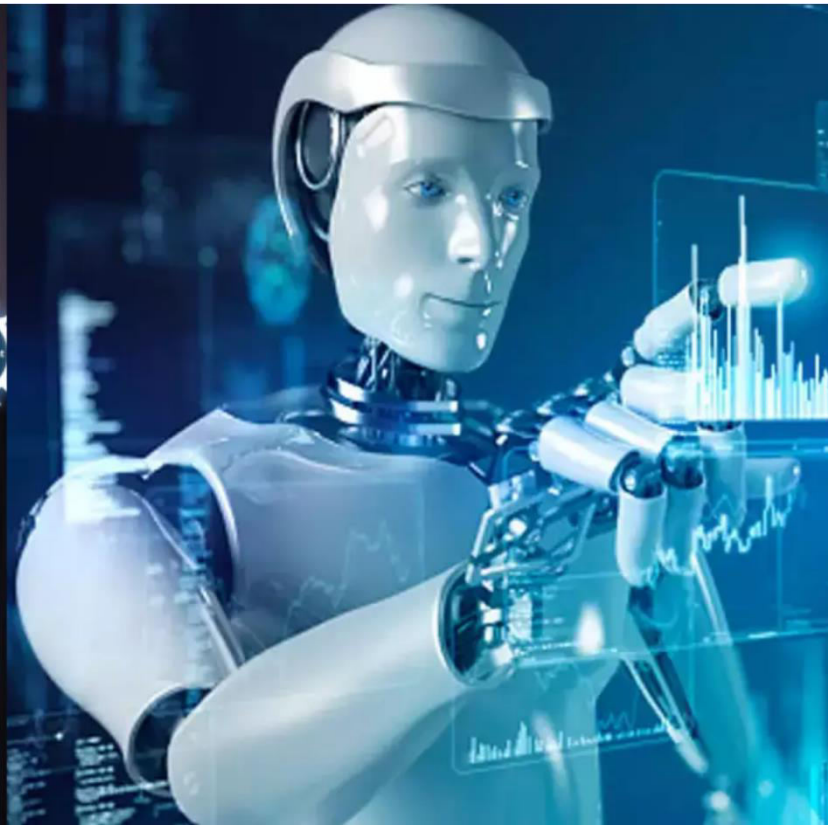
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 6, June 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406181|

IPFS based File Storage Access Control and Authentication Model for Secure Data Transfer using Blockchain Technique

S. Vindhyasri[1], B. Uday Kiran [2], M. Rachana[3], Mr.G.Prasad[4]

U.G. Student, Department of Information Technology, ACE Engineering College, Ankushapur, Telangana, India[1,2,3]

Assistant Professor, Department of Information Technology, ACE Engineering College, Ankushapur, Telangana, India[4]

ABSTRACT: Large files cannot be efficiently stored on blockchains. On one hand side, the blockchain becomes bloated with data that has to be propagated within the blockchain network. On the other hand, since the blockchain is replicated on many nodes, a lot of storage space is required without serving an immediate purpose, especially if the node operator does not need to view every file that is stored on the blockchain. It furthermore leads to an increase in the price of operating blockchain nodes because more data needs to be processed, transferred and stored. IPFS is a file sharing system that can be leveraged to more efficiently store and share large files. It relies on cryptographic hashes that can easily be stored on a blockchain. Nonetheless, IPFS does not permit users to share files with selected parties. This is necessary, if sensitive or personal data needs to be shared. Therefore, this paper presents a modified version of the Interplanetary Filesystem (IPFS) that leverages Ethereum smart contracts to provide access-controlled file sharing. The smart contract is used to maintain the access control list, while the modified IPFS software enforces it. For this, it interacts with the smart contract whenever a file is uploaded, downloaded or transferred.

KEYWORDS: IPFS (Inter Planetary File System), Blockchain, Smart Contracts, Decentralized Storage, Access Control, Authentication, Data Security, File Sharing, Ethereum, Content Identifier (CID), Cryptographic Hashing, Data Integrity, Secure Data Transfer, Web3, MetaMask, Python Flask, XAMPP Server, MySQL Database, Encryption and Decryption, Distributed Systems.

I. INTRODUCTION

In today's digital world, the demand for secure and scalable data storage solutions is rapidly increasing. Traditional centralized storage systems, like cloud servers, face limitations such as single points of failure, lack of transparency, and vulnerability to data breaches. Blockchain technology offers immutability and transparency but is inefficient for storing large files due to high costs and storage constraints.

To overcome these challenges, this project presents a hybrid storage solution that integrates the InterPlanetary File System (IPFS) with blockchain-based smart contracts. IPFS allows efficient storage and distribution of large files in a decentralized manner, while blockchain ensures secure access control and maintains immutable records of file access.

Smart contracts are used to manage user permissions and authenticate access requests. File hashes and metadata are stored on the blockchain, while actual files are stored in IPFS. This model ensures data confidentiality, integrity, and traceability without overloading the blockchain.

The system is user-friendly, featuring a simple interface for file uploading, permission management, and secure sharing. This project is especially useful for sectors like healthcare, education, and legal industries, where data security and control are critical. By combining the strengths of IPFS and blockchain, the solution supports secure, transparent, and decentralized file management for the future.

II. LITERATURE SURVEY

1. G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in 2015 IEEE Security and Privacy Workshops, May 2015, pp. 180–184.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406181|

They proposed a **decentralized personal data management system** using blockchain. Their work focused on giving users more control over their data. They used smart contracts to manage access, while storing data off-chain. However, they faced challenges like performance issues, storage limits, and user complexity.

2. X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A taxonomy of blockchain-based systems for architecture design," in 2017 IEEE International Conference on Software Architecture (ICSA), April 2017, pp. 243–252.

   This paper presented a **taxonomy for blockchain-based systems**, helping developers understand different types of blockchain architectures (public, private, etc.). It provided a structured approach to choosing the right blockchain setup, but lacked real-world validation and quickly became outdated due to fast tech changes.

3. Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," CoRR, vol. abs/1802.04410, 2022. [Online].

   They developed a **smart contract-based access control system for IoT** devices. Their model provided secure, decentralized access management using blockchain. While effective, it suffered from high transaction costs, limited performance, and was difficult for non-technical users to implement.

III. METHODOLOGY

This project involves the integration of decentralized technologies—namely, the InterPlanetary File System (IPFS) and blockchain—combined with smart contracts to create a secure and efficient data storage and access control system. The process begins with user registration and authentication, managed via a web-based interface. When a user uploads a file, the file is first encrypted and then stored in IPFS, which generates a unique content identifier (CID) for the file. Instead of storing the file itself on the blockchain, only the CID along with metadata and access permissions are recorded using blockchain smart contracts. These smart contracts are written in Solidity and deployed on platforms like Ethereum. They manage and enforce user-defined access rules, ensuring only authorized users can access or download the files. When a data requester seeks access, they must send a request to the data owner. If approved, a decryption key is shared securely. Throughout this process, all transactions—including uploads, access requests, and permissions—are logged on the blockchain to maintain transparency, auditability, and immutability. The frontend of the system is developed using HTML, CSS, and JavaScript, while the backend is built using Python with Flask, and the blockchain interactions are handled using Web3 libraries. This hybrid approach ensures scalability, security, and user control over data, making it well-suited for sensitive data sharing in various domains like healthcare, education, and legal services.

Architecture:

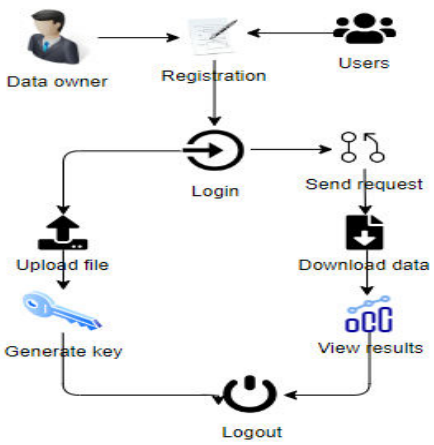


Fig.1 Architecture

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406181|

IV. EXPERIMENTAL RESULTS

New registration: In above screen click on 'New User Signup Here' link and then add 3 different users so we can provide access between them.

Registration Page: In below screen adding user details and any user can upload data and become "data owner" and any user can get access from data owner and then click on 'Submit' button to store data in Blockchain and get below output.

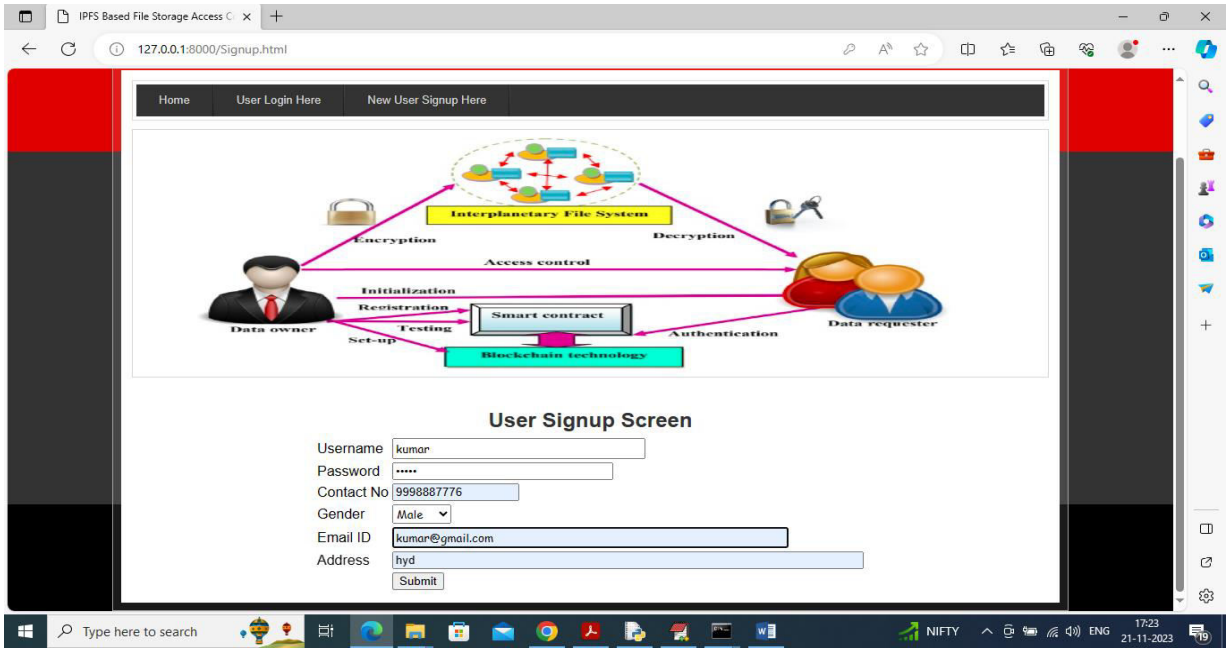


Fig.2 Registration Page

Login Data owner: In below screen owner is login and after login will get below page.

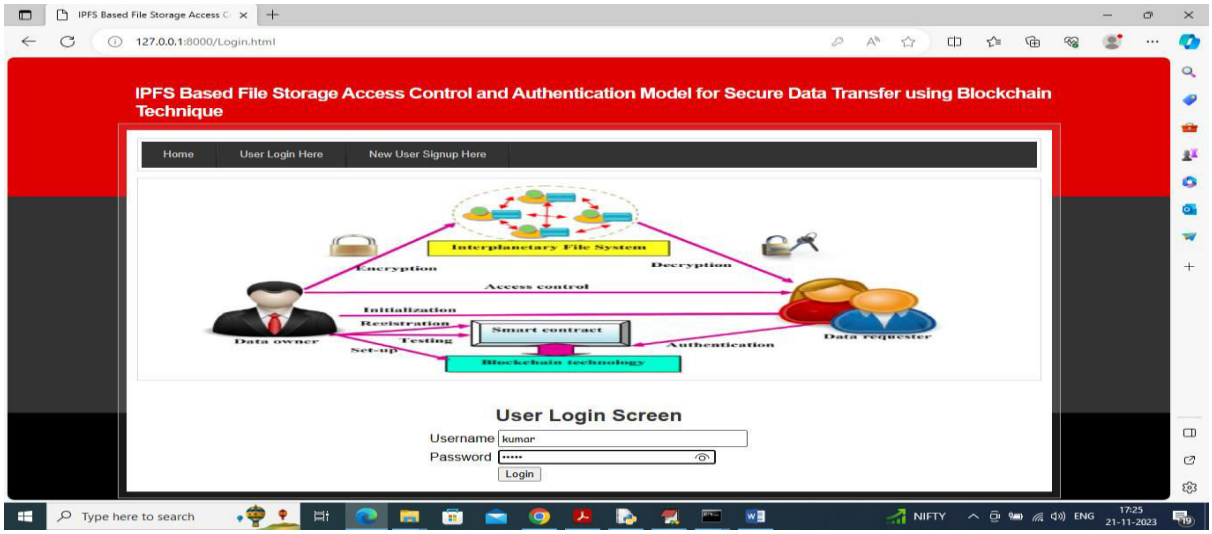


Fig.3 Login Data Owner

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406181|

Share secured data: In below screen user can click on 'Shared Secured Data' link to get below page.

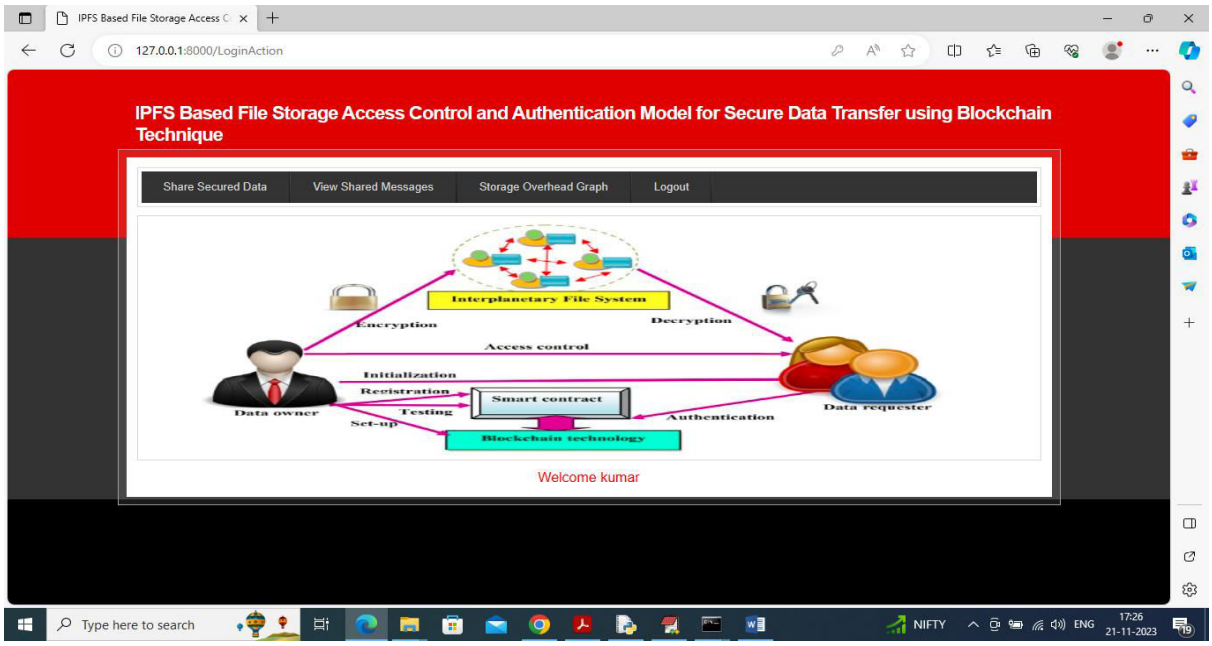


Fig.4 Share Secured Data

Upload file: In below screen data owner can write some description and then upload file which has to share and then he can see list of data requester and from above data requester list he can select desired requester and generate keys to give access to them.

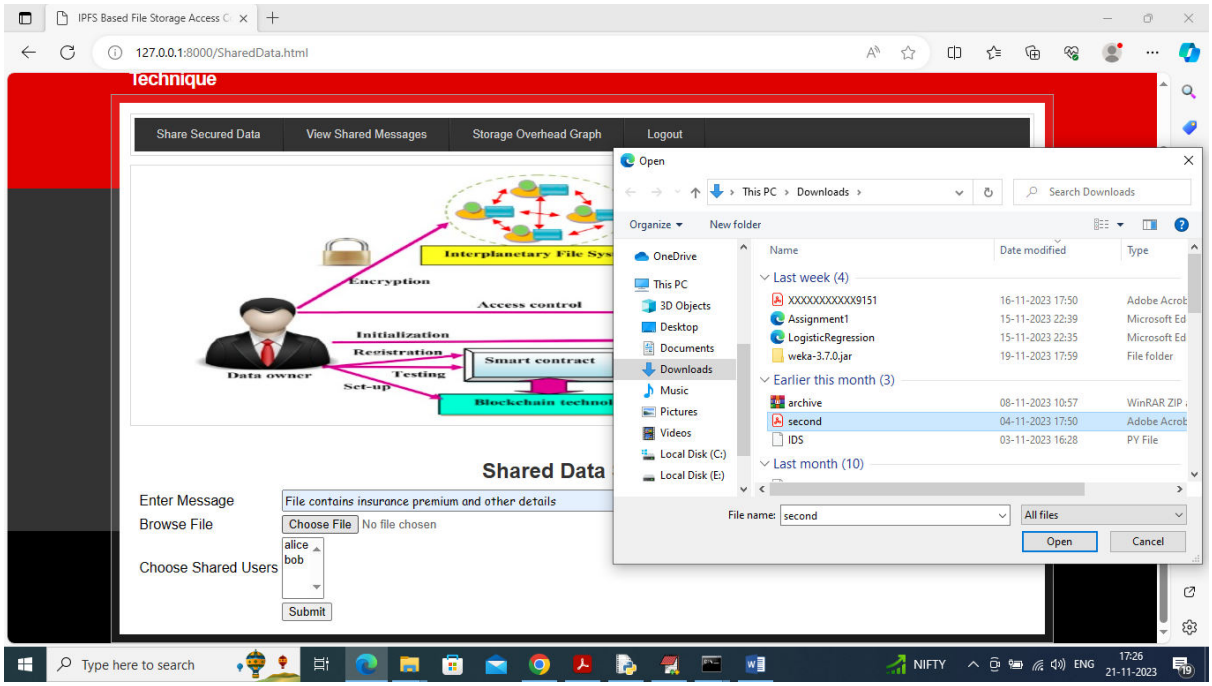


Fig.5 Upload File Page

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406181|

View file details: In below table data requester Alice can view all details and then can click on 'Click Here' link to decrypt and download file like below screen.

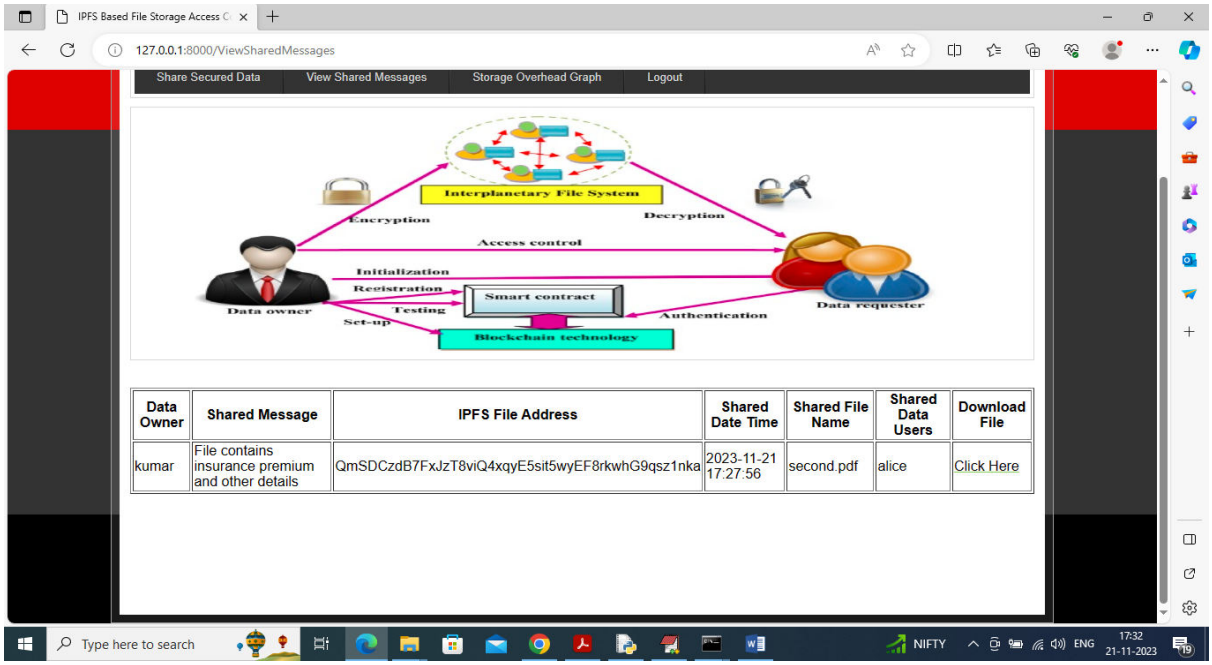


Fig.6 Viewing File Details

View no access user: In below screen we can see bob has no access permission so he cannot view or download file. Similarly, by following above screens you can control shared data permissions.

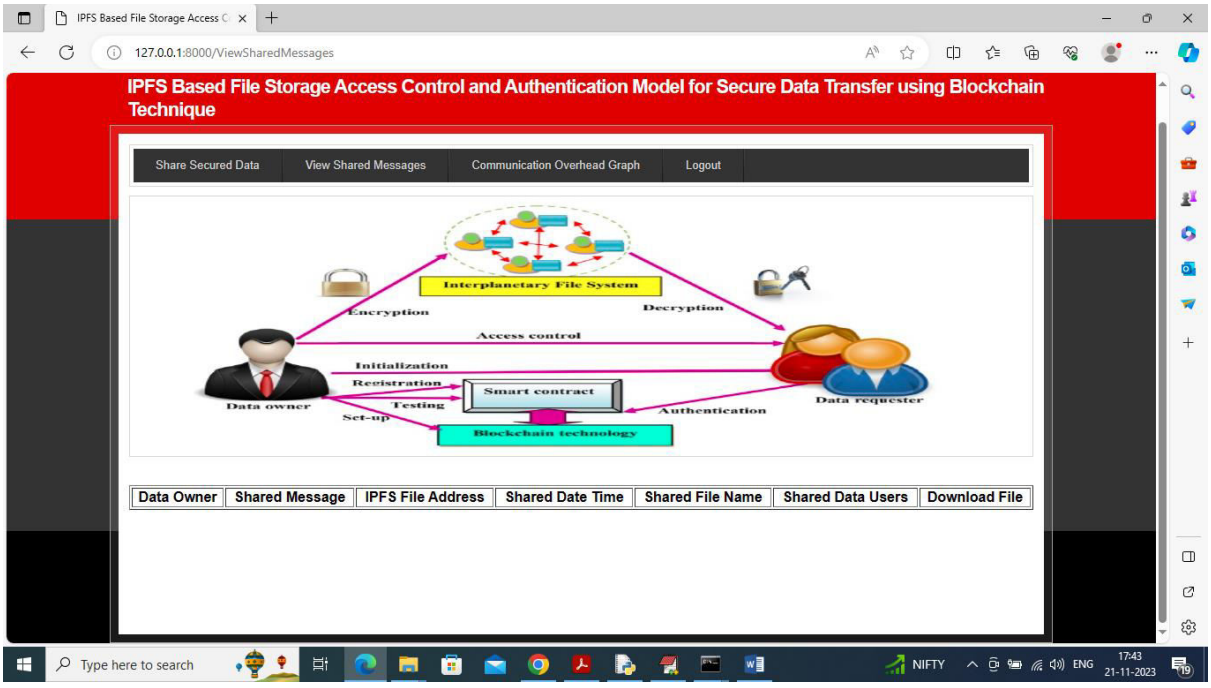


Fig.7 Viewing no Access User

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406181|

V. CONCLUSION

This project successfully demonstrates a secure and decentralized method for storing and sharing large files by integrating IPFS and blockchain technology. By storing files in IPFS and managing access permissions through blockchain smart contracts, the system ensures data confidentiality, integrity, and controlled access. Unlike traditional centralized systems, this hybrid approach eliminates single points of failure, reduces data breaches, and ensures tamper-proof records. The use of smart contracts allows transparent and automated enforcement of access rules without relying on a third party. A user-friendly interface was also developed to allow users to easily upload, share, and manage file access. Overall, the project offers a scalable, cost-effective, and trustworthy solution suitable for sectors like healthcare, law, and academics, where secure data handling is crucial.

REFERENCES

[1] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops, May 2015, pp. 180 184.
[2] G. Wood. (2018) Ethereum: A secure, decentralized generalized transaction ledger. [Online]
[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[4] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A taxonomy of blockchain-based systems for architecture design," in 2017 IEEE International Conference on Software Architecture (ICSA), April 2017, pp. 243–252.
[5] C. K. and T. M. V., Distributed Access Control in Cloud Computing Systems. Wiley Blackwell, 2016, ch. 35, pp. 417– 432. [Online].
[6] S. Alansari, F. Paci, and V. Sassone, "A distributed access control system for cloud federations," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), June 2017, pp. 2131–2136.
[7] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," CoRR, vol. abs/1802.04410, 2018. [Online]. Available: http://arxiv.org/abs/1802. 04410.
[8] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in 20.
[9] I. Baumgart and S. Mies, "S/kademlia: A practicable approach towards secure key-based routing," in Proceedings of the 13th International Conference on Parallel and Distributed Systems - Volume 02, ser. ICPADS '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 1–8. [Online]. Available: http://dx.doi.org/10.1109/ICPADS.2007. 4447808.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details