Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 2s (2025)

Secure Electronic Health Records Against Insider Attacks Using Blockchain

Dr. Uruj Jaleel[1], R. Lalmawipuii[2]

[1]Associate Professor, Department of CS & IT, Kalinga University, Raipur, India.

[2]Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.

Article History:

Received: *11-09-2024*

Revised: *18-10-2024*

Accepted: *28-10-2024*

Abstract:

Patient health information is provided by Electronic Health Record (EHR) systems. The security, integrity, and management of electronic health records are critical issues. EHRs facilitate online data storage and lessen human labour by making data maintenance simple. Traditional EHRs are currently vulnerable to a variety of assaults, such as internet and insider transactions. Diverse fraudulent schemes attempt to manipulate data in order to profit from it globally. Usually, this entails manipulating or hacking the data to produce fictitious reports. This is primarily due to the fact that patients are unable to follow their records. Here, a unique framework utilising the blockchain concept in the healthcare industry has been introduced. Implementing Block Chain for electronic health records (EHR) is the main objective of this proposed study. The decentralised nature of Block Chain lessens the possibility of a single point of failure, resulting in a robust system. Together with addressing the extensibility issue that Block Chain shares, the proposed approach makes use of an off-chain data source. The findings show that, as compared to the conventional health record system, computers is far more safe and scam-free. Lastly, the suggested method offers situations, like in EHR, where the given method ought to work well.

Keywords: Healthcare, Electronic Health Record, Block Chain, Online Security.

1. INTRODUCTION

It is often observed that as automation, or the use of technology in all areas of work, increases, the actual workload for humans is actually declining. Innovation has affected a wide range of industries, including the business and technology sectors, production businesses, the automobile industry, and many more. Dentistry and the medical field are two examples of such fields [1]. Electronic Health Records (EHR) are a type of data used in the healthcare industry that include patient information and records, appointment schedules, diagnoses, prescriptions, and medication information [16]. Unfortunately, just as innovation has become ingrained, so too have the practices that disrespect security and protection online [2]. Particularly the medical care sector has often been a major target for data theft because patient addresses, names, and government-issued retirement numbers are routinely contained in prosperity records [14] [17]. The robbery of EHRs is gradually becoming normal and ridiculously simple because of the requirement for a strategy and the instability of security systems [4]. Since most EHRs are run by a single vendor, all personal data is kept in data sets that are overseen by the vendor that manages the archive. It raises difficulties that need to be resolved related to control, securities, and protection [6]. This is where blockchain technology comes into play. In a nutshell, blockchain technology is a distributed ledger that is decentralised and

monitors the origin of digital assets. Blockchain was initially introduced for exchanges and cryptocurrencies that did not need to be under the jurisdiction of a centralisedorganisation or system [8]. Every document in the blockchain is safeguarded by a distinct blockchain ID, which keeps the records safe and restricts access to authorised personnel only [3]. When the dentistry industry is taken into account, medical professionals and their helpers have power over the patient's credentials. As a result, they may readily verify the patients' medical histories with the aid of regulated, decentralised blockchain architecture. The system's architecture establishes the capabilities and roles of each entity, which are subsequently applied to modify the inter-entity interactions. Blockchain is therefore utilised to implement efficiency and security. [13].

2. PROPOSED OBJECTIVES

The goal of selecting an EHR-based Blockchain system is to eliminate the need for paperwork, which can be lost or require a lot of effort to locate. It is uncommon to use EHR as a solution to difficulties people encounter, but when it is implemented using blockchain technology, it becomes genuine, secure, and more effective. These days, blockchain technology is incredibly effective and has been increasing. EHR is utilised to increase cost-effectiveness, security against data leakage, and efficiency against data loss. Because the data is organised steadily, there is no chance of data manipulation or leaking [5] [10]. Knowing a patient's past was difficult in the past, but blockchain technology combined with electronic health records makes it possible [12]. The suggested project's goal is to:

- Creating an interface to guarantee the security and protection of medical records while facilitating communication between physicians and patients.
- Use blockchain technology to store patient and doctor credentials and establish a connection with a web application.
- Provide a review platform where patients may read and compare the evaluations and ratings of their doctors.
- One of the most important components of health care records is probably record keeping.
- It might be challenging for a doctor to assess a patient and their problems if they cannot be credibly identified or provided with a complete medical history.
- The patient also provides surveys to the expert, which calls for a strategy to support the advancement and practical improvement of the expert as well.

The organization of the remaining sections is as follows: Section 2 presents a challenges associated with security in the healthcare system, research motivation, goals, and contributions, and a detailed explanation of the research activity; in Section 3 identifies how electronic Health records can be authenticated by implementing Smart Contracts and assesses its performance evaluation of the proposed system.Section 4 presents the findings and discussion of the proposed model, and Section 5 concludes with a summary of the contributions to the research and future extensions.

3. SYSTEM DESIGN

There are two different user types in the proposed EHR design that can upload and get data from the

system. The built-in framework is in charge of data storage and communication within the blockchain network. The EHR Smart Contract includes a recursive block of records or data [18]. Every transaction that occurs within the blockchain network must be validated by the blockchain administration module. The processing module makes sure that all requirements have been met and that the transaction under inquiry has been validated by the smart contract. The confirmed records or data are added to the databases once all parameters have been set. The database helps to ensure that the system is current and useful.The majority of the provided Blockchain architecture is composed of the following key elements, as illustrated in Figure 1.

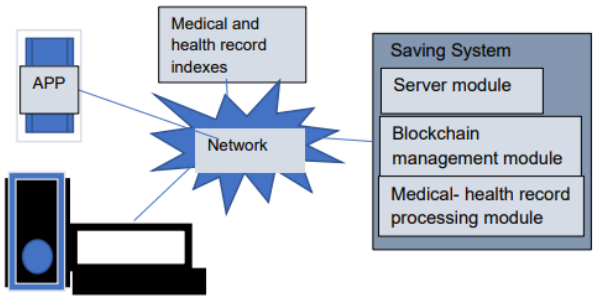

Figure 1: EHR Framework

Server System

There are two categories of patient-related credentials in electronic health records (EHRs): those that are required and those that don't really care about the patient's security or privacy. It is in charge of data storage and communication inside the blockchain network. The EHR Smart Contract is a layered block of records or data. Every transaction that occurs within the blockchain network must be validated by the blockchain administration module. The processing module verifies that all requirements have been completed and that the transaction related to the investigation has been approved by the Summary Contract. The verified data or records are added to the databases once all conditions have been satisfied [7].The blockchain's database is in charge of preserving all previous information in addition to the current and pertinent data. In comparison to other centralised alternatives, blockchain databases are comparatively slow.

The technique for creating a blockchain account is described in Figure 2. Before any transaction can start, a number of sub-level transactions need to be finished. This starts as soon as the software is launched. A connection is established with the Serving System, which manages several critical functions, including receiving and processing patient requests and authenticating and documenting each patient transaction. The user interface makes it possible to update the patient's personal information and perform different authentications, including private key and certification data, once a connection has been made. The key is obtained at this phase [15]. A user may create a Blockchain account provided that they fulfil the requirements as outlined in the Registrar Contract. The newly established user receives a unique unification key that they can use to construct a digital signature. In order to guard against unauthorised access to both their data and the Blockchain as a whole through their user interface, the newly established user can also set a password. This is followed by the data being stored.

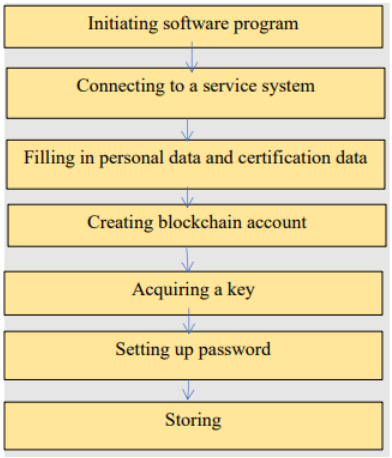

Figure 2: Steps to create a blockchain account

Figure 3 shows some information from the database that can be queried. receiving a connection request from a terminal device in the first module. This module handles a request to query a database for information coming from an external device. Next, identity verification is carried out, in which each networked computer verifies the request by comparing it to a set of validation guidelines established by the blockchain network's founders. After that, we verify user authority. Verifying User Authority is the process of determining whether or not the user submitting the request is authorised. A blockchain ID would be the focal point of blockchain authentication. Following the user authority confirmation, we give the user access to the query interface so they can obtain the data for which a query is needed [9]. Next, a Receiving Query Command is produced. When this module receives the matching query, we wish to gather user information and submit it to the blockchain for verification. The received inquiry is confirmed by blockchain verification. After the blockchain verification is complete, we link the request-related database record in this step based on the index. The query result is the last thing the module does before sending it to the user who initiated the request.

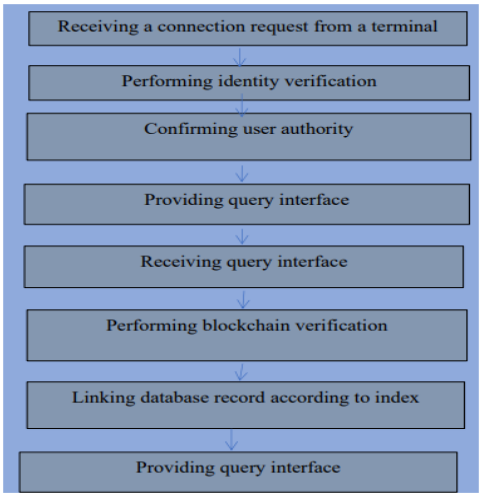

Figure 3: Query Information from Database

To get a patient's medical record, a doctor creates a request, as shown in Figure 4, asking for particular data to be requested from the database from the patient's medical record. We authenticate

the doctor after generating the request. The person executing the authentication is known as the "verifier," and the person making the request for authentication is known as the "requester." The process of obtaining the patient's record from the database in response to the doctor's request is referred to as "acquiring the patient's record according to the doctor's request". Subsequently, new diagnostic data is generated and presented to the physician. The last step is encrypting the medical record. This ensures that the record that needs to be provided is secure. [19].

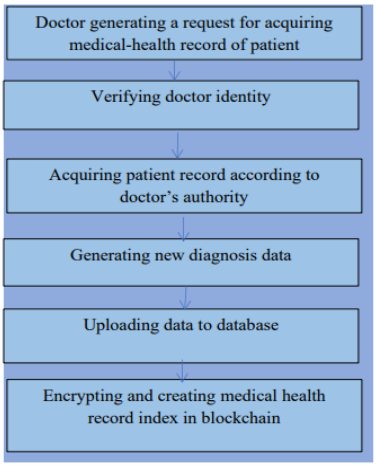

Figure 4:A physician asks to obtain certain data on the patient file

A Blockchain-based distributed, decentralised, and secure network for medical records has been developed through the creation of a framework. This technique helps to check the lack of transparency among medical professionals by limiting access to the EHR system to approved users. Our focus on improving health record data security opens up new directions for future research to meet more security requirements. Future security models that are more universal, address the need for health data protection, and identify untrusted hosts will be beneficial for the deployment of critical applications for any medical purpose [11]. In addition to saving computer time, this would aid in preventing cheating. The suggested effort will benefit several new apps that aim to establish transparency towards patients, medical professionals, and related fields.

4. EXPERIMENTAL RESULTS AND DISCUSSION

There have been multiple steps developed to link at the backend files in order to transition the system into a functional module. Tools have been included in the suggested system to guarantee better security and authenticity. Figure 5 demonstrates the rapid construction of Ethereum and Corda apps with the usage of Ganache Software. Not only can we create apps, but we can also test and implement them. Therefore, blockchain authentication raises intriguing parallels between safeguarding technology and the technology itself.

Figure 5: Ganache Software

A local server was used in the creation of the front end. All user interactions with the dental care system, both from the doctor and the patient, were based on this frontend. We saw how the use of smart contracts to enable the ReactJS frontend made the data incredibly safe and impermeable, meaning it could not be wiped. Rise. Using sh, the front end was deployed. It was given the name dental chain.surge.sh. This makes it possible for the software to safely store user-related data on remote servers or the cloud and to give every user, on any device, a customised experience.

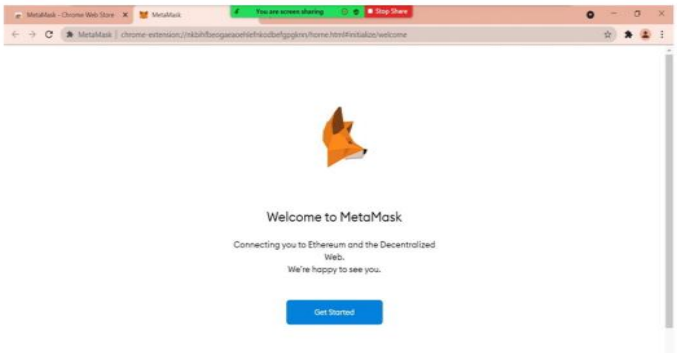

Figure 6: Metamask Software

You can store, access, and share files using IPFS (The Interplanetary File System), a peer-to-peer network and protocol for a decentralised distributed file system. You can use IPFS to store files from your Ethereum network for safe sharing and protected file access, as seen in Figure 7.The Ethereum protocol, which consists of a unique state machine, is responsible for ensuring that the system as a whole stay immutable, continuous, and uninterrupted.

Figure7: Interplanetary File System

Depending on who is attempting to log in, the login page requests the patient's or doctor's email address and password. Figure 8 shows our doctor and patient login page connected to our Ethereum network (Personal Ethereum Network using Ganache). Using IPFS (The Interplanetary File System), we are able to store and view patient details, and every small operation is stored with a unique address for security.

Figure8: Login Interface

This interface gives clinicians a categorical way to look for patients they have treated using the ReactJS framework. This includes all of the patient's records, including any previous visits with the same or different physicians. The physician has the ability to archive their accomplishments within their speciality. A new patient's diagnosis may be added by the doctor at any time. The doctor can use this form in Figure 9 to exercise his authority to add a new patient.

Figure 9:Physician's Interface

The patient-side interface contains all of the data, including past appointments, medications, tests, and other information. The patient can review all of this information whenever and wherever they want. Figure 10 demonstrates that a unique address is generated and a fuel fee is deducted upon completion of any activity.

Figure 10: Patient’s Interface

Solidity is being used to write the backend of the system, which is being assembled on the online

IDE remix. The compiler supports every CRUD action, including adding a new patient, retrieving and reading the required patient data, changing patient data in compliance with requirements, and removing patient data. A compilation that reinitialises the blockchain and updates it with a patient's most recent information is depicted in Figure 11.

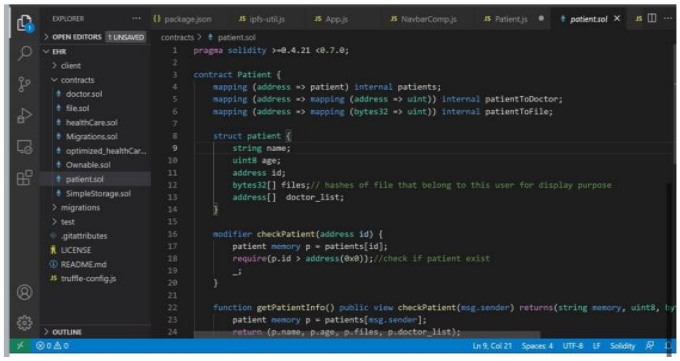

Figure11: Solidity Compiler Updating Patient Information

The new data is updated on the blockchain upon a successful compilation and transaction. The UI is briefly described in the screenshot below, which also displays the wallet balance and the Gas token that is necessary for every transaction. The transaction may proceed if the user has sufficient Gas Tokens in their wallet. Figure 12 illustrates how the Blockchain stores all transaction history. Because the Blockchain is immutable, all transaction information is secure and unchangeable.

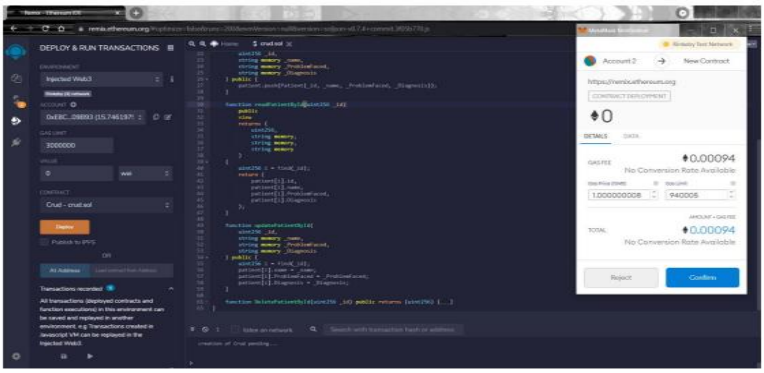

Figure12:Metamask wallet

The blinded, appropriated re-encryption feature of the blockchain's authentication EHR utilises the benefits of both blockchain innovation and re-encryption. This type of re-encryption measures represents different exchanges between intermediary hubs.

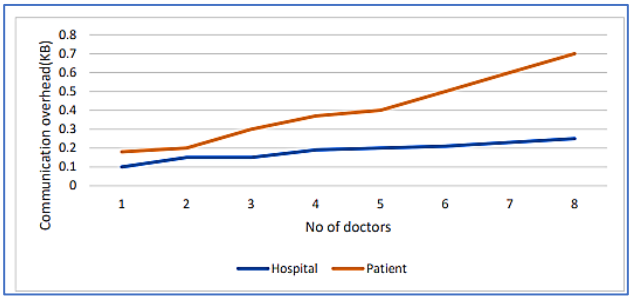

Figure13:Overhead in patient and hospital communications

The authorisation can be changed to select any re-encryption within the system, using pseudorandom decision-making. Moreover, the re-encryption may build up a limit to such an amount that lone a certain number of intermediates in the gathering need add to re-scramble the key. The freshly encoded symmetric key would then be restored to the authorisation by the re-encryption, which would also be responsible for handling the intermediary re-encryption. Additionally, a graph is generated as illustrated in Figure 13 utilising the data from the table, indicating that the number of doctors and patient communications are strongly correlated with communication overheads.

5. CONCLUSIONS

One of the most important issues that still has to be addressed in EHR systems is how to securely store medical records while information is being shared between various parties. This study describes the design of a novel extension that uses the blockchain technology to safeguard medical records. This new strategy provides a strong EHR program and guarantees the integrity of all records. The distributed ledger's foundation, efficiency and security, are all provided by blockchain-based electronic health records. Ethereum was chosen as the foundation because it facilitates the creation of smart contracts quickly and effectively, preventing fraud and data leaks or copies. Ethereum also supports Blockchain technology. The healthcare system has numerous difficulties, such as information loss, data copying, incorrect data interpretation, etc. Interoperability is another barrier to efficient and quick data sharing. However, with the aid of Distributive Ledger technology, or Blockchain, each participating member, or node, will have access to an updated copy of the records, and the system ensures complete transparency throughout the process. Additionally, the users' data is safeguarded through carefully crafted authorisations based on their user type. Although blockchain has been utilised in the past, its introduction to security management has been a significant implementation.

REFERENCES

[1] Kim, MyeongHyun, SungJin Yu, JoonYoung Lee, YoHan Park, and YoungHo Park. "Design of secure protocol for cloud-assisted electronic health record system using blockchain." Sensors 20, no. 10 (2020): 2913.

[2] Veera Boopathy, E., Peer Mohamed Appa, M.A.Y., Pragadeswaran, S., Karthick Raja, D., Gowtham, M., Kishore, R., Vimalraj, P., &Vissnuvardhan, K. (2024). A Data Driven Approach through IOMT based Patient Healthcare Monitoring System. Archives for Technical Sciences, 2(31), 9-15.

[3] Akhter Md Hasib, Kazi Tamzid, Ixion Chowdhury, Saadman Sakib, Mohammad Monirujjaman Khan, Nawal Alsufyani, Abdulmajeed Alsufyani, and Sami Bourouis. "[Retracted] Electronic Health Record Monitoring System and Data Security Using Blockchain Technology." Security and Communication Networks 2022, no. 1 (2022): 2366632.

[4] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

[5] Dr.R. Mohandas, Dr.S. Veena, G. Kirubasri, I. Thusnavis Bella Mary, &Dr.R. Udayakumar. (2024). Federated Learning with Homomorphic Encryption for Ensuring Privacy in Medical Data. Indian Journal of Information Sources and Services, 14(2), 17–23. https://doi.org/10.51983/ijiss-2024.14.2.03

[6] Cao, S., Yang, H., Lu, S., and Qian, F. "Fine Tuning SSP Algorithms for MIMO Antenna Systems for Higher Throughputs and Lesser Interferences." *International Journal of Communication and Computer Technologies*, vol. 12, no. 2, 2024, pp. 1-10.

[7] Baotic, A., and Silva, D. "Techniques on Controlling Bandwidth and Energy Consumption for 5G and 6G Wireless Communication Systems." *International Journal of Communication and Computer Technologies*, vol. 12, no. 2, 2024, pp. 11-20.

[8] Madhavi, M., Sasirooba, T., & Kumar, G. K. (2023). Hiding Sensitive Medical Data Using Simple and Pre-Large Rain Optimization Algorithm through Data Removal for E-Health System. Journal of Internet Services and Information Security, 13(2), 177-192.

[9] Chenthara, Shekha, Khandakar Ahmed, Hua Wang, Frank Whittaker, and Zhenxiang Chen. "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology." Plos one 15, no. 12 (2020): e0243043.

[10] Sonya, A., & Kavitha, G. (2022). A Data Integrity and Security Approach for Health Care Data in Cloud Environment. Journal of Internet Services and Information Security, 12(4), 246-256.

[11] Ajayi, Oluwaseyi, Meryem Abouali, and Tarek Saadawi. "Secure architecture for inter-healthcare electronic health records exchange." In 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), pp. 1-6. IEEE, 2020.

[12] Malathi, K., Shruthi, S.N., Madhumitha, N., Sreelakshmi, S., Sathya, U., & Sangeetha, P.M. (2024). Medical Data Integration and Interoperability through Remote Monitoring of Healthcare Devices. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 60-72. https://doi.org/10.58346/JOWUA.2024.I2.005

[13] Ajayi, Oluwaseyi, Meryem Abouali, and Tarel Saadawi. "Blockchain architecture for secured inter-healthcare electronic health records exchange." In Advances in Intelligent Networking and Collaborative Systems: The 12th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2020) 12, pp. 161-172. Springer International Publishing, 2021.

[14] Mansouri, S. (2023). Application of Neural Networks in the Medical Field. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14(1), 69-81.

[15] Shahnaz, Ayesha, Usman Qamar, and Ayesha Khalid. "Using blockchain for electronic health records." IEEE access 7 (2019): 147782-147795.

[16] Bobir, A.O., Askariy, M., Otabek, Y.Y., Nodir, R.K., Rakhima, A., Zukhra, Z.Y., Sherzod, A.A. (2024). Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity. Natural and Engineering Sciences, 9(1), 72-83.

[17] Rai, Bipin Kumar. "PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0." Health Services and Outcomes Research Methodology 23, no. 1 (2023): 80-102.

[18] Haque, Rafita, Hasan Sarwar, S. Rayhan Kabir, Rokeya Forhat, Muhammad Jafar Sadeq, Md Akhtaruzzaman, and Nafisa Haque. "Blockchain-based information security of electronic medical records (EMR) in a healthcare communication system." In Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2019, pp. 641-650. Singapore: Springer Singapore, 2021.

[19] Sharma, Yogesh, and Balamurugan Balamurugan. "Preserving the privacy of electronic health records using blockchain." Procedia Computer Science 173 (2020): 171-180.