Here every certificates number will be created as a block. For every block an hash code will generate for security.

Block chain code generation:
In this module, based on certificate numbers Block code will generate. While creating Blockchain code user can increase the count based on their needs. The major advantage of this module user can share the Block chain code to another person in case of necessity.

Verifier:
Verifies the data of the blockchain so it ensures the Encryption & Decryption of data according to user's block.



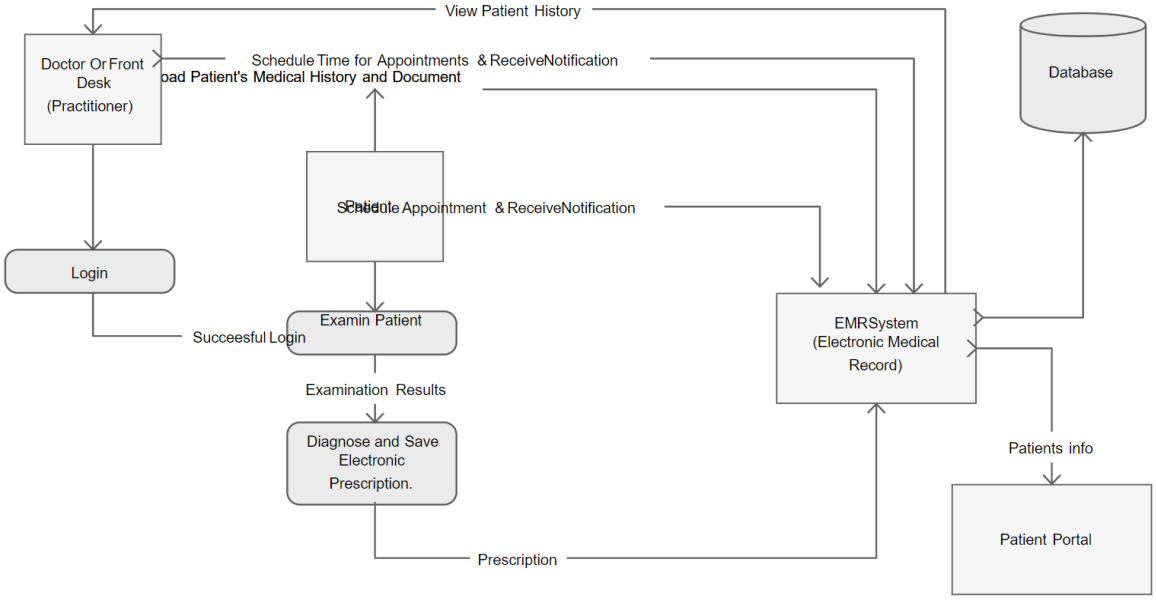


Fig 3.3 Design of EHR Database

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12314

IV. RESULT AND DISCUSSIONS

The Outcomes of the project are:

- Store information of an individual patient
- Data validation
- Safety and transparency
- Health record keeping
- Display information
- Identification of false content
- Patient monitoring

Accurate and complete medical data is a valuable asset for patients. Privacy and secure storage of medical data are key issues in medical services. The safe storage and full use of personal health records has always been a concern of the general public.The rise of blockchain technology has brought new ideas to solve this problem. As a decentralized, verifiable, and tamperproof hash chain, blockchain technology can be used to securely store personal medical data.In this article, we design a storage scheme based on blockchain and cloud storage to manage personal medical data. In addition, a service framework for sharing medical records is described. In addition, the characteristics of the medical blockchain are demonstrated and analyzed by comparing with traditional systems. The proposed storage and sharing system does not depend on any third party and no party has absolute power to influence the processing.

V. CONCLUSION

In this article, we explain how blockchain technology can be useful for the healthcare sector and how it can be used for electronic health records. Despite advances in healthcare and technological innovations in EHR systems, they still face some of the problems that this new technology, namely blockchain, solves. Our proposed framework is a combination of secure storage of records and precise access rules to those records.This creates such a system which is easier to use and understand for users. The framework also offers measures to ensure that the system resolves data storage issues as it uses the off-chain storage mechanism of IPFS. Role-based access also benefits the system, as medical records are only accessible to trusted and relevant people. It also solves the problem of information asymmetry in the EHR system.In the future, we plan to implement payment modules in the existing framework.For this, we have to consider some factors, because we have to decide how much a patient will pay for a medical consultation on a decentralized system running on the blockchain. We also need to define certain policies and rules that align with the principles of the healthcare industry.

REFERENCES

[1].Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using blockchain for medical data access and permission management", Proc. 2nd Int. Conf. Open Big Data, pp. 25-30, 2016. Google Scholar
[2].Waters, "Ciphertext-policy attribute-based encryption: An expressive efficient and provably secure realization", Proc. Int. Workshop Public Key Cryptogr., pp. 53-70, 2008.
[3].Hoffman and A. Podgurski, "In sickness health and cyberspace: Protecting the security of electronic private health information", BCL Rev., vol. 48, no. 331, 2007.
[4].N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption", Proc. Pairing-Based Cryptogr. – Pairing, pp. 248-265, 2009.
[5].S. Narayan, M. Gagné and R. Safavi-Naini, "Privacy preserving EHR system using attribute- based infrastructure", Proc. ACM Workshop Cloud Comput. Secur. Workshop, pp. 47-52, 2010. Google Scholar
[6].Sun, Y.; Zhang, D. Diagnosis and Analysis of Diabetic Retinopathy Based on Electronic Health Records. IEEE Access 2019, 7, 86115–86120. Google Scholar
[7].Shahnaz, A.; Qamar, U.; Khalid, A. Using blockchain for electronic health records. IEEE Access 2019, 7, 147782–147795. 3 Google Scholar
[8].K. Gu, W. Jia, G. Wang, and S. Wen, Efficient and secure attribute-based signature for monotone predicates, Acta Inf., 2017, vol. 54. no. 5, pp, 521-541,.
[9].Gao F, Zhu L, Shen M, Sharif K, Wan Z, Ren K. A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks. IEEE Network 2018 Nov;32(6):184-192.