Permission-Based Blockchain with Proof of Authority for Secured Healthcare Data Sharing

Conference Paper · November 2020

DOI: 10.1109/ICAICT51780.2020.9333488

4 authors, including:

Md. Tausif Elahi

1 PUBLICATION **0** CITATIONS

SEE PROFILE

Abdullah Al Hasan

Bangladesh University of Professionals

4 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Mohammad Abu Yousuf

Jahangirnagar University

62 PUBLICATIONS **254** CITATIONS

SEE PROFILE

2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT) | 978-0-7381-2323-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICAICT51780.2020.9333488

Permission-Based Blockchain with Proof of Authority for Secured Healthcare Data Sharing

Nafiz Al Asad
Department of Information and Communication Technology
Bangladesh University of Professionals
Dhaka, Bangladesh
nafiz.al.asad@gmail.com

Md. Tausif Elahi
Department of Information and Communication Technology
Bangladesh University of Professionals
Dhaka, Bangladesh
mdtausifelahi@gmail.com

Abdullah Al Hasan
Department of Information and Communication Technology
Bangladesh University of Professionals
Dhaka, Bangladesh
hshasan224@gmail.com

Mohammad Abu Yousuf
Institute of Information Technology
Jahangirnagar Univesity
Dhaka, Bangladesh
yousuf@juniv.edu

Abstract— ***Electronic exchange of healthcare data between hospitals and institutions is limited by privacy, interoperability, and dependency on centralized data management systems. Sharing patients' data without their consent is a violation of the law and bears the risk of identity hack and misuse of healthcare data. Not all healthcare institutions follow a similar structure and semantic to store patients' data, making it almost impossible to share the data for research and better patient management. Centralized data management system is vulnerable to cyber-attacks and data theft. It also creates lock-in problems for patients intending to migrate their data to any other institute. In this paper, a permissioned Blockchain with Proof of Authority (PoA) technology has been proposed that guarantees data privacy, data owner's control on sharing their sensitive information, and effective distributed management of healthcare records. It also addresses the importance of managing medical records in an interoperable manner, and the use of de facto standards such as Fast Healthcare Interoperable Resources (FHIR), which helps the meaningful exchange of healthcare records among all participants. The work is based on simulating the outcome of using PoA to understand the efficacy of this consensus algorithm when using Blockchain technology for secure data sharing.***

Keywords—blockchain, PoA, FHIR, healthcare, privacy, interoperability, security

I. INTRODUCTION

A blockchain is a distributed ledger containing transactions [1]. It is composed of transaction blocks which are interlinked to one another using intriguing properties. Firstly, each block contains a hash of its contents, making the blocks verifiably immutable, ensuring the integrity of the transactions inside a block. Next, the hash of a block is derived using the hash of its previous block. This effectively ensures the entire blockchain's history remains immutable, as modifying the hash of any block would also change the hash of all the blocks in the blockchain. The blockchain does not depend on a central trusted authority; instead, all nodes participating in the network carry the same copy of the blockchain. As there is no presence of a centralized authority to verify the blockchain's validity, a mechanism for attaining consensus in the network must be applied.

Proof of Authority (PoA) is an algorithm for consensus in the blockchain that proposes an effective and efficient solution for data privacy in blockchain networks. The PoA algorithm utilizes the value of identities to impose security by validating subjectively selected nodes as trustworthy. The Proof of Authority algorithm depends on a restricted number of block validators, making it a highly scalable system. Blocks and transactions are verified by pre-approved peers acting as moderators of the system [2]. The Proof of Authority model enables organizations to maintain their privacy while availing of the benefits of blockchain technology. Microsoft Azure is an example of where PoA is being implemented. The Azure platform provides solutions for private blockchain networks, without a native currency like the ether 'gas', as there is no need for mining [2]. Smart contracts are piece of software or codes in a blockchain that is managed by a P2P network of computers. Smart contracts are rights management tools that provide a coordination and enforcement framework for agreements between network participants, without the need for traditional legal contracts. They can be used to execute simple agreements between two parties, the bylaws of an organization, or to create tokens. Smart contracts are, in the context of blockchain, particular logic embedded in a blockchain, that can receive or perform transactions like any address (transactions may be rejected or require unique arguments to the function), and that can act as an immutable agreement. The purpose of the smart contracts is to act as a "computerized transaction protocol that executes terms of a contract"[3].

Fast Healthcare Interoperability Resources (FHIR) [4] enables the separation of Electronic Health Record (EHR) into defined structured data types or resources [1]. FHIR resources follow Representational State Transfer (ReST) protocols and validates structural conformity with the standard, refined by additional agreements called Profiles [1]. Electronic exchange of clinical information enables care givers, and patients to share vital medical information

978-0-7381-2323-3/20/$31.00 ©2020 IEEE

electronically—improving the pace, quality, security, management, and expense of patient care [5].

Blockchain contains blocks of transactions and their hashes to maintain data integrity. A transaction in the healthcare domain is defined as a procedure of generating, uploading, or transmitting EMR data that is executed within the connected nodes. [6]

This paper intends to propose a framework for secure and interoperable healthcare data sharing using Blockchain and FHIR technology. Addressing the problem of existing processes and analysing future requirements a model is proposed. Chapter two describes the relevant works and studies in the area of healthcare data sharing using Blockchain. Chapter three gives an overview of a proposed system architecture concerning the use cases as an example. Chapter four shows the relevant configuration and steps to implement the proposed model. Chapter five shows the simulation and results of deploying the framework in a test environment. Improvement in the process and performance of the proposed model is discussed in the final chapter.

II. RELATED WORKS

A. Complexities in Healthcare Data Sharing

Inability to protect the patient information has financial and legal repercussions, and the potential to severely affect patient care. Therefore, maintaining the security of the electronic medical record is very challenging [1]. Data privacy ensures that only authorized entities may access the medical information, as maintaining patient's privacy is an ethical responsibility as well as a legal obligation [2]. The interoperability of healthcare records is the extent to which the clinical intent conveys across institutional boundaries [1]. Given the complex nature of data in the healthcare domain, this is inherently difficult to achieve [3]. The heterogeneous structures and complexity of healthcare data decrease the effectiveness of analysis and reduce understandability. Several industry-wide standards are advancing to reduce this complexity[4].

Data anonymity is another way for securing the medical record. In this way, information that are identifiable are left out, and only summary data is shared. Although acceptable, it becomes complex, when a large number of attributes with potential resource value have to be removed from the record, so that it can become unidentifiable [5]. Patients may also require to agree upon a consent that indicates the type of data that will be collected when sharing his clinical data for the purpose of research, or transferring them from one medical institution to another. The contract may also carry specific details about the recipient, and the timeframe during which the recipient can retain the data. Such a contract could be remarkably difficult to manage, especially in situations when a patient moves to a different location and may not be familiar with the caregiver or the hospital from where he would receive care in future [6].

Depending on a central data management system that stores and manages the patients' data, and access control system raises the risk of a single point of failure and a bottleneck of the framework. It also requires that all the operations should be conducted over encrypted data or having a trusted third party who will be able to access to sensitive data of the patients. The former still requires managing large memory space and is not achievable by all hospital infrastructure. The latter is quite difficult to put to practice. An example of the GoogleHealth wallet has indicated that patients are more cautious about their privacy, and aware of the potential consequences of having their sensitive information to be misused [7]. Centralization also increases the security risks, and requires trust in a single authority, while transmitting bulk data forces organizations to yield operations of their data [1].

B. Blockchain Based Solutions

Kevin Peterson et al. [4] showed that to share data effectively, networks require to agree upon data structure, meaning, and security. They proposed that a blockchain can be a solution to enable data sharing within a network, and have defined the structures and protocols for applying this technology to healthcare. A ledger which is distributed, immutable, and has a transparent history of all the transactions that have happened to all the nodes of the network, overcome the issues such as privacy, interoperability, decentralized data management [1]. Al Omar et al. [7] put forward a data management system for patient healthcare, which employs blockchain to secure private storage. Their framework addresses the issue of losing control when storing encrypted data within the system. One of the key aspects of blockchain is the consensus algorithm. There are quite a few algorithms that exist, but Proof of Authority (POA) algorithm [8] suites perfect for implementing a smart contract for permission-based blockchain. POA provides authorization and authentication of data in a very cheap and efficient way [9]; without requiring complex computing hardware and resources and complex algorithms.

Zyskind et al. suggested a blockchain usage for managing access control, and securing data storage [10]. Encrypted data will be stored by trusted third-party services and log of events are stored in the blockchain. But, there is no reliable third party providers in the real world, which raises the risk of data exposure. Xia et al. proposed a blockchain based system to manage and protect medical records effectively. system to manage and protect medical records effectively. The system provides data protection and management for shared medical data in cloud repositories among big data entities. To ensure data security identities and cryptographic keys are verified. [11]. But the model does not address the risk of data disclosure, where the hospital is unwilling to share the data with a third party. This exposes a flaw in the proposed scheme. Alevtina Dubovitskaya et al. proposed a permission-based blockchain framework to manage metadata and access control rules and a cloud infrastructure to store patients' information in encrypted format.[12]

Asaph Azaria et al. described how leveraging distinctive properties of blockchain, helps to manage authentication, confidentiality, accountability, and data sharing- crucial considerations when handling sensitive information.[13] In recent years, blockchain has proved to be a potential solution to implement Personal Health Information (PHI) distribution with security and preserving privacy because of its nature of immutability [14]. In their paper, Hongyu Li et al. [15] presented a narrative on data preservation system for medical data. The proposed system suggests a reliable storage to ensure the primitiveness and integrity of stored data while securing users' privacy. Permission for accessing patients' medical records across multiple

healthcare organizations and devices needs to be designed cautiously. Blockchain is not designed as a large-scale storage system. In the healthcare context, a decentralized storage system would greatly complement the weakness of blockchain in this perspective[16].

D. Baars [17] have compared the three consensus algorithms in terms of Speed, Power consumption, permission, costs etc. The comparison of the algorithms has been summarized in TABLE I

TABLE I: COMPARISON SUMMARY OF POA WITH PROOF OF WORK AND PROOF OF STAKE

	Proof of Work	**Proof of Stake**	**Proof of Authority**
Speed	Slowest	Average	Fastest
Power Consumption	Inefficient	Efficient	Efficient
Security	Permission less, untrusted	Permission less, untrusted	Permissioned, trusted
Maturity	Tested	Untested	Safe
Costs	Costly	Less Cos	No Cost

Based on the review of these existing works, this proposed method tries to establish a secure system for healthcare data sharing, leveraging POA to ensure data privacy and harnessing blockchain's in built characteristics to ensure data integrity,

III. PROPOSED SYTEM ARCHTECTURE

Addressing the problem of existing Healthcare Data Sharing and studying the relevant work of others, a system architecture is proposed in this chapter. It will give an overview of how a user obtains a blockchain by registering to the system, how new nodes are added based on user's permission along with shading light on the process of data sharing and finally explaining the distributed interoperable healthcare data sharing system.

A. Registration to the System and Obtaining Blockchain

The user journey begins by registering to the system. Upon successful registration, the user becomes the owner of his/her blockchain. The genesis block is created after registration is completed. Fig. 1 illustrates the data flow of the registration process.

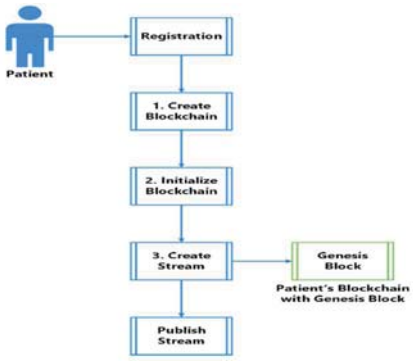

Fig. 1: Registration process and creating genesis block

The registration process includes completing a general patient information form. As this form's design is in line with FHIR format, it becomes interoperable to all who get access to the patient's blockchain. To access their data, patients would need to login to the system. Therefore, upon registration, patients would receive their username and password on their email addresses and update them later on to maintain security. It should be noted that after inserting data in a blockchain, they become immutable. Therefore, not all information of a patient can be added to a blockchain. Otherwise, the need for maintaining a local database arises, which contradicts the idea of a distributed ledger system. To mitigate this problem and have all general information of patients in the blockchain, moving the storage system to the cloud is suggested, so that it can be accessible by any node connected to the blockchain, and the patient's general information can be stored in the cloud database. Christian Esposito et al. [18] proposed a blockchain-based solution to store healthcare data in the cloud.

Blockchain ensures that sharing of medical information takes place without involving a trusted mediator. This helps to avoid a performance degradation, and a single point of failure. Patients will have control over their data by having the ability to permit trusted authorities to access and share their information. Medical history as a blockchain data also assures integrity of data and it is also non repudiated and distributed in decentralized manner. All members of the patient network are notified about any changes in the blockchain, and all data insertions are verifiably immutable. Also, any unauthorized alterations of data can be easily detected.

B. Adding New Block to Blockchain

When the user, in this case, the patient goes to a hospital to receive healthcare service, the hospital authority requests for accessing the patient's blockchain. The hospital has to be enlisted or registered in the system in order to be eligible to request access to the patient's data. The patient or any person, having authority to provide permission, can use a smart contract and Proof of Authority to grants access to the blockchain. The hospital authority uses the smart contract to assign or delegate access to a doctor who enters the medical records. The record is added to the blockchain as a new block.

In Fig. 2, this process of connecting to blockchain has been depicted.

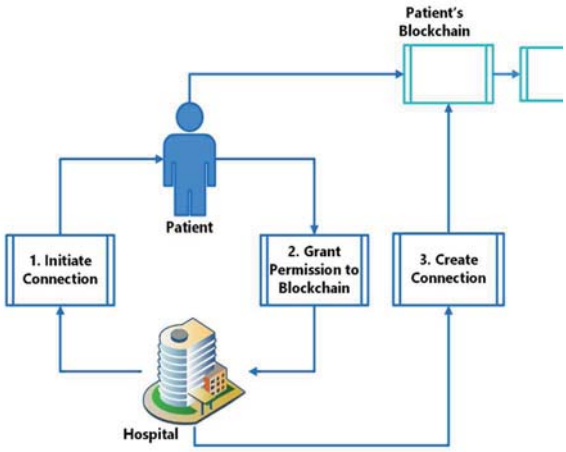

Fig. 2: Process of Connecting to Patient's Blockchain

Fig. 3 demonstrates the process of adding a new block or new stream of data to the blockchain. Each actor in this use case is a node trying to access the patient's data or seeking permission to the patient's blockchain. Once the patient grants permission to an authorized hospital authority to his /her blockchain, then that authorized person can now authorize the doctor to view the patient's data and add a new block of information to the blockchain.

Proof of Authority allows the patient to dictate whether to authorize anyone to access the blockchain, and set the permission level for using the data in the blockchain. For example, doctors would have access to only view and add new data; they will not have access to share the blockchain with any other nodes. Thus the access control level is maintained in order to keep the authorized hospital authority responsible for patients' data sharing and management where the patient dictates the authorization rules.

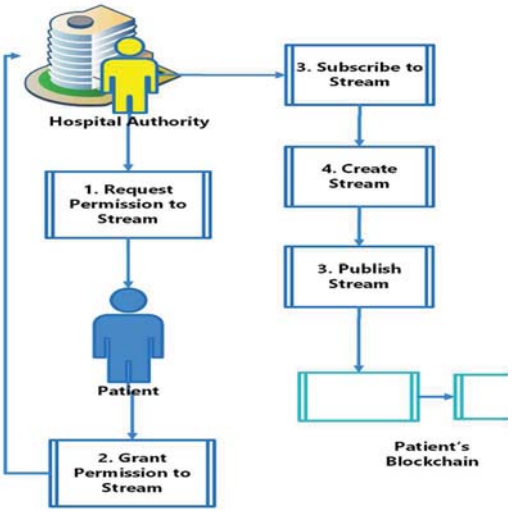

Fig. 3: Adding new block in the blockchain with patient's record

By default, nodes will get connect access, but the owner of the blockchain can grant send and create access as well. That allows the nodes to create data stream and share or publish the stream for other nodes to access. In this way, only authorized entities are allowed to execute various operations on the blockchain.

C. Sharing the Blockchain

Along with establishing mechanisms for interoperability and permission-based access control to the patients' blockchain, a method to share the information among healthcare institutions to increase patient care and easing patients hurdles to provide necessary information whenever they visit any hospital or clinic is also proposed. Sharing patient information helps healthcare institutions to reduce readmissions, avoid medication errors, and even lessen the amount of duplicate pathological testing[19]. The goal of this framework is to enable the sharing of interoperable patient data among healthcare institutions in a secure way by keeping the permission granting mechanism to patients.

The data sharing process is described in Fig. 4. Assuming hospital-2 would like to access the patient's record from hospital-1. In such a case, upon placing the request for access, hospital-1 has to forward the request to the patient or patient's nominated authority using a smart contract that will mention who is willing to access the blockchain for what purpose. If permission is granted, hospital-2 will receive a copy of the patient's blockchain as well. Once received, the later one will be able to access data according to the permission set by the first party during the grant process. The second party can only use data dictated by the rules set by the contract, which is reviewed by the patient or patient's authorized nominee.

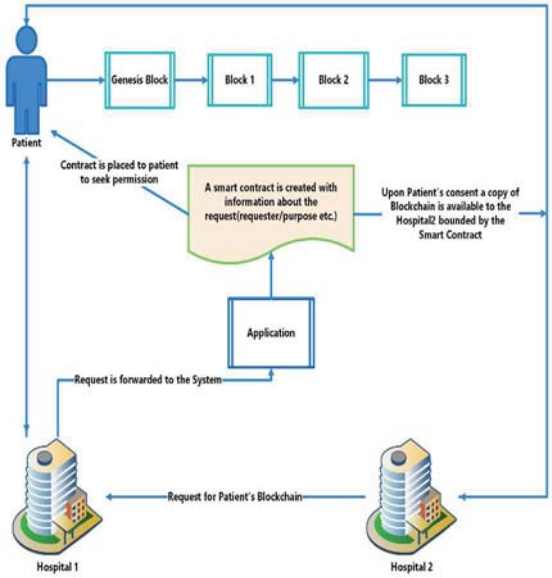

Fig. 4: Sharing Blockchain Using Smart Contracts

D. A Distributed System

Distributed ledgers use independent computers (or nodes) to record, share, and synchronize transactions electronically instead of keeping data centralized as in a traditional database. Blockchain organizes data blocks by chaining them together in an append-only mode [20].

Copies of the blockchain, are stored by many authorities in the decentralized network. Due to the encrypted information in the blockchain, patients' privacy is secured when it is transferred between stakeholders, and each of the stakeholders only access information to which they are specifically allowed by receiving permission granted by authorized entities. Each stakeholder can rely on the information he received to be accurate, because each has an immutable chain that is identical to the other chains, and that they can perform audit to test its integrity [21].

In the proposed system, the inbuilt characteristic of blockchain's distributed ledger has been utilized, which makes sure that whenever a new block is added to the blockchain, the system will broadcast the update. Upon receiving the update, each copy of the blockchain will have a newly added block making it a decentralized distributed database for patient healthcare records. Fig. 5 shows the distributed system at work. The smart contract allows owners to control the privacy of their data by deciding whether to allow someone to access the data, and for what purpose, and what period the data should be accessible. The

system broadcasts changes in any copy of the blockchain in any node for events such as adding a new block.

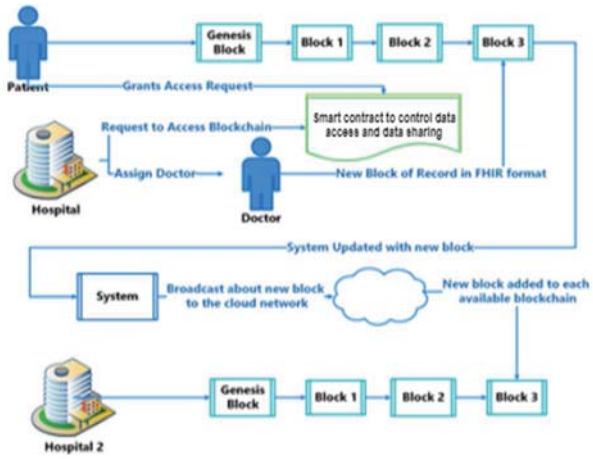

Fig. 5: A Proposed Distributed System

IV. IMPLEMTATION AND RESULT

This chapter discusses the implementation of the framework and the tools and technologies being used to achieve the designed framework.

A. *High Level Architecture*

The backend service layer implements the classes Blockchain and RPC and provides required services with necessary parameters, which are then referred to in the application layer. The application layer consists of modules that are responsible for interacting with the blockchain services. The client application only requires to access these modules in order to connect to the backend to make any transaction supported by the framework. Fig. 6 illustrates the high level architecture of the proposed framework.

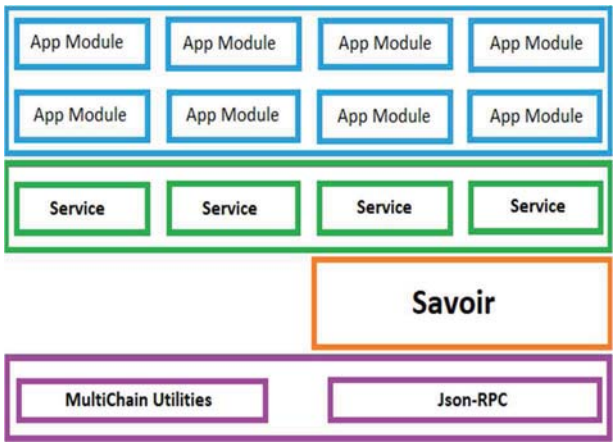

Fig. 6: A high-level architectural overview of blockchain based framework

B. *The Blockchain Layer*

The MultiChain technology is a platform that helps users to establish a certain private Blockchain that can be used by the organizations for secure transactions. MultiChain provides a command line tool to access its APIs, and build services based on the business logic of an application.

C. *The Service Layer*

The service layer uses the Blockchain and RPC objects to create an interface for the application that will consume the services from the Service object. Each method of the Blockchain and RPC objects are implemented with the necessary parameters to be exposed by the application. The framework abstracts MultiChain utilities, the framework implements Savoir, which is a JsonRPC wrapper for MultiChain written in Python.

D. *The Application Layer*

The application layer of the framework exposes the services that the framework provides for any client to consume. It is the interface through which a client application can use this framework.

E. *Simulation and Result*

After successfully developing the framework, simulations have been run to create, publish, and share streams between two nodes and simulated grant permissions on the nodes to utilize the permission-based workflow of MultiChain blockchain. The inner functionalities of MultiChain has been abstracted with framework's methods. Fig. 7 demonstrates the initialization of blockchain and Fig. 8, and Fig. 9 shows the permission request and grant mechanism to a different requester node.

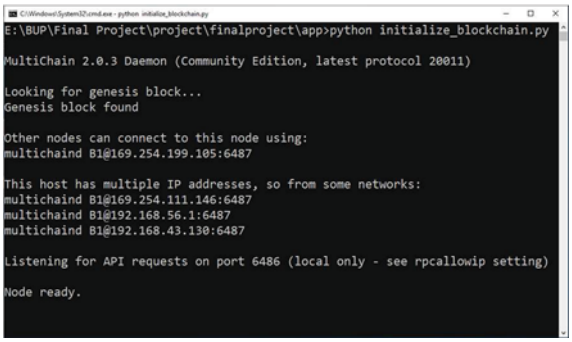

Fig. 7: Initializing blockchain using MultiChain RPC

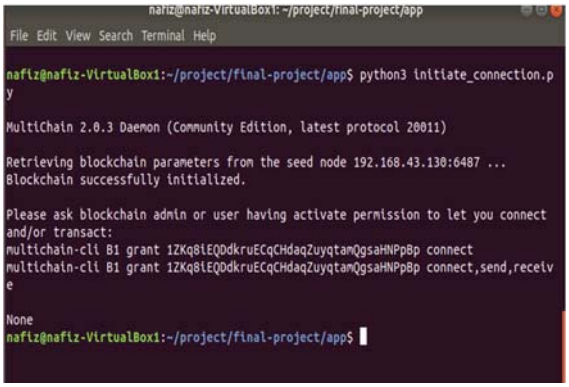

Fig. 8: A requester node trying to connect to seed node

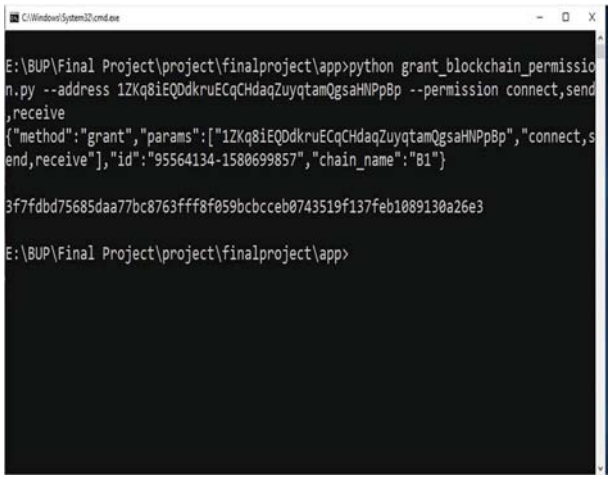

Fig. 9: Seed node granting permission to requester node

Now that the requester node has permission to access the patient's blockchain, it can now add new blocks to the blockchain and also delegate permission to other requesting nodes to share data. The smart contract would control this permission delegation process by ensuring the patient controls with whom the first party is sharing his data and for what purpose. This enables the owners to control the privacy of their data and the rights to know how their data is being used by an authorized entity.

V. CONCLUSION

The proposed framework in this paper implements a blockchain-based healthcare data sharing approach to share data effectively. It also emphasizes on maintaining interoperability and privacy and achieve a decentralized and secured Health Information Sharing system. The work has been based on several proposed frameworks as referenced, and a unique solution focusing on improvement for security and manageability has been identified by utilizing the MultiChain platform, and simulating the process of permission-based access and data sharing using blockchain infrastructure. It has been shown how Proof of Authority is a better choice of consensus algorithm than other traditional mining algorithms. Data blocks are hashed in blockchain, ensuring the utmost integrity, which is a crucial requirement for medical data security. Furthermore, along with Smart Contract and Proof of Authority data connectivity between the chain and end-users are authenticated, and made data is regulated only within verified nodes.

REFERENCES

[1] B. A. Tama, B. J. Kweka, Y. Park and K. Rhee, "A critical review of blockchain and its current applications," 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, 2017, pp. 109-113, doi: 10.1109/ICECOS.2017.8167115.

[2] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Pbft Vs Proof-Of-Authority: Applying The Cap Theorem To Permissioned Blockchain." Zenodo, 2017.

[3] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, ''Blockchain technology use cases in healthcare,'' Adv. Comput., vol. 111, pp. 1–41, Jan. 2018

[4] Peterson, Kevin, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Boles. "A blockchain-based approach to health information exchange networks." In Proc. NIST Workshop Blockchain Healthcare, vol. 1, no. 1, pp. 1-10, 2016.

[5] Dubovitskaya, Alevtina, Zhigang Xu, Samuel Ryu, Michael Schumacher, and Fusheng Wang. "Secure and trustable electronic medical records sharing using blockchain." In AMIA annual symposium proceedings, vol. 2017, p. 650, 2017.

[6] Barrows Jr, Randolph C., and Paul D. Clayton. "Privacy, confidentiality, and electronic medical records." Journal of the American Medical Informatics Association 3, no. 2, pp. 139-148, 1996.

[7] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, pp. 534-543, 2017.

[8] Li, Xiaoqi, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. "A survey on the security of blockchain systems." Future Generation Computer Systems 107, pp. 841-853, 2020.

[9] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.

[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," in IEEE Access, vol. 5, pp. 14757-14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[11] "MultiChain JSON-RPC API commands," Open source blockchain platform.[Online].Available:https://www.multichain.com/developers/json-rpc-api/. [Accessed: 10-Dec-2019].

[12] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In 2015 IEEE Security and Privacy Workshops, pp. 180-184. IEEE, 2015.

[13] Li, Hongyu, Liehuang Zhu, Meng Shen, Feng Gao, Xiaoling Tao, and Sheng Liu. "Blockchain-based data preservation system for medical data." Journal of medical systems 42, no. 8, p. 141, 2018.

[14] Zhang, Aiqing, and Xiaodong Lin. "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain." Journal of medical systems 42, no. 8, p. 140, 2018.

[15] Li, Hongyu, Liehuang Zhu, Meng Shen, Feng Gao, Xiaoling Tao, and Sheng Liu. "Blockchain-based data preservation system for medical data." Journal of medical systems 42, no. 8, p. 141, 2018.

[16] Zhang, Mian, and Yuhong Ji. "Blockchain for healthcare records: A data perspective." PeerJ Preprints 6, 2018.

[17] Baars, D. S. "Towards self-sovereign identity using blockchain technology." Master's thesis, University of Twente, 2016.

[18] C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, 2018.

[19] E. Snell, "Benefits, Challenges of Secure Healthcare Data Sharing," HealthITSecurity, 20-Oct-2017. [Online]. Available: https://healthitsecurity.com/features/benefits-challenges-of-secure-healthcare-data-sharing. [Accessed: 10-Dec-2019].

[20] "Blockchain & Distributed Ledger Technology (DLT)," World Bank.[Online].Available:https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt. [Accessed: 10-Dec-2019].

[21] M. A. Engelhardt, "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector," Technology Innovation Management Review, vol. 7, no. 10, pp. 22–34, 2017.