

# Mobile Cloud Based Secure Electronic Healthcare Records Sharing System Using Blockchain

Ms. Vaishali Vijay Wagh<sup>1</sup>, Mr. Sharad M. Rokade<sup>2</sup>  
 vaishali0707@rediffmail.com<sup>1</sup>, sharad.rokade@pravara.in<sup>2</sup>  
 Department of Computer Engineering<sup>1,2</sup>  
 Sir Visvesvaraya Institute of Technology, Nashik, India<sup>1,2</sup>

**Abstract:** In recent years, at EHR, we have encountered a number of innovative technologies that integrate mobile devices and cloud computing to facilitate the exchange of medical data between patients and medical institutions. Medical care operates with low cost, high flexibility and safety. In the old system, patient files are stored in a file database, which may lead to high risks, such as theft of the file or the tampering of the patient data in the file by a thief. To solve this problem, we created a decentralized system by implementing EHR based on blockchain technology. Here, we have created an access control system with smart contracts, which is very powerful and can ensure the safe exchange of electronic medical records between patients and healthcare providers. The system proposed in contains cryptocurrency from potential threats (Ethereum stores sensitive health information). The proposed system also led to the certification of doctors, patients and pharmacists. When a patient registers for, a unique block and a hash value are created. As soon as the patient talks about his condition, the doctor can analyze it and prescribe medication. The pharmacist will update and bill later.

**Keywords-** Security, Blockchain, Ethereum, Patients Record, Cloud Computing, Flexibility, Currency, Technology

## I. INTRODUCTION

This kind of intelligent electronic health system can not only realize remote monitoring of patients, but also provide outpatient home care. It can not only support home medical treatment, but also bring economic benefits to patients. In addition, the full availability of EHR in the cloud helps healthcare providers. Follow the patient. Be healthy and provide adequate medical services as part of diagnosis and treatment. In addition to these advantages, the concept of cloud storage also brings security challenges, making it difficult to provide electronic medical services in the cloud. The exchange of information between patients and medical institutions through EHR is also one of these themes.

Access to unauthorized objects without the patient's consent may compromise the integrity, confidentiality, and security of the data. In addition, patients will find it difficult to track and record their health. Therefore, it becomes important to provide effective access control for mobile cloud systems. Data owners rely entirely on traditional EHR access control methods, allowing servers to control access and enable services. However, for mobile cloud, traditional assumptions are useless, because the server is honest, but also very curious.

## II. BLOCKCHAIN

The cloud server will safely execute data requests, but at the same time it will also collect personal data without the patient's consent, leading to information leakage and network security breaches. The concept of blockchain is one of the important characteristics of the digital currency Bitcoin. The blockchain follows a distributed database of records derived from digital transactions carried out by parties in the network. Every transaction in the network is authenticated by most participants in the network system. This concept stores every transaction record. The pure application of blockchain is Bitcoin. The reason for this is that all transactions are recorded through digital ledgers distributed on the network. When a block stores new data, it will be added to the blockchain series. Blockchain is a series of blocks linked together [8]. To add a block to the blockchain, you need to do the following four things. First, the transaction must be completed. Take, for example, a sudden purchase on Amazon. Crazy clicking on a lot of items, we found it by accident and finally bought it.

Second, the transaction needs to be confirmed. After we purchase the item, we must confirm the transaction user done. Considering other public registration systems such as Wikipedia, there will be quality control for new records, but in the case of the blockchain, it is a computer network with thousands of computers scattered around the world. The computer network is used to check whether the transaction occurred, that is, they check the details of the purchase, such as transaction time and amount. Third, the confirmed transactions are stored in a block. After verified the transaction, the green light turns on. All transaction details such as amount, customer signature and Amazon signature are stored in the block. This block will link together thousands of other blocks like this block.

Finally, a hash value must be assigned to the added block. After the transaction is confirmed, the block is assigned a unique number and an identifying hash value. Once a block is hashed, it will be added to the blockchain. After adding a block, everyone (including users) can see when, where and by whom the block was added to the blockchain.

### Different Types of Blockchain

- **Public Blockchain** - The public blockchain is designed to be completely decentralized, and no natural or legal person can control which transactions are recorded on the blockchain or how they are processed.

- **Private Blockchain-** Private blockchains are more centralized than public blockchains. Transactions are private and only available to ecosystem members who are allowed to join the network.
- **Consortium / Hybrid Blockchain -** By working together in certain aspects of the business, they can increase individual and collective efficiency. The members of the blockchain alliance can include anyone from the central bank to the government to the supply chain.

### III. LITERATURE REVIEW

The document proposes a new medical data exchange program that combines the advantages of cloud storage and blockchain technology. Our solution uses cloud servers to store encrypted medical data, and uses the blockchain system to store the corresponding ciphertext addresses of medical data and related medical information. Therefore, the proposed scheme meets the requirements of immutability and unforgeability.

The attribute-based cryptosystem guarantees the confidentiality of medical data in the cloud and can verify the source of medical data. In addition, the use of ODABE can reduce the computational workload of medical data users. The analysis results show that the proposed system has high performance in terms of computational cost and security.<sup>[1]</sup>

*Bihuan Chen, Zhixiong Tan, Wei Fang*, in a previous work, they proposed a blockchain-based financial product management platform. It forms a network structure for managing financial product information, and provides a transparent and secure environment for information exchange. Use Hyper Ledger Fabric as the underlying architecture to perform key financial product operations, such as continuous product maintenance, multiple data retrieval functions, and financial product tracking.

*Xing Liu*, this article introduces Chain Tutor, a Java application for learning the concepts of blockchain technology. Although the concept of blockchain is widely known and used in various fields such as health, some of the concepts are not unfamiliar to novices. Textbooks may be difficult to understand. Even the blockchain image may be lost in these documentation descriptions. Using the Java application introduced in this document, users can implement the concept of blockchain technology through a graphical interface. Understand how mining works and how each block is added to the blockchain.

*Andrei Cirstea, Nicu Bizon, Cosmin Stirbu*, this document briefly introduces the concept of blockchain, and then briefly outlines its medical applications. The purpose of this application is to make the medical field more efficient. This technology can change medicine and any other field to disperse the world safely and effectively. The main idea of this document is to demonstrate the extraordinary potential of this technology and how it can change all the ways of receiving, protecting and transmitting information.

*Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee*, this paper presents a complete survey on existing technology of blockchain protocol for IOT networks. This paper starts with introduction of blockchain and explains the existing survey that is associated with the blockchain concept. Then an overview of application domain of blockchain in IOT is provided. Moreover, the five main classification of blockchain in IOT is also provided briefly.

### IV. EXISTING SYSTEM

Intervention of medical data is always possible because the existing system is a centralized and distributed system. The current system has disadvantages such as insufficient data protection, low reliability, and poor network security when exchanging medical files between cloud servers. There may be a point in the existing system that makes the data unavailable. Because the existing system faces storage problems, it still lacks the data recovery process.

### V. PROPOSED SYSTEM

Among the proposed technologies, the EHR blockchain provides a decentralized system. The proposed system provides a powerful access control mechanism by using smart contracts to ensure the safe exchange of EHR between patients and healthcare providers (including hospitals and Pharmacies). The patient can register and submit his health data, then hash it using the SHA 256 algorithm, and then embed it in the QR code. With this hash value of, doctors and hospitals can see the details of the solution. Doctors can now release medications by viewing patient records, which will be converted into scratch pads. The pharmacist can view this block and automatically create an invoice. The proposed system also integrates a cryptocurrency, Ethereum, to protect sensitive health information from the threat. Cryptocurrency can also be used to schedule doctor appointments and pay fees.

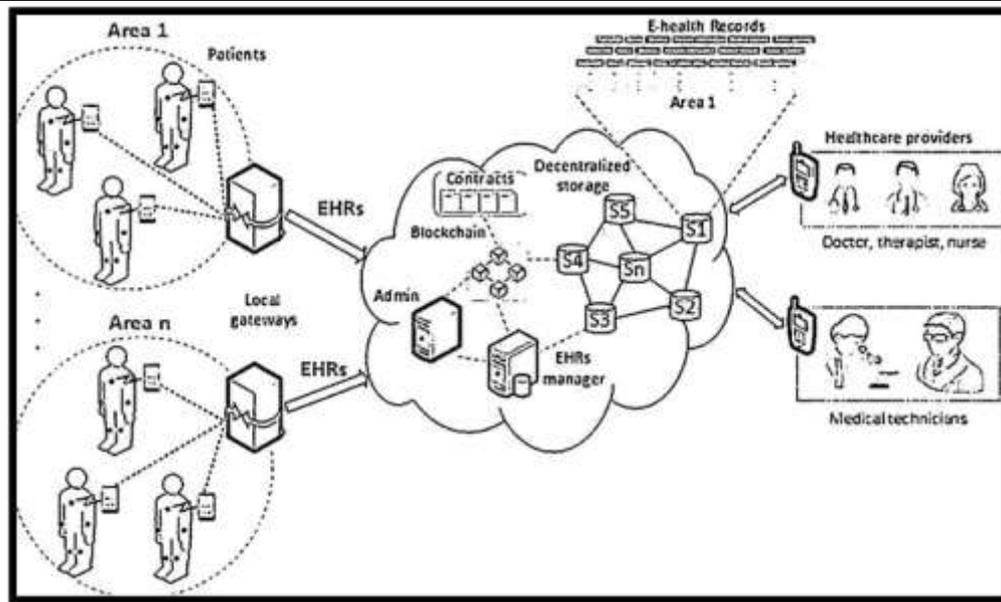


Fig 1. Architecture Diagram

The proposed work is a secure medical application with multiple sub-modules, such as downloading patient records, key generation, patient record encryption, block creation, uploading and downloading patient records, and cloud ID. Medical records. The health application is provided as a cloud application, in which it provides the ability to download patient records into the application. Test the functionality of the application by checking the file size (this is a number, if the healthcare system is efficient, it can load as much data as possible at the same time for processing. The module loads patient records and displays the total number of records in the database, check Data and upload to the database.

#### [A] User Registration

The registration module supports doctors and patients to register their data. This module collects user data. For Doctor, you must provide your name, date of birth, address, email address, phone number, and registration number. Doctors in the system contact one of the service providers; for patients, they must provide their name, date of birth, address, phone number, and information about their health insurance. You must enter a valid password. The patient also records detailed information about the patient's disease. All this data is converted in block and a hash value is generated. The SHA 256 algorithm is used to encrypt these values. No one saw him. Before the patient gave the doctor permission, even doctors could not view the patient data.

#### [B] Blockchain Based Smart Contracts for Healthcare

Data transactions are signed using the private key of the owner (patient or doctor). The content of the system block represents the data ownership and public rights shared by members of the private peer-to-peer network. Blockchain technology supports the use of smart contracts, which allows us to automate and track certain transitions between states (such as changing viewing permissions or creating new system records). We record the relationship between patients and suppliers through smart contracts on the Ethereum blockchain, link medical records with access rights and data recovery instructions (essentially information notifications), and run external servers to ensure that the blockchain Operation to ensure the integrity of the data.

#### [C] Hash Key Value Creation

Encrypted hashing is defined as an algorithm that takes input data and converts it into a fixed value output. The output is a combination of letters and numbers. There are different types of cryptographic hashes. An example is Bitcoin, which uses SHA. 256 algorithms. A hash algorithm is a calculation function that converts input data into a fixed value output called a hash value. Hash values are used to compare files with data, identify them and perform calculations.

#### [D] Block Creation

First, it creates a set of consecutively numbered blocks from 1 to N, N depends on the size of the transaction, and after the record is loaded into the application, it involves the block creation operation, and creates a chain to dynamically connect each Dynamic block creation. All blocks are linked in the hierarchical chain. This block is used to store patient information. We can also view the blocks and upload them to the cloud. Patients will receive EHR notifications that must be approved by them. The approval form avoids double-spending attacks. After checking the EHR, the Block Builder module will generate a block with EHR parts. Each block in the blockchain has a separate block data hash.

#### [E] Data Privacy & Protection

Blockchain technology acts as an end-to-end solution for data protection and security. These blocks are connected together in the form of chains. Each block in the blockchain consists of a block header, transaction, and transaction counter.

## [F] Cryptocurrencies

Cryptocurrency is a digital asset that can serve as a medium of exchange. This blockchain technology provides an appropriate level of security for cryptocurrencies to withstand system attacks and avoid double spending. When user sends encrypted currency, manual currency exchange is not performed, but attributes are signed in the addresses of sender and receiver. When the sender sends the public key, the receiver must have the private key to access the sent currency. [6] If the receiver's private key matches the sender's public key, the transaction is recorded on the blockchain and the balance is recorded. Notification Sender and recipient addresses. With the help of cryptocurrency, patients can pay bills, medical expenses, admission fees, etc.

## CONCLUSION

Since blockchain provides the highest level of security and availability, the technology can be used in many different areas of the healthcare system. For example, there are currently limited research on blockchain healthcare applications, but more research is available every day. Blockchain is one of the most active areas of software research today, and it is possible to reshape the health level by regaining control over patient medical records and health data.

Identify the problems in the EHR system and propose solutions to solve these problems through the realization of real prototypes. The main goal of the project is to develop a powerful access control mechanism based on the smart contract to ensure that users share EHR efficiently and securely [2]. This access control can detect and prevent unauthorized access to the electronic medical system to achieve the required level of data protection and network security. In addition, machine learning technology allows you to immediately provide medicines to patients based on their illnesses.

## REFERENCES

- [1] Xiaodong Yang 1 , (Member, Ieee), Ting Li 1 , Xizhen Pei 1 , Long Wen 1 , And Caifen Wang<sup>1,2</sup> "Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology" r 10.1109/Access.2020.2976894, Volume 8, 2020.
- [2] Dr. A. Poobalan, Dr. N. Uma Maheswari, 3Dr. R. Venkatesh, "Cloud Computing Security for Electronic Healthcare Records Using Block-chain Model" European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 7, Issue 4, 2020.
- [3] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: A survey. *Journal of Healthcare Engineering*, 2019.
- [4] Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. (2018, December). BHEEM: A blockchain-based framework for securing electronic health records. In *2018 IEEE Globecom Workshops (GC Wkshps)* (pp. 1-6). IEEE.
- [5] Al-khafajiy, M., Baker, T., Chalmers, C. et al. Remote health monitoring of elderly through wearable sensors. *Multimed Tools Appl* 78, 24681–24706 (2019). <https://doi.org/10.1007/s11042-018-7134-7>.
- [6] Kuo TT, Kim HE, and Ohno-Machado L, "Blockchain distributed ledger technologies for biomedical and health care applications," *Ame. Medi. Infor. Assoc. J.*, vol. 6, pp. 1211-1220, 2017.
- [7] Gordon W and Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," *Comput Struct Biotechnol J.*, pp. 224-230, 2018.
- [8] Shan Jiang, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, Jianfei He, "BloCHIE: A BLOCKchain-Based Platform for Healthcare Information Exchange," in *Proc. IEEE on Smart Compu. (SMARTCOMP)*, 2018.