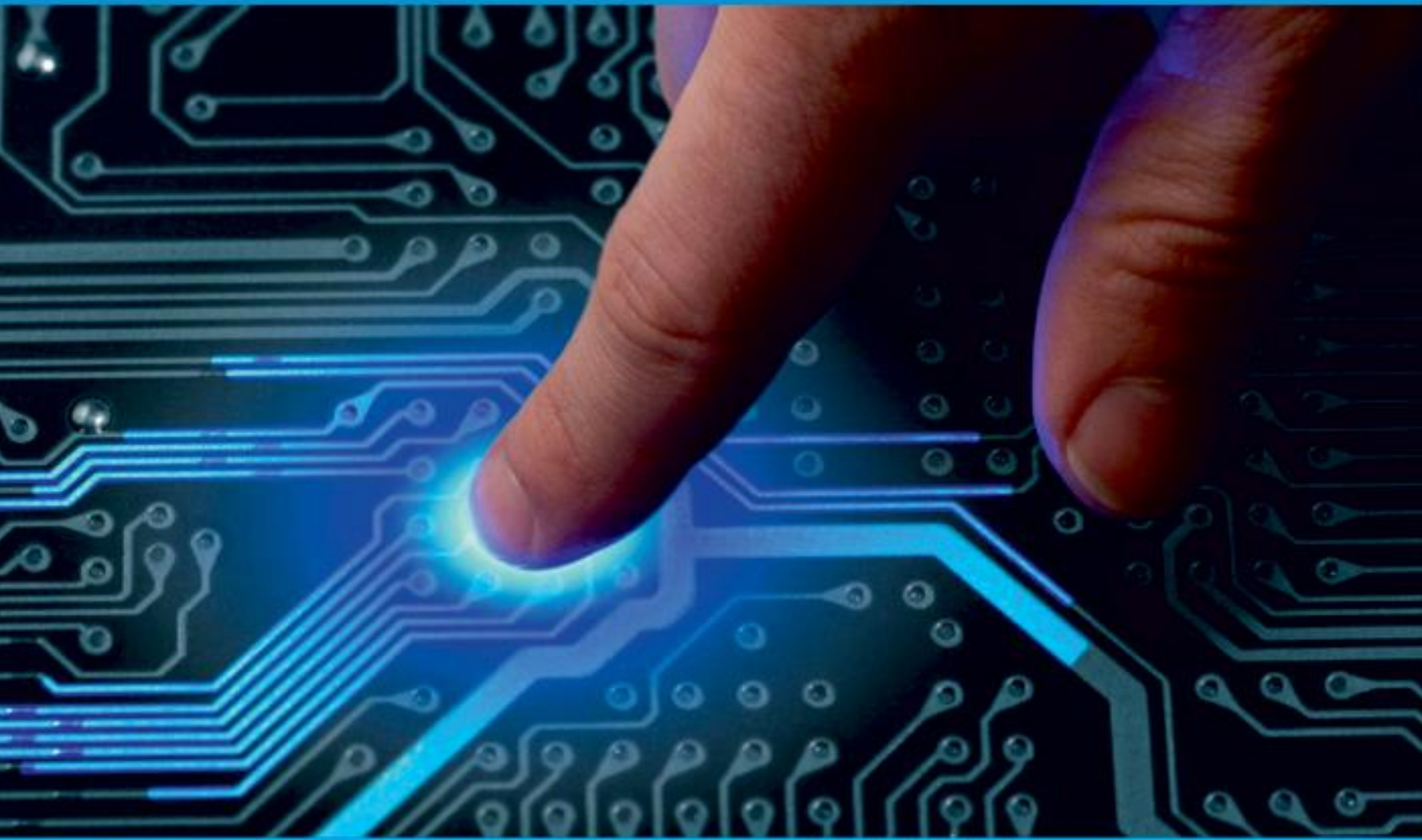
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204203|

Blockchain based Cloud File Sharing System

Abhishek V[1], Aditya D Benkikere[2], Anoop M[3], Sagar K R[4], Dr. Chetana Prakash[5]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering andTechnology, Davangere, Karnataka, India[1]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering andTechnology, Davangere, Karnataka, India[2]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering andTechnology, Davangere, Karnataka, India[3]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering andTechnology, Davangere, Karnataka, India[4]

Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[5]

ABSTRACT: Cloud file sharing has become increasingly popular due to its convenience and accessibility. However, traditional cloud systems are centralized, leading to concerns about security, privacy, and data integrity. To address these issues, this paper proposes a blockchain-based cloud file sharing system. The system utilizes blockchain technology to decentralize the storage and sharing of files. Each user maintains control over their files through private keys, ensuring data privacy and security. Smart contracts are used to manage file sharing permissions, enabling users tosecurely share files with others. By leveraging blockchain technology, users can have greater control over their data andreduce reliance on centralized third parties.

KEYWORDS: Blockchain; Cloud Computing; File Sharing; Security; Privacy; Smart Contracts.

I. INTRODUCTION

File sharing system play a pivotal role in facilitating seamless collaboration, data distribution and communication. These systems enable users to share, access and collaborate on files and documents, fostering efficiency and connectivity across the diverse environments. This introduction provides an overview of file sharing systems, their significance, key features and the evolving landscape of file sharing technologies.

File sharing systems have become integral to modern communication and collaboration, providing a dynamic framework for the exchange of information. The evolving landscape including Blockchain integration underscores the ongoing quest for innovation in file sharing technologies. In navigating these advancements, organizations must strike abalance between fostering collaboration and safeguarding data security and privacy of the user.

Blockchain is a decentralized, distributed ledger technology that securely records transactions across a network of computers. Each transaction is recorded in a block, which is then linked to previous blocks, creating a chain of blocks (blockchain). This chain is immutable, meaning once a block is added, it cannot be altered, ensuring the integrity of the data.

Blockchain promotes transparency as all participants have access to the same information, and security is ensured through cryptographic techniques. Smart contracts, which are self-executing contracts with predefined rules, can also be deployed on blockchain networks. With its potential to enhance security, transparency, and efficiency, blockchain is being explored in various industries, including finance, supply chain, healthcare, and more.

A blockchain-based cloud file sharing system is a decentralized network that allows users to store and share files securely. This system leverages the power of blockchain technology to ensure the integrity and security of data.

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that produces a 256-bit (32-byte) hash value. It's commonly used in blockchain technologies as a part of the block verification process. In our file sharing system, SHA-256 is used to generate a unique hash for each file or block of data, ensuring data integrity and security.

The InterPlanetary File System (IPFS) is a protocol designed to create a permanent and decentralized method of storing and sharing files. In our system, IPFS is used for decentralized storage, allowing files to be stored across multiple nodes in the network. This ensures that even if a single node goes down, the file can still be accessed from other nodes.

AES-256 (Advanced Encryption Standard 256-bit) is a symmetric encryption algorithm that provides a high level of security. It's used in our system to encrypt the files before they are stored on the IPFS network, adding an extra layer of security and ensuring that only authorized users can access the files.

Together, SHA-256, IPFS, and AES-256 create a secure, efficient, and decentralized cloud file sharing system. This system ensures data integrity, availability, and confidentiality, making it an excellent solution for secure file storageand sharing.

II. LITERATURE SURVEY

In order to get required knowledge about various concepts related to the present application, existing literature was studied. Some of the important conclusions were made through those are listed below.

Mohit D Gandhi et al[1]: This system leverages cloud computing to provide a centralized platform for secure storage, sharing, and access to files over the internet, eliminating the need for physical storage devices. Key features include secure data storage, efficient file synchronization, robust access controls, and real- time collaboration capabilities. The system ensures privacy and integrity through data encryption and authentication, mitigating risks of unauthorized access or data loss. Automatic synchronization facilitates access to the latest file versions across multiple devices, promoting seamless collaboration and productivity. Keywords include file sharing, data accessibility, collaborative file sharing, document collaboration, and remote file access.

Suresh Dara et al[2]: This paper introduces an approach aimed at efficiently sharing group resources across cloud users while maintaining privacy and security. Despite the benefits of cloud computing, the challenge of securely sharing information among multiple owners persists. The proposed solution leverages the Diffe-Hellman algorithm and techniques such as group signature and dynamic broadcast encryption to enable secure data sharing among multiple owners within the cloud environment, even for rotating groups. This system allows any cloud user to anonymously share data with others while ensuring that revoking access for certain users does not increase storage overhead or encryption computation costs. Rigorous proofs are provided to assess the scheme's security, and tests are conducted to validate its effectiveness. Overall, the paper presents a promising solution for secure and efficient data sharing in multi-owner cloud environments.

Kensho Yamamoto and Toshio Hirostu[3]: The paper proposes a solution in the form of a secure cloud filesystem that addresses these issues by transparently encrypting and decrypting files during storage and retrieval. The system employs key-based encryption for individual files, with the keys securely indexed based on file paths within the cloud filesystem. This approach ensures user-friendly, secure cloud storage without requiring specialized knowledge of encryption, allowing for confidential data management and sharing across multiple cloud storage providers.

Michal Wasserbauer[4]: This study explores the role of cloud storage and IT infrastructure in file security. Using a descriptive qualitative research method, the study aims to understand how these technologies contribute to securing files. The findings reveal that cloud storage facilitates easier access to computing resources without relying on hardware disk space, enhancing file security. Additionally, a robust IT infrastructure, encompassing network, hardware,and software components, simplifies file protection and accessibility. Improving internet speed further aids in efficient file transfer, backup, and recovery in case of hardware attacks. Moreover, developing customized applications allows companies to tailor operations to their specific needs, bolstering security measures. The study also identifies employee performance, education, and competitive advantage as other influential factors in file security.

Lewis Goligthly et al[5]: Over the years organizations have heavily riled on cloud computing as a medium of storing &sharing files the to others. But public clouds aren't suitable for an organization as anyone can get access to the public clouds and Private clouds are suitable but have some disadvantages establishing physical infrastructures and when it comes to upscaling the size of cloud storage it isn't that feasible as it requires huge cost and time. By integrating blockchain technology with cloud computing scalability isn't a issue as there is no limitation of storage capacity data stored by individual users are much secured because only the encrypted hash value associated with the files are storedin the cloud servers.

Ion Zhou et al[6]: The proposed Privacy-Preserving Peer-Review System (P3ERS) advocates for a blockchain-based approach to distribute trust among authors and reviewers, mitigating bias and addressing reviewers' opportunity costs. The architecture includes a blockchain system for file storage and access, introducing AcadCoin, a digital currency, to alleviate reviewers' costs. Essential components involve the system admin, network updates, and the integration of cryptocurrency. To prevent human errors in the blockchain operation, custom resource states and variables are defined.

Tiago Olivera et al[7]: The widespread use of cloud storage in the last few years can be attributed to the existence of appealing applications such as file backup, data archival and file sharing. File sharing in particular, is implemented in different ways by distinct cloud storage services. But since here the security is handed over to a third party service provider the users data is still vulnerable to data thefts which can lead to leakage of some confidential organization data. But it is not an issues when it comes to blockchain based cloud file sharing service as it follows decentralized architecture thus eliminating any chances of data thefts.

Deepak Guled et al[8]: Security is one of the most important factor when it comes to maintaining data secrecy and also confidentiality and Data Encryption Standard(DES) is used by these researchers for the purpose of encryption and decryption of data. DES is basically a asymmetric cryptographic key generation technique which involves much complex mathematical equations and requires huge computational cost and also has some performance issues when compared to Advanced Encryption Standards(AES).

2.1 Literature review summary

These literature surveys focuses on the integration of blockchain technology with cloud computing for secure file sharing, utilizing SHA-256, IPFS, and AES-128 encryption. Blockchain ensures data integrity and security, while IPFS decentralizes file storage, eliminating single points of failure. AES-128 encryption further strengthens data confidentiality. The combination of these technologies provides a robust solution for secure and efficient file sharing in cloud environments. Studies suggest that integrating blockchain with cloud computing enhances scalability, security, and data integrity, making it an appealing option for organizations seeking secure file sharing solutions.

III. PROPOSED SYSTEM

The proposed blockchain-based file sharing system is designed to revolutionize digital content distribution by leveraging the decentralized, immutable nature of blockchain technology. Users can securely upload, share, and access files through smart contracts, ensuring transparency, traceability, and tamper-proof transactions. The system employs a distributed ledger to record file ownership, permissions, transactions, eliminating need for centralized authorities and reducing the risk of data manipulation.

IV. METHODOLOGY

- **User Authentication and Authorization:**
  - Users log in to the system using their credentials (username/password or cryptographic keys).
  - The system verifies the user's identity and permissions stored in the blockchain.
- **File Upload:**
  - Users select a file to upload through the user interface.
  - The file is encrypted using the AES-128 algorithm with a unique key.
  - The encrypted file is divided into smaller chunks, each typically around 256 KB to 1 MB in size.
- **File Chunking and Hashing:**
  - Each file chunk is hashed using the SHA-256 algorithm to create a unique identifier (hash) for the chunk.
  - The hashes are used to verify the integrity of the file during download and to locate the file chunks on IPFS.

- **File Encryption:**
    - AES-128 encryption ensures that the file content is secure and can only be decrypted with the corresponding AES-128 key.
- **File Storage on IPFS:**
    - The encrypted file chunks are uploaded to the IPFS network using the IPFS API.
    - IPFS provides a distributed storage solution, and each chunk is stored on multiple IPFS nodes to ensureredundancy and availability.
- **Metadata and File Tracking on Blockchain:**
    - Metadata about the file (e.g., file name, owner, permissions, IPFS hash of each chunk) is stored in a smartcontract on the blockchain.
    - The smart contract also keeps track of who has access to the file and any updates to its permissions.
- **Blockchain Transaction:**
    - A transaction is created and added to the blockchain whenever a file is uploaded or its permissions areupdated.
    - The transaction includes details such as the file's metadata and IPFS hashes of its chunks.
- **File Sharing:**
    - Users can share files by updating the smart contract with the recipient's public key or username and thepermissions granted.
    - The file is encrypted using the recipient's public key before being shared, ensuring that only the recipientcan decrypt and access the file.
- **File Download and Decryption:**
    - To download a file, the user requests the file's metadata and IPFS hashes from the blockchain.
    - The file chunks are fetched from IPFS using the IPFS API and assembled into the original file.
    - The file is decrypted using the AES-128 key associated with the file.
- **Access Control and Permissions:**
    - Access control is enforced by the smart contract, which checks the permissions of the user requestingaccess to the file.
    - Permissions can be updated by the file owner or users with the appropriate privileges.
- **Audit Trail and Logging:**
    - All file-related actions (upload, download, share) are logged in the blockchain for auditing purposes.
    - Audit logs include details such as the user performing the action, the file affected, and the time of theaction.

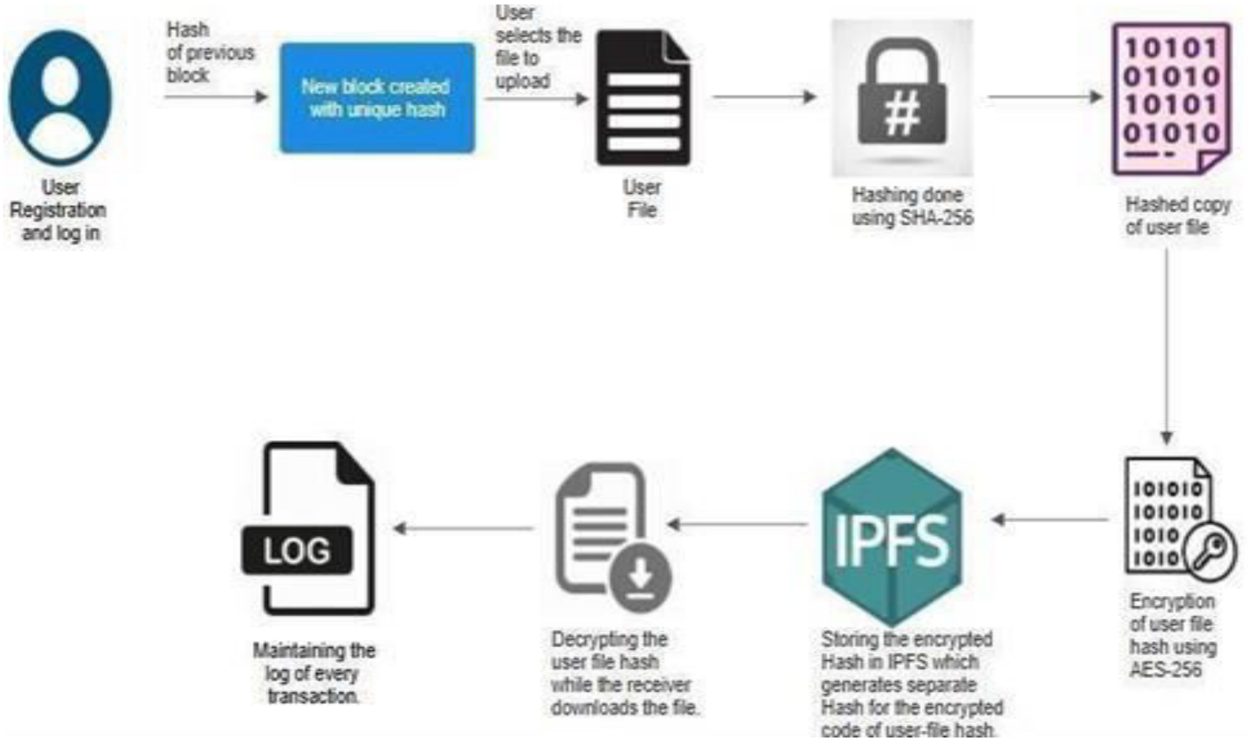
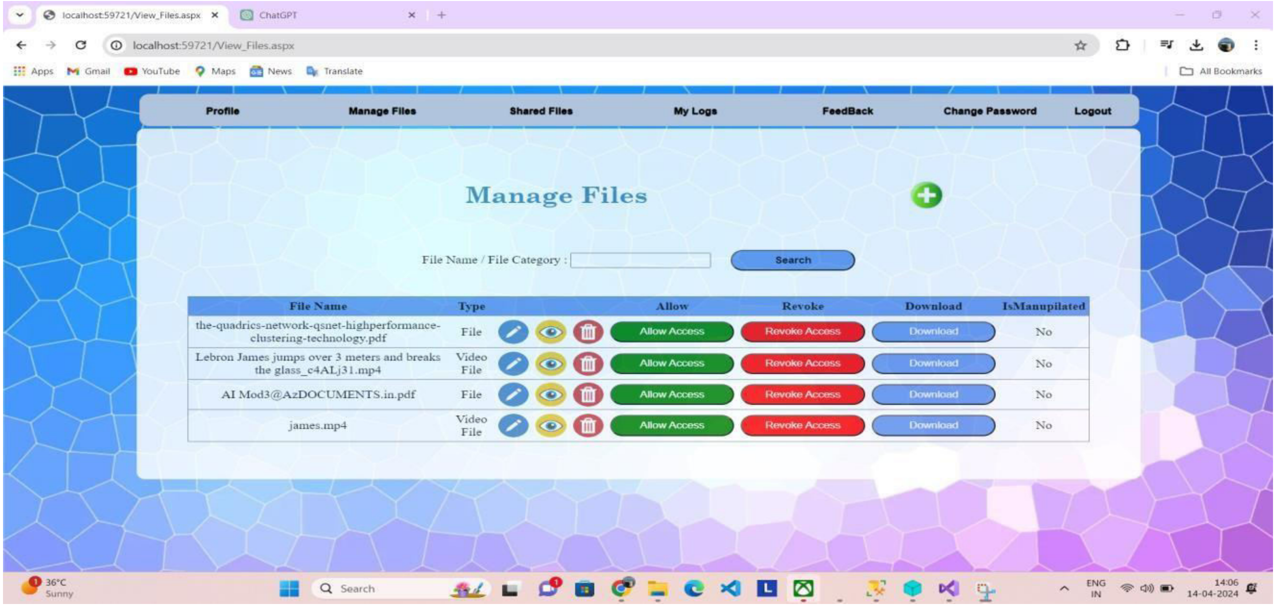

User Registration and log in
Hash of previous block
New block created with unique hash
User selects the file to upload
User File
Hashing done using SHA-256
10101
01010
10101
01010
Hashed copy of user file
Encryption of user file hash using AES-256
IPFS
Storing the encrypted Hash in IPFS which generates separate Hash for the encrypted code of user-file hash
Decrypting the user file hash while the receiver downloads the file.
LOG
Maintaining the log of every transaction.

Fig 4.1 Workflow of the system

V. RESULTS



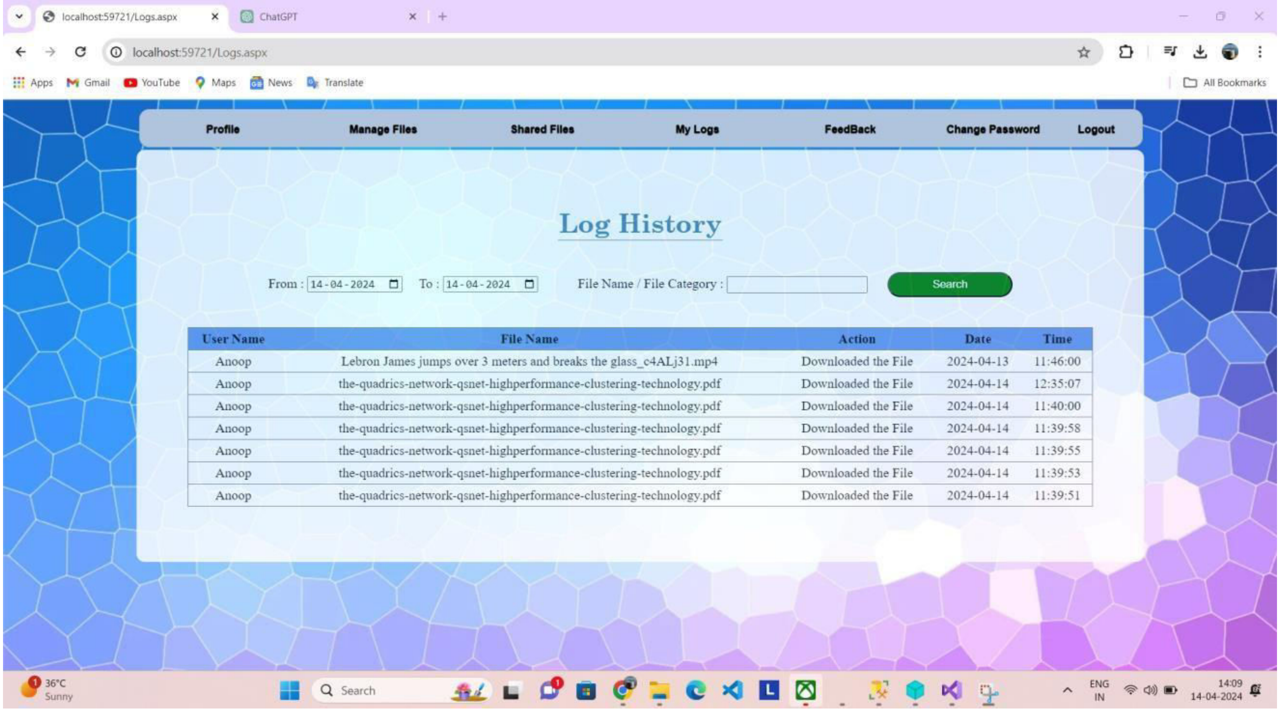
Manage Files

File Name / File Category :

Search

File Name	Type		Allow	Revoke	Download	IsManupilated
the-quadrics-network-qsnet-highperformance-clustering-technology.pdf	File	✎ 👁 🗑	Allow Access	Revoke Access	Download	No
Lebron James jumps over 3 meters and breaks the glass_c4ALj31.mp4	Video File	✎ 👁 🗑	Allow Access	Revoke Access	Download	No
AI Mod3@AzDOCUMENTS.in.pdf	File	✎ 👁 🗑	Allow Access	Revoke Access	Download	No
james.mp4	Video File	✎ 👁 🗑	Allow Access	Revoke Access	Download	No

Fig. 5.1 Manage Files

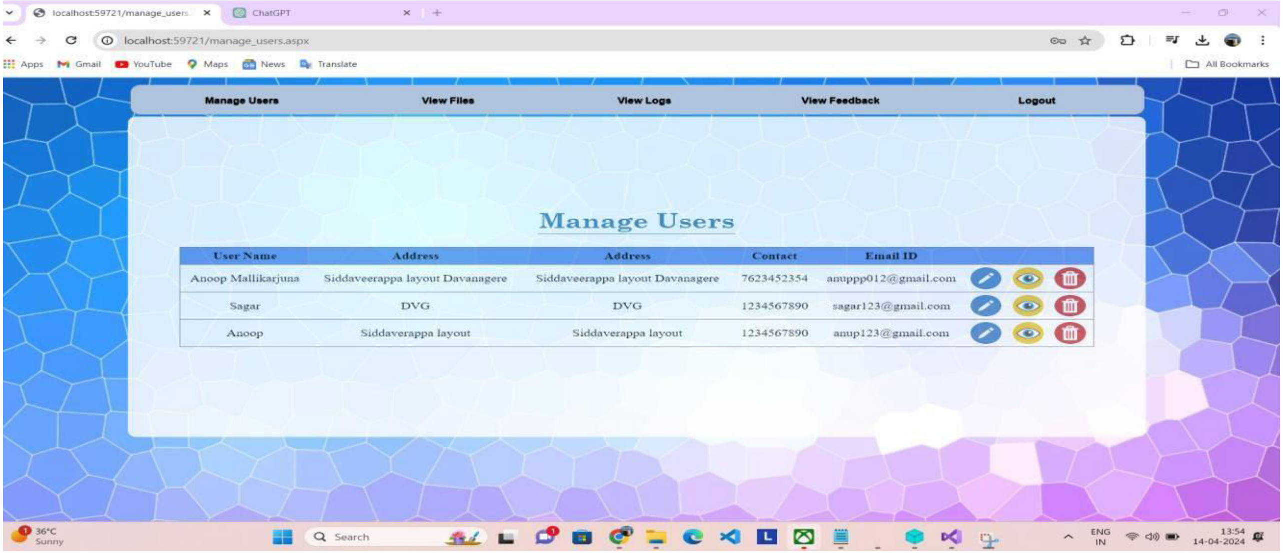


Log History

From : 14-04-2024 To : 14-04-2024 File Name / File Category : Search

User Name	File Name	Action	Date	Time
Anoop	Lebron James jumps over 3 meters and breaks the glass_c4ALj31.mp4	Downloaded the File	2024-04-13	11:46:00
Anoop	the-quadrics-network-qsnet-highperformance-clustering-technology.pdf	Downloaded the File	2024-04-14	12:35:07
Anoop	the-quadrics-network-qsnet-highperformance-clustering-technology.pdf	Downloaded the File	2024-04-14	11:40:00
Anoop	the-quadrics-network-qsnet-highperformance-clustering-technology.pdf	Downloaded the File	2024-04-14	11:39:58
Anoop	the-quadrics-network-qsnet-highperformance-clustering-technology.pdf	Downloaded the File	2024-04-14	11:39:55
Anoop	the-quadrics-network-qsnet-highperformance-clustering-technology.pdf	Downloaded the File	2024-04-14	11:39:53
Anoop	the-quadrics-network-qsnet-highperformance-clustering-technology.pdf	Downloaded the File	2024-04-14	11:39:51

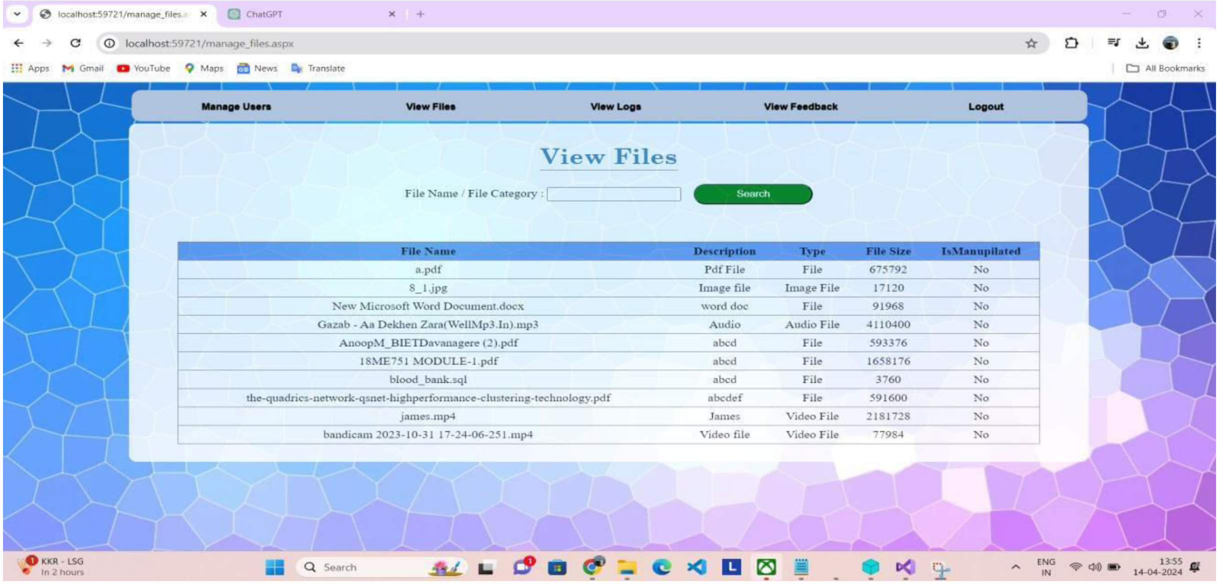
Log History



Manage Users

User Name	Address	Address	Contact	Email ID			
Anoop Mallikarjuna	Siddaveerappa layout Davanagere	Siddaveerappa layout Davanagere	7623452354	anuppp012@gmail.com	✎	👁	🗑
Sagar	DVG	DVG	1234567890	sagar123@gmail.com	✎	👁	🗑
Anoop	Siddaverappa layout	Siddaverappa layout	1234567890	anup123@gmail.com	✎	👁	🗑

Fig. 5.3 Manage Users



View Files

File Name / File Category :

Search

File Name	Description	Type	File Size	IsManupilated
a.pdf	Pdf File	File	675792	No
8_1.jpg	Image file	Image File	17120	No
New Microsoft Word Document.docx	word doc	File	91968	No
Gazab - Aa Dekhen Zara(WellMp3.In).mp3	Audio	Audio File	4110400	No
AnoopM_BIETDavanagere (2).pdf	abcd	File	593376	No
18ME751 MODULE-1.pdf	abcd	File	1658176	No
blood_bank.sql	abcd	File	3760	No
the-quadrics-network-qsnet-highperformance-clustering-technology.pdf	abcdef	File	591600	No
james.mp4	James	Video File	2181728	No
bandicam 2023-10-31 17-24-06-251.mp4	Video file	Video File	77984	No

Fig 5.4 View Files

VI. CONCLUSION AND FUTURE WORK

In conclusion, a blockchain-based cloud file sharing system using SHA-256 for hashing, IPFS for decentralized storage, and AES-256 for encryption represents a significant advancement in secure and efficient data storage and sharing. The use of SHA-256 ensures the integrity of data by generating a unique hash for each file or block of data. IPFS provides a decentralized storage solution, ensuring data availability even if a single node goes down. The application of AES-256 encryption adds an extra layer of security, ensuring that only authorized users can access the files. This system leverages the strengths of blockchain technology, including decentralization, transparency, and security, to overcome the limitations of traditional cloud storage systems. It offers potential benefits such as enhanced data security, improved privacy, reduced reliance on a single provider, and increased control over data. However, there is room for future enhancement, such as implementing smart contracts for more complex access control and exploring scalability options to accommodate a larger user base. Additionally, integration with other blockchain-based services and technologies could further enhance the system's functionality and security. Overall, the integration of blockchain technology with cloud file sharing systems opens up new possibilities for secure and efficient data storage and sharing.

REFERENCES

1. Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities Author: Imran Bashir
2. “Cloud based file sharing system” by Mohit D Gandhi, Sagar K Jain and Roopashree C S, 7th July 2023
3. “Secure cloud storage privacy-preserving in public auditing” by Suresh Dara, K. Poojitha,I. Shanti, K.V. S. Rushitha, V. Saikavya, 3rd May 2023
4. “File System to support secure cloud based sharing” by Kensho Yamamoto and Toshio Hirostu, 23rd March 2023
5. “Determination of cloud storage and IT infrastructure on file security” by Michal Wasserbauer, 30th March 2023
6. “Adoption of cloud computing as innovation in the organization” by Lewis Goligthly, Victor Chang, and Ben SC Liu , 31st May 2022.
7. “Blockchain based file sharing system” by Ion Zhou, Imran Makhdoom, Mehran Abolhasan, 2019
8. “Sharing files using Cloud Storage Services” by Tiago Olivera, Ricardo and Alysson S Bessani, 24th February 2019.

9. “Implementation of Data encryption and decryption using DES algorithm” by Deepak Guled, Nagaraj Angadi, Soumya Gali, Vidya M and Deepti Raj, 20th Jan 2019
10. Cloud Storage Forensics By Darren Quick, Ben Martini, and Raymond Choo
11. Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, Shahed Latif