KLE Society's
KLE Technological University

Blockchain and Distributed Ledgers Course Project Report

On

Patient-Centric Image Management System(Access control using Ethereum)

Submitted By

Shankarling Halemani	01FE20BCS170
Tafreen Hussain	01FE20BCS172
Shravan Nayak	01FE20BCS174
Fayaz	01FE20BCS177
Sana Razeen	01FE20BCS184

Under the guidance of

Proff. Manjula Pawar

School of Computer Science and Engineering
,
Vidyangar, Hubballi – 580031, India.

Academic year 2022-23

ABSTRACT

In recent years, many researchers have focused on developing a feasible solution for storing and exchanging medical images in the field of health care. Current practices are deployed on cloud based centralized data centers, which increase maintenance costs, require massive storage space, and raise privacy concerns about sharing information over a network. Therefore, it is important to design a framework to enable sharing and storing of big medical data efficiently within a trustless environment. In this project, we propose a novel proof-of-concept design for a distributed patient-centric image management (PCIM) system that is aimed to ensure safety and control of patient private data without using a centralized infrastructure. In this system, we employed an emerging Ethereum blockchain and a distributed file system technology called Interplanetary File System (IPFS). Then, we implemented an Ethereum smart contract called the patient-centric access control protocol to enable a distributed and trustworthy access control policy. IPFS provides the means for decentralized storage of medical images with global accessibility. We describe how the PCIM system architecture facilitates the distributed and secured patient-centric data access across multiple entities such as hospitals, patients, and image requestors. Finally, we deployed a smart contract prototype on an Ethereum testnet blockchain and evaluated the proposed framework within the Windows environment. The evaluation results demonstrated that the proposed scheme is efficient and feasible.

CONTENTS

1. Introduction

Blockchain is a decentralized, distributed ledger technology that enables the secure and transparent recording of transactions across multiple parties. It consists of a chain of blocks, where each block contains a list of transactions. The technology ensures that the data recorded on the blockchain is immutable, meaning it cannot be altered or tampered with easily. This property makes blockchain suitable for applications requiring trust, security, and transparency. In the healthcare domain, medical images play a crucial role in diagnosis, treatment planning, and monitoring of patients. Traditional image management systems often suffer from issues such as fragmented data, lack of interoperability, and limited patient control over their own medical records. To address these challenges, the concept of patient-centric image management has emerged, focusing on empowering patients by giving them more control over their medical images, facilitating seamless sharing among healthcare providers, and ensuring privacy and data security.

The motivation behind our problem statement lies in the need for an efficient, secure, and patient-centric approach to managing medical images. Currently, medical images are often stored in centralized systems, making it challenging for patients to access and share their own data across different healthcare providers. Additionally, the centralized nature of these systems raises concerns about data security, privacy, and the potential for unauthorized access or tampering. By leveraging blockchain technology, it is possible to develop a distributed image management system that addresses these challenges. Blockchain can provide secure and transparent storage of medical images, enable patients to have control over their data, facilitate interoperability between different healthcare providers, and enhance data privacy and security by utilizing cryptographic techniques.

The contribution of work is as follows :

1. We provide a brief overview on the structure of the proposed PCIM system.
2. We propose a patient-centric access control protocol using a smart contract (PCAC-SC). Specific functions are considered to transmit information in and out of the Ethereum blockchain and give access privileges between entities.
3. We implement a framework to test feasibility of the concept. We have developed a PCAC-SC prototype on an Ethereum test network.
4. We verify the functionality using different test cases.

The rest of the report is organized as follows: In Section 2, we discuss the related work on our problem statement. The proposed framework, system model, algorithms are discussed in Section 3. We discuss results in section 4 and conclusion in section 5.

2. Literature review

[1] *Mohamed Yaseen Jabarulla and Heung-No Lee* proposed a blockchain based patient image management system (PCIM).The main components of PCIM are Ethereum blockchain, IPFS storage, Securing medical images. Patient centric access control protocol using smart contract is used to transmit information in and out of the ethereum blockchain. The objective here is to decrease the maintenance cost with less storage space and to raise privacy concerns while sharing information over a network.

[2] *Syed Agha Hassnain Mohsan, Abdul Razzaq, Shahbaz Ahmed Khan Ghayyur, Hend Khalid Alkahtani, Nouf Al-Kahtani and Samih M. Mostafa* proposed a Patient centric test report and image management (PCRIM). Objective of this paper is to provide a framework that allows for the efficient exchange and storage of large amounts of medical data in a secure setting. A distributed architecture - Patient centric test report and image management (PCRIM) is implemented to facilitate patient privacy and control. Ethereum and distributed file system technology called the interplanetary file system (IPFS) is used. IPFS allows decentralized storage of medical metadata such as images with worldwide accessibility.

[3] *Wen-Xin Yuan, Bin Yan, Wen Li, Liu-Yao Hao & Hong-Mei Yang* proposed The patient's medical health record system(PHMR). The patient's medical health record (PMHR) has always provided a large amount of research data to medical institutions and pharmaceutical companies, etc., and has contributed to the development in medical research. However, such PMHR data contains the patient's personal privacy and should be shared under the control of the patients, not the hospital where this data is acquired. In order to protect the privacy of PMHR data while realizing efficient data sharing, this work proposes a blockchain-based sharing and protection scheme. In this solution, the PMHR data is encrypted and stored in a cloud server, which is equipped with an access control scheme implemented as a smart contract on a blockchain. Different from previous works, in order to ensure efficient access and reduce the workload of patients, the types of users who can apply for access are limited to hospitals and pharmaceutical companies. In order to resist the potential Man-in-the-middle (MITM) attack, we have introduced an improved proxy re-encryption scheme to ensure the secrecy of PMHR data while reducing the computational complexity. The whole system is implemented using Solidity and tested on 10 nodes for function verification. Experimental results show that the proposed system is more efficient than previous systems. Security under the MITM attack is also ensured by security analysis.

[4] *Thein Than Thwin and Sangsuree Vasupongayya* proposed a Personal health record system (PHR system). Personal health record system (PHR system) stores health-related information of an individual. PHR system allows the data owner to manage and share his/her data with selected individuals. The originality or tamper resistance feature is crucial for the PHR system because of the irreversible consequence of incorrect information. Blockchain technology becomes a potential solution due to its immutability and irreversibility properties. Unfortunately, some technical impediments such as limited storage, privacy concern, consent irrevocability, inefficient performance, and energy consumption exist. This work aims to handle these blockchain drawbacks and propose a blockchain-based PHR model. The proposed model is built using the blockchain technology to support a tamper resistance feature. Proxy re-encryption and other cryptographic techniques are employed to preserve privacy. Features of the proposed model include fine-grained and flexible access control, revocability of consent, auditability, and tamper resistance. A detailed security analysis shows that the proposed model is provably secure for privacy and tamper resistance. The performance analysis shows that the proposed model achieves a better overall performance compared with the existing approach in the literature. Thus the proposed model is more suitable for the PHR system usage.

[5] *Yinghui Zhang, Xuanni Wei, Jin Cao, Jianting Ning, Zuobin Ying, Dong Zheng* proposed this work. With the rapid development of edge computing technologies, smart healthcare significantly improves people’s lives by collecting and analyzing health data in real time. However, security and privacy issues impede the wide deployment of smart healthcare systems (SHS). Most existing solutions still have drawbacks with respect to computation efficiency and users’ privacy. In this paper, a blockchain-enabled attribute-based access control scheme with hidden policies is proposed for SHS. The scheme introduces multiple authorities to avoid single point failure. Especially, the mode of online-offline encryption relieves users’ online computation burden by transferring computation tasks to the idle time of users, and policy hiding protects users’ sensitive information. Furthermore, fair payments are realized based on blockchain and smart contracts to support the outsourcing of decryption between users and mobile edge computing servers. Finally, the proposed scheme is proven secure in the random oracle model, and experimental results show that it is computationally efficient and hence can be used in the edge computing environment.

3. Proposed Work

3.1 Architecture of PCIM

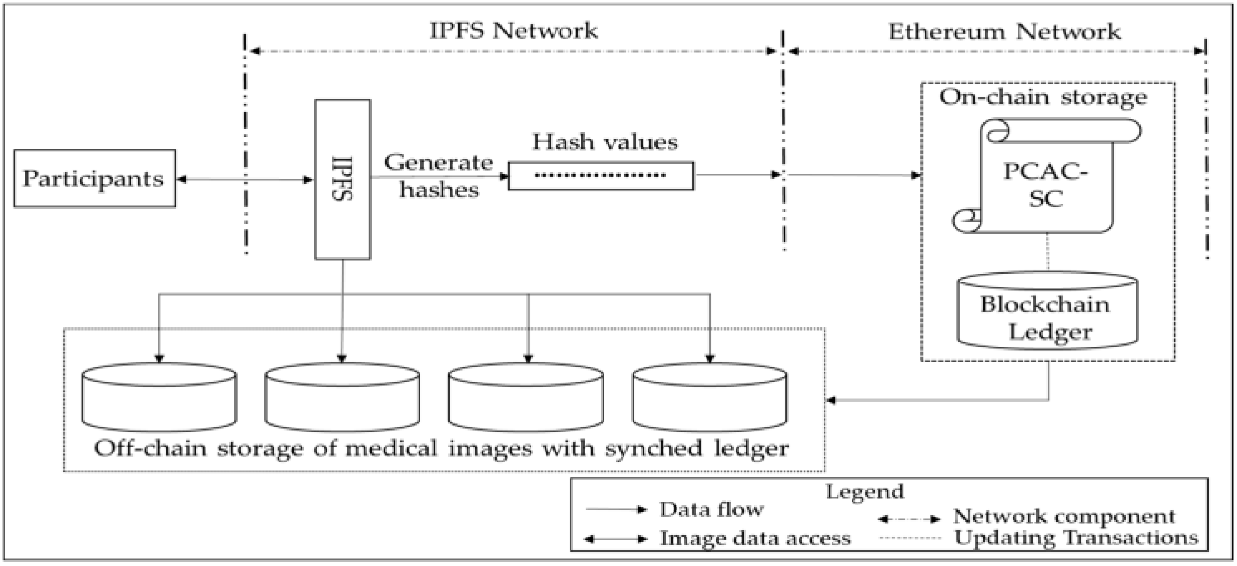


Figure 1. Architecture of patient-centric image management (PCIM) system. The architecture component split into two main decentralized modules: IPFS and Ethereum network.

3.2 System Model

The participants of the proposed PCIM system are defined below:

Patient: Patients are the owners of their medical images. A patient is required to create PCAC-SC and store this SC in the Ethereum blockchain. The patient is responsible for defining the access rights to the images in the IPFS network. This definition is done within his/her own PCAC-SC.

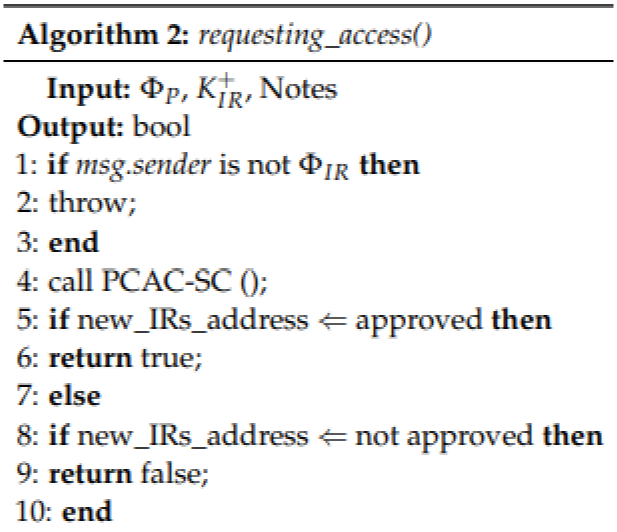
Radiologist: A radiologist is able to generate medical images for a patient. The prime responsibility of the radiologist is to upload the patient's encrypted medical images to the IPFS network and to verify the patient's initial transaction on blockchain.

Image Requestors (IRs): Clinicians, medical institutions, research groups, insurance companies, and general practitioners interested in accessing patient medical images are all considered as image requestors IRs. The patient can grant access privileges to any IRs based on the authorization policy defined in PCAC-SC.

3.3 PCAC-SC(Patient centric access control smart contract) protocol

msg.sender: the address variable of the owner who interacts with the smart contract.

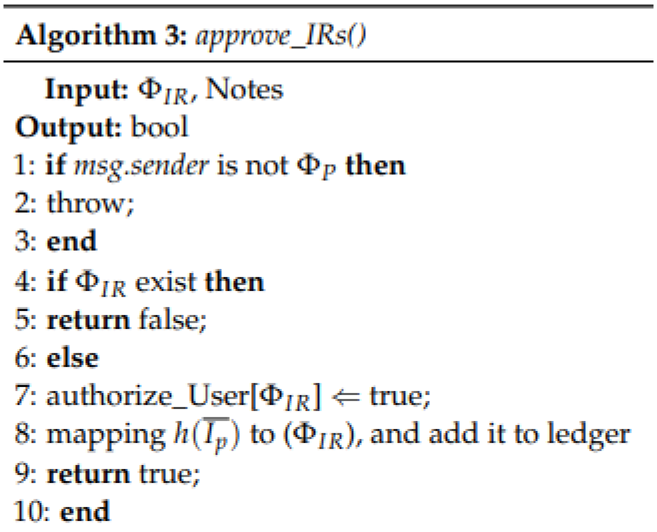
requesting_access(): this function is executed by IRs to obtain access permission from the patient. IRs includes as input the patient blockchain address ΦP and IRs public key K + IR to encrypt medical images and additional information, such as usage notes as shown in Algorithm 2.



Algorithm 2: *requesting_access()*

```
  Input: $\Phi_P$, $K^+_{IR}$, Notes
Output: bool
if $msg.sender$ is not $\Phi_{IR}$ then
    throw;
end
call PCAC-SC ();
if new_IRs_address $\Leftarrow$ approved then
    return true;
else
    if new_IRs_address $\Leftarrow$ not approved then
        return false;
    end
```

approve_IRs(): this function can only be executed by the patient. As shown in Algorithm 3, it grants/denies access permission by using as input the IRs blockchain address ΦIR, IRs public key $K + IR$, and notes from IRs. The input notes contain relevant information such as the expiration date and message for requestors.



Algorithm 3: *approve_IRs()*

```
Input: $\Phi_{IR}$, Notes
Output: bool
if $msg.sender$ is not $\Phi_P$ then
    throw;
end
if $\Phi_{IR}$ exist then
    return false;
else
    authorize_User[$\Phi_{IR}$] $\Leftarrow$ true;
    mapping $h(\overline{I_p})$ to ($\Phi_{IR}$), and add it to ledger
    return true;
end
```

rejectRequest(): this function is only executed by a patient. The patient can reject the image requester's request by executing this function.

ishashHampered(): this function checks whether the hash given by the patient to the image requester is valid or not.

3.4 Working of the system

3.4.1 Steps involved in system interaction between patient and radiologist

•**Step 1:** Offline interaction between the patient and the radiologist. Step 1.1: The patient requests the radiologist to store his/her medical image. Step 1.2: The radiologist asks the patient to provide its encryption key. Step 1.3: The patient generates a pair of encryption keys: public K + P and private K − P . Step 1.4: The patient sends the public key K + P to the radiologist through a secure communication medium for creating image authentication and encrypting the original medical image. Step 1.5: K − P is protected and kept safe by the patient.

• **Step 2:** The radiologist encrypts with K + P while concealing the patient private information on a medical image. Encrypted image IP is uploaded to the IPFS network, which returns a hash h(I p) to the radiologist.

• **Step 3:** The radiologist shares h(Ip) with the patient.

• **Step 4:** The patient creates a contract using the PCAC-SC protocol and executes it.

• **Step 5:** The created contract function signs a transaction on the Ethereum blockchain along with patient public key (Φ + P), h(I p), time, image description (ΔP) such as patient blockchain address (ΦP), and an imaging modality from which the data are obtained (e.g., CT, US, MRI, etc.). This transaction is verified by the radiologist and included in the blockchain. This verification process prevents multiple entities from executing create_contract() function on the same image hash.

• **Step 6:** The patient owns the medical images within the PCIM system. The patient can access, audit, prove the ownership, and authorize any other IRs (e.g., clinicians, medical institutions, research groups and general practitioners) to use their medical images based on PCAC-SC

3.4.2 Steps involved in medical image access sharing

• **Step 1:** Requestor shares K + IR a public key using requesting_access() a SC function.

• **Step 2:** Patient downloads the encrypted image from the IPFS network using the IPFS hash value.

• **Step 3:** Patient decrypts the encrypted image with patient's own private key K − P .

• **Step 4:** Patient obtains the requestor's public key by providing the requestor's blockchain address.

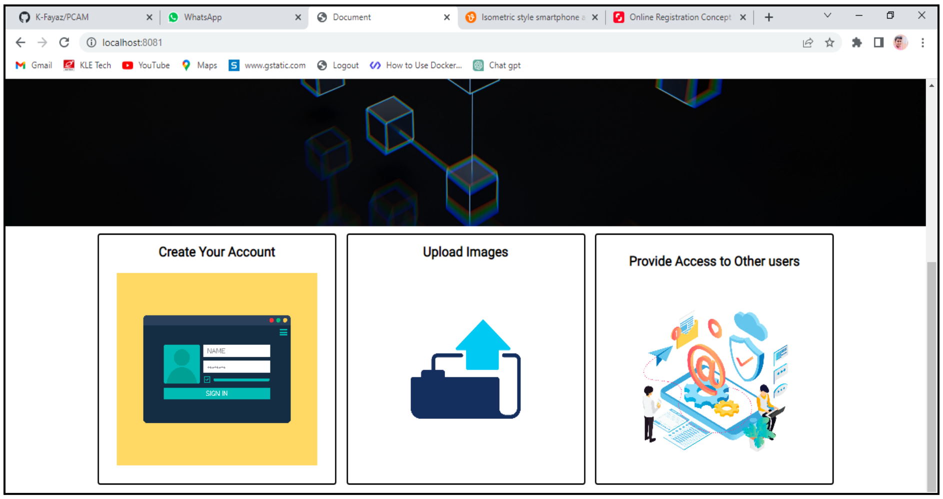
• **Step 5:** Patient encrypts the original image with the requestor's public key K + IR and uploads the encrypted image to the IPFS network.

• **Step 6:** Patient signs a transaction on the blockchain along with the requestor's public key, the patient's public key and the IPFS hash value using approve_IRs() function.

• **Step 7:** The image requestor is able to retrieve the medical image using the IPFS hash value and decrypts with his/her own private key K − IR. In this way, medical images are shared between the patient and the requester.

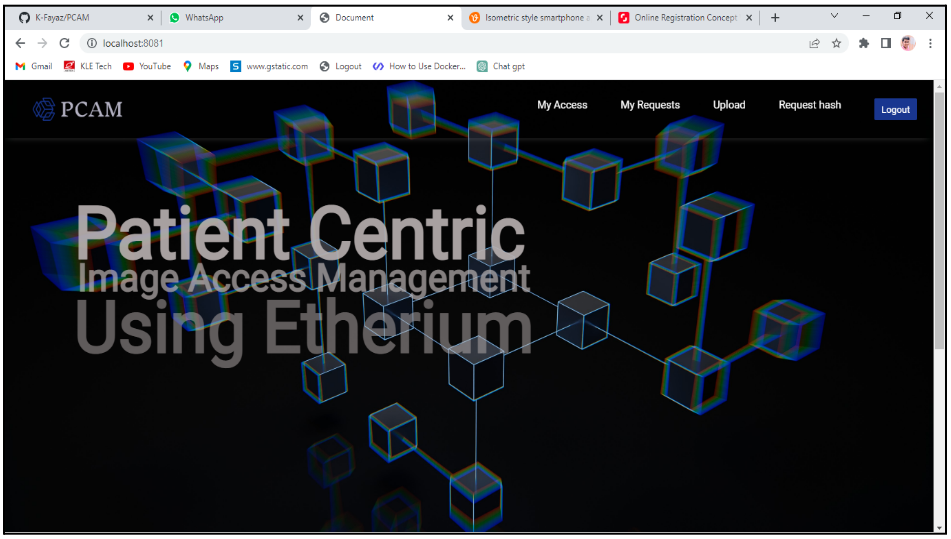
4. Results and Discussion

A. Login page of PCIM



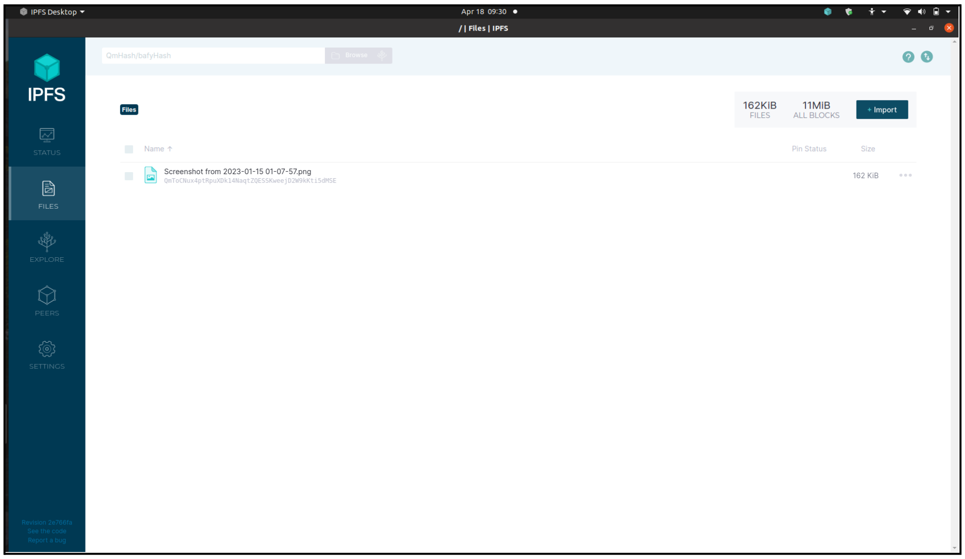
- Patients can login to the PCIM website and upload the hash of the images to the blockchain network.
- Image Requester can also login to PCIM website to request for a patient's medical image.

B. Home Page of PCIM



- If a patient is logged in he/she can check for the requests and give access to image requesters
- If a image requester is logged in he/she can request for patient's medical image and can access that image once patient grants access

C. Radiologist Uploads Patients medical images to IPFS network.



Name ↑	Pin Status	Size
Screenshot from 2023-01-15 01-07-57.png QmToCNux4ptRpuXDk14NaqtZQESSKweejD2W9kKti5dMSE		162 KiB

- Radiologist uploads patient’s images to IPFS network which returns hash value which is given to Patient for smart contract creation using PCAC-SC protocol.

D. Patient Uploads Image hash to BC network

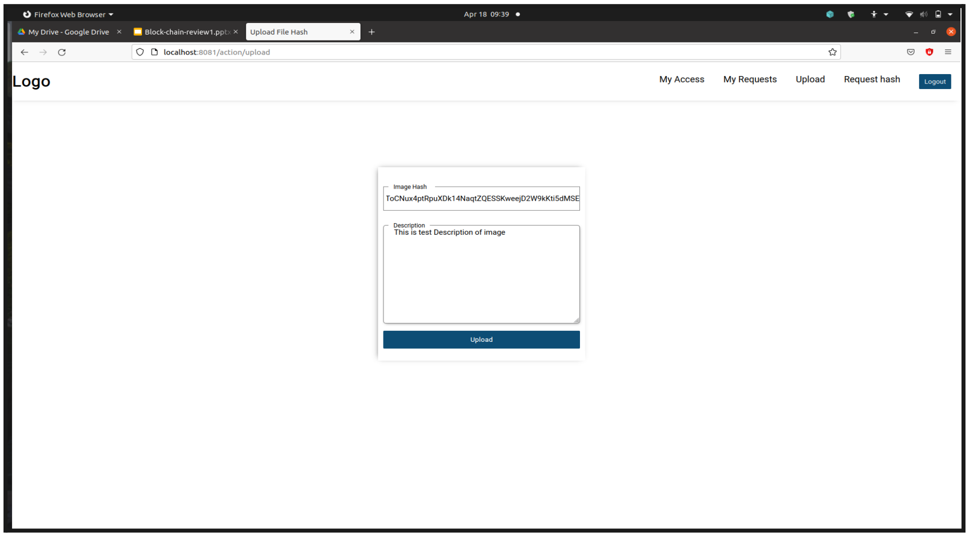
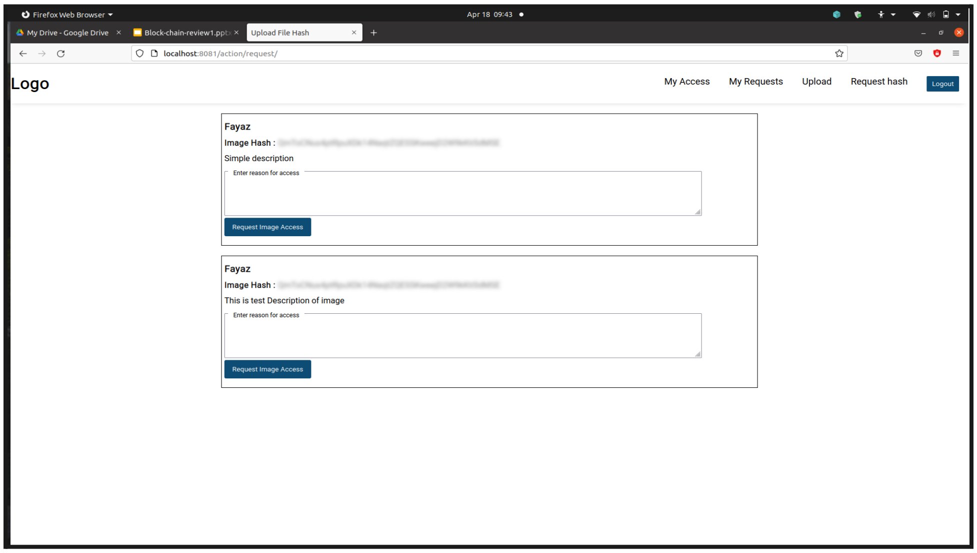


Image Hash: ToCNux4ptRpuXDk14NaqtZQESSKweejD2W9kKti5dMSE

Description: This is test Description of image

- Patient uploads image hash to blockchain network with proper description.
- Anyone who wants the image based on image description can request for image hash.

E. Image requesters can request for a patient's images.



Fayaz

Image Hash : [redacted]

Simple description

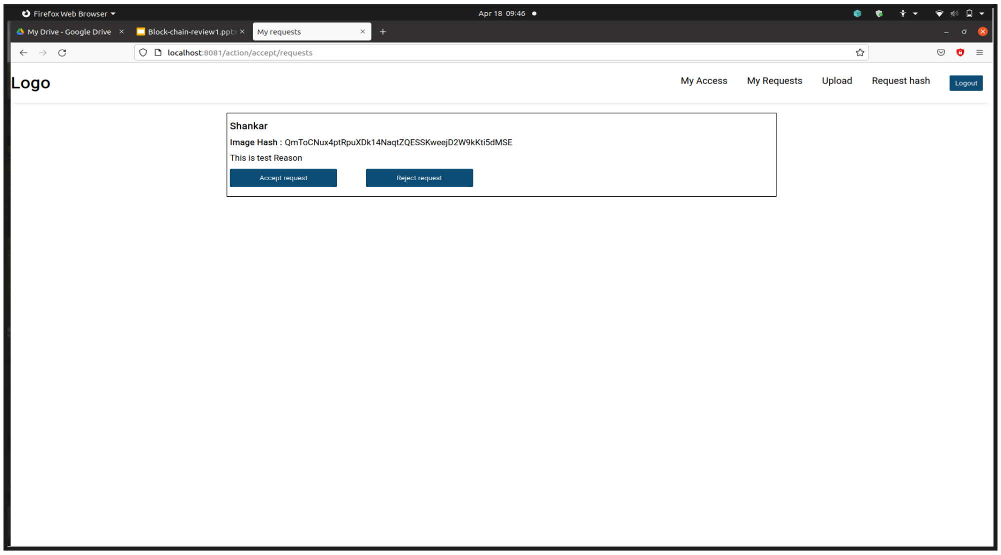
Fayaz

Image Hash : [redacted]

This is test Description of image

- Image requesters can request for a patient's image with proper reason. If the patient is okay with the reason and gives the access key to the image requester then he/she can access the patient's image.

F. Patient can grant or deny the access



Shankar

Image Hash : QmToCNux4ptRpuXDk14NaqtZQESSKweejD2W9kKti5dMSE

This is test Reason

- Patient can grant access to his/her medical image data based on the image requester's reason. If the reason is proper he/she can grant access otherwise he/she can deny the access.

5. Conclusion

Patient medical images are the most valuable asset of any healthcare system's intelligence. Most of the time, these medical images are indeed scattered across different systems, and sharing them is influential for establishing effective and cohesive healthcare. In addition, a centralized hosting location of image data (e.g., cloud-based solution) can be a single point of a security attack. With growing recognition of the distributed nature of health services, attention has been increasingly focused on decentralized architectures and system interoperability. We presented the Proof of concept design of the proposed PCIM system: an Ethereum blockchain and IPFS-based decentralized framework for storing and sharing access to medical images. Moreover, we introduced a new access management system called PCAC-SC that enables authorized entities to access the relevant blockchain data. The PCIM system facilitates a unique way to improve the rights of patients by providing full control over their medical images using PCAC-SC protocol. Patients have complete transparency over their medical images and can grant permission to access or revoke the image for clinical trials or research purposes. We performed the experimental implementation to analyze and evaluate efficiency, rationality and feasibility of the proposed scheme. The proposed system facilitates patient access to an immutable medical database providing higher efficiency, data provenance, and effective audit while sharing access to medical images. The data storage and exchange model is also decentralized; therefore, the necessity to involve third-party intermediaries and administrative structures is eliminated.

REFERENCES

1. *Jabarulla, Mohamed Yaseen, and Heung-No Lee*. "Blockchain-based distributed patient-centric image management system." *Applied Sciences* 11.1 (2020): 196.
2. *Mohsan, Syed Agha Hassnain*, et al. "Decentralized Patient-Centric Report and Medical Image Management System Based on Blockchain Technology and the Inter-Planetary File System." *International Journal of Environmental Research and Public Health* 19.22 (2022): 14641.
3. *Yuan, Wen-Xin, et al*. "Blockchain-based medical health record access control scheme with efficient protection mechanism and patient control." *Multimedia Tools and Applications* (2022): 1-22.
4. *Thwin, Thein Than, and Sangsuree Vasupongayya*. "Blockchain-based access control model to preserve privacy for personal health record systems." *Security and Communication Networks* 2019 (2019).
5. *Zhang, Yinghui, et al*. "Blockchain-Enabled decentralized Attribute-Based access control with policy hiding for smart healthcare." *Journal of King Saud University-Computer and Information Sciences* 34.10 (2022): 8350-8361.