SECURE FILE SHARING SYSTEM

King Saud University College of Applied Studies and Community Service

MAY 10, 2024

Contents

Executive Summary

Secure file sharing is an essential aspect of modern information exchange, particularly within organizational contexts where sensitive data must be safeguarded from unauthorized access. Traditional file sharing methods often lack robust access control mechanisms, leaving them vulnerable to security breaches. This project aims to address these vulnerabilities by developing a secure file sharing system with stringent access controls.

Utilizing advanced encryption algorithms such as AES and RSA, along with hashing techniques, the system ensures that files are protected both during transmission and at rest. Authentication mechanisms, including multi-factor authentication and biometric verification, bolster security by verifying user identities. Access control policies, implemented through role-based access control (RBAC) and attribute-based access control (ABAC), restrict file access to authorized users only.

The methodology involves a combination of technologies, including blockchain for decentralized and tamper-resistant transaction recording, and the Inter Planetary File System (IPFS) for decentralized storage and retrieval of large files. The system architecture incorporates components such as the IPFS proxy for distributed access control and group key management, enhancing security and scalability, IPFS Server for securing and storing uploaded files, a proxy server responsible for communicating between IPFS, storage and application and Solidity contracts for interacting with user operations and storing results on blockchain.

This report presents the motivation, problem definition, objectives, previous work, access control mechanisms, encryption algorithms, code preview, and references for the secure file sharing system. By implementing these measures, organizations can ensure the confidentiality, integrity, and availability of shared files, mitigating the risks associated with unauthorized access and insider threats.

Introduction

In the contemporary digital landscape, the exchange of information is ubiquitous, driving the need for secure file sharing systems to protect sensitive data from unauthorized access. Access control plays a pivotal role in ensuring that only authorized individuals can access and manipulate files within computer systems and networks. However, conventional file sharing methods often fall short in providing adequate security measures, leaving organizations vulnerable to various threats.

This report presents a comprehensive solution to the challenges of secure file sharing by introducing a system that incorporates robust access control mechanisms, advanced encryption algorithms, and decentralized storage technologies. By addressing inadequacies in encryption, authentication, access control, vulnerabilities in file transfer protocols, and insider threats, the system aims to fortify the security posture of organizations and mitigate risks associated with unauthorized access to sensitive information.

Drawing upon technologies such as blockchain and IPFS, the proposed system offers a decentralized and tamper-resistant platform for secure file sharing. Through a combination of encryption, authentication, and access control measures, the system ensures the confidentiality, integrity, and availability of shared files while minimizing the potential for security breaches.

Proposed Solution Architecture

This was the proposed solution architecture for securing the file sharing utilizing inter-planetary file system and blockchain.

Main architecture included uploading of files by group owner or members on IPFS storage utilizing file encryption mechanism from IPFS proxy and storing the file hashes on local ganache blockchain. This way the encrypted files were shared within group securely where it was stored on local IPFS storage and on local ganache blockchain.

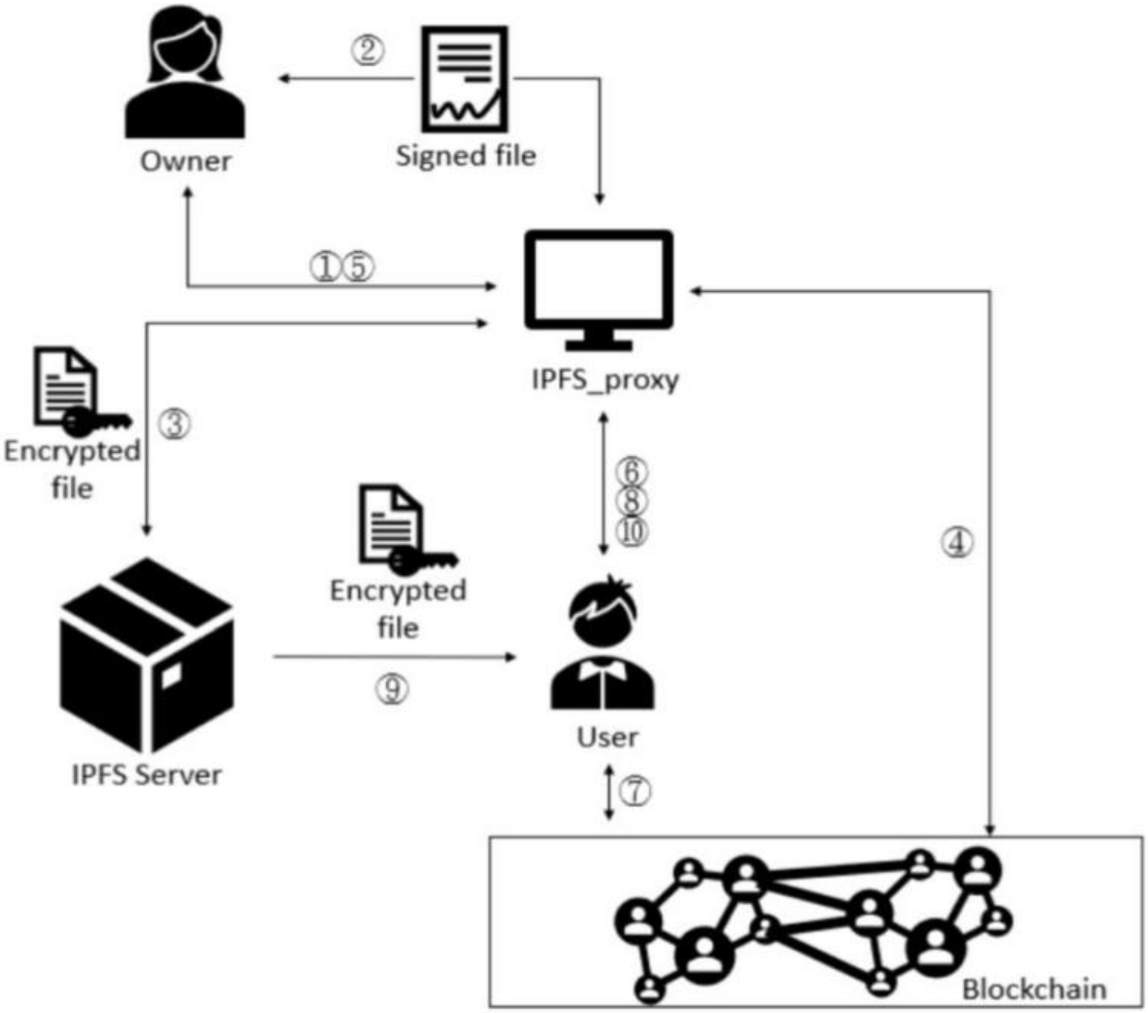


Figure 1. Overview of the proposed secure file sharing system

Technologies Utilized for Development

Following is the tech stack or technologies that we have utilized for the implementation if this secure file sharing protocol:

1. MetaMask: Your Wallet to store accounts information by connecting with local blockchain and providing test accounts for testing operations developed in the solution.
2. Ganache: Local Blockchain to provide accounts with public and private keys for MetaMask to run operations developed in the solution on the local blockchain.

3. IPFS Desktop: Locally hosted inter planetary file system to securely store uploaded files by accounts imported in MetaMask from ganache in from the application.
4. Node Js: As a backend service to communicate between IPFS storage and front end application. Working as the IPFS Proxy as described in the proposed solution.
5. React JS Web3, ethers: Frontend application developed as a center of attraction for every component of the application and is responsible for communicating operations between user and solidity contract deployed on local ganache blockchain. Working as IPFs UI.
6. Hardhat Contract Setup: Utilizing hardhat for deploying custom written solidity contract on local blockchain and communicating with IPFS UI utilizing contract address and address byte code of deployed solidity contract.

- MetaMask accounts imported from ganache will be acting as owners and members of a certain group.
- IPFS proxy or node Js backend developed will be responsible for communicating uploading and retrieval of encrypted files on IPFS, communicating with local API for groups and users regular pupation and encryption and decryption of uploaded and retrieved data utilizing public and private group keys and AEs keys for data encryption.
- IPFS Desktop will be acting as IPFS server to store the encrypted files on blockchain.
- Hardhat solidity contract is serving as uploaded encrypted files storage on blockchain.

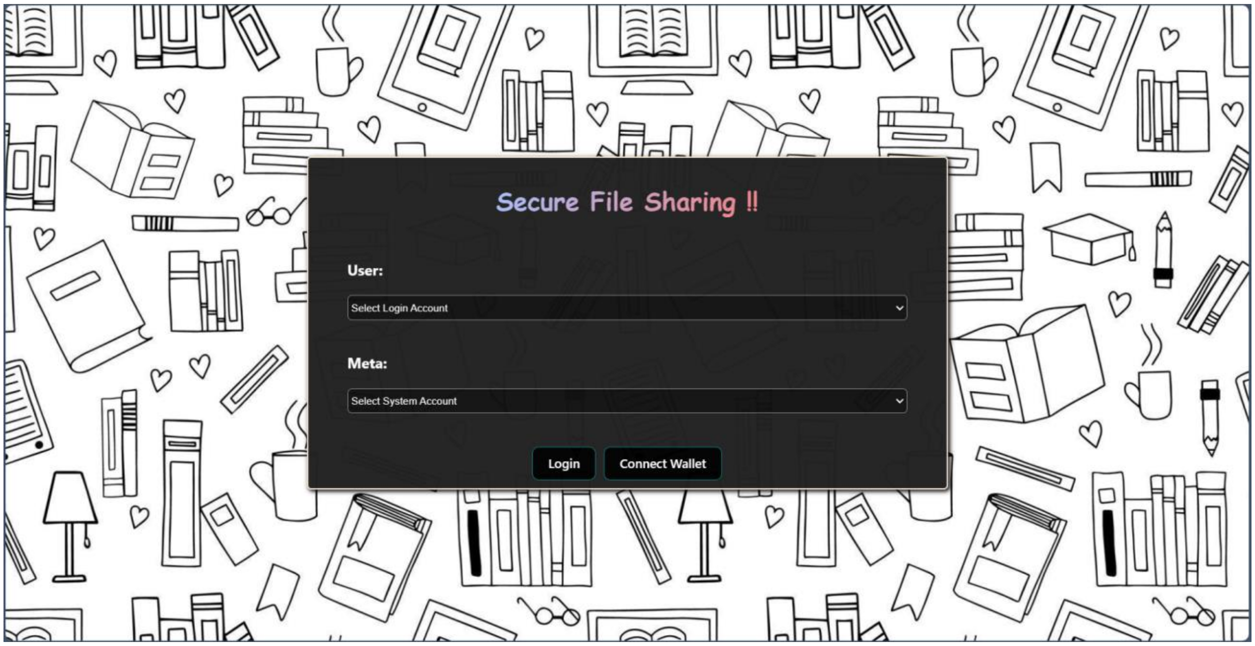
Solution Overview:

Let’s start with running our application and step by step guiding you through the solution of securing file sharing system implemented utilizing this trend of technologies defined above. So, without any further ado let’s start with the application:

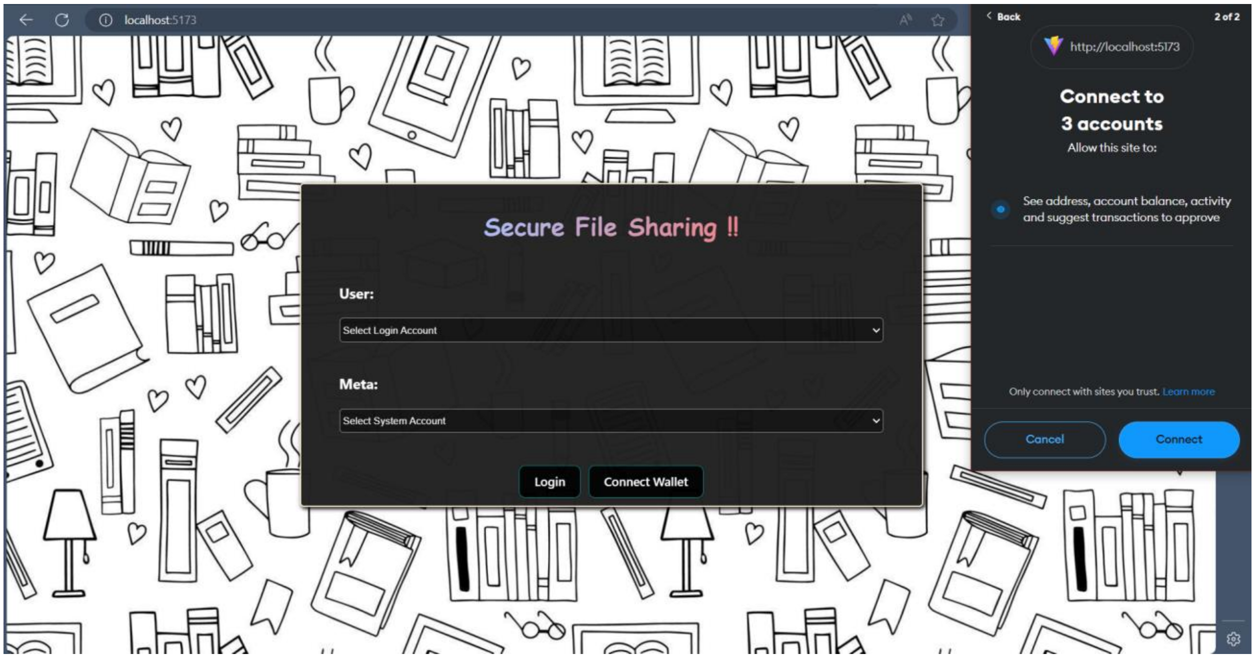
We will start by importing the MetaMask accounts into our application and then selecting those accounts to log into the application and move further.

Application Start up UI

- Importing accounts into our application using MetaMask and Ganache.



First of all user will need to connect his MetaMask Wallet by clicking connect wallet and connect any number of accounts he desires as shown below:



Connect to 3 accounts

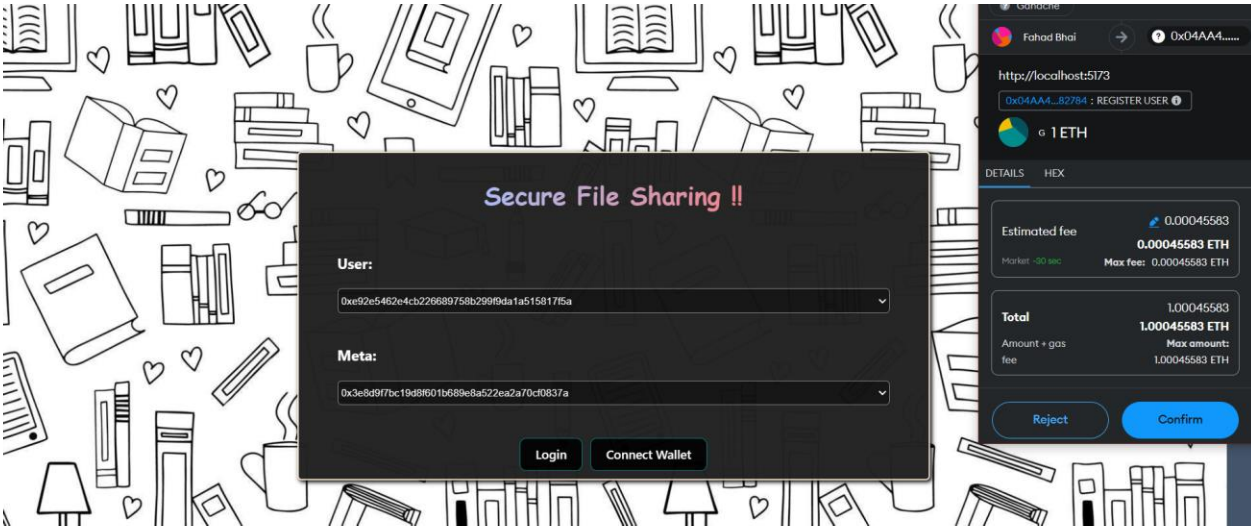
Allow this site to:

See address, account balance, activity and suggest transactions to approve

Only connect with sites you trust. Learn more

I went ahead and selected 3 accounts and used any one of those accounts to login to the application.

Logging into the application will require 1 Ethereum so create your wallet with some test money in it.



Ganache

Fahad Bhai → 0x04AA4......

http://localhost:5173

0x04AA4...82784 : REGISTER USER

G 1 ETH

DETAILS HEX

Estimated fee 0.00045583
0.00045583 ETH
Market ~30 sec Max fee: 0.00045583 ETH

Total 1.00045583
1.00045583 ETH
Amount + gas fee Max amount: 1.00045583 ETH

Reject Confirm

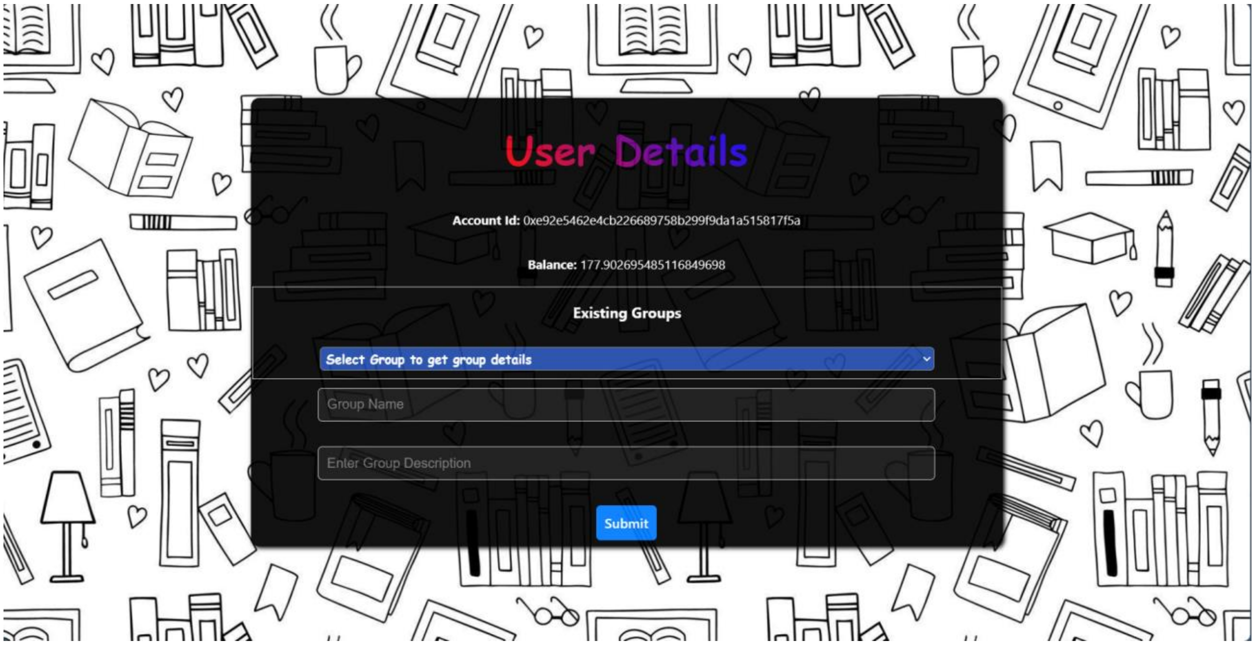
Secure File Sharing !!

User: 0xe92e5462e4cb226689758b299f9da1a515817f5a

Meta: 0x3e8d9f7bc19d8f601b689e8a522ea2a70cf0837a

Login Connect Wallet

Confirm the transaction log in and you'll see something like this:



User Details

Account Id: 0xe92e5462e4cb226689758b299f9da1a515817f5a

Balance: 177.902695485116849698

Existing Groups

Select Group to get group details

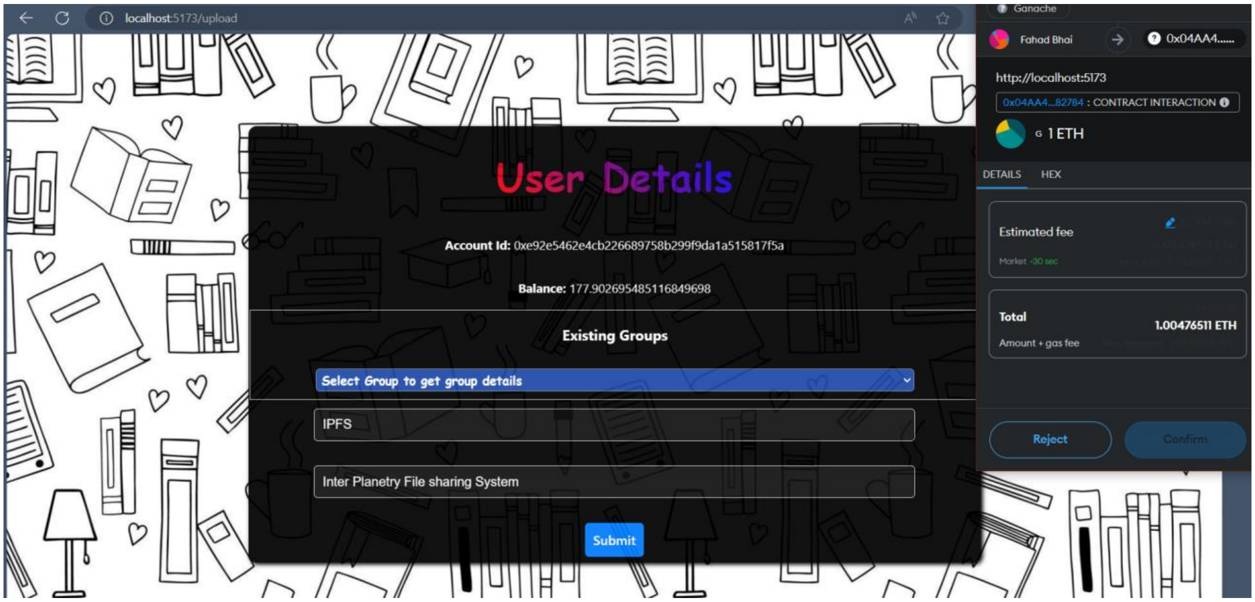
Group Name

Enter Group Description

Submit

You can select one of the previous groups or you can create a new group. Let's Create a new group by the name of IPFS and some description in it:

You will be required to confirm the transaction as this will cost you some gas since you are interacting with smart contract implemented in the code base to store the group details over the local ganache blockchain:



User Details

Account Id: 0xe92e5462e4cb226689758b299f9da1a515817f5a

Balance: 177.902695485116849698

Existing Groups

IPFS

Inter Planetry File sharing System

http://localhost:5173

0x04AA4...82784 : CONTRACT INTERACTION

1 ETH

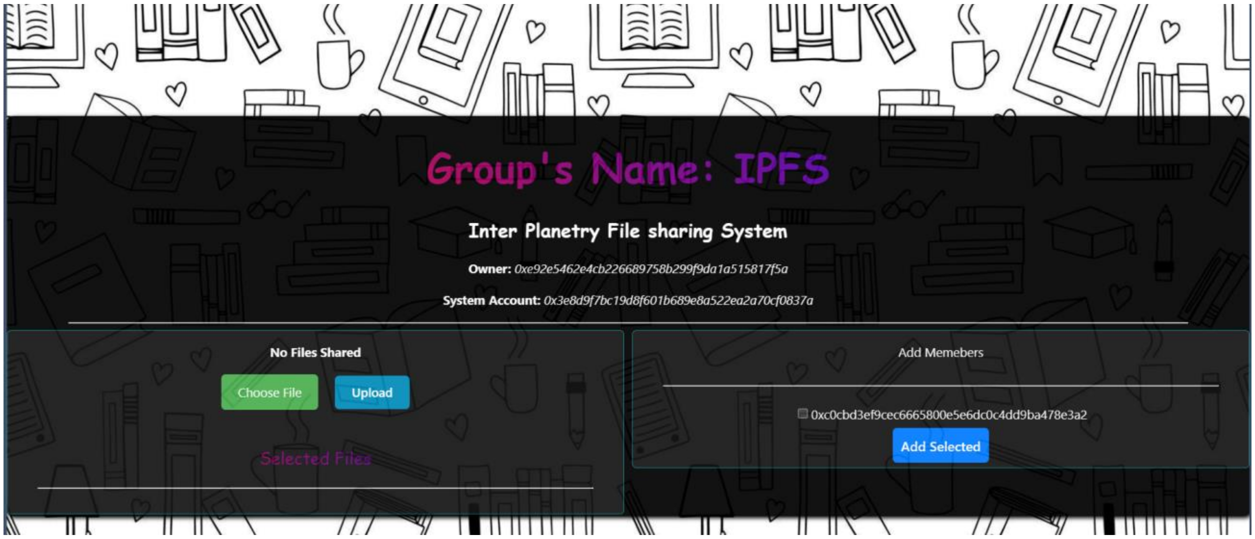
Estimated fee

Market -30 sec

Total 1.00476511 ETH

Amount + gas fee

After successfully creating group you'll be able to add members and upload files for the group:



Group's Name: IPFS

Inter Planetry File sharing System

Owner: 0xe92e5462e4cb226689758b299f9da1a515817f5a

System Account: 0x3e8d9f7bc19d8f601b689e8a522ea2a70cf0837a

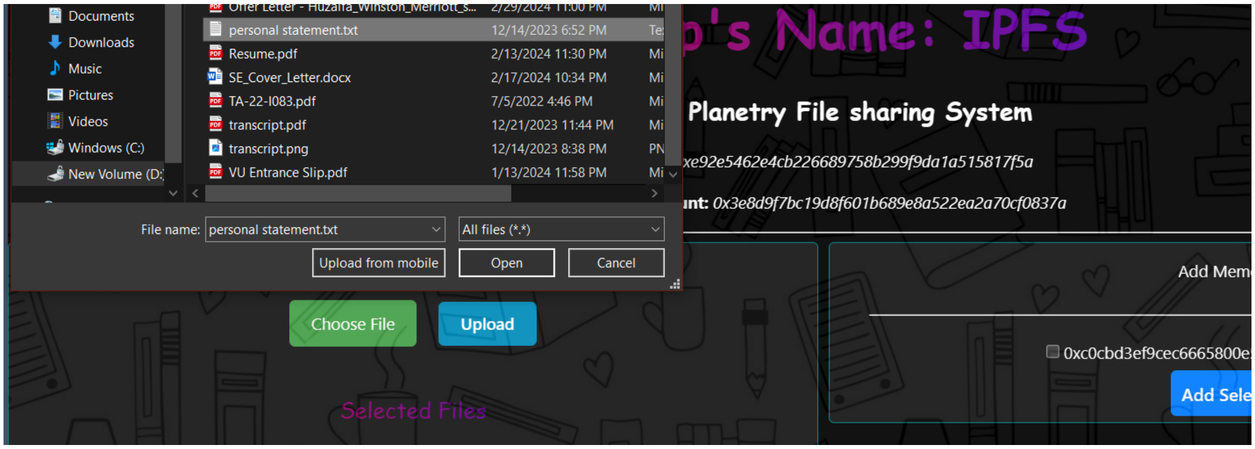
No Files Shared

Selected Files

Add Memebers

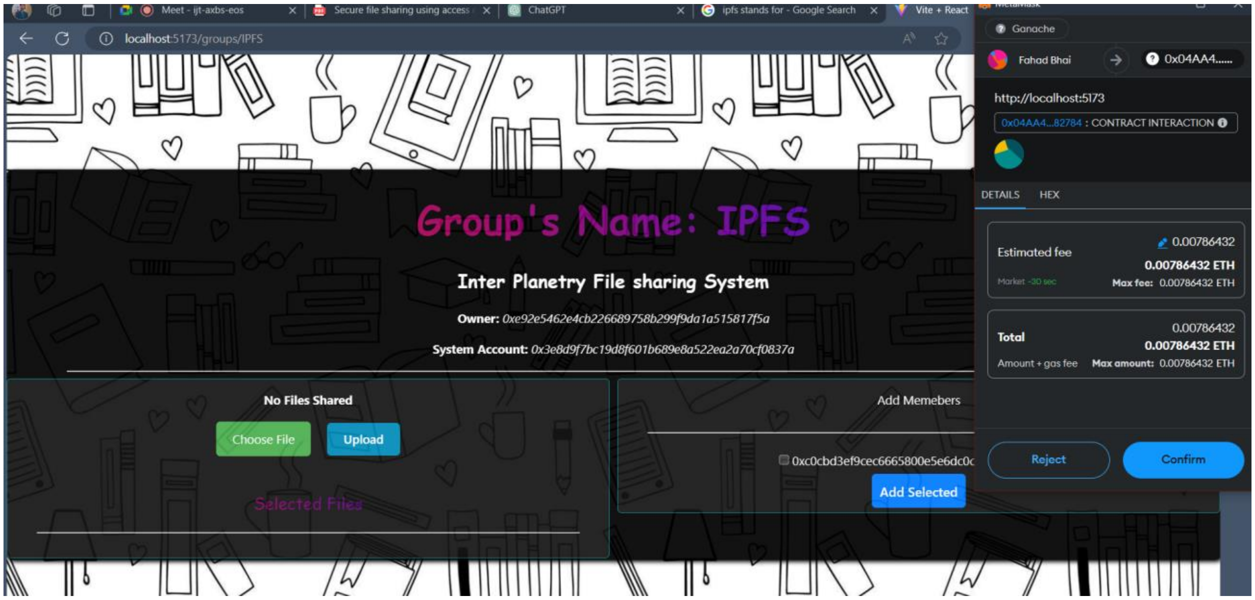
□ 0xc0cbd3ef9cec6665800e5e6dc0c4dd9ba478e3a2

As you can see above all other accounts other then login account and system account will be available for adding as members, you can upload files from your system as well:



Offer Letter - Huzaifa_Winston_Merriott_s...	2/29/2024 11:00 PM	Mi
personal statement.txt	12/14/2023 6:52 PM	Te:
Resume.pdf	2/13/2024 11:30 PM	Mi
SE_Cover_Letter.docx	2/17/2024 10:34 PM	Mi
TA-22-I083.pdf	7/5/2022 4:46 PM	Mi
transcript.pdf	12/21/2023 11:44 PM	Mi
transcript.png	12/14/2023 8:38 PM	PN
VU Entrance Slip.pdf	1/13/2024 11:58 PM	Mi

File name: personal statement.txt



localhost:5173/groups/IPFS

Group's Name: IPFS

Inter Planetry File sharing System

Owner: 0xe92e5462e4cb226689758b299f9da1a515817f5a

System Account: 0x3e8d9f7bc19d8f601b689e8a522ea2a70cf0837a

No Files Shared

Add Memebers

□ 0xc0cbd3ef9cec6665800e5e6dc0c

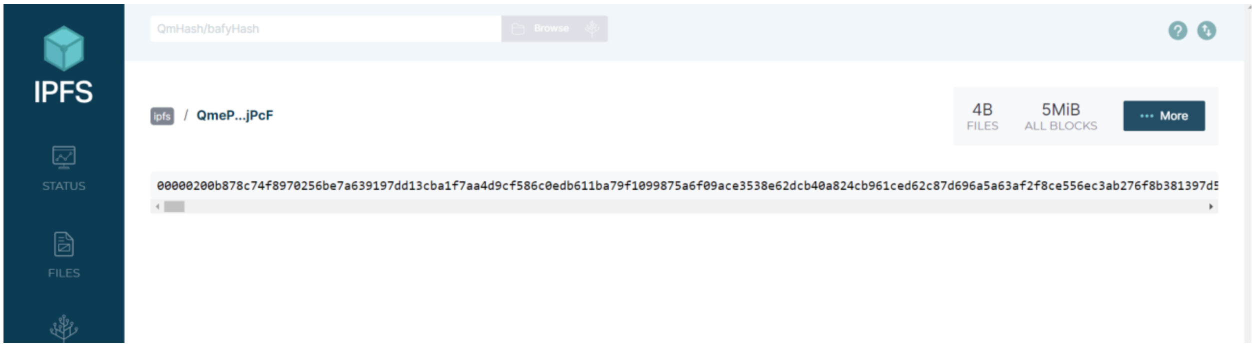
http://localhost:5173

0x04AA4...82784 : CONTRACT INTERACTION

Estimated fee 0.00786432 ETH — Max fee: 0.00786432 ETH

Total 0.00786432 ETH — Amount + gas fee — Max amount: 0.00786432 ETH

You'll have to make confirm the transaction since it is communicating with contract to upload the files on local blockchain. I can access the path to this file and check the encrypted file stored on IPFS as well.

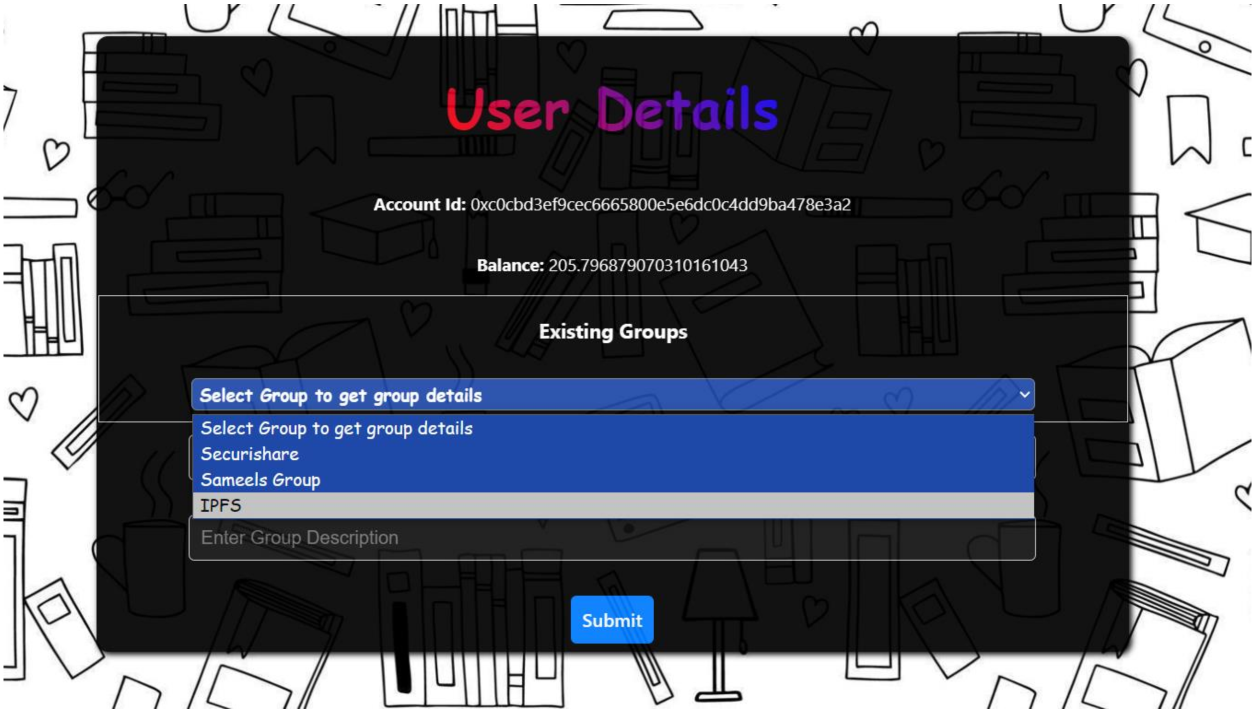


ipfs / QmeP...jPcF

```
00000200b878c74f8970256be7a639197dd13cba1f7aa4d9cf586c0edb611ba79f1099875a6f09ace3538e62dcb40a824cb961ced62c87d696a5a63af2f8ce556ec3ab276f8b381397d5
```

Now let's login in with the account of the member that we added in our group and check if we can access "personal statement.txt" or not.

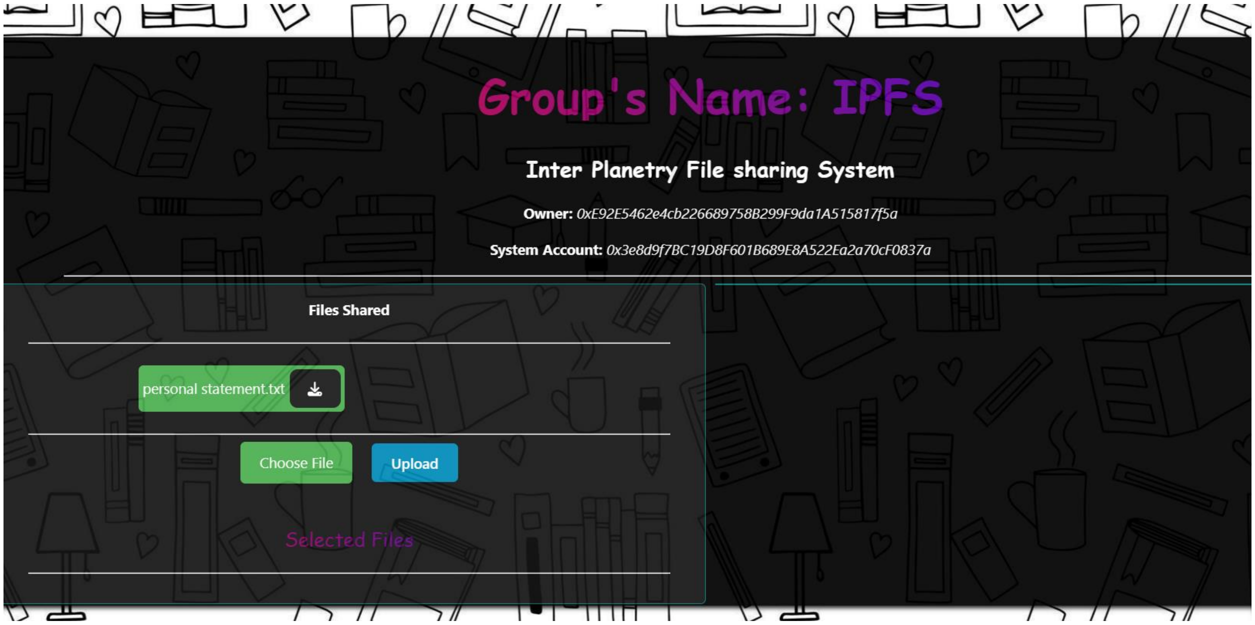
When I logged in with the above member account you can see that because the account was the member of the group he can see “**IPFS**” group in his previous groups as shown below:


User Details

Account Id: 0xc0cbd3ef9cec6665800e5e6dc0c4dd9ba478e3a2

Balance: 205.796879070310161043

Now select IPFS and see if you can see “personal statement.txt” in the uploaded files.

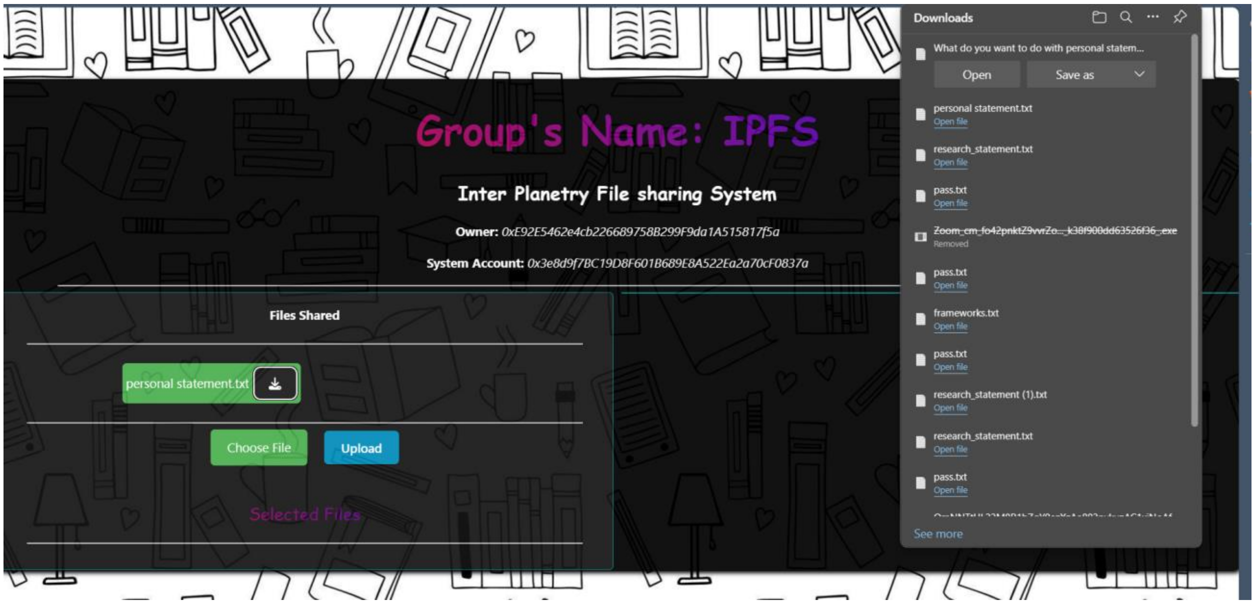

Group's Name: IPFS

Inter Planetry File sharing System

Owner: *0xE92E5462e4cb226689758B299F9da1A515817f5a*

System Account: *0x3e8d9f7BC19D8F601B689E8A522Ea2a70cF0837a*

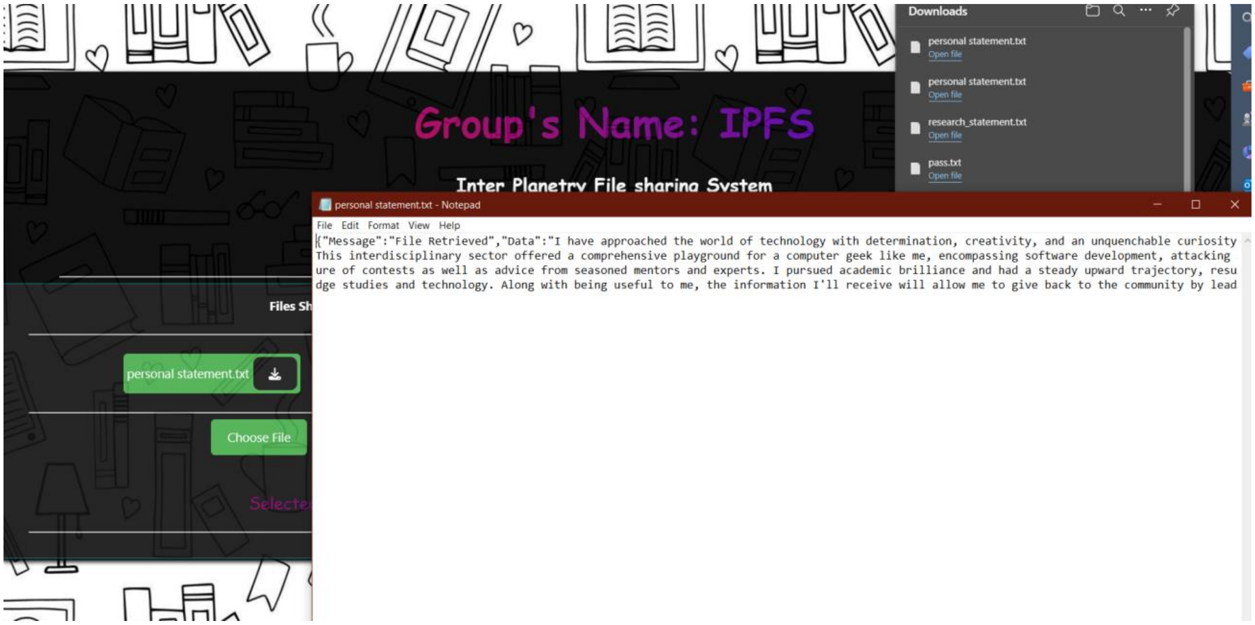
As you can see in the screenshot above that we have personal statement uploaded in the groups shared files. Let’s try to access it.



Owner: 0xE92E5462e4cb226689758B299F9da1A515817f5a

System Account: 0x3e8d9f7BC19D8F601B689E8A522Ea2a70cF0837a

As you can see that we can download the file and read its contents as well:



```
{"Message":"File Retrieved","Data":"I have approached the world of technology with determination, creativity, and an unquenchable curiosity
This interdisciplinary sector offered a comprehensive playground for a computer geek like me, encompassing software development, attacking
ure of contests as well as advice from seasoned mentors and experts. I pursued academic brilliance and had a steady upward trajectory, resu
dge studies and technology. Along with being useful to me, the information I'll receive will allow me to give back to the community by lead
```

Implementation

Implementation Explanation:

Our secure file sharing system has been meticulously crafted to provide organizations with a robust platform for safeguarding sensitive data through advanced encryption, decentralized storage, and stringent access controls. This comprehensive solution comprises several interconnected components, seamlessly integrated to ensure the confidentiality, integrity, and availability of shared files.

Smart Contract Deployment with Hardhat:

The backbone of our system lies in the smart contract deployed using Hardhat. This contract facilitates the creation of groups, addition of members, and storage of file metadata on the local Ganache blockchain. By leveraging Ethereum's blockchain technology, we ensure tamper-resistant transaction recording and decentralized control over file sharing operations.

React.js Frontend Interface:

Our frontend interface, built using React.js, provides users with intuitive access to the secure file sharing functionalities. Divided into three main pages—Home, Uploads, and Groups—the interface offers a seamless user experience. The Home page enables users to log in using their MetaMask accounts, ensuring secure authentication. The Uploads page empowers users to create groups and store group data securely on the blockchain. The Groups page allows users to upload files, add members to groups, and securely store file metadata on the blockchain.

Node.js Server for Local API Communication:

To facilitate local API requests and responses between the frontend and backend components, we've implemented a Node.js server. This server handles the synchronization of local copies of group data, member information, and file metadata. Additionally, it manages the encryption and decryption of files before storing and retrieving them from the local IPFS storage. This ensures end-to-end encryption and enhances data security.

Local Ganache Blockchain:

Our implementation utilizes a local Ganache blockchain environment for deploying Ethereum accounts and executing smart contract transactions. This local blockchain environment provides a sandboxed testing environment, enabling seamless integration testing and development iteration cycles.

Conclusion:

Through the meticulous integration of smart contracts, frontend interfaces, backend servers, and local blockchain environments, our implementation delivers a comprehensive and secure file sharing solution. By leveraging cutting-edge technologies such as Ethereum blockchain, React.js, Node.js, and IPFS, we empower organizations to protect their sensitive data and mitigate the risks associated with unauthorized access and data breaches. This professional implementation adheres to industry best practices and ensures the seamless execution of secure file sharing operations in diverse organizational contexts.