AN EFFICIENT AUTHENTICATION SCHEME FOR BLOCKCHAIN-BASED ELECTRONIC HEALTH RECORDS

MR.Raghuvaran M.E. , Assistant Professor, Department of Computer Science and Engineering

Mr.S.Muniyappan B.E, Student of Computer Science Engineering

Mr.k.Manikandan, B.E, Student of Computer science and Engineering

St. Joseph College of Engineering, Sriperumbudur, Chennai.

Abstract

Block chains are cryptographically secure and the data present therein can be authenticated using digital signature that are unique to each person, this technology could be the answer to most of these concerns We create a Blockchain for each patients for storing their medical information. Details like health insurance, doctor, lab results, medicine details etc. If patient visit different hospital they identified patients previous details using patient key .healthcare insurance and pharmacy also know patient details. Secures the transfer of funds by using a digital signature algorithm to prove ownership. And finally allow users to make transactions on your Block chain

Introduction

Blockchain are cryptographically secure and the data present there in can be authenticated using digital signature that are unique to each person, this technology could be the answer to most of these concerns

We create a Blockchain for each patient for storing their medical information. Details like Health insurance, doctor, lab results, medicine details etc.

If patient visit different hospital they identified patients previous details using patient key. The healthcare insurance and pharmacy also know patient details.

Secures the transfer of funds, by using a digital signature algorithm to prove ownership and finally allow users to make transactions on your Blockchain

BLOCKCHAIN:

- A Blockchain is a digitized, decentralized ledger of transactions. Blockchains record a continuously growing list of records, called blocks, which are linked and secured. It is a ledger of transactions.
- Blockchain – The revolutionary technology impacting different industries miraculously was introduced in the markets with its very first modern application Bit coin. Bit coin is nothing but a form of digital currency (crypto currency) which can be used in the place of fiat money for trading. And the underlying technology behind the success of crypto currencies is termed as Blockchain.
- A Blockchain is a distributed ledger that is completely open to any and everyone on the network. Once information is stored on a Blockchain, it is extremely difficult to change or alter it.

- With the use of Blockchain, the interaction between two parties through a peer-to-peer model is easily accomplished without the requirement of any third party.
- Each transaction is digitally signed to ensure its authenticity and that no one tampers with it, so the ledger itself and the existing transactions within it are assumed to be of high integrity.
- After the new block is added to the chain, the existing copies of Blockchain are updated for all the nodes on the network.

Literature Survey

A Block chain-Based Medical Data Sharing and Protection Scheme

- Authors : Fagen Li
- Center for Cyber Security, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China
- Electronic Health Record (EHR) has recorded the process of occurrence, development, and treatment of diseases. So it has high medical value. Owing to the private and sensitive nature of medical data for patients, the data sharing and privacy preservation are critical issues in EHR. Blockchain technology may be a promising solution for the problems above since it holds the features of decentralization and tamper resistance. In the paper, we propose a medical data sharing and protection scheme based on the hospital's private blockchain to improve the electronic health system of the hospital. Firstly, the scheme can satisfy various security properties such as decentralization, openness, and tamper resistance. A reliable mechanism is created for the doctors to store

medical data or access the historical data of patients while meeting privacy preservation. Furthermore, a symptoms-matching mechanism is given between patients. It allows patients who get the same symptoms to conduct mutual authentication and create a session key for their future communication about the illness. The proposed scheme is implemented by using PBC and Open SSL libraries. Finally, the security and performance evaluation of the proposed scheme is given.

System Design

An efficient authentication scheme for blockchain-based electronic health records (EHRs) should aim to provide a secure and tamper-proof system that allows only authorized personnel to access and modify patient data. Here's a suggested system design for such a scheme:

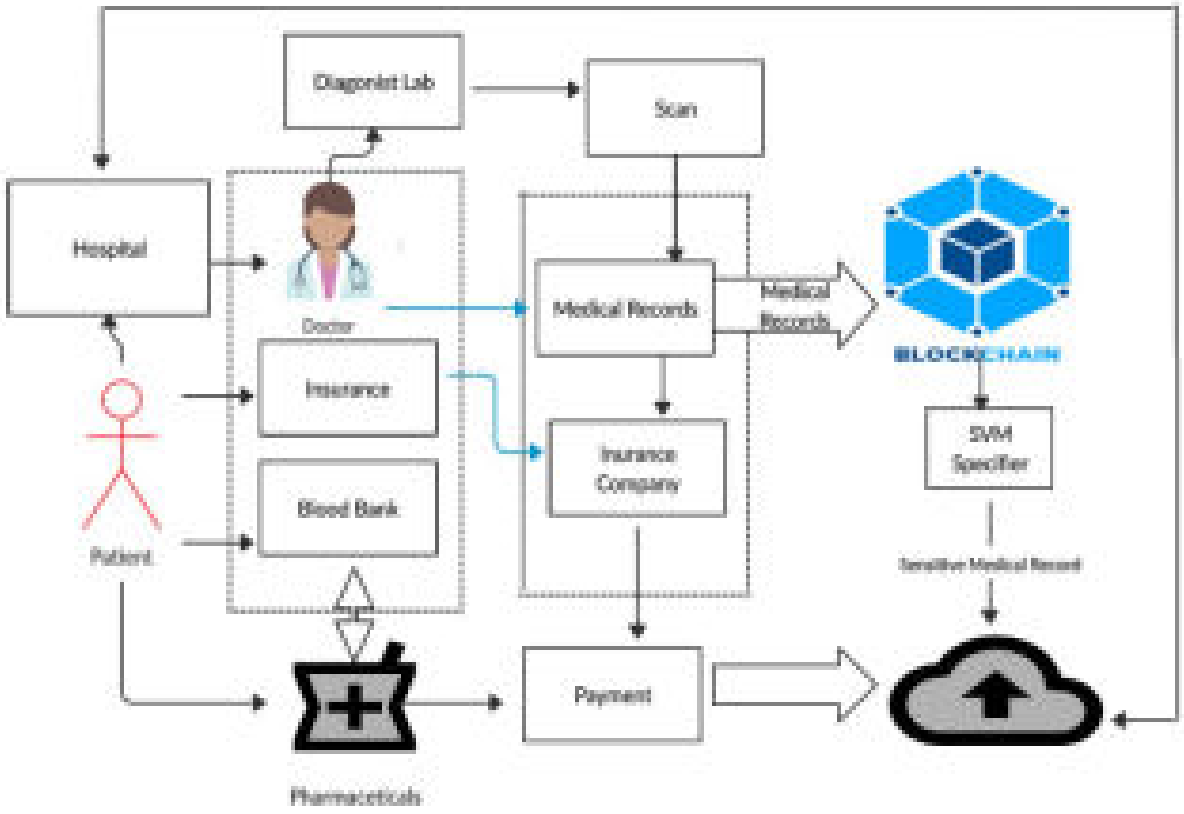
1. Blockchain-based EHR System: The system will be built using blockchain technology, which is a distributed ledger that ensures data integrity, immutability, and transparency. The blockchain will store patient data and access control information.

2. User Authentication: To access the EHR system, users will need to authenticate themselves using a username and password. Additionally, users will be required to provide their public key, which will be used to sign and encrypt data.

3. Role-based Access Control: The EHR system will implement role-based access control (RBAC) to control access to patient data. Different roles will be created based on job functions and responsibilities. The RBAC system will assign roles to users based on their job functions.

4. Data Encryption: Patient data will be encrypted using the public key of the authorized user. This ensures that only authorized personnel can access the data.

5. Audit Trail: The EHR system will maintain an audit trail of all access and modification of patient data. The audit trail will record the user, date, and time of access or modification.



6. Two-Factor Authentication: To provide an additional layer of security, the EHR system will implement two-factor authentication (2FA). Users will be required to provide a second form of authentication, such as a one-time password (OTP) sent to their registered mobile phone number.

7. Data Backup and Recovery: Regular data backups will be taken to prevent data loss due to system failures or disasters. A disaster recovery plan will also be put in place to restore the system in case of a catastrophic event.

8. Privacy and Security: The EHR system will comply with relevant privacy and security laws and regulations, such as HIPAA. The system will also implement

security measures such as firewalls, intrusion detection and prevention, and regular vulnerability assessments.

In summary, the proposed authentication scheme for blockchain-based EHRs uses RBAC, data encryption, audit trails, 2FA, data backup and recovery, and privacy and security measures to provide a secure and tamper-proof system that allows only authorized personnel to access and modify patient data.

IMPLEMENTATION

UTXO is a special pattern of currency circulation. The transaction constructed with the UTXO model mainly relies on an InputSet and OutputSet to accomplish the currency circulation. Furthermore, the InputSet and OutputSet contain several Inputs and Outputs separately. We elaborate the details in the following section. **Table 1** and **Table 2** present the notations and definitions covered in this section.

Table 1. Basic notations of UTXO structure.

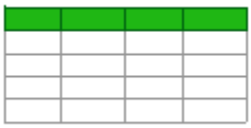
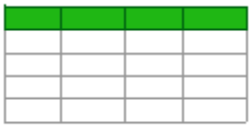


Table 2. Cryptographic algorithms of UTXO structure.



provides transaction object information, which contains two elements, V,Hpk

Output←(V,Hpk)….eq(1)

where Hpk is the hash value of the transaction object's public key, which represents the target of this output, and V represents the transaction value for one object. Notably, both Hpkand V are public information.

The Inputof the current transaction is generated based on the previous transaction Output

. We illustrate the specific composition of Input

$$Input \leftarrow (PIDt, Nout, pk, \sigma sk) \ldots\ldots eq(2)$$

Input

contains four elements, PIDt,σsk PIDt

represents the retrieval index of the transaction. The Input

of the current transaction is generated based on the previous transaction Output

. Therefore, Nout is utilized to mark the position of the Output in the output set of the previous transaction. pk is the public key to verify the signature σskand the σsk is the signature of PIDt using the secret key corresponding the Hpk which is utilized to prove the legitimacy of the output that is marked by Nout

.

Verification Mechanism

Generally, the InputSet consists of multiple Input

. The verifier confirms the legitimacy of the transaction through the following operations. First, it compares whether the hash value of pk

in the current Inputand Hpk in Output that is marked by Nout are consistent. Second, it verifies the signature with the pk

. We explain the verification operation in Algorithm 1.

Algorithm 1 Verification Algorithm.

Require:R.

Ensure:true

or error_code

.

1: $R \leftarrow (PIDt, pk, Hpk, \sigma sk)$

2: if formal check on the R is ok then

3: $Hashlock \leftarrow HashPubKey(pk)$

4: else return error_code

5: if Compare(Hashlock,Hpk)=?true

then

6: if Verify(pk,σsk)=?true

then

7: return ture

8: end if

9: end if

10: end if

11: return error_code

Algorithm 1 involves three main steps, described as follows.

Step 1-1 (Step 1 in Algorithm 1): The user sends the tuple R to the object located within its communication range.

$$R=(PIDt,pk,Hpk,\sigma sk) \ldots\ldots\ldots eq(3)$$

After receiving the message, the verifier performs a formal check on the R, which is to confirm the integrity of the message. After this, Equation (4) is leveraged to calculate the hash value of pk

.

$$Hashlock=HashPubKey(pk)\ldots..eq(4)$$

The function HashPubKey

is utilized to compute the hash value of the public key, which is constructed in a smart contract. Specifically, we implement the hash computation in the smart contract by considering the relevant functions in the standard cryptography library. After the smart contract is deployed to the blockchain, the corresponding public key hash value is obtained by considering the smart contract and using the pk

as the input parameter of the smart contract.

Step 1-2 (Step 5 in Algorithm 1): Comparing whether the hash value of pk

in the current Input

and Hpk

in Output

that is marked by Nout

are consistent. Here,

Equation (5) is leveraged to determine whether Hashlock and Hpk are equal.

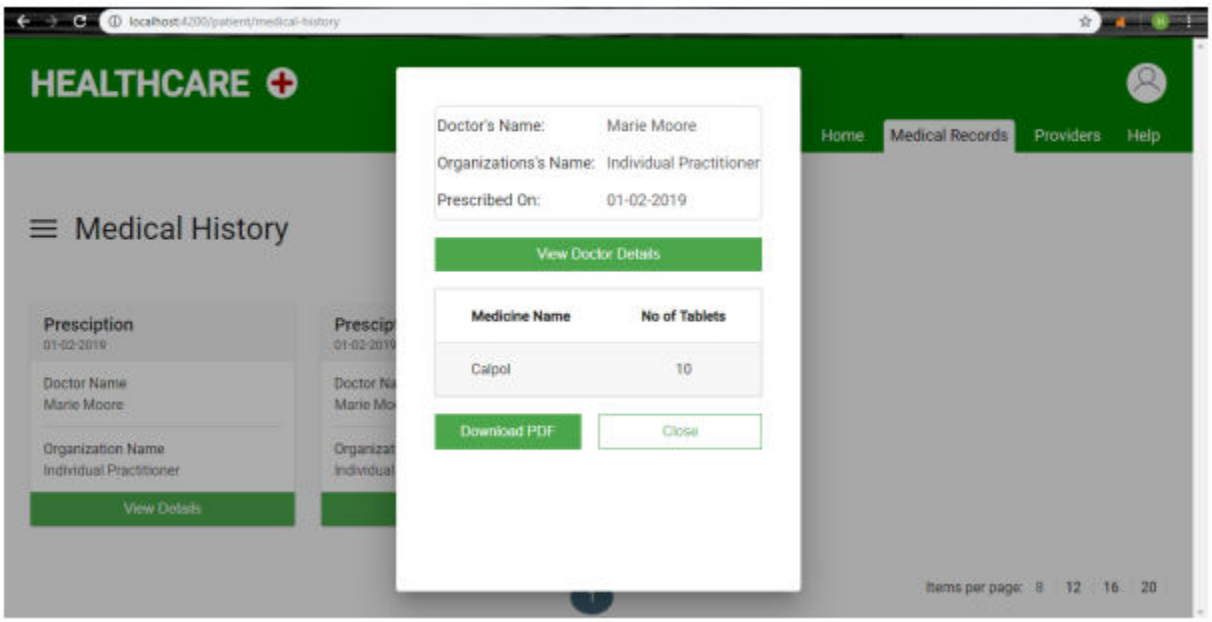
$$Compare(Hashlock,Hashpk)=?true\ldots.eq(5)$$

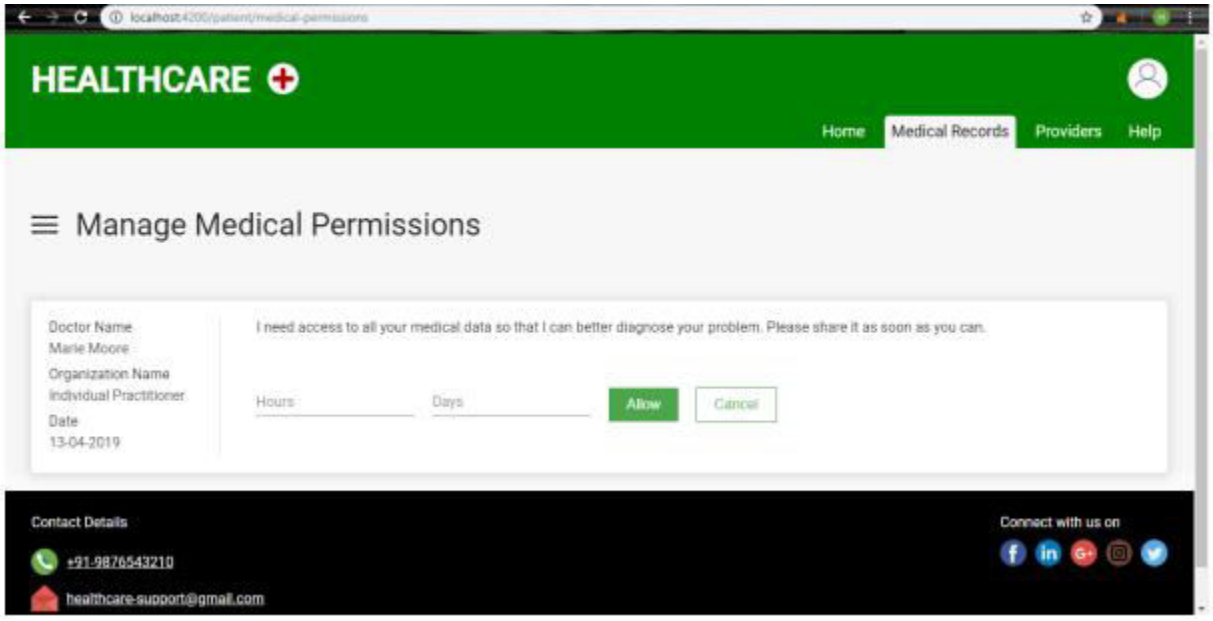
Step 1-3 (Step 6 in Algorithm 1): Next, Equation (6) is utilized to verify the validity of the signature based on the asymmetric cryptography.

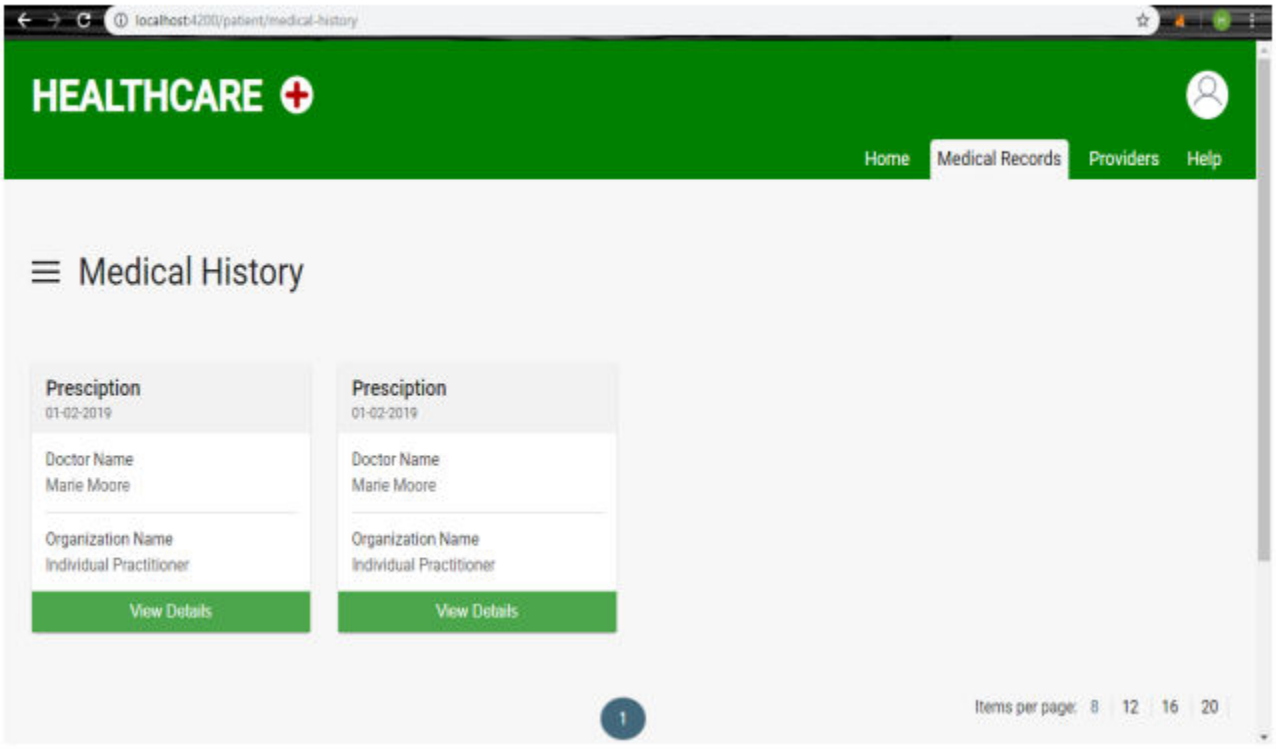
$$Verify(pk,\sigma sk)=?true\ldots..eq(6)$$

Thus, the recipient can verify whether the transaction is valid with the verification mechanism.

SNAPSHOTS




HEALTHCARE
Home
Medical Records
Providers
Help
Manage Medical Permissions
Doctor Name
Marie Moore
Organization Name
Individual Practitioner
Date
13-04-2019
I need access to all your medical data so that I can better diagnose your problem. Please share it as soon as you can.
Hours
Days
Allow
Cancel
Contact Details
+91-9876543210
healthcare-support@gmail.com
Connect with us on


HEALTHCARE
Home
Medical Records
Providers
Help
Medical History
Presciption
01-02-2019
Doctor Name
Marie Moore
Organization Name
Individual Practitioner
View Details
Presciption
01-02-2019
Doctor Name
Marie Moore
Organization Name
Individual Practitioner
View Details
1
Items per page: 8 12 16 20

CONCLUSION

In order to realize the authentication scheme of EHRs machine based totally on block chain. We first formally define the EHRs gadget model within the putting of consortium block chain. Then we design an identification-primarily based signature scheme with a couple of authorities for the block chain-primarily based EHRs machine. The scheme has green signing and verification algorithms.

FUTURE ENHANCEMENTS

Blockchain has a place in healthcare claims management. Recognizing the difficult challenges healthcare providers and payers face with claims management in the era of value-based care, advanced blockchain technologies are helping them to reduce claims denials, increase claims processing transparency and improve collection of patient financial responsibilities. These solutions provide next-generation workflow and advanced technologies, including machine learning and blockchain/private distributed ledger technology (DLT), to prospectively help providers reduce claims denials and secure payment of patient financial responsibilities for care. Payers are now able to create new levels of transparency around real-time adjudication of claims and reimbursement, as well as the immediate generation of explanation of benefits (EOBs) for members.

REFERENCES:

[1] M. Braunstein and B. Todd, “Disruptive Technology in the Healthcare Space”, GaTech Seminar on technology innovation in the healthcare space, Atlanta, Georgia, on February 10, 2016.

[2] W. Liu, T. Mundie, U. Krieger, E.K. Park and S.S. Zhu, "Rapid delivery e-Health service (RDeHS) platform”, Proceedings of HealthCom-2016, International Conference on e-Health Communications, Services and Applications, Munich,

[3] G. G. Dagher, J. Mohler, M. Milojkovic, P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", *Sustain. Cities Soc.*, vol. 39, pp. 283-297, May 2018.

[4] W. J. Gordon, C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability", *Comput. Structural Biotechnol. J.*, vol. 16, pp. 224-230, 2018.

[5] R . Guo, H. Shi, Q. Zhao, D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems", *IEEE Access*, vol. 6, pp. 11676-11686, 2018.

AUTHOR 1

MR.RAGHUVARAN ME, is Assistant Professor in Department of Computer Science and Engineering at ST.Joseph College of Engineering ,Sriperumbadur, Chennai, Tamil nadu He has done his M.E, CSE in Univercity Chennai in the year 2014.He has done his B.E CSE in Anna university Chennai in the year 2012 and 2 year of experience in industrial field

AUTHOR 2

Mr.S.Muniyappan B.E., Student of Computer Science and Engineering at St.Joseph College of Engineering, Sriperumbudur, Chennai, TamilNadu. I had attended many Workshops, Seminars in Blockchain. I got placed in Reputed Companies like Q Spider and some respected companies.

AUTHOR 3

Mr.k.ManigandanB.E., Student of Computer Science and Engineering at St.Joseph College of Engineering, Sriperumbudur, Chennai, TamilNadu. I had attended many Workshops and Seminars in the area of blockchain