IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Permissioned Medic-Blockchain Based Patient Healthcare Record Sharing And Retrieving System

Priyanka Sonar
Department Of Computer Engineering
Research Scholar
Mumbai University
Mumbai, India

Prof. K. JayaMalini
Department Of Computer Engineering
Research Scholar
Bharath University
Assistant Professor @ SLRTCE
Chennai, India

Abstract— ***The healthcare blockchain structure permits patients and healthcare providers to admittance and share health records in a confidential-conserving way. It permits patients to give or withdraw consent for regulating admittance to their records. To protect medical data, this healthcare blockchain uses an encryption mechanism and enforces a smart contract based access control mechanism for regulating access. To create this type of system, we are using Hyperledger fabric for designing our network system. Hyperledger fabric is an open source blockchain framework which helps to develop a network system. Hyperledger Fabric Composer has been used to develop a permissioned blockchain technology, which is suited towards the use-cases that require privacy.***

Index Terms— Electronic Healthcare Record , Sharing And Accessing, Hyperledger fabric/composer, Consent mechanism, smart contract.

I. Introduction

In this paper, we present Medi-Blockchain, a secure healthcare system. Blockchain technology address the problem in a fragmented manner with existing health solutions by providing a distributed yet interconnected data storage framework. With the use of the blockchain, there is no central authority managing all data. Instead, ownership remains with the patients who are empowered to access their EHRs and share them with healthcare providers on the network. The immutable and transparent nature of data on the blockchain enables data auditability and provenance, allowing patients to see how their healthcare records are used and enabling them to have a more active role in managing their health. Furthermore, a blockchain network has no single point of failure, offering continuous data availability that otherwise is difficult to achieve with centralized systems. The data stored on the blockchain nodes must be secured with an encryption mechanism and access control policies must be enforced to regulate access to sensitive data. It enables patients to share their health records but does not provide any way to manage consent revocation. Medic Blockchain employs a consent management system at a healthcare provider level so that patients can control which providers are able to access their records at any given time. This is achieved by using smart contracts enforcing access control policies. Important cryptographic material used to secure records or to share records is managed by an authentication server to prevent users from losing or exposing the material to unauthorized parties. The core contributions of this paper is the Medic-Blockchain system, empowers patients to securely share their medical data with healthcare providers, as well as offering the ability to capture patient consent. It protects data by employing encryption schemes and enables secure access to medical data. This brings convenience for the users of the system, as they do not have to be concerned about how they should keep their cryptographic material secure.

Blockchain also reduces the complexity involved in sharing data and agreements between physicians, hospitals and public health departments, allowing all the organizations to securely and quickly move patient medical data in a legal manner with trust each other in organization. All members of network or organization needs to know is other member is a valid member. Healthcare sector concentrating on the important aspect provided by the Blockchain technology like immutability of the data in ledger. Identification of thefts, financial data crimes and spamming, as patients don't have control over their medical records, which could be misused too. So Hyperledger fabric provides the solution for such problems. Transactions that are having patient's health

information are recorded on the ledger. Whenever any healthcare provider needs to access data of patient, the transaction ID assigned needs to be matched only then the related information is displayed. Hyperledger Fabric is distributed ledger technology for any business network. Following four key characteristics of hyper-ledger fabric has made it most suitable for implementing distributed ledger technology. 1) Ability of creating permissioned blockchain network 2) Confidential transactions 3) Cryptocurrency is not involved 4) Programmable Hyperledger fabric provides the trust, transparency and accountability. Hyperledger Fabric is designed for many business use cases, where the block chain is generally operated by a set of identified and trusted participants and this ability is called as permissioned block chain. Permissioned network restricts who can access and do what on the network. It requires participant should be known. Transaction is validated by known validators. Hyperledger fabric puts participants in control of visibility of transactions. Hyperledger does not have concept of cryptocurrency because no need to incentivize the network for validations. Hyper ledger fabric is programmable by the way of construct of smart contract- It is the business logic of a blockchain application and even are invoked by an application external to the blockchain when that application needs to interact with the ledger. Smart contracts have been designed for different medical workflows and then managing data access permission between different entities in the healthcare ecosystem.
Smart contracts work by following simple "if/when…then…" statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. The blockchain is then updated when the transaction is completed.

A. Use Case Scenarios

Here we explain the scenario requirement. So the Bombay Hospital and Auckland Healthcare uses a shared EHR system to manage patients data. We consider that, Marry who just moved to Auckland from the Mumbai for her work. And has not enrolled with Auckland healthcare system.
1) Scenario 1: Registration: Soon after Marry moved to Auckland, she encountered a heart condition and went to Auckland healthcare for her treatment. In order to keep a record of this treatment and make the further treatments of her illnesses minimal, Marry wants to register with Auckland healthcare.
2) Scenario 2: Record Access: After Marry was treated by Auckland healthcare, she wants to evaluation the particulars of her illness and the medication that she was prescribed with.
3) Scenario 3: Consent: So now as the Marry returns back to Mumbai. Unfortunately, she got ill again was taken to Bombay Hospital for treatment. To allow the doctors in Bombay Hospital to learn the details about her existing condition, Alice needs to give Bombay Hospital her consent to let them view her health records. And after the treatment, Marry would also withdraw the given consent.

III Review Of Related Work

Jack Huang, Yuan wei Qi, Muhammad Rizwan Asghar, Andrew Meads, and Yu-Cheng Tu[1]. In this paper, the authors has presented a blockchain-based secure EHR system that enables patients and healthcare providers to access and share health records in a usable yet privacy-preserving manner.

Naveen Kumar S, Dr. M Dakshayini [2]. In this paper they introduce a Hyperledger fabric frame work based permissioned blockchain network which is proposed and established among patents and medical institutes to achieve the secured and reliable sharing of the patient's data. Implemented results had shown, the Hyperledger fabric based Blockchain removes the unreliability in sharing of data among health care centers, doctors, public health departments and hospitals

Uttkarsh Goel, Ron Ruhl, Pavol Zavarsky [3]. In this paper they have discussed, a dual blockchain model for the healthcare sector. The model combines healthcare authority blockchains and private patient blockchains for a tamperproof permission tracking system which ensures increased security and privacy while improving record and permission redundancy.

Vinay Mahore, Priyanshi Aggarwal, Nitish Andola, Raghav, Dr. S. Venkatesan [5]. In this paper the author have highlighted the problem i.e. there is a lack of trust between these independent eHealth care systems which makes it difficult to establish an end-to-end accessible network. Blockchain technology can be a potential solution. After which they have proposed a model which focuses on providing healthcare data to researchers for statistical analysis and providing privacy at the same time. The model exhibits high data security by aggregating the customized access control protocol and asymmetric cryptography for sensitive medical information sharing.

Ruksudaporn Wutthikarn, Yan Guang Hui [7]. Have mentioned about the This paper discussed on the permissioned blockchain technology and Hyperledger fabric and even focuses on the study to develop a prototype of healthcare service application in dental clinic service.

III System Necessities

We have created a set of system necessities as listed below:

• Patient Power Driven Healthcare- The patient grants the doctors to view their health records/prescription is referred as a patient permission or the consent. Our EHR system should empower the patients by enabling them to have a more active role in managing their health and provide them with a convenient platform to engage with the system. The stewardship of health records is handled by the patients so that they no longer need to request access to their records from their healthcare providers. In addition to this, the system should provide patients with the ability to give and withdraw consent based on which healthcare provider can access their health records.

• Security and privacy- The system should preserve the confidentiality of the patients' health records and protect the privacy of the patients. This includes the enforcement of several access control rules. Additionally, even if an attacker manages to obtain any data from the storage systems, the data should still remain protected.

• Efficiency- The system should be efficient enough so common operations such as accessing records and managing consent can be performed in a timely fashion.

•Scalability- The system should be scalable enough to deal with all the citizens.

• Availability- Patients and healthcare providers should always be able to access health records, where the system must have no single point of failure.

IV. System Representation

A. Models Of The System:

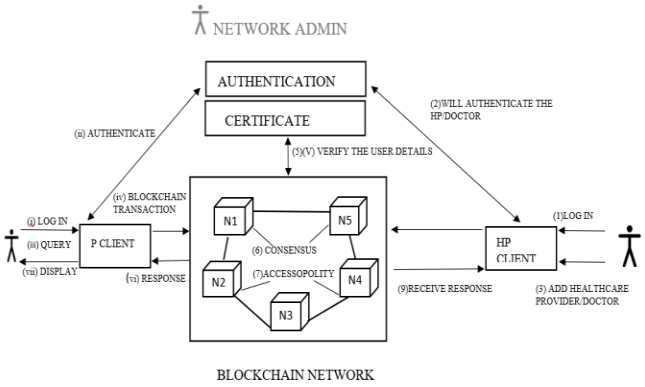

Fig 4.1 The above fig represents block diagram.

1. Patient- The access of the record/prescription is granted to the patient/user of the system. There is no way that the patient can amend or obliterate the medical record/prescription provided by the HP. And even they can elect who can admission to the precise medical records that will be used for the additional therapeutic treatment. Patient has a right to query the blockchain for the evidence concerning their therapeutic history.

2. Healthcare Provider- An HP is any healthcare specialists who are responsible for generating health histories for the patients. These records/prescriptions must be encrypted before they are interleaved into the blockchain. The healthcare provider are able to regain the record of the patient from the blockchain but data needs to be decrypted on their side. They are also able to update and delete data, once the patient has given them the consent to admittance the medical record.

3. Network Manager- The blockchain nodes are maintained on the network by the network admin. They are accountable for handling patient identities and ensuring the establishment of most health amenities in their respective area.

4. Certification Authority- A CA issues digital certificates for participants on the blockchain using Public Key Infrastructure (PKI). These documentations represent the identities of entities contributing in the blockchain system and therefore this certificate is attached to transactions made on the blockchain network by the participant. This allows beneficiaries of the system to authenticate the source's individuality and the veracity of the message.

5. Authentication Server- It is used to validate participants and the authenticated participants are permitted to join the blockchain network.

6. Service Client- The client is the first point of contact for a user with the blockchain. It submits transactions to execute CRUD (Create, Read, Update, Delete) operations on the ledger. Users must provide their login details if they wish to access the client. Different clients are provided to each type of user in the system, each one offering a different set of functionalities. For instance, only the network administrator's client may register new patients on the blockchain.

7. Blockchain Network- This is the core organization structure of the system. The network is made up of interconnected "peer" nodes with a shared ledger. Participating nodes are responsible for storing ledger data, executing smart contracts, validating transactions, and committing blocks onto the ledger.

B. Transaction Details:

As every data is transparent on the blockchain, we propose authentication servers and Certificate Authorities, to provide means to issue identities and secure the cryptographic which will be used to encrypt all data on the blockchain. We will also use blockchain specific features, primarily smart contracts, to enforce access control rules. These techniques will help keep data confidential and safeguard patient's privacy. This techniques will also allow our system to have the capability to facilitate healthcare record sharing and to capture patients consent. The patient health records are encrypted and stored on the blockchain. Different users can interact with the blockchain such as making transactions and querying the ledger.

1) *Registration*: The registration process, where patients wants to be registered with Medic Blockchain. To do so, the patient must first fill his/her personal details. After all the necessary information is supplied, the client service will use the username and password pair to compute an authentication user key and a verification value using some random user key. When the authentication server receives patient's registration request, it will create the ID of the patient. The authentication server will form an identity for patient via the Certificate Authority and use that identity to create a network identity card. This network identity card contains an identity private key and an identity public key which is certified by the certificate authority, for an effective encryption of the patient's record/prescription. This network identity card, will allow patient to connect to Medic Blockchain network and sign the transactions with the issued identity. The identity card will be encrypted with the patient's public key.

2) *Attestation:* If the patient wishes to access his/her prescription/records, then the patient must first log in to Medi Blockchain using the patient client service. After entering the username and password, the client will contact the authentication server, and then it will attestation the particular patient. After successful attestation, the authentication server will send the encrypted identity card and patient's private key to the client service. The decrypted identity card, via the client service can then be used to connect to Medic Blockchain

network. Similarly, when an HP attempts to log in to Medic Blockchain, the same process takes place.

3) *Sharing Records*: Now if the patient would like to share his/her health details with the specialist of the Bombay hospital. In order for Bombay hospital to view and add records for a particular patient, they must have access to patient key, which is used to encrypt all records for a patient. A hospital can request for patients private key using their client service. When the request is made, Bombay hospital's client will direct the request to the blockchain networks peer nodes as a transaction. When the transaction is executed, the peer nodes will send a notification event to other clients. The corresponding patient's client, which subscribes to Request Key event, will receive the message. This request will show up as a notification on patients client. If the patient wishes to grant consent to Bombay hospital to let them access his/her records/prescriptions, the patient must share his/her patient private key with the hospital. After the consent list is successfully updated, the peer node will trigger a Share Key event. Bombay hospital's client will receive the event and then show a notification on the client to indicate that patient has shared the key with them. Bombay hospital will now know that they can access patients records as shown in fig 5.2.

4) *Retrieving Records/data:* Now after a successful authentication, whether the user is an healthcare provider or patient, their client service will have their private key, which is necessary for accessing records. If Bombay hospital wishes to access patient's records, using healthcare provider's client service, after the patient has granted them the consent, they can send a request for patients record and encrypted patient key, as a transaction to the blockchain nodes via their client. The smart contracts on the blockchain will verify that patient has listed the identity of Bombay hospital in her consent list. After successful verification, smart contract execution and the encrypted records it is send to Bombay hospital client. The client will decrypt the record and then the decrypted record, will be displayed for viewing. A similar process occurs when patient attempts to access her records. The smart contract will not check for consent but instead, just use patients identity to retrieve every record that patient owns.

V. Result Discussion

Here, we discuss on a blockchain that supports electronic healthcare record sharing and accessing. We implemented blockchain network using the Hyperledger Fabric platform. Hyperledger Fabric is a permissioned smart contract based blockchain platform designed for enterprise use. It does not employ Proof-of-Work consensus, commonly known as mining. Instead, it relies on the Practical Byzantine Fault Tolerant algorithm as its main consensus mechanism. This means that nodes do not have to expend as much energy as the ones in Proof-of-Work based blockchain platforms, such as Bitcoin or Ethereum. All nodes run within their own Docker container on a single machine. The version of Fabric we used is v1.1. Our experiments emphasis on the effect that access control policies and cryptography have on performance. The software that is used is Ubuntu 18.04: It is a Linux distribution based on Debian and composed mostly of free and open-source software. And the IDE used is Visual Studio Code. Hence through the below screenshots of the output it is shown that how the patient can provide the consent to the HP and how the HP will able to view the patients record. The CryptoJS a JavaScript library is used to provide the cryptographic encryption and decryption.

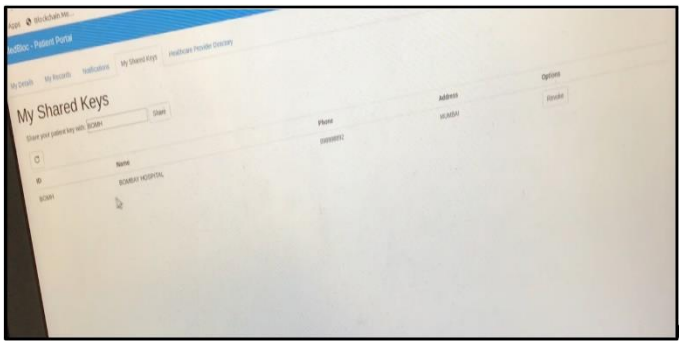

Fig 5.1 In the above figure is of patient portal where the details of the HP is displayed with whom the patient will share the data/medical records.

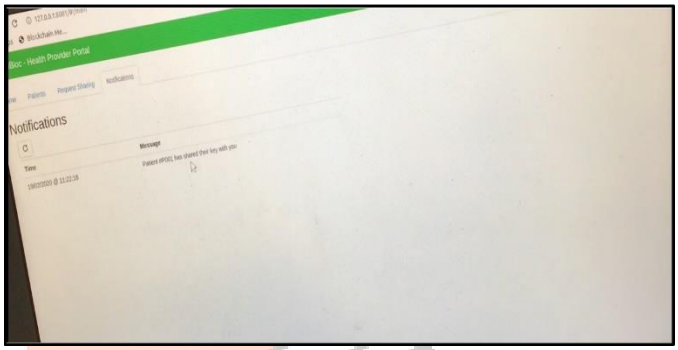

Fig 5.2 In the above figure of HP portal, after clicking on notification option the HP can view the particular patient sharing the medical records.

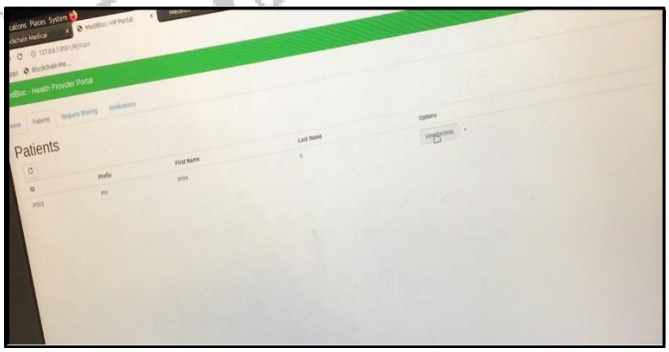

Fig 5.3 In the above figure when HP clicks on view record option under patients tab, then he will be able to view the patient's medical record.

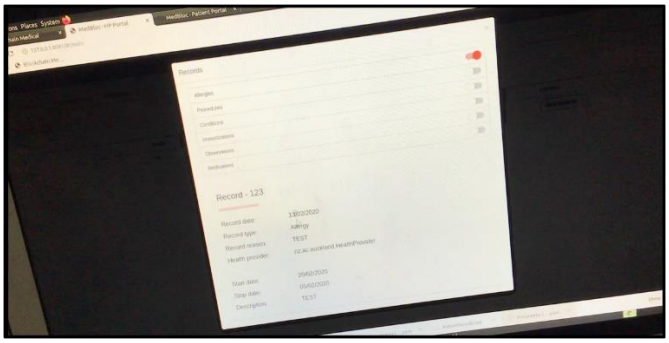

Fig 5.4 In the above figure the HP/doctor is able to view the patient's medical record. After getting the consent from the patient.

VI. Conclusion

We showed that Medic-Blockchain is a people/client powered shared electronic healthcare system that allows patients and healthcare providers to access and share health records conveniently through a dedicated client service. Through the use of smart contracts and cryptographic techniques, patients can give and withdraw consent at any time. Healthcare providers can request for consent and add records which are encrypted and stored securely on the blockchain. Using the sophisticated encryption scheme, Medi-Blockchain also protects patients' privacy. Medi-Blockchain immutable access control policies prevent any unauthorized actions from being performed.

VII. References

[1] Jack Huang, Yuan wei Qi, Muhammad Rizwan Asghar, Andrew Meads, and Yu-Cheng Tu, "A Blockchain-based Secure EHR System for Sharing and Accessing Medical Data", 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering.

[2] Naveen Kumar S, Dr. M Dakshayini, "Secure Sharing of Health Data Using Hyperledger Fabric Based on Blockchain Technology", October 28, 2020.

[3] Uttkarsh Goel, Ron Ruhl, Pavol Zavarsky, "Using Healthcare Authority and Patient Blockchains to Develop a Tamper-Proof Record Tracking System", 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing (HPSC), and IEEE Intl Conference on Intelligent Data and Security (IDS).

[4] Shishir Ranjan, Amit Negi, Himansh Jain ,Bhuvnesh Pal and Himanshu Agrawal, "Network System Design using Hyperledger Fabric: Permissioned Blockchain Framework"-2019-IEEE..

[5] Vinay Mahore, Priyanshi Aggarwal, Nitish Andola, Raghav, Dr. S. Venkatesan, "Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain", 2019 IEEE Conference on Information and Communication Technology (CICT).

[6] Yiheng Liang, "Identity Verification and Management of Electronic Health Records with Blockchain Technology", IEEE-2019.

[7] Ruksudaporn Wutthikarn, Yan Guang Hui, "Prototype of Blockchain in Dental care service application based on Hyperledger Composer in Hyperledger Fabric framework", IEEE-2018.

[8] Rishav Raj Agarwal, Dhruv Kumar, Lukasz Golab, Srinivasan Keshav, "Consentio: Managing Consent to Data Access using Permissioned Blockchains", IEEE-2020.

[9] Tomasz Hyla, Jerzy Pejas, "eHealth Integrity Model Based on a Permissioned Blockchain", 2019 Cybersecurity and Cyberforensics Conference (CCC).

[10] Anang Hudaya Muhamad Amin, Sharmila Siddartha, Rashed Khalifa Matar Obaid M Almehairi, Yousuf Hussain Mohammad Ali Albalooshi, Saeed Adnan Saeed Alkhatibi Alsuwaidi, Jawahir Obaid Saeed Obaid Kannoun Shamsi, Ali Nasser Thani Rashed Almatrooshi, "Permissioned Blockchain Design for Integrated Healthcare Data Management", IEEE-2019.