WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Proxy Re-Encryption for Secure Medical Data Sharing in Clouds

P.KUMAR[1] ,DR.VAIDEHI.V [2]

[1].PG Student, [2].Professor
pkumarpkumar054@gmail.com vaidehi.mca@drmgrdu.ac.in
Department of Computer Applications
DR.MGR.Educational & Research Institute,Chennai-95

ABSTRACT:

Proxy re-encryption schemes, users delegate their encrypted files to other users by using re-encryption keys, which elegantly transfers the users' burden to the cloud servers. Moreover, one can adopt conditional proxy re-encryption schemes to employ their access control policy on the files to be shared. However, we recognize that the size of re-encryption keys will grow linearly with the number of the condition values, which may be impractical in low computational devices. data security has become a critical issue in various kinds of applications. Users may prefer storing their files in an encrypted manner and delegating decryption rights efficiently.

Keywords: Proxy Re-Encryption,Secure Data Sharing,Medical Data Privacy,Cloud Computing ,Asymmetric Encryption ,Access Control

I.INTRODUCTION:

A private blockchain information. However, as noted, then current blockchain is not effective in sharing patient data between different healthcare organizations, so they proposed a patient-centric healthcare sharing system that implements the query in a single a keyword blockchain [1].
Weaknesses of inefficient transactions and higher energy consumption compared to HyperledgerFabric. So they used Hyperledger Fabric in their plan. However, he pointed out that the system limited the scalability of the blockchain. proposed a new approach, known as Patient-Centric Health Information Management, to store certain data in the IPFS datum blockchain [2].
IPFS replaces traditional domain addressing with content-based addressing, eliminating the need to care about the location of servers or storage paths and file names. Every time a file is uploaded to an IPFS node, a unique encrypted hash value is created based on the contents of the pride. The hash value reflects the contents of the file, so even a slight change in one bit will result in a different hash value. When IPFS receives a file hash request, it uses a distributed hash table to find the corresponding file node and retrieve and verify its content information [3].
Proposed an in-product searchable cryptosystem with multiple keyword searches based on blockchain. a bondless and blockchain-friendly universal designated verifier signature proof (UDVSP) system.It is worth noting that the system is the first system to distribute malware so far. Based on the above work, we have created a framework for reliable information sharing [4].
Pointed out that excessive searches can sometimes fail to validate all returned results, resulting in a waste of resources. Therefore, they proposed a scheme to reduce the number of attribute encryptions and decryptions in an cloud environment that enables effective data access control. pointed out that cloud servers are not completely reliable [5].

II.LITERATURE SURVEY:

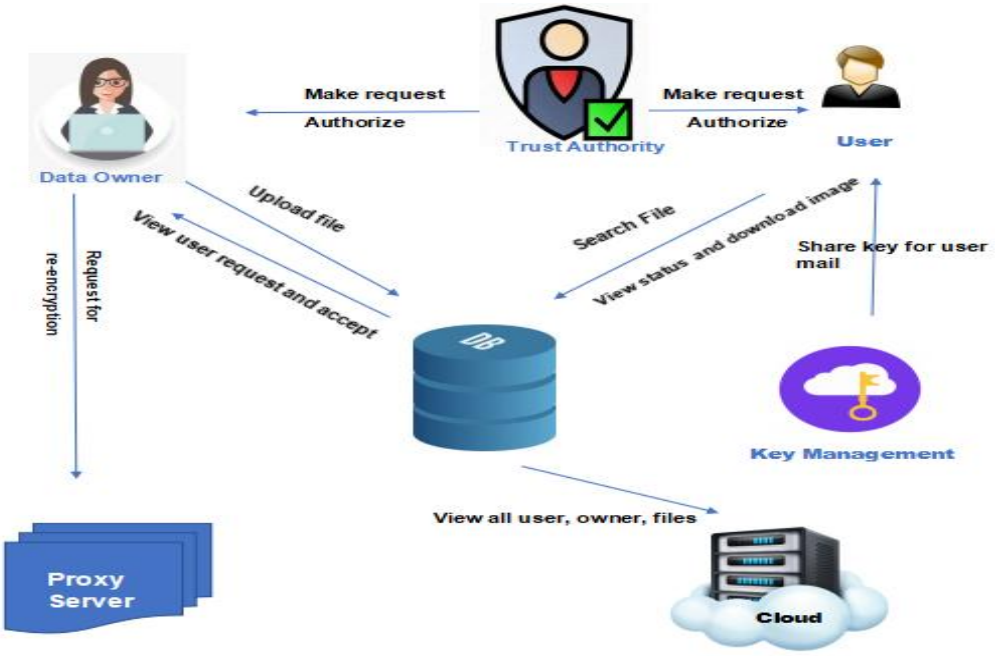
According to **Ahsan Manzoor**.et al., 2021 Data is central to the Internet of Things (IoT) ecosystem. With billions of devices connected to each other, most current IoT systems use centralized cloud-based data systems that are difficult to scale to meet the needs of future IoT systems. The involvement of such a third-party service provider also requires the trust of both sensor owners [6].
According to **Yejin Kim**.et al., 2021 The security and privacy of electronic health records (EHR) have received much attention from health care professionals and researchers. Various encryption and decryption methods and key management protocols have been developed to ensure security. However, due to fragmentation and scalability issues, additional security techniques have been proposed [7].
According to **Bhavye Sharma**.et al., 2020 Developing a robust, transparent and interoperable eHealth infrastructure has been a difficult task due to many regulations and laws such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). Healthcare providers prefer to keep information about their patients under lock and key [8].
According to **Wenxuan Cheng**.et al., 2023 Information processing technology has continuously developed, and the hospital information system (HIS) has become more and more comprehensive. However, the innovation rate of security attack technology is much higher than people's expectations. HIS faces significant challenges in the secure sharing of medical privacy data. Therefore, a robust blockchain-based medical data sharing system (BMDSS) is proposed [9].

According to **Lihua Zhang**.et al., 2023 A large amount of valuable data is stored in the data centers of intelligent networks, but since the diversity of resources of one data center is limited, information sharing becomes especially important for the implementation of an effective data mining process. However, traditional data sharing models often use centralized systems without authentication of shared objects, making it difficult to establish trust relationships and ensure data protection [10].

III.PROPOSED SYSTEM:

We have proposed a proxy re-encryption scheme for E-healthcare data sharing on fog computing, which deals with the problem of overhead and delay of previously proposed PRE schemes.Our scheme reduces the commutation cost and communication overhead of the resource-constraint IoT devices.When we need to share encrypted data with multiple participants, we can achieve significant performance by using the proxy re-encryption scheme

ARCHITECTURE DIAGRAM:



Explanation:

1.Data Sources: These are the entities that generate medical data, such as hospitals, clinics, or individual patients. Each data source has its own set of sensitive medical records.
2.Cloud Storage Providers: These are the cloud service providers where the medical data is stored. They provide the infrastructure for data storage and management.
3.Data Owners: Data owners are individuals or organizations who have control over the medical data. They authorize access to the data and specify the conditions under which it can be shared.
4.Proxy Re-Encryption Service: This is the core component of the architecture. It facilitates secure data sharing by allowing data owners to delegate access rights to other users without revealing the underlying data. Proxy re-encryption algorithms are used to transform encrypted data from one key to another, enabling data sharing without the need for decryption and re-encryption.
5.Key Management System: This system manages the cryptographic keys used for encryption and re-encryption. It ensures that only authorized parties have access to the keys necessary to decrypt or re-encrypt the data.
6.Access Control Mechanism: This mechanism enforces access policies specified by the data owners. It determines who is allowed to access which portions of the medical data and under what conditions.
7.User Interfaces: These interfaces allow data owners to manage access control policies, monitor data access, and perform other administrative tasks related to the sharing of medical data.

IV.RESULT AND DISCUSSION:

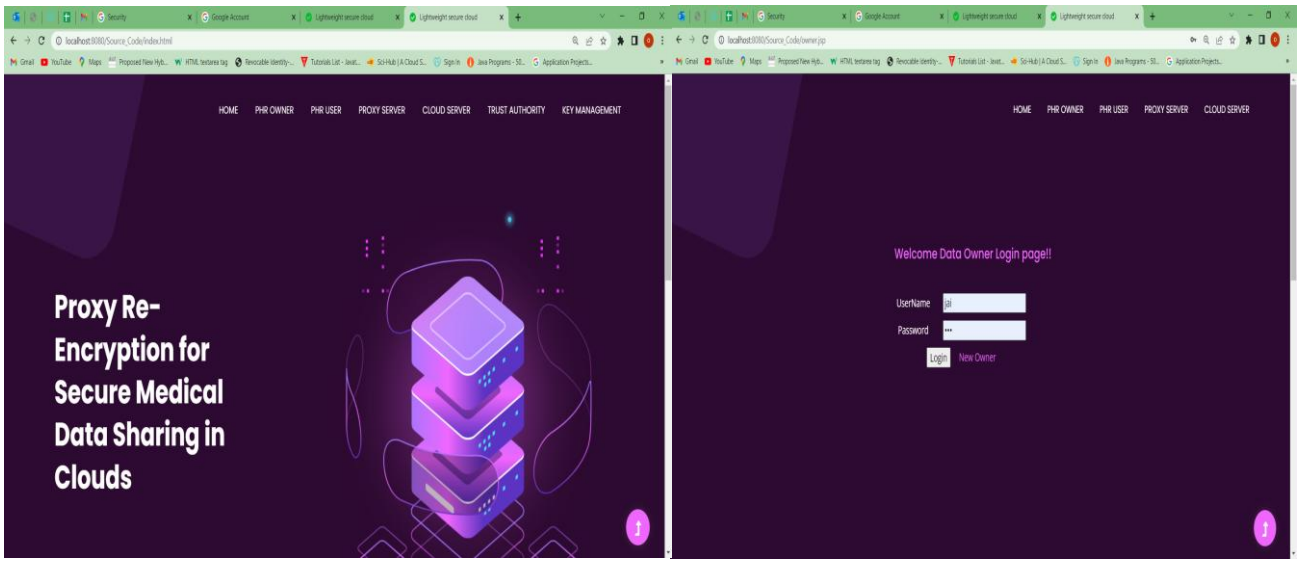


Fig1.HOMEPAGE LOGIN

a)Homepage: This would be the main landing page of the application, where users can find general information about the project, its purpose, and possibly some navigation links to other sections of the application.

b)Login: This page allows users to authenticate themselves by providing their credentials, such as username and password, to gain access to the system. This ensures that only authorized users can interact with the system and access sensitive medical data.

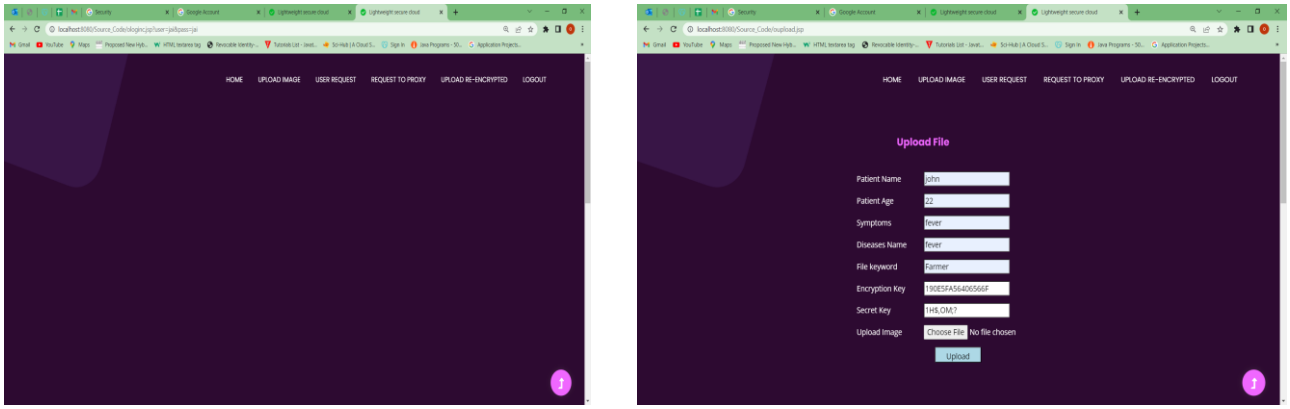


Fig2.USER REQUEST UPLOADFILE

a)User request: This feature allows authenticated users to send requests for specific actions or permissions within the system, such as requesting access to certain medical data or requesting assistance from administrators**.**

b) Upload file: Users with appropriate permissions can upload medical files or documents to the system. These files are securely stored in the cloud infrastructure, ensuring confidentiality and integrity.

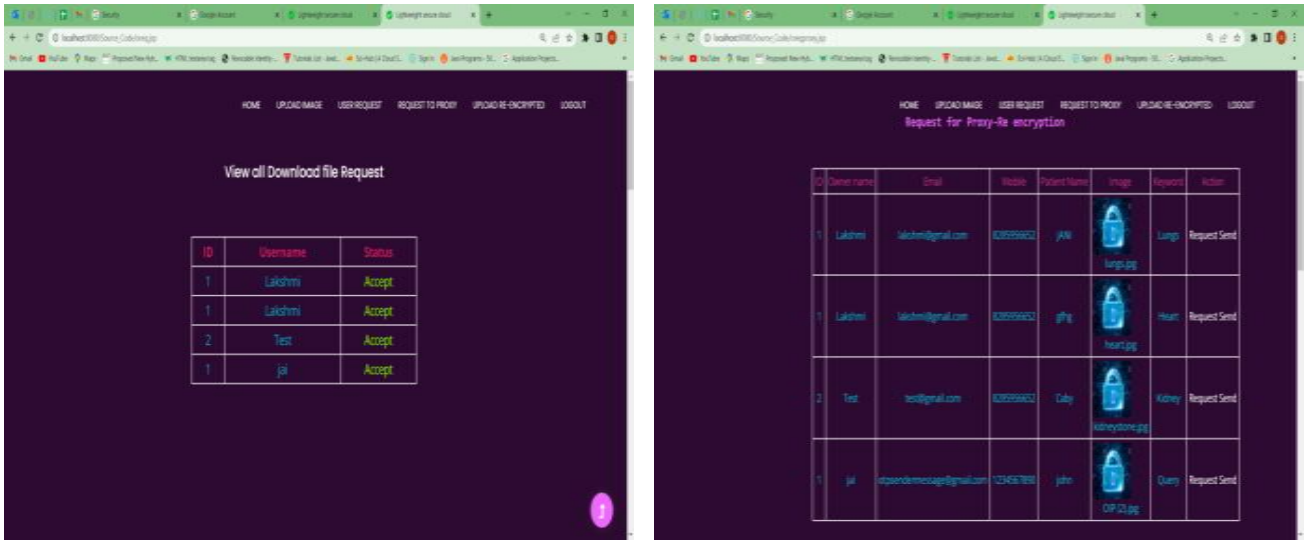


Fig3.DOWNLOAD FILE REQUEST PROXY ENCRYPTION

a)Download all file: Users may have the ability to download all files associated with their account or a specific subset of files. This allows them to retrieve medical data for analysis or sharing purposes.

b) Request for Proxy-Re encryption: This feature enables users to request the re-encryption of their medical data using proxy re-encryption techniques. Proxy re-encryption allows a trusted third party to transform encrypted data from one user to another without accessing the plaintext data, ensuring secure sharing of medical information.

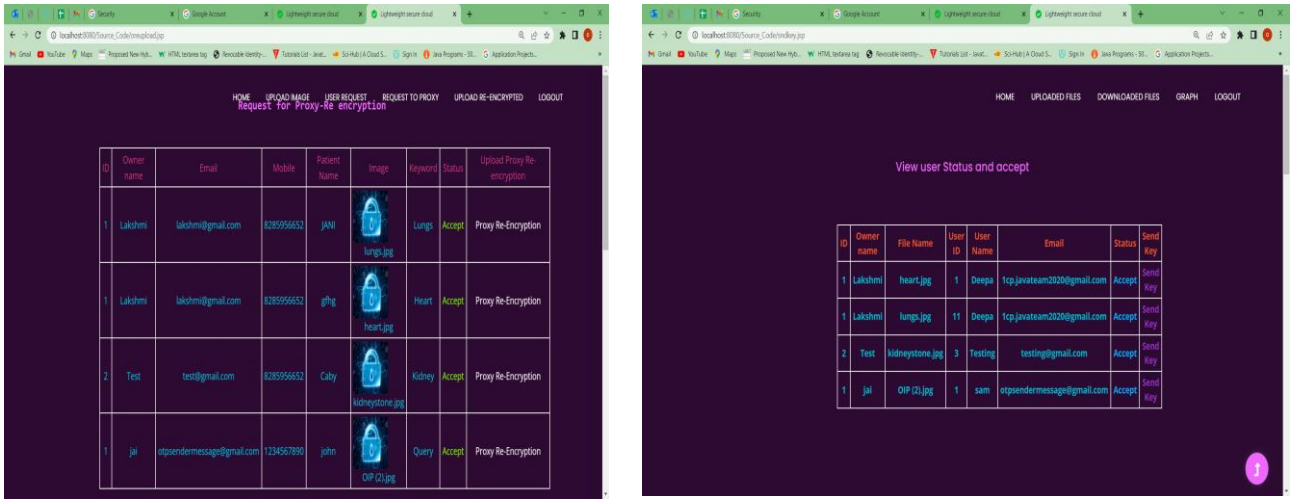


Fig4.VIEW USER STATUS

a).View user Status and accept: Administrators or authorized users can view the status of user requests and take action accordingly, such as approving or denying access to certain medical data or granting permission for proxy re-encryption.

V.CONCLUSION:

In cloud computing security is an important aspect of quality of service. To keep the sensitive user data confidential against untrusted servers several proxy re-encryption techniques are used.This scheme performs arbitrary computations on encrypted data without decrypting it.This scheme can avoid potential security risks that are raised by the delay of issuing the PRE keys.

REFERENCE:

[1].Al Omar A, Bhuiyan MZA, Basu A, Kiyomoto S, Rahman MS (2019) Privacyfriendly platform for healthcare data in cloud based on blockchain environment. Future Generation Comput Syst 95:511–521

[2].Chi J, Li Y, Huang J, Liu J, Jin Y, Chen C, Qiu T (2020) 'A secure and efcient data sharing scheme based on blockchain in industrial internet of things.' J Netw Comput Appl 167:102710–102720.

[3].Mani V, Manickam P, Alotaibi Y, Alghamdi S, Khalaf OI (2021) 'Hyperledger healthchain: Patient-centric IPFS-based storage of health records.' Electronics 10(23):3003.

[4].Lin C, Huang X, He D (2023) Efcient blockchain-based electronic medical record sharing with anti-malicious propagation. IEEE Trans Serv Computer 16(5):3294–3304.

[5].Jiang P, Guo F, Liang K, Lai J, Wen Q (2020) Searchain: Blockchain-based private keyword search in decentralized storage .Future Generation Comput Syst 107:781–792.

[6].Ahsan Manzoor, An Braeken, Salil S Kanhere, Mika Ylianttila, Madhsanka Liyanage 2021,Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain Journal of Network and Computer Applications 176, 102917.

[7].Young-Hoon Park, Yejin Kim, Shin-Ok Lee, Kwangman Ko 2021,Secure outsourced blockchain-based medical data sharing system using proxy re-encryption Applied Sciences 11 (20), 9422.

[8].Bhavye Sharma, Raju Halder, Jawar Singh 2020,Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption, International Conference on COMmunication Systems & NETworkS (COMSNETS)

[9].Wenxuan Cheng, Bo Zhang, Zhongtao Li 2023,Robust Medical Data Sharing System Based on Blockchain and Threshold Rroxy Re-encryption, International Conference on Algorithms and Architectures for Parallel Processing, 112-131.

[10].Lihua Zhang, Qianqian Yang, Yi Yang, Shihong Chen, Jinguang Gu 2023,Data Sharing Scheme of Smart Grid Based on Identity Condition Proxy Re-Encryption, Electronics 13 (1), 139.