


Patient-Centric Multichain Healthcare Record

Bipin kumar Rai, ABES Institute of Technology, India*

 <https://orcid.org/0000-0002-9834-8093>

Sumrah Fatima, ABES Institute of Technology, India

Kumar Satyarth, ABES Institute of Technology, India

ABSTRACT

In this paper, the authors have amplified the concept that EHRs need to be patient-centric and patient-driven, that is the patient should be the real owner as well as the manager of his medical records. The authors propose patient-centric multichain healthcare record (PCMHR) that implements health records using smart contracts on ethereum blockchain and also utilizes the multichain framework - Polygon. PCMHR can concurrently implement blockchain functionality while addressing the concerns of interoperability among authorized hospitals and patient health information confidentiality that damages our healthcare system. The authors propose a solution to fully decentralize the current medical healthcare system by storing PCMHR on IPFS (InterPlanetary File System) to resolve the limitation of blockchain-based applications in scalability and high cost. The authors have depicted the cost and time analysis of transactions on the polygon framework to give a clear view of this multichain framework and its advantages over the ethereum blockchain.

KEYWORDS

Blockchain, HER, Ethereum, IPFS, Polygon

1. INTRODUCTION

We have shifted from a document-based storage system to Electronic Health Records(EHR) but the ownership of such crucial and private data remains in the hands of anonymous people and thus vulnerable to security breaches(Kumar Rai, n.d.; Rai et al., 2021). EHR is a digitized record of the medical history of the patient, including diagnosis, treatments, follow-up appointments, allergy records, laboratory, and test results. The family history can be included by the patient in his record. All such data requires high privacy from the outside world and must be shared with authentic entities only. Blockchain technology has proven to be a boon for sharing such confidential information because of its features like an immutable, secure, and reliant ledger. It is a decentralized platform that provides network security at every level, stores data in immutable form, and is highly efficient allowing authorized access to health records. Such features help in reducing human and system errors and increased the accuracy and easy accessibility of records(Kheizr et al. 2019). There are different kinds of blockchain technology that are being used for enterprise purposes. Ethereum and Hyperledger are two of the most widely used blockchains(Kheizr et al. 2019). Ethereum has its popularity as it provides

DOI: 10.4018/IJEHMC.309439

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

a permissioned network as well as high performance for its transactions. The purpose of Ethereum is to integrate and improve on the ideas of scripting, cryptocurrencies, and on-chain meta-protocols, allowing developers to create arbitrary consensus-based applications with scalability, standardization, feature-completeness, development simplicity, and interoperability(Buterin n.d.). Thus Ethereum gives its users the benefits of possessing their data records and also sharing them in a secure way. PCMHR makes patients the owner of their health records as they become better informed and more involved in their care. At each step of treatment, the patient controls who has access to their information securely and efficiently. It has enabled us to build care around the patient and bring transparency to the patient-doctor relationship.. Thus Ethereum gives its users the benefits of possessing their data records and also sharing them in a secure way. PCMHR makes patients the owner of their health records as they become better informed and more involved in their care. At each step of treatment, the patient controls who has access to their information securely and efficiently. It has enabled us to build care around the patient and bring transparency to the patient-doctor relationship.

There are several cases where the need for PCMHRs is highly recommended, such as A patient with HIV who wants to keep a detailed record of the treatment process, as well as post-treatment, recovery, and monitoring. A thorough examination of his medical history may be critical to his recovery (Narendra Kumar Rao and Bhaskar Kumar Rao 2019). Patients should also be able to build a point-to-point channel to communicate information about their history and present drugs while transferring from one hospital to another (Madine et al. 2020). He will very certainly be needed to sign a consent form that specifies the types of data that may be provided, the facts about the beneficiary, and the length of time that the information can be accessible by the beneficiary. This may be difficult to do, particularly if a patient is relocating to a different city, region, or state and does not know the hospital where he will be treated shortly (Narendra Kumar Rao and Bhaskar Kumar Rao 2019). PCMHRs have their use cases at all such places where communication between two hospitals is required and both the hospitals use a different kind of EHR software. Since PCMHR is a multichain system it can share data of a patient regardless of any public blockchain platform it is being shared on. However, it is hard to store whole EHR data in blockchain because of the size and the price of the blockchain (Narendra Kumar Rao and Bhaskar Kumar Rao 2019). Thus, it is seen as a challenge while using blockchain technology to provide enough storage capacities for higher scalability. Therefore, in PCMHR we have adopted IPFS for storing the records in a decentralized file system to enhance the scalability and resolve the storage problem associated with blockchain storage.

1.1 Research Objectives

Following are the objectives of our proposed solution:

- a) To provide patients with the ownership of their health data, the rights to decide whom to give access to and what data to share, that is the EHRs should be patient-centric and patient-driven.
- b) Using blockchain technology to increase confidentiality in PCMHR and ensuring data availability while retaining the integrity and confidence between doctor and patient.
- c) To implement PCMHR in such a way that it can be interoperable among authorized hospitals.
- d) Provide a less expensive and enhanced speed, decentralized second layer solution to patients and hospitals using the Polygon framework.

1.2 Structure of the Paper

In section 2, we present the previous and related work done in the field of electronic health records leveraging blockchain technology. We have also listed the previous analysis of various blockchain technologies that help us to choose the best framework for our proposed solution. Section 3 explains some of the key technologies used in our proposed work. Section 4 highlights the details of our proposed Patient-Centric Multichain Health Record solution along with its system architecture,

design, and sequence of actions. We have also explained the algorithm of the smart contracts and their implementation with diagrammatic representation. Section 5 compares and contrasts other projects with our proposed solution. And also specifies the technology used for the project's implementation. Section 6 contains the conclusion and lists the appendix for the short forms we have used while writing the paper and mentions the papers that we have used as a reference for our proposed work.

2. RELATED WORK

Extensive research is being done to implement blockchain in our healthcare system. Satoshi Nakamoto has first introduced decentralized transactions and storage using bitcoin on blockchain and excluding financial institutions for better privacy and user control. There have been various incidents of security attacks on hospitals. The authors S Kumar et al.(Kumar, Bharti, and Amin 2021) have highlighted some of such attacks. For eg, an Email phishing attack on a diagnostics vendor of clinical genomics, named "Ambry Genetics", compromised the data of 232772 patients. Ancile(Dagher et al. 2018) focussed on the issue of inaccessibility of data to the patients and the security breaches that private data of patients suffer.

Such attacks and security breaches have intensified the need for more secure health records at hospitals.

We make use of Ethereum based smart contracts which were first proposed by Vitalik Buterin(Buterin n.d.) that get implemented automatically once the defined conditions are met.

Mohammad Moussa Madine et al.(Madine et al. 2020) have focussed on the personal health records(PHR) of patients. The authors have proposed ethereum based smart contracts to establish secure and immutable health records. The proposed system uses InterPlanetary File Systems (IPFS) as database storage and "reputation-based oracles". Despite the use of smart contracts for decentralization, they rely on third-party oracles to get data from IPFS storage. But the records are limited to the authority which is registered on their smart contract and data cannot be shared among various hospitals. Also, their PHRs are not upgradable. Our solution takes reference from other concepts mentioned in (Madine et al. 2020) specifically for storage and access control mechanisms.

P. E. Velmovitsky et al.(Velmovitsky et al. 2021) have mentioned blockchain solutions that aim to solve challenges in health care from an industrial viewpoint, delivers solutions that attempt to tackle difficulties in health care, including the usage of blockchain in the drug supply chain, health insurance, linking users and buyers directly, and policies for consent management. Although, the solutions provided are yet to be checked for easy and efficient implementation.

We studied the paper by Agbo et al.(Agbo and Mahmoud 2019), which compared and assessed several blockchains such as ethereum, bitcoin, and Hyperledger fabric for a medical healthcare system. This study examined the most prominent blockchain platforms in a methodical way, taking into account technological aspects essential to healthcare applications and giving a reference for the selection of suitable blockchain platforms for specific requirements in healthcare and biomedicine.

T. T. Kuo et al. (Kuo, Zavaleta Rojas, and Ohno-Machado 2019) utilized a systematic review technique to analyze major blockchain platforms and give a reference for selecting a suitable blockchain platform based on criteria and technology aspects prevalent in healthcare and biomedical research applications.

D. Spatar et al. (Spatar et al. 2019) list the factors that reflect upon the adoption of EHR systems, quality of care, and help in selecting an EHR that is in accordance with the needs of the users.

3. PRELIMINARIES

3.1 Blockchain

In 2008, the concept of blockchain was proposed by Satoshi Nakamoto and introduced the cryptocurrency called Bitcoin which implements the concept of P2P value exchange without the interference of centralized third parties. The term blockchain has enhanced its significance in the medical world due to its secure and immutable features. It acts as a storehouse of all records of patients'

medical data and these records are stored on-chain as separate transactions. Thus it is a distributed, decentralized ledger as data is not stored on a central server rather on a peer-to-peer network of nodes.

It does not require any third-party organization authentication services and thus helps in making health records patient-centered and patient-driven. Also, it has boosted the environment for various fields. (Daraghmi, Daraghmi, and Yuan 2019)

A blockchain (as its name indicates) is built up using basic blocks and connecting them together in a chain through various cryptographic techniques. Each block is unique in itself and contains a timestamp that makes it trackable and verifiable as well.

Each block consists of Block Header and Block Body, each block header comprises the pointers that link it to the block headers of the previous block, the Merkle root is a hash of all the hashes of all the transactions on the blockchain network and a timestamp. The data we need to store in a block is contained in the block body. Every block is linked to its previous block and thus if an attacker tries to mutate a certain block, he needs to change every block in a blockchain which is nearly impossible to do.

3.2 InterPlanetary File System(IPFS)

IPFS provides efficient decentralized storage of data as it was previously aimed by the idea of the internet in our lives i.e users should be the sender and receiver of the data, not any centralized single authority. Blockchain provides a very secure decentralized storage of data but it has certain limitations when it comes to the cost of large data storage on a chain. Hence we use IPFS with blockchain to deal with its expensive storage and minimize the cost of maintaining the health care system.

IPFS is a peer-to-peer hypermedia protocol that is used in a distributed file system to store and share data. IPFS uses content-addressing to distinguish each file in a global namespace that connects all computing devices.

Whenever we add the file to IPFS, our file is split into sub-files that are cryptographically hashed, and each sub-file is assigned a CID (content identifier) which is a unique fingerprint. This CID acts as a permanent record of the file.

When other nodes on the network search for our file, they enquire about the nodes where the data is stored and these are referenced by the file's CID. A cache of copy is created when we view or download our file and that node then becomes the provider of our file content. IPFS files are resistant to manipulation and censorship, which means that any changes to a file do not overwrite the original, and common sections between files can be reused to reduce storage costs. As a result, whenever a new version of a file is added to IPFS, it creates a different hash and hence a new CID.

3.3 Polygon

Polygon provides us with the second layer solution for ethereum blockchains. It is a multi-chain system that provides the best features of ethereum and shows compatible features with other blockchains as well. This opens up the prospects of interoperability among authorized identities and in our case it is hospitals.

As we experience the high gas fees in ethereum-based transactions and comparably the reduced speed due to the growing rate of transactions, Polygon is a solution without compromising on the security of our data.

Features of Polygon:

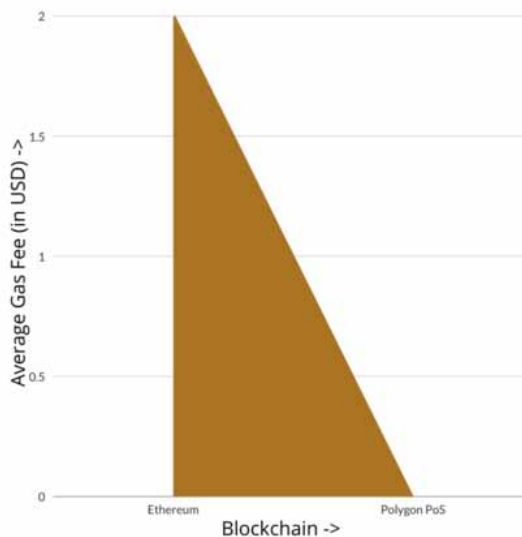
- Polygon is compatible and scalable with Ethereum as well as other blockchain networks. It provides a trustable technology stack, various tools, supports different languages and standards all over the world. Apart from dedicated blockchains, scalable consensus methods, execution environments like Wasm are also available.
- It has a dedicated module for “security as a service”
- Polygon offers interoperability by connecting to external systems and providing native support for delivering arbitrary messages (tokens, contract calls, etc).
- Provides good user Experience through “zero-gas” transactions, and robust transaction completion.

- Its modules are highly customizable, extensible, and upgradeable.

The graph shown in Figure 1 compares the average gas fee on Ethereum blockchain with Polygon PoS. Since ethereum transactions are now more than 20x costlier than most other popular blockchains therefore it is better to use layer 2 solutions like Polygon for executing transactions.

Polygon has low gas fees and reduced transaction time thus increasing the efficiency of the system it is implemented in.

Figure 1. Comparison of Average gas fee on Ethereum blockchain with Polygon PoS



3.4 Smart Contract

Smart contracts are programs that are deployed on the ethereum blockchain. It consists of code (functions) and data (its state). Rules are defined in the smart contract as per the purpose it is being used for just like a contract in real life between the parties using the services and is automatically gets enforced in the network. Smart contracts are immutable in nature which prevents attackers from corrupting the data stored on the blockchain.

Ethereum virtual machines are used to execute smart contracts (EVMs). Ethereum uses the Proof Of Work (PoW) function(Madine et al. 2020) as a consensus mechanism to ensure distributed EVMs follow their agreements on execution. Smart contracts are not controlled by any user, rather they are deployed on the blockchain networks and are executed as programs. Smart contracts are composable in nature and can be related to open APIs. Smart contracts communicate with one another by transmitting data in a safe cryptographic manner. We have proposed two smart contracts in this paper to manage the health records in our blockchain network.

3.5 Ethereum

Ethereum is a blockchain that is both decentralized and open source. Its operation is based on smart contracts. Ether is the platform's native cryptocurrency. Gas costs must be paid whenever an ethereum transaction happens. Gas is the unit of measurement for the cost of running a function in a smart

contract. Wei is the lowest denomination of ether. The typical price of gas is around 100 Gwei, where $1 \text{ wei} = 10^{-18} \text{ Ether}$ and $1 \text{ Gwei} = 10^9 \text{ wei}$.

Challenges/Limitations of Ethereum Blockchain

Ethereum has low throughput and a poor user experience due to fluctuating gas prices and delayed PoW5 finality. Many projects are turning to Ethereum-compatible blockchains to get past the constraints mentioned above while still utilizing Ethereum's rich ecosystem. However, there is no specific infrastructure for creating such blockchains, and there is no protocol for connecting them. As a result, major development challenges, as well as fragmented ecosystems, have arisen.

4. PROPOSED SOLUTION OF PCMHR

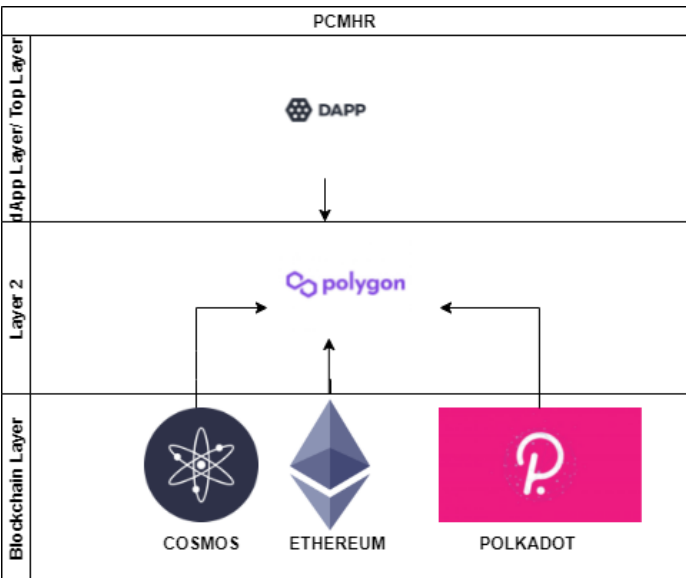
Considering the current scenario of EHRs, we propose a decentralized solution PCMHR. It is a multichain system that provides users with a facility to deploy its smart contract on polygon which is a Layer 2 solution for the ethereum blockchain. Polygon is an Ethereum-compatible blockchain network creation and connecting technology and architecture. Such smart contracts which are deployed on polygon are interoperable among authorized hospitals which might be using other blockchain platforms like Polkadot, cosmos, ethereum, etc. Diagram in figure 2 gives an overview of the layers of PCMHR.

Layer 1 at the bottom level includes the blockchain networks of Ethereum, Cosmos, Polkadot.

Layer 2 is the polygon network layer that is built over the ethereum layer. It is responsible for processing the transactions in batches. The cost of executing transactions is much lower than the transaction cost on ethereum. The user interacts with Layer 3 which is the Dapp layer or the top layer.

The third layer is made interactive using various technologies like NodeJS, HTML, CSS so that it becomes easy for the user to access and upload his records.

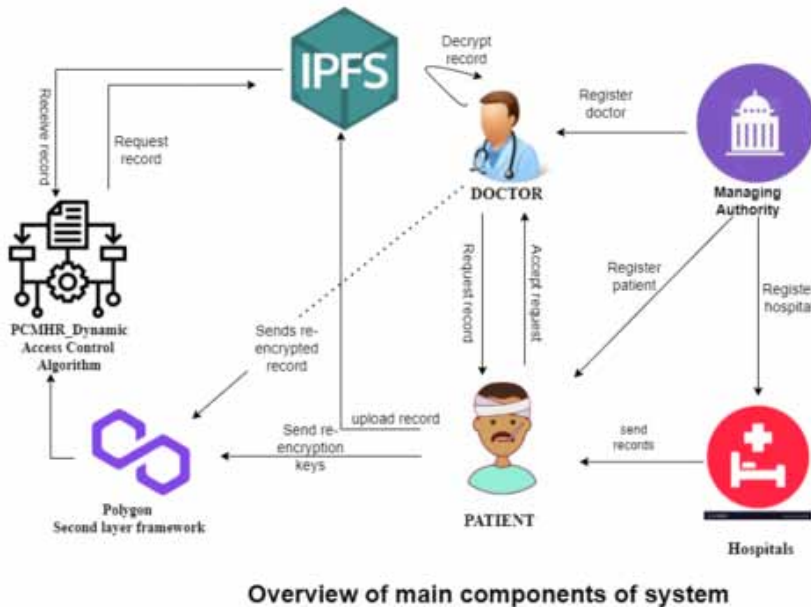
Figure 2. Structure showing the layers of PCMHR



4.1 System Architecture

Every entity of PCMHR must first be registered on the blockchain network. The system's primary components which are shown in figure 3 are:

Figure 3. The architecture of PCMHR



Managing Authority

The government or a trustworthy public body is in charge of registering hospitals, patients, and doctors, as well as regulating the overall procedure.

Hospital

Hospitals are registered by managing authority on the factory smart contract. They send requests to the patient whenever they are in need of their health records.

Patient

PCMHR software will be deployed by the managing authority, which can be a government or a trusted public authority. Now, this software will be used to register hospitals, patients and doctors.

Patients can register themselves on PCMHR and can upload their medical record files. Patients also decide whether to accept or reject the request from their doctors and hospitals to share medical records.

Doctor

The doctor requests the medical record files (in encrypted form) from the patient and then decrypts them.

IPFS

A P2P hypermedia protocol, is used for storing files and data in a distributed file system.

There are two smart contracts that manage the entities such as patient and doctor:

PCMHR_Factory Smart Contract (PCMHR_FSC)

It is deployed only once and is responsible for adding, updating, and deletion of doctor and patient information. And it also deploys other smart contracts.

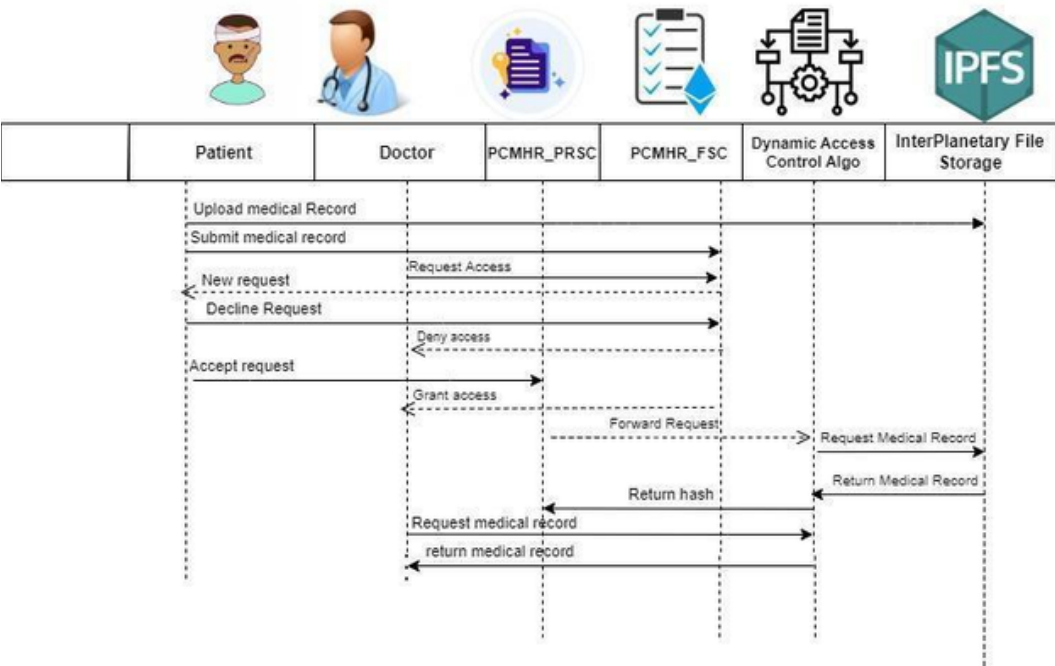
PCMHR_Patient Record Smart Contract (PCMHR_PRSC)

PCMHR_PRSC is deployed per patient and is responsible for uploading the patients' medical records. PRSC allows the patients to respond to access requests of authorized entities and accept/deny the requests of doctors to share the records with them or any hospital. Its functioning includes storing records on IPFS and its corresponding hash to the address in itself.

The sequence of actions is as follows:

- 1) To encrypt the records in PCMHR, the patient creates a symmetric key and compares it to the record file. The patient's public key is used to encrypt the generated symmetric key. The encrypted PCMHR record and encrypted symmetric key files are both uploaded to IPFS, and the hash of the encrypted medical record file is stored on the blockchain.
- 2) The doctor first determines the record of the patient he needs to access and then requests the patient to grant access to the record. Consequently, PRSC notifies the patient to either approve or reject the request by deciding whether he wants the doctor to access the record or not.
- 3) If the patient approves the access request of the doctor, he/she signs the transaction on the blockchain and simultaneously doctor will be notified for the approval.
- 4) Now, the PCMHR's dynamic access control algorithm will fetch the hash that is associated with the needed record from the blockchain. Then, this received hash will be used to retrieve the record stored on IPFS.
- 5) Thus doctor receives the health in record readable form.

Figure 4. Sequence diagram of PCMHR



4.2 IMPLEMENTATION

Figure 5 shows the use cases of the project. Firstly the patient registers on PCMHR and then the doctor registers on the platform. The patient uploads his/her records on the platform and when the doctor requests to access the records, the patient approves or rejects the access request.

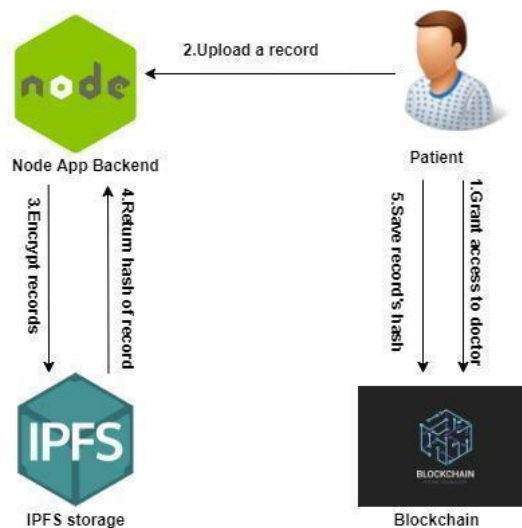
Figure 5. Use case diagram of PCMHR



High Level Use Case Diagram

Figure 6 demonstrates the process of uploading PCMHR on the dApp as soon as the registration of authenticated entities gets completed.

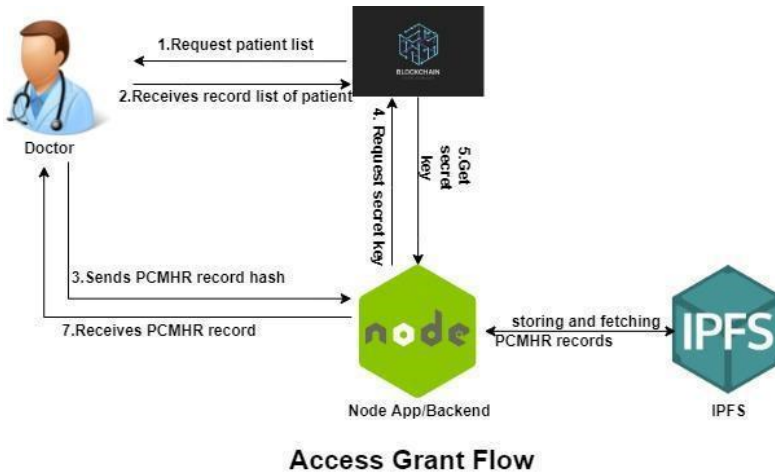
Figure 6. Diagram showing how the user uploads the records on PCMHR



1. The patient grants access to the doctor to view his PCMHR records via blockchain.
2. And the patient has uploaded its record on PCMHR dApp which has Node backend.
3. The encrypted record is stored on IPFS.
4. The hash of the encrypted record is returned to the backend of the dApp.
5. The patients' record hash is then sent to the blockchain.

In Figure 7, we have displayed how a doctor will gain access to a patient's PCMHR records. Firstly, the doctor requests the records of the patients from the PCMHR platform. On receiving the records after access is granted by the patient to the doctor, the doctor sends the PCMHR record hash to the Node app/backend. The backend will fetch the record from IPFS when the doctor wants to retrieve the record and also store the record when the patient uploads it. Finally, the doctor receives decrypted PCMHR record of the patient.

Figure 7. Access granting of records on PCMHR



PCMHR_Factory Smart Contract(PCMHR_FSC)

```

function addDoctorInfo(address doctorID, string memory
doctorInfoHash) onlyAdmin() public
Doctor storage doctorInfo = Doctors[doctorID];
doctorInfo.doctorHash = doctorInfoHash;
Doctor_ids.push(doctorID) - 1;
doctor.add(doctorID);
end

```

```

function updateInfo(address doctorId, string memory
doctorInfoHash) onlyAdmin() public
Doctor storage doctorInfo = Doctors[msg.sender];
doctorInfo.doctorHash = doctorInfoHash;
Doctor_ids.push(doctorId) - 1;
end

```

```

function addDoctor(address newDoctor) external onlyAdmin()
doctor.add(newDoctor);
end

```

```

function delDoctor(address doctorId) external onlyAdmin()
doctor.remove(doctorId);
end

```

```
function addPatientInfo(address patientID, string memory
patientInfoHash) onlyAdmin() public
Patient storage patientInfo = Patients[msg.sender];
patientInfo.patHash = patientInfoHash;
Patient_ids.push(msg.sender) - 1;
patient.add(patientID);
end

function addPatient(address newPatient) external onlyAdmin()
patient.add(newPatient);
end
```

PCMHR_Patient Smart Contract (PCMHR_PRSC)

```
function addMedicalRecord(string memory recordHash, address
patientID) onlyPatient() public
MedicalRecord storage record = Records[patientID];
record.RecordHash = recordHash;
RecordHashes.push(recordHash) - 1;
end

function viewMedicalRecord() public view
return (Records[get_patient_id].RecordHash);
end
```

5. DISCUSSION COMPARISON

Through PCMHR, our objective is to provide secure, interoperable, reliable, and efficient access to the medical records of a patient while maintaining the patient's privacy which is very crucial (Rai & Srivastava, 2014) (Rai, 2022).

PCMHR provides wider scalability and interoperability due to the utilization of multichain framework-Polygon for its implementation while other solutions mentioned in the table follow the single blockchain-platform approach. We have listed a project named Ancile by Dagher et al (Dagher et al. 2018) that utilizes smart contracts in an Ethereum-based blockchain. The doctor-centric approach is proposed i.e doctor and patient decide whom to give access control of records but in PCMHR the patient is the master of all access controls. Ancile has the additional functionality of keyword index searching for encrypted health records but the prospects of scalability across different platforms are not well discussed though it is possible in PCMHR through Polygon multi-chain functionalities.

MedRec has proposed the incentive mechanism and focused on mining incentives as well. Medical researchers and healthcare authorities are encouraged to participate in the mining process in order to obtain access to network participants. However, PCMHR focuses on how to make transactions cost low on ethereum blockchain-based EHRs and share a load of transactions with the help of layer 2 solutions while maintaining the privacy and security of patients' health records.

MeDShare highlights the privacy concern while dealing with medical records shared over public platforms like various cloud service providers. Data stored still has a centralized approach due to the usage of cloud services while in PCMHR, the medical records of the patients are stored in a distributed file storage system such as IPFS.

6. CONCLUSION

In this paper, we have proposed a multichain solution PCMHR for blockchain-based electronic medical records. We have emphasized giving patients access controls and will decide whom to share records with as the need arises in order to protect the data from security attacks and misuse. Privacy is established by using blockchain for the implementation of the system. PCMHR focuses on patients owning and controlling their data without compromising security or limiting different hospitals' ability to provide services. Hence, we have made the complete system decentralized by using IPFS for off-blockchain storage solutions. The system is made interoperable and can interact with different ethereum compatible blockchain platforms of different hospitals using the multi-chain framework Polygon. It acts as the bridge to other external systems. The scalability of the system is ensured by using scalable consensus algorithms and a customizable Wasm execution environment of Polygon. It will make the transfer of patients and sharing of their previous medical history from one hospital to other easier, more secure, and more efficient.

CONFLICT OF INTEREST

The authors of this publication declare there is no conflict of interest.

FUNDING AGENCY

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

- Agbo, C. C., & Mahmoud, Q. H. (2019). Comparison of Blockchain Frameworks for Healthcare Applications. *Internet Technology Letters*, 2(5), e122. doi:10.1002/itl2.122
- Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. 2016. MedRec: Using Blockchain for Medical Data Access and Permission Management. *Proceedings - 2016 2nd International Conference on Open and Big Data*. doi:10.1109/OBD.2016.11
- Buterin, Vitalik. (n.d.). *A Next-Generation Smart Contract & Decentralized Application Platform*.
- Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. *Sustainable Cities and Society*, 39, 283–297. doi:10.1016/j.scs.2018.02.014
- Daraghmi, E. Y., Daraghmi, Y. A., & Yuan, S. M. (2019). MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. *IEEE Access: Practical Innovations, Open Solutions*, 7, 164595–164613. doi:10.1109/ACCESS.2019.2952942
- Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Applied Sciences (Switzerland)*, 9(9), 1736. doi:10.3390/app9091736
- Kumar, S., Bharti, A. K., & Amin, R. (2021). Decentralized Secure Storage of Medical Records Using Blockchain and IPFS : A Comparative Analysis with Future Directions. *Security and Privacy*, 4(5), 1–16. doi:10.1002/spy2.162
- Kumar Rai, B., & Rai, B. K. (n.d.). Ephemeral pseudonym based de-identification system to reduce impact of inference attacks in healthcare information system. *Health Serv Outcomes Res Method*. 10.1007/s10742-021-00268-2
- Kumar Rao, B. N., & Kumar Rao, B. B. (2019). BlockChain Based Implementation of Electronic Medical Health Record.Service, Cloud, and Providers Via. 2017. *MeDShare : Trust-Less Medical Data Sharing Among Cloud Service Providers Via Blockchain*, 3536(c), 1–10. doi:10.1109/ACCESS.2017.2730843
- Kuo, T. T., Rojas, H. Z., & Ohno-Machado, L. (2019). Comparison of Blockchain Platforms: A Systematic Review and Healthcare Examples. *Journal of the American Medical Informatics Association: JAMIA*, 26(5), 462–478. doi:10.1093/jamia/ocy185 PMID:30907419
- Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., & Ellahham, S. (2020). Blockchain for Giving Patients Control over Their Medical Records. *IEEE Access: Practical Innovations, Open Solutions*, 8, 193102–193115. doi:10.1109/ACCESS.2020.3032553
- Rai, B. K. (2022). Patient-Controlled Mechanism Using Pseudonymization Technique for Ensuring the Security and Privacy of Electronic Health Records. *International Journal of Reliable and Quality E-Healthcare*, 11(1), 1–15. doi:10.4018/IJRQEH.297076
- Rai, B. K., & Srivastava, A. K. (2016). Pseudonymization Techniques for Providing Privacy and Security in EHR. *International Journal of Emerging Trends & Technology in Computer Science*, 5(4).
- Rai, B. K., Verma, R., & Tiwari, S. (2021). Using Open Source Intelligence as a Tool for Reliable Web Searching. *SN Computer Science*, 2(5).
- Spatar, D., Kok, O., Basoglu, N., & Daim, T. (2019). Adoption Factors of Electronic Health Record Systems. *Technology in Society*, 58(February), 101144. doi:10.1016/j.techsoc.2019.101144
- Velmovitsky, P. E., Bublitz, F. M., Fadrique, L. X., & Morita, P. P. (2021). Blockchain Applications in Health Care and Public Health: Increased Transparency. *JMIR Medical Informatics*, 9(6), e20713. doi:10.2196/20713 PMID:34100768

APPENDIX

The following abbreviations are used in the paper:

EHR: Electronic Health Record

IPFS: InterPlanetary File System

P2P: Peer to Peer

CID: Content Identifier

PoS: Proof of Stake

PoW: Proof of Work

PRSC: Patient Record Smart Contract

FSC: Factory Smart Contract

HTML: Hypertext Markup Language

CSS: Cascading Style Sheets

Wasm: WebAssembly

dApp: Decentralized Application

API: Application Programming Interface

EVM: Ethereum Virtual Machines