Journal of Current Research in Engineering and Science
JCRES
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume7-Issue1, January 2024
Paper: 7

A Blockchain Based Secure Mechanism for Sharing Medical Data in the Cloud

R. Thendral[1]
DeptofInformation Technology
IFET College of Engineering
Villupuram,India.
thendralamutha@gmail.com

G. Abirami[2]
DeptofCSE
IFET College of Engineering
Villupuram,India.
abiramig2506@gmail.com

G. Harini[3]
DeptofCSE
IFET College of Engineering
Villupuram,India.
hariniwish807@gmail.com

***Abstract* - Blockchain model has a lot of potential for improve the productivity, security, and confidentiality of EHR sharing systems. Current solutions which depend on a centralized database, on the other hand, are vulnerable to conventional database security problems like Denial of Service (DoS) attacks as well as a potential weak point. Furthermore, previous solutions left users vulnerable to privacy connecting attacks and failed to address performance and scalability issues. To address the identified problems, we developed a authenticating Block chain-based healthcare shared medical data solution which incorporates Blockchain mechanism, a distributed file management system, and a threshold signature. Proposed model is based on the IBFT consensus methodology and the Interplanetary File management System (IPFS). The developed prototype was built on the Hyperledger Ethereum Blockchain. We analyzed the suggested system's performance using numerous performance standards such as transaction lag, bandwidth, and failure rate. The number of transactions and network size were varied in the experiments. The results of the experiments demonstrates that the suggested system outclasses existing Blockchain-based systems. Furthermore, the decentralized file provides more security than centralized database systems while maintaining the level of performance.**

***Keywords* - Blockchain, EHR, Security, Sub Carrier, Information Leakage Reduction.**

I.INTRODUCTION

Patients frequently go to different hospitals or doctors throughout their entire lives due to life conditions and the necessity to receive treatment options from various medical stations [1]. The proposed system uses Blockchains to manage permissions, with data stored off-chain in the Interplanetary File System, a secure decentralized storage system (IPFS)[2].

When able to delegate access to patient records, data ownership is also critical. What data will be owned by whom, and how will data authority be delegated? Responsibility for data ownership must also be did manage transparently [3]-[4].

When tried to compare to other solutions that keep information in a centralized location, this makes the system more resistant to data breaches like DoS and integrity attacks There is currently no industry-wide record-torecord matching standard [4]-[5].

When a user attempts to access a medical record, only authorized persons will be allowed to do so. A few remedies based on smart cards have been suggested [6]-[8].

This refers to the accuracy and consistency of medical records, as well as the integrity and consistency of physical computers connected to the network. Hacking into EHR systems can result in the loss of patient data or the destruction of healthcare workflows [9-10].

Electronic systems should be able to provide position access, passwords, and audit trails. Genetic testing is fraught with privacy issues. People are worried about losing one‘s jobs and their life insurance. The refusal for using effective genetic screening has consequences for individuals, researchers, and physicians [11]-[12].

II.METHODOLOGY

A prototype implementation of the EHRCHAIN system has been developed. The following features are included in this prototype implementation.

1. Under this EHRCHAIN system, Aadhaar numbers are used in India, but any federal level biometric authentication ID can be used in other countries to prevent forgery of own health - care information in the database.

2. Patient will generate a unique pseudonym number by having to pass a few secret information. To protect patient privacy, this pseudonym would be used to store healthcare information.

3. During the hashing process, all relation to specific from a hospital's health record are removed, ensuring that intruders would be unable to ascertain the owner of a specific health record, maintaining confidentiality.

4.Simulation results from some basic healthcare actions were performed in just this prototype system of the EHRCHAIN system.

5. Because identifiers/quasi-identifiers are not stored in the EHRCHAIN patient record database, this potential alternative opens up a lot of doors for medical research into specific diseases.

6. A patient's access control policy can be updated at any time.

7. The pseudonym and personal information of patients are stored in an encrypted EHRCHAIN Patient Profile database. As a result, this system ensures the privacy and security of healthcare data.

8. After revealing his identity, any service provider would be able to access the data for medication or any other purpose. This proposed EHRCHAIN scheme has significant outcomes in this way.

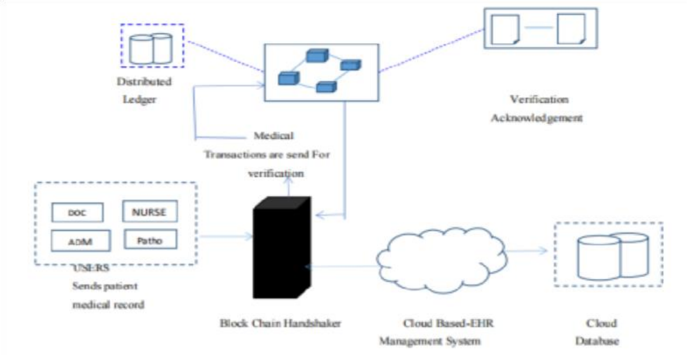


Figure 1. Flow diagram for Data Detection

III.SECURITY AND PRIVACY ISSUE

Because of the risks associated with EHR, it is critical to ensure patient confidentiality. While attempting to access or transacting EHR, any healthcare entity should be aware of the main security concerns. Authentication Methods: When a user attempts to access a medical record, only authorized persons will be allowed to do so. A few remedies based on smart cards have been suggested [6]. To authenticate users people get access to records, a biometric authentication method is also used. Confidentiality and Integrity: This refers to the accuracy and consistency of medical records, as well as the integrity and consistency of physical computers connected to the network.
Hacking into EHR systems can result in the loss of patient data or the destruction of healthcare workflows[10].If indeed the remote connection isn't really secure, an unidentified user can easily gain access to the network [12]. Electronic systems should be able to provide position access, passwords, and audit trails. Genetic testing is fraught with privacy issues. People are worried about losing one‘s jobs and their life insurance. The refusal for using effective genetic screening has consequences for individuals, researchers, and physicians [12].

1. When able to delegate access to patient records, data ownership is also critical. What data will be owned by whom, and how will data authority be delegated? Responsibility for data ownership must also be did manage transparently[3].

2. Policy on Data Protection: Because the healthcare diagnosis management includes multiple entities that cross organisational boundaries, acceptable and consistent safety is required. To prevent theft or loss of physical media and devices, business owners must follow strict policies and procedures.

Electronic health records require ongoing functionality advancement to handle security, add amount of safety, block access to various notes or outcomes, track versioning, as well as mask delicate entries for passing information from one person [4]. Profiles of Users: The healthcare system involves clients, professionals, health systems, trusted third parties, chemists, and other entities. As a result, issues such as defining users and roles are required to distinguish between users' functionality and security levels [4].

Patient id systems in health centers vary widely and are incompatible, trying to identify patients uniquely within a facility either between entities. Interoperability requires the existence of a system for identifying patients across entities. There is currently no industry-wide record-torecord matching standard [5]. Misuse of Health Records: Some EHR websites are unconcerned about privacy, particularly those that offer free storage space. They could sell the data to other companies or advertise on the same site as that of the patient's content [9].

In a multispecialty setting, medical file security can be challenging. Because the treatment of the these patients can span multiple medical specializations and document types, organizations must be able to separate any documents pertaining to substance abuse treatment.

IV. PROPOSED SYSTEM

Countries have different options related to community needs, but the majority of EHR solutions advocate for doctor because it provides the patient full control.[4][13][14][26][27][34]. EHRCHAIN is a patient-centered system. As long as the documents are depersonalized, page hashing of sensitive collected data supports both primary and secondary privacy-preserving usage.

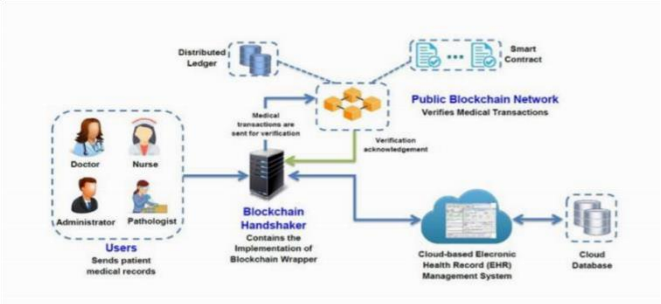

Distributed Ledger
Smart Contract
Public Blockchain Network
Verifies Medical Transactions
Medical transactions are sent for verification
Verification acknowledgement
Doctor
Nurse
Administrator
Pathologist
Users
Sends patient medical records
Blockchain Handshaker
Contains the Implementation of Blockchain Wrapper
Cloud-based Elecronic Health Record (EHR) Management System
Cloud Database

Figure 2. Flow diagram for System Architecture

As shown in Figure 2, the EHRCHAIN system architecture consists of two distinct databases, EHRCHAIN Patient Record registry and EHRCHAIN Patient Persona data system, a Hash functions module,

Access control modules for patients and doctors/healthcare authorities, and shared data policy and sharing management. The functionality of each has been described in the following section.

A.EHRCHAIN Database:

When an attacker is successful in gaining access to the data, the patient's confidentiality may be jeopardized, so strong privacy protection is required. EHRCHAIN maintains two databases, one for data encryption identifying details and the other for pseudonymized health records:

i.The EHRCHAIN Healthcare Information database, which includes patient medical records after they have been hashed

ii. The EHRCHAIN Patient Persona database, which stores encrypted applying psychological and pseudonyms.

B.Hashing Module:

Prior to actually storing patient/healthcare central medical files in the EHRCHAIN Healthcare Information database, the Hash based module means removing only those signifiers and semi from patient's medical record so that if an intruder gains access to database, he will be unable to conclude who owns which medical record. The Pseudonym Generation method allowed each patient to develop a distinct pseudonym (digital long random). Without any exchange of information between EHRCHAIN and Patient, a pseudonym can be making in her own environment. Pseudonyms are not guessed from the patient's data and do not need to be remembered. The pseudonym is kept in an encrypted format. When a new record is committed to the database, the patients decrypt it.

C.Patient's Profile & Hash Encryption:

Public key is used to encrypts the pseudonym of the patient (by asymmetric cyrpto methods). Identity, birth date, age, mobile number, Aadhaar - based number, email address, and other fields have been recognized as person a identification information. When a patient go to a new healthcare facility for the very first time, this identifiable information is required. Figure.3 shows how a shared key (utilizing symmetric cryptography) encrypts all of this identifiable information.

The secure EHRCHAIN Patient Persona database stores the encrypted portfolio and encrypted pseudonym. When a new record is added, the pseudonym is decrypted using the private key provided by the patient's, which is only known by patient.

D.Access Control Module:

Several access control models have been discussed. But there are some variations, RBAC is perhaps the most commonly used models. Each entity in the health system has its own level of access requirements, which even the access central controller should be able to handle without compromising patient privacy. The EHRCHAIN system will register every entity in the healthcare system, including patients, doctors, and health centers/health authorities. The AADHAR number of each entity was used for verification. As a result, the identity of the accessing applicant is confirmed. All of the patient's medical records, including his pseudonym, are available to him. To begin, the client must decrypt his pseudonym using his private key. Only the patient has access to this private key. As a result, privacy is preserved. Doctors and healthcare officials have restricted access. They can only see the health records or parts of the medical files that the patients have given them permission to see. To begin, the patient must use her/his private key to decrypt her/his pseudonym. This private key is only accessible by the patient. By having to repeat the decryption process, the doctor/healthcare organization will reveal his pseudonym. The access central controller will give entry to those medical files using the patient's pseudonym as well as the doctor's or healthcare authority's pseudonym. As a result, it will be possible to verify who had access to the health records.

V.RESULTS AND DISCUSSION

Thi**s** system provides trustworthy access control mechanism by using the smart contracts in order to achieve secured Medical Data sharing between the patients and the health care providers including hospital and pharmacist. A patient can register and feed his details regarding health which then will be converted into hash value using SHA 512 algorithm and then it will be embed to a Medical Data Using this hash value the doctor and the hospital can view the details permitted by the patients.

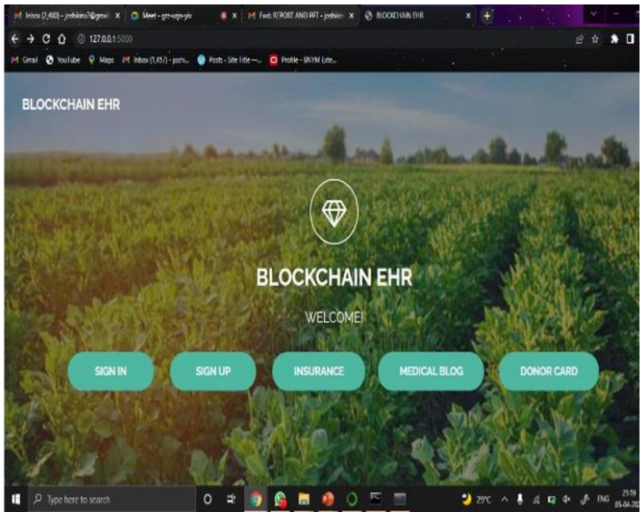


Figure 3. HomePage

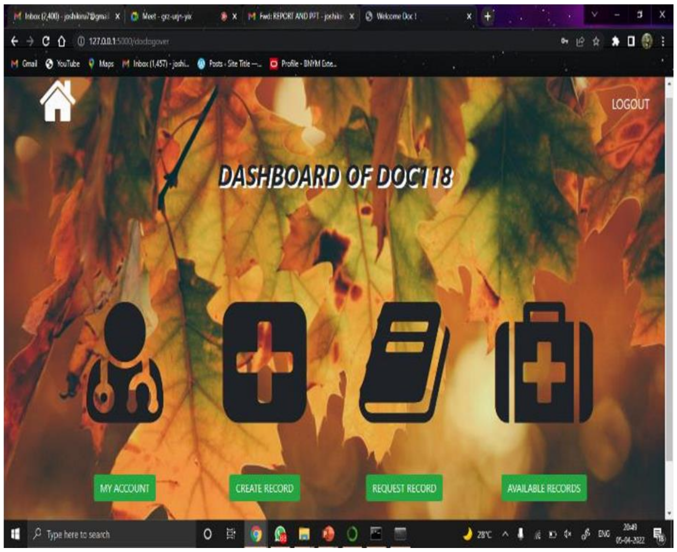


Figure 4. Dashboard Page For Doctor

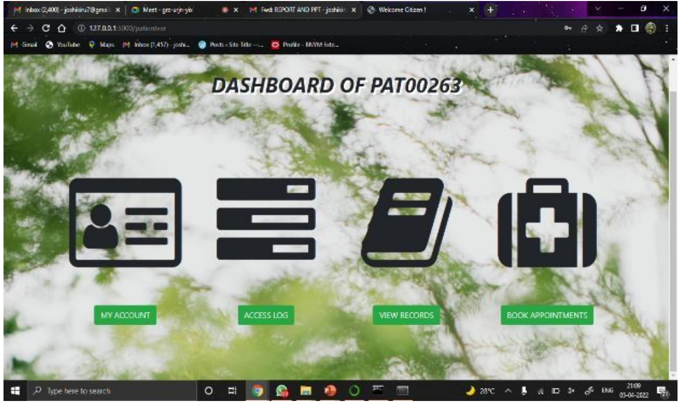
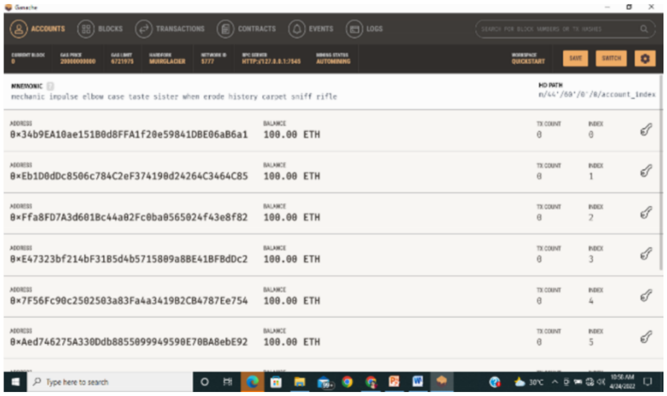


Figure 5.Dashboard Page For Patient



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
0	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

MNEMONIC
mechanic impulse elbow case taste sister when erode history carpet sniff rifle

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×34b9EA10ae151B0d8FFA1f20e59841DBE06aB6a1	100.00 ETH	0	0
0×Eb1D0dDc8506c784C2eF374190d24264C3464C85	100.00 ETH	0	1
0×Ffa8FD7A3d601Bc44a02Fc0ba0565024f43e8f82	100.00 ETH	0	2
0×E47323bf214bF31B5d4b5715809a8BE41BFBdDc2	100.00 ETH	0	3
0×7F56Fc90c2502503a83Fa4a3419B2CB4787Ee754	100.00 ETH	0	4
0×Aed746275A330Ddb8855099949590E70BA8ebE92	100.00 ETH	0	5

Figure 6. Patient Report Page

VI. Conclusion & Future work

Because anybody can obtain an information of the patients from his medicare card without his permission, most national healthcare solution providers do not give the patient full control but are not highly privacy protective. Countries make different decisions related to community needs, but the most well-known EHR solutions advocate for patient-centered care because it gives patients complete control. As a result, we developed the doctor EHRCHAIN system, which provides a user-friendly, secure mechanism. With the patient's consent, it will make the people's clinical content accessible to any medical center at any time. As long even as delicate data records are flier, hashing them supports both secondary confidentiality uses. It is strongly recommended for use in a hospital information system. As a result, Hashing methods and encryption mechanisms have been merged in EHRCHAIN to provide an effective healthcare system for security and privacy.

We modeled a few basic healthcare activities in the prototype of the EHRCHAIN health service. By using the

Hashing process, all signifiers and semi from a patient's medical record are excluded, making it impossible for an intruder to determine who owns a specific health record if he gains access to the data.

There are even more activities related to EHR safety and patient confidentiality that need to be investigated to see if our pseudonym solution can support them. The proposed solution provides a plethora of potentials for medical science on a specific disease by using anonymous health data. It could provide scientists with unnamed health data which does not reveal the patient's identity. As a result, researchers will have access to anonymous health data without jeopardizing their privacy. Security and privacy as cloud-based solutions become more prevalent in healthcare, ensuring the security and privacy of patient data will remain a top priority. Future work will likely focus on developing new technologies and best practices to protect patient data from cyber threats.Interoperability refers to the ability of different systems and software to exchange data and work together seamlessly. In the context of cloud medical data sharing, interoperability will be key to enabling healthcare providers to share data across different systems and platforms.Standardization of data formats and protocols will be important to ensure that different healthcare providers can share and use patient data effectively. Future work will likely focus on developing and implementing standardization protocols for medical data. Artificial intelligence and machine learning use of artificial intelligence and machine learning in healthcare is rapidly growing, and cloud medical data sharing will play a critical role in enabling these technologies. Future work will likely focus on developing and refining AI and machine learning algorithms to improve diagnosis, treatment, and patient outcomes. Cloud medical data sharing can also help to engage patients in their own healthcare by enabling them to access their medical records and communicate with healthcare providers more easily. Future work will likely focus on developing user-friendly interfaces and tools to improve patient engagement and empowerment.

REFERENCE

[1] Al-Hamdani, W. A. (2010, October). Cryptography based access control in healthcare web systems. In 2010 Information Security Curriculum Development Conference (pp. 66-79).

[2] Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In 2010 IEEE 3rd International Conference on cloud Computing (pp. 268-275). IEEE.

[3] Huda, M. N., Sonehara, N., & Yamada, S. (2009). A privacy management architecture for patientcontrolled personal health record system. Journal of Engineering Science and Technology, 4(2), 154-170.

[4] Vucetic, M., Uzelac, A., & Gligoric, N. (2011, October). E-health transformation model in Serbia: Design, architecture and developing. In 2011 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (pp. 566-573). IEEE.

[5] Ateniese, G., & de Medeiros, B. (2002, November). Anonymous e-prescriptions. In Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society (pp. 19-31).

[6] Yang, Y., Han, X., Bao, F., & Deng, R. H. (2004). A smart-card-enabled privacy preserving e-prescription system. IEEE Transactions on Information Technology in Biomedicine, 8(1), 47-58.

[7] Pandey, P., & Litoriya, R. (2020). Securing and authenticating healthcare records through blockchain technology. Cryptologia, 44(4), 341-356.

[8] Poag, S., & Deng, X. Information security andprivacy concerns of online prescription systems. refered research paper, okland University.

[9] Neubauer, T., & Kolb, M. (2009, March). Technologies for the pseudonymization of medical data:a legal evaluation. In 2009 Fourth InternationalConference on Systems (pp. 7-12). IEEE.

[10] Riedl, B., & Grascher, V. (2010, May). Assuringintegrity and confidentiality for pseudonymized healthdata. In ECTI-CON2010: The 2010 ECTI InternationalConference on Electrical Engineering/Electronics, Computer, Telecommunications and InformationTechnology (pp. 473-477). IEEE.