SECURE DOCS :

A DECENTRALIZED FILE ENCRYPTION, STORAGE AND SHARING PLATFORM

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

This project proposes a blockchain-based framework for secure and tamper-proof data sharing among multiple parties. Leveraging blockchain's inherent properties of decentralization, immutability, and transparency, the system aims to overcome challenges in traditional data-sharing architectures, such as centralized vulnerabilities and unauthorized access. Key components include data encryption, decentralized storage, and smart contracts for access control. These features ensure robust privacy, integrity, and accountability while providing tamper-proof audit trails. The project integrates multi-factor authentication, real-time threat intelligence, and immutable logging with alert systems to enhance security further. By combining blockchain with decentralized storage systems like IPFS and scalable smart contract solutions, the project aims to deliver a secure, transparent, and scalable data-sharing platform suitable for modern multi-party environments.

1.INTRODUCTION

1.1 Overview

This project aims to develop a blockchain-based system that ensures secure and tamper proof data sharing across multiple parties. The system will leverage blockchain technology's inherent properties of immutability, transparency, and decentralization to enable a secure data sharing platform. By incorporating data encryption, decentralized storage, and smart contracts, the system will provide robust access control and audit trails for all data access and modifications, ensuring privacy, integrity, and accountability in data transactions.

In a multi-party environment, securely sharing sensitive data while preserving its integrity is a challenge. Conventional data-sharing systems often rely on centralized architectures, making them vulnerable to data tampering, unauthorized access, and single points of failure. Furthermore, tracking data access and modifications across a distributed network in a transparent yet secure manner is complex. Therefore, there is a need for a system that enables secure, transparent, and tamper-resistant data sharing without compromising control over data access.

1.2 Motivation

Securely sharing sensitive data is a critical challenge in multi-party environments. Traditional centralized systems are vulnerable to hacking, data breaches, and single points of failure. For example, centralized servers can be targeted by attackers, compromising the confidentiality and integrity of data. Blockchain’s decentralized architecture provides a robust alternative, ensuring that no single entity has absolute control over the data. This project is motivated by the need to address these vulnerabilities by creating a secure, decentralized data-sharing platform.

2. SOFTWARE REQUIREMENTS

- **Blockchain Platform**:
  - **Ethereum**:

    Ethereum serves as the foundational blockchain platform, allowing you to deploy and interact with decentralized applications.
- **Decentralized Storage**:
  - **IPFS**:

    IPFS will be used for decentralized file storage, ensuring efficient and distributed access to files like media, documents, or other assets.
- **Encryption Techniques**:
  - **AES**:

    AES (Advanced Encryption Standard)will ensure secure data encryption and decryption for sensitive information exchanged between users or stored in off-chain systems.
- **Frontend & Backend**:
  - **Frontend**:
    - **React.js**: For building user interfaces.
    - **HTML, CSS, JavaScript**: For structure, styling, and interactivity.
  - **Backend**:
    - **Node.js**: To handle server-side logic, API requests, and blockchain integration.
- **Database**:
  - **MongoDB**:

    Use MongoDB for off-chain metadata storage, such as user profiles, logs, or transaction details that do not need to be stored on-chain.

3. Work Flow Diagram

Fig 3.1 provides a structured overview of a secure data-sharing system, highlighting key processes. It begins with User Registration and Authentication, ensuring that only authorized users can access the platform. Next, Data Encryption utilizing AES and RSA algorithms ensures data confidentiality during sharing or storage. The encrypted data is then stored securely using Decentralized Storage (IPFS) to eliminate centralized vulnerabilities. User Authorization manages access control, ensuring only permitted users can interact with specific data. Lastly, Security Audits and Data Privacy ensure the system's integrity, compliance, and trustworthiness, maintaining transparency and protecting sensitive information.

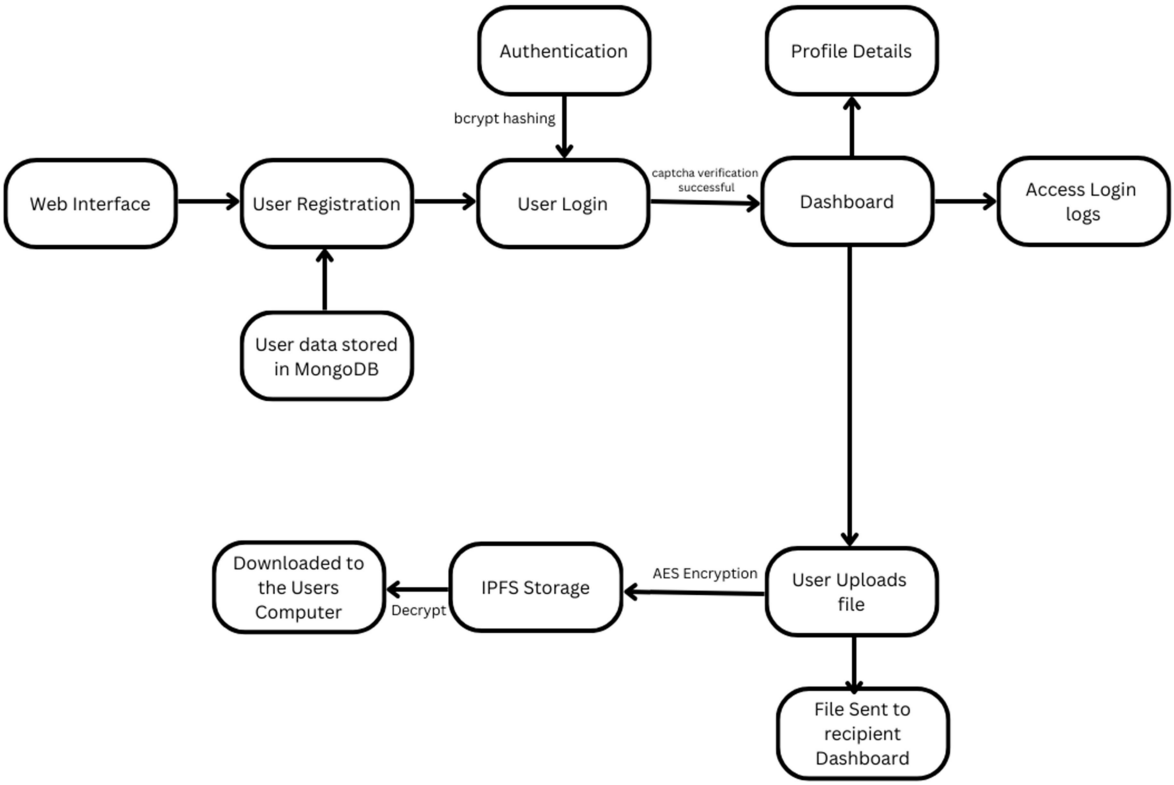

Fig 3.1: Work Flow diagram

4. DESIGN AND IMPLEMENTATION

4.1 Dashboard

Fig 4.1.1 designed to introduce the platform's purpose and core values to users. It establishes trust by highlighting security and transparency, provides a clear overview of the platform's functionality, and encourages user engagement through a call-to-action ("Get Started"). This ensures that visitors quickly understand the platform's benefits and are motivated to explore further.

Fig 4.1.1: Dashboard

4.2 Features

Fig 4.2.1 describes the various features of the application

- **Multi-Factor Authentication (MFA)**
  - Enhances security by requiring multiple verification methods (something you know, have, and are) before granting access.
- **Audit Trails**
  - Maintains a chronological record of system activities, tracking user actions and system events to enhance accountability and security.
- **Incentivized Storage**
  - Rewards participants with tokens for providing storage space, ensuring a scalable and cost-effective decentralized storage network**.**

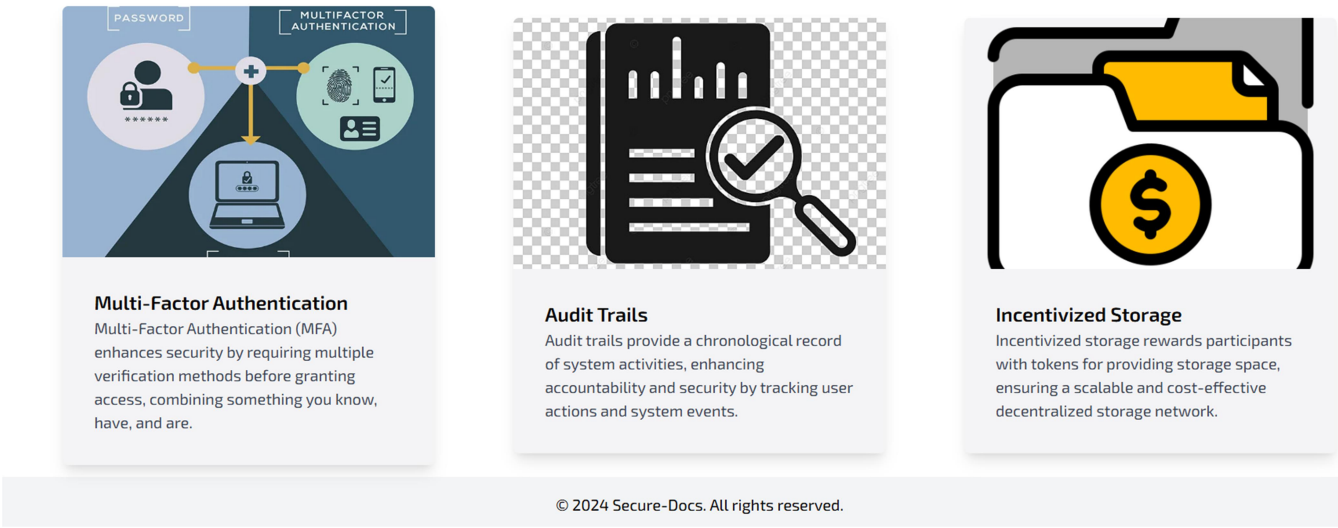

Fig 4.2.1: Features

Fig 4.2.2 describes the various features of the application

- **Data Encryption**
  - Ensures enhanced data security by encrypting data before sharing. Only authorized parties with decryption keys can access the data.
- **Decentralized Storage**
  - Distributes encrypted data across a network of nodes using blockchain technology, ensuring both security and scalability.
- **Secure File Sharing**
  - Facilitates secure file sharing by leveraging blockchain technology for transparency and security, eliminating the need for intermediaries.

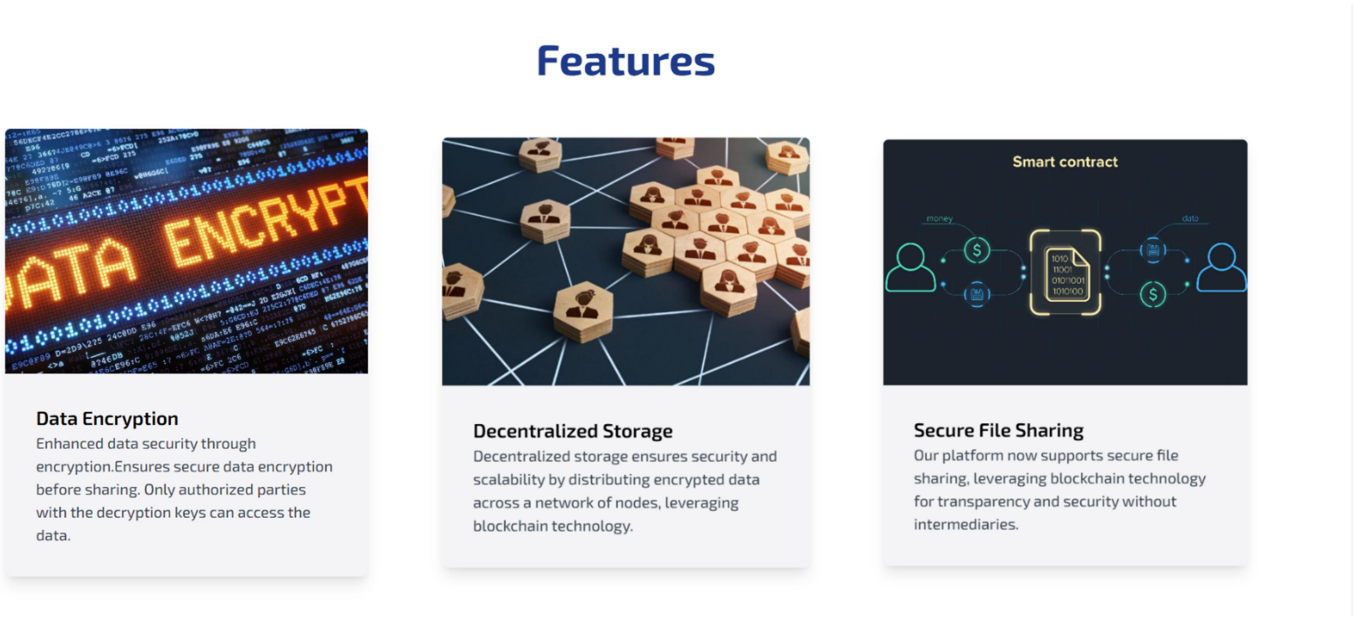

Fig 4.2.2: Features

4.3 SignUp/Register Page

Fig 4.3.1 shows the Sign-Up/Register page allows users to create an account on the platform by providing their email ID and setting a secure password. This ensures that only authenticated users can access the platform's features, maintaining security and personalized access. The "Register" button facilitates account creation, while the "Close" option provides flexibility to exit the process.

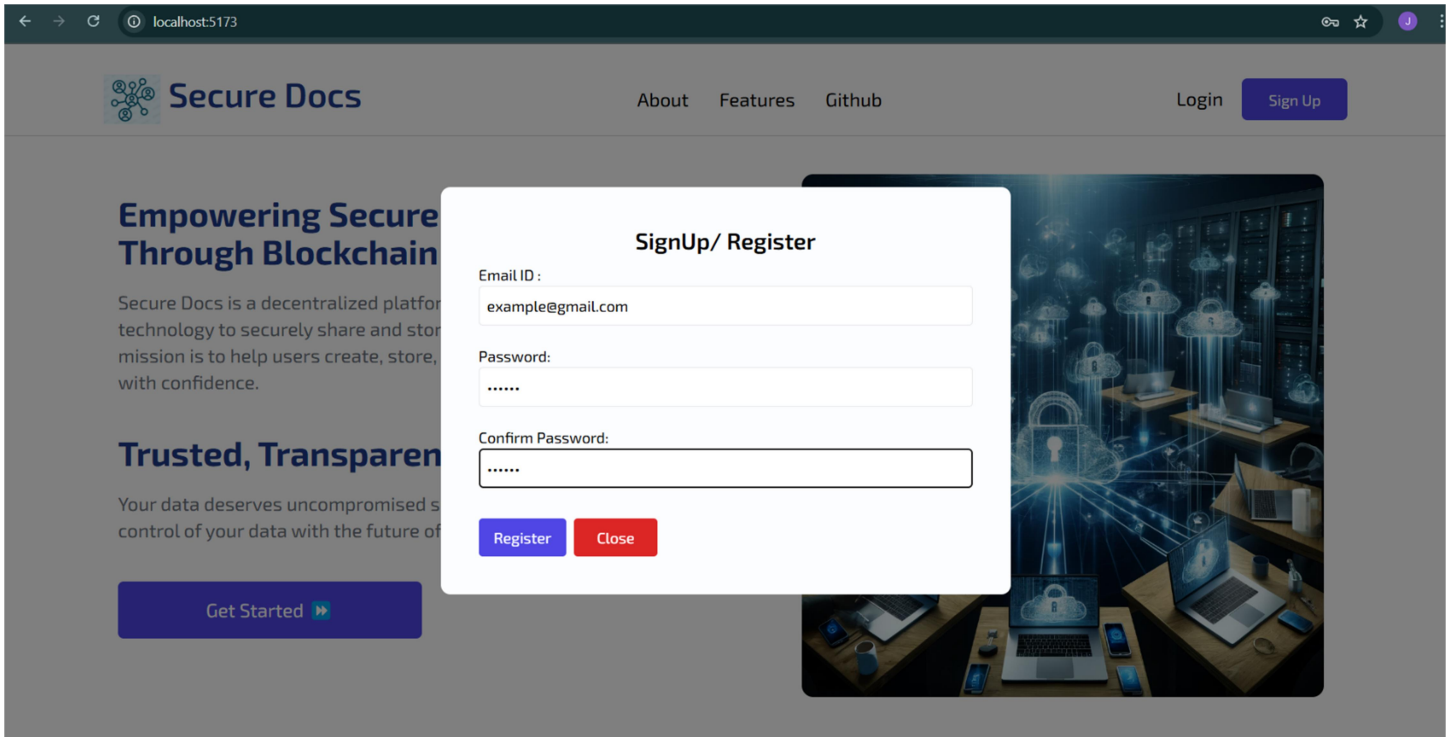

Fig 4.3.1: SignUp/Register Page

4.4 CAPTCHA Verification

4.4.1 CAPTCHA

Fig 4.4.1 shows the CAPTCHA system of the Secure Docs website which is a security feature designed to distinguish human users from bots. It requires users to select all images containing a specified object (e.g., bicycles) from a grid and click "Verify." This ensures that the login attempt is legitimate and prevents automated bots from gaining unauthorized access. By incorporating CAPTCHA, Secure Docs enhances the security of user authentication, protecting sensitive data and mitigating the risk of brute force or automated attacks. This aligns with the platform's focus on secure and transparent data management.

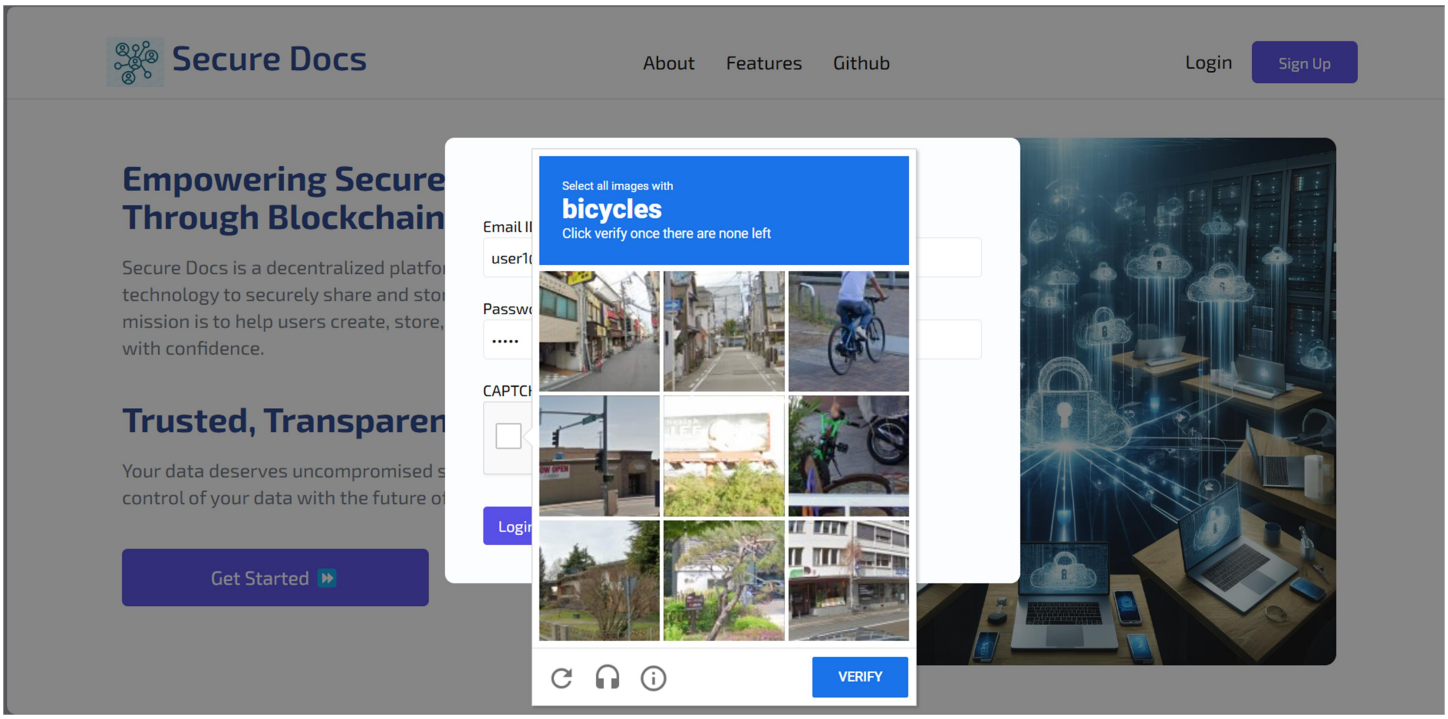

Fig 4.4.1: CAPTCHA

4.4.2 Google reCAPTCHA

Fig 4.4.2 displays the Google reCAPTCHA analytics dashboard which provides critical insights into the effectiveness of the CAPTCHA system implemented on a website. It tracks the total number of verifications, suspicious activity, and user interaction outcomes, such as successful or failed CAPTCHA attempts. This information is essential for evaluating the system's ability to differentiate between legitimate users and potential bots, ensuring secure access to the platform. By analyzing these metrics, website administrators can identify trends, monitor suspicious activity, and optimize the CAPTCHA configuration for better user experience and security. It serves as a valuable tool to maintain the integrity of a website's authentication process.

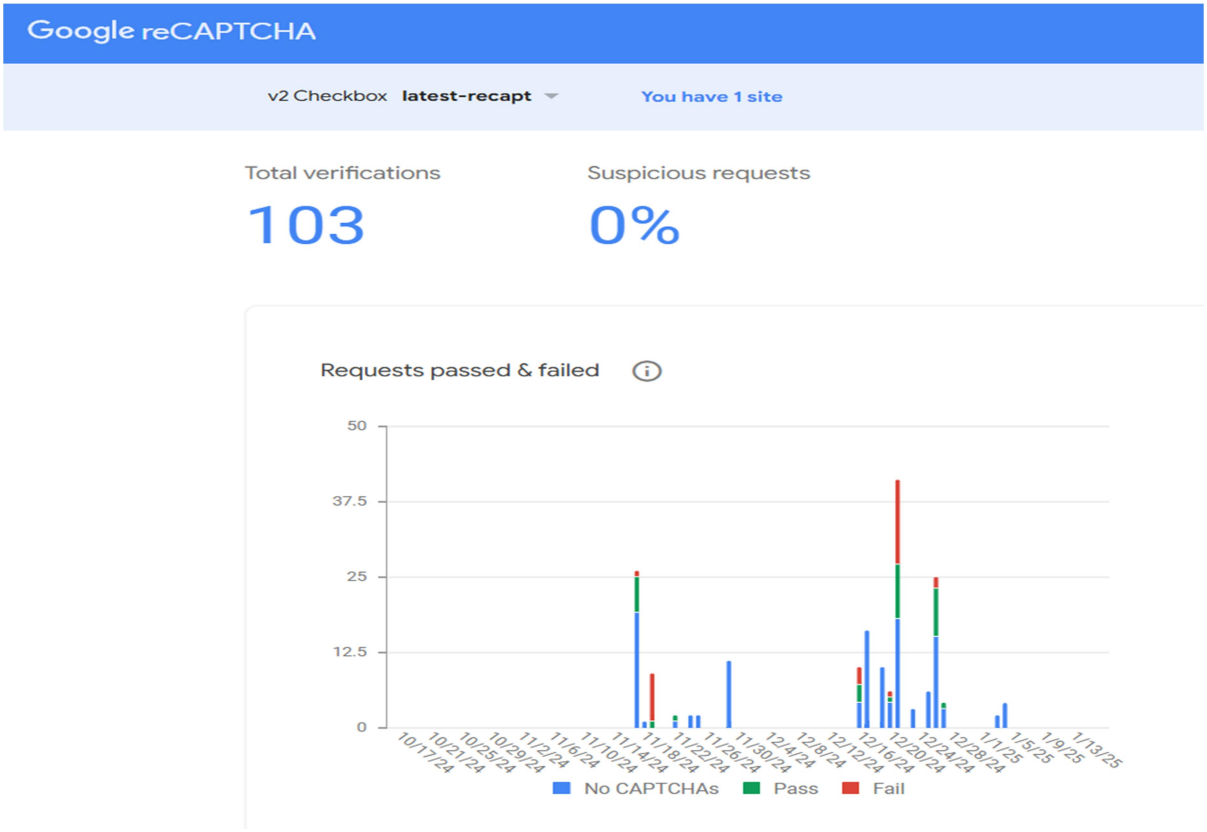

Fig 4.4.2: Google reCAPTCHA

4.5 Successful Login

Fig 4.5.1 displays the login feature of the "Secure Docs" platform ensures secure access for users by requiring their email ID, password, and CAPTCHA verification, adding an extra layer of protection against automated attacks. Upon successful authentication, a pop-up message appears with the notification "Login successful!" to confirm access and provide user feedback, enhancing the overall experience and reinforcing security assurance.

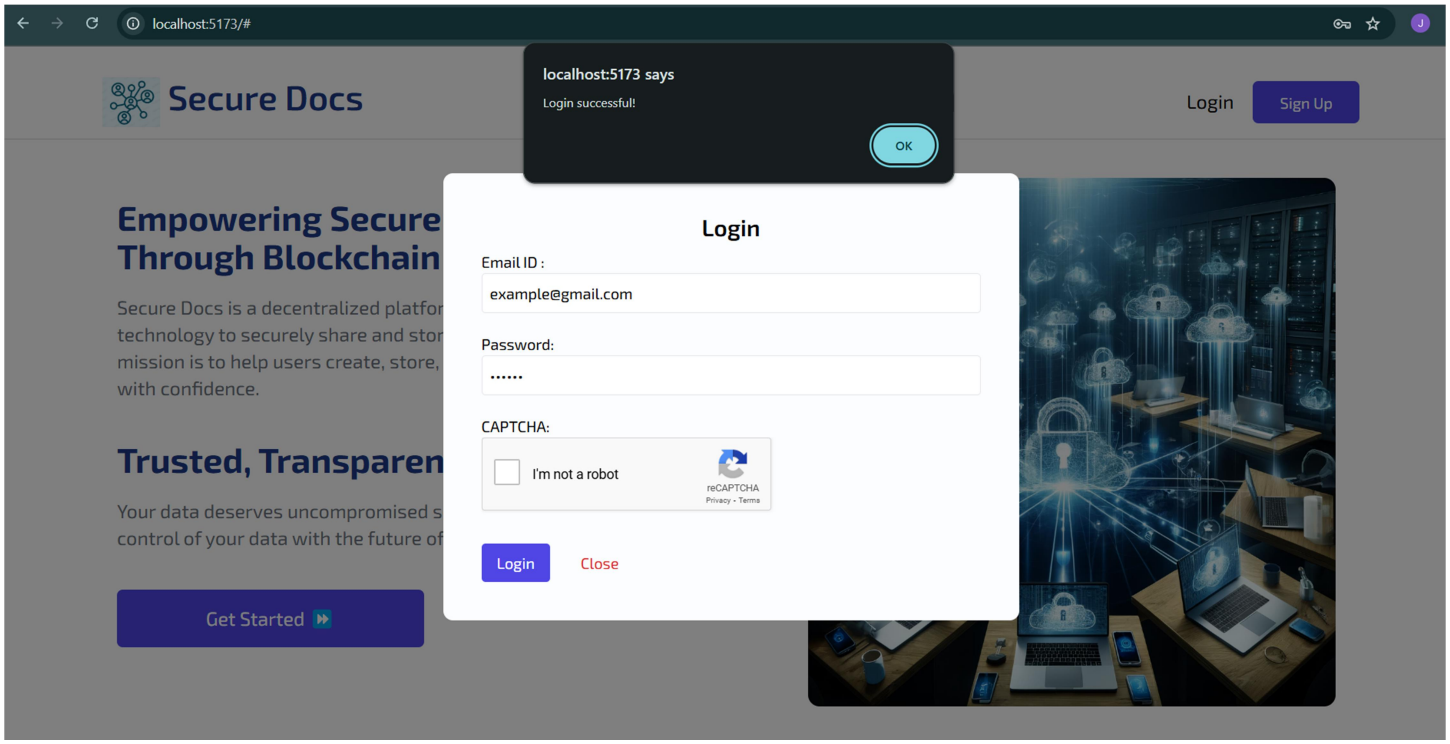

Fig 4.5.1: Successful Login

4.6 File Uploading Dashboard

Fig 3.6.1 shows the dashboard page as a user interface for managing file-related operations in a blockchain-based secure data-sharing platform. It allows users to perform essential functions, including uploading, decrypting, and sharing files securely. The page displays the user's **profile information**, such as their registered email and the date and time of account registration, establishing a personal touch for authenticated users.

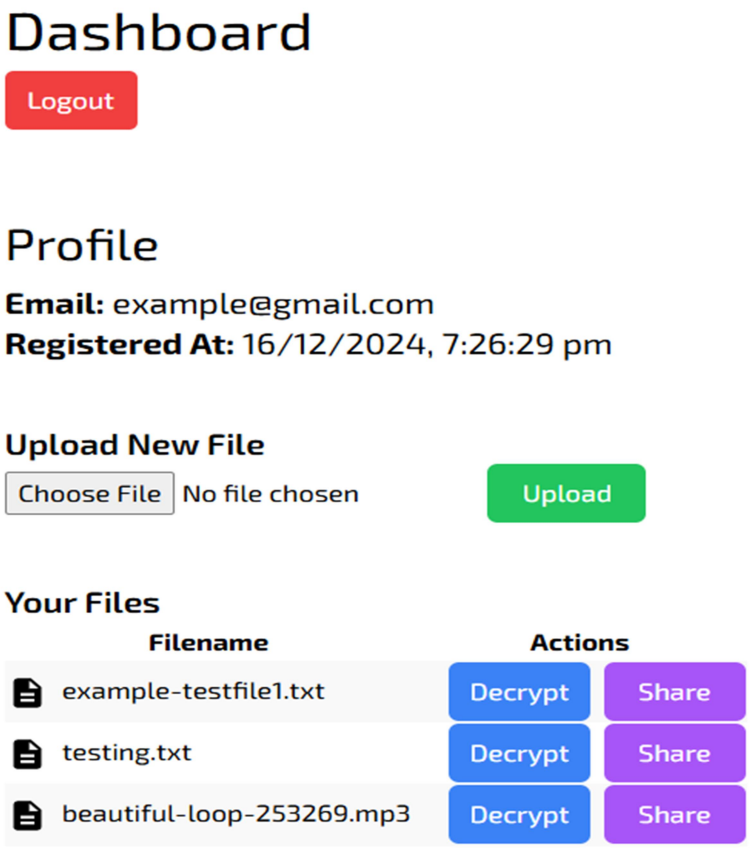

Fig 4.6.1: File Uploading Dashboard

The **file upload section** enables users to add new files to the platform using a simple "Choose File" and "Upload" button workflow. Once uploaded, files are listed under "Your Files," showing their filenames and two primary actions: **Decrypt** and **Share**. The Decrypt action allows users to decrypt files they previously encrypted, ensuring secure access to their content. The Share option facilitates secure file sharing with others while maintaining the integrity and confidentiality provided by blockchain technology.

This dashboard page serves as a centralized hub for user interaction, ensuring data security and usability through blockchain-backed operations.

4.7 IPFS Storage

Fig 4.7.1 describes about IPFS (Inter Planetary File System) storage interface used for storing uploaded files in a blockchain-based data-sharing system. The platform, powered by Pinata, allows users to manage files uploaded to the decentralized IPFS network. The key elements of the interface include:

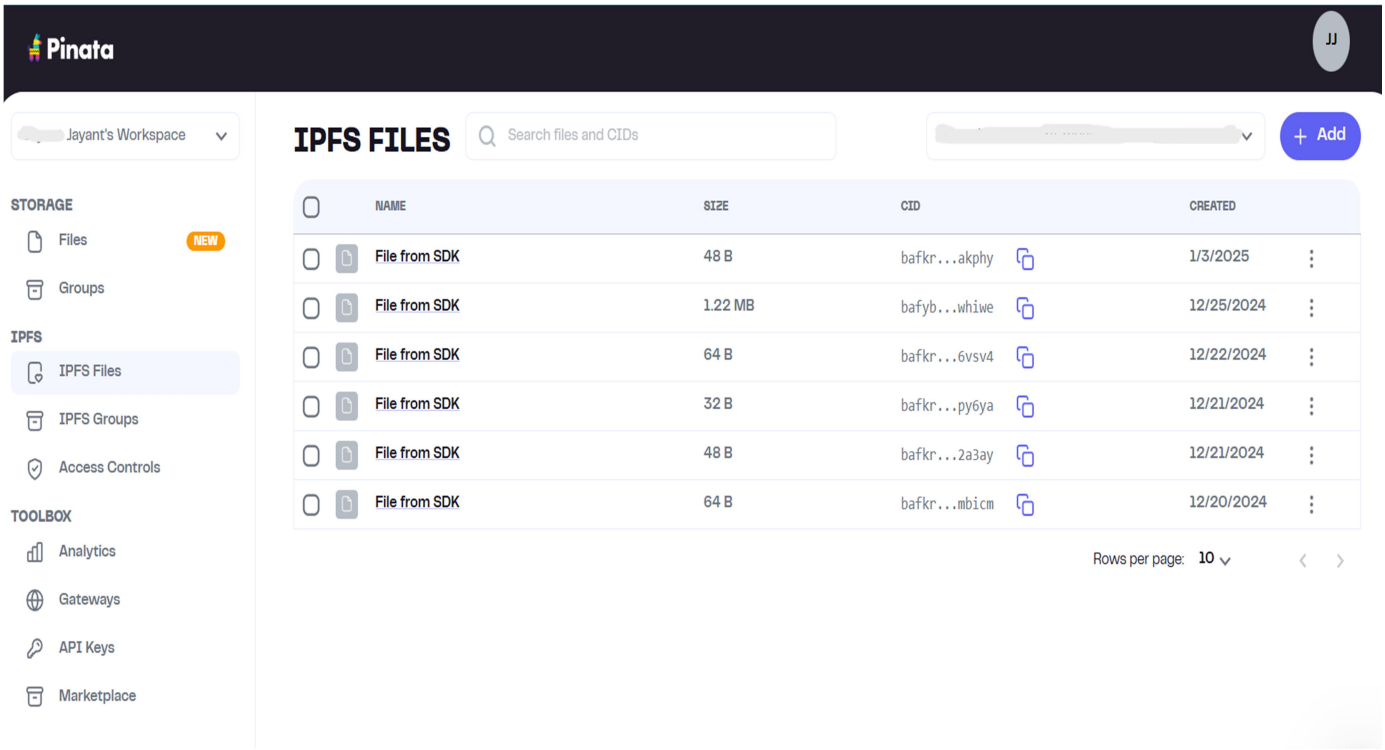

Fig 4.7.1: IPFS Storage

- **File List**: Displays the files stored in IPFS with their metadata, including:
  - Name: The name given to the files (e.g., "File from SDK").
  - Size: Indicates the file size, ranging from bytes to megabytes.
  - CID (Content Identifier): A unique identifier for each file in the IPFS network, ensuring file integrity and enabling decentralized access.
  - Created Date: Shows when each file was added to the network.

- **Functionality:**
  - The CID can be copied using the icon next to it, which allows users to retrieve the file securely via IPFS gateways.
  - Files are organized for easy access and retrieval within the user's workspace.
- **Storage Features:**
  - The left panel provides access to related functionalities, such as managing files, groups, access controls, and API keys.
  - Decentralized file storage ensures redundancy, scalability, and secure access by distributing files across the IPFS network.

This interface is essential for users to upload, store, and manage files securely in a decentralized manner, ensuring data permanence and integrity through blockchain-based storage.

4.8 Login Logs

Fig 4.8.1 shows the login logs feature which records the date and time of every user login, providing a detailed history of access to the website. This functionality enhances security by allowing monitoring of login patterns and detecting any unusual or unauthorized access. It also ensures user accountability by maintaining a transparent record of access. Additionally, the logs assist in troubleshooting user issues and support compliance with auditing and security standards. By maintaining a detailed login history, the platform reinforces trust and provides a secure environment for managing sensitive data.

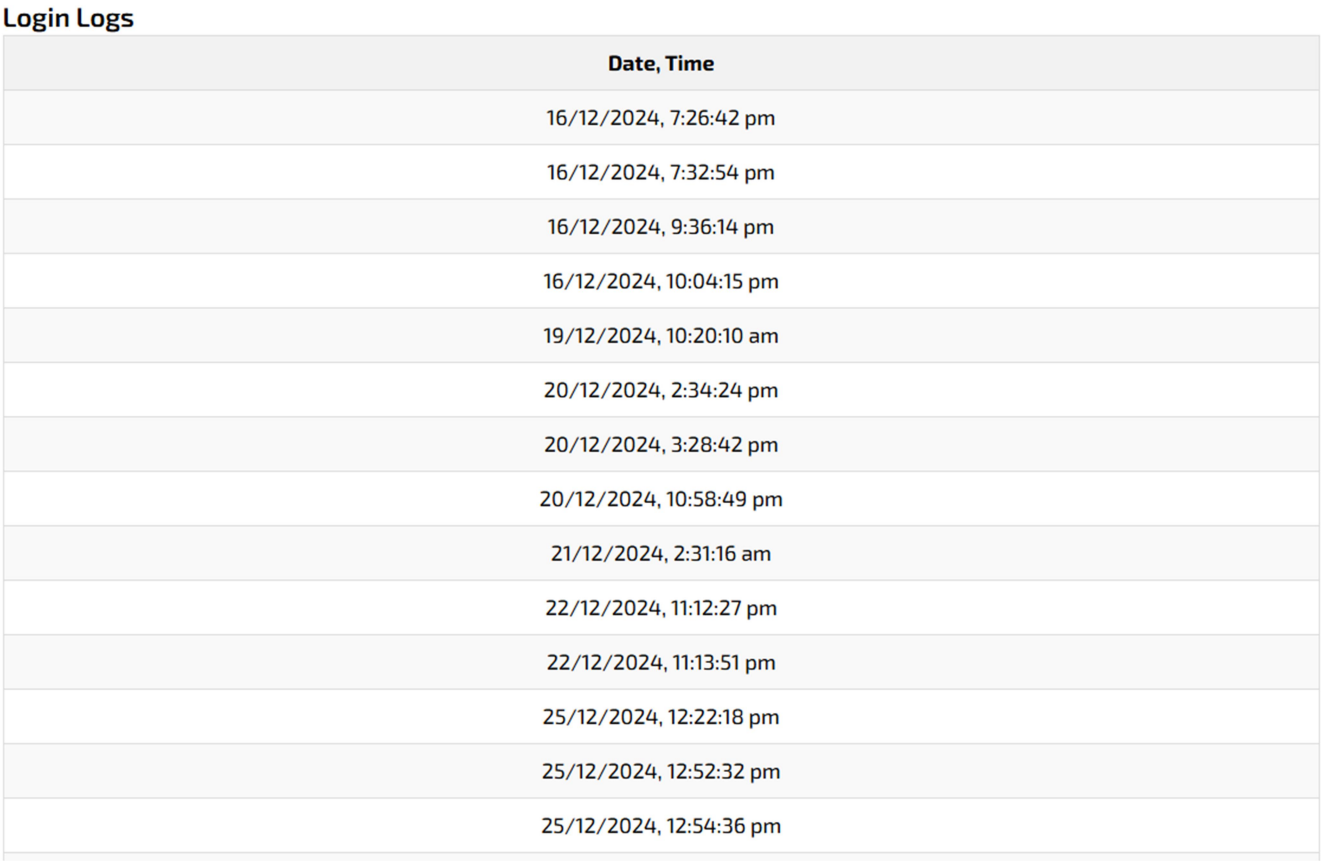

Fig 4.8.1: Login Logs

4.9 Sharing Files Functionality

Fig 4.8.1 provides a secure file-sharing feature through a "**Recipient's Email**" prompt. When a user clicks the "**Share**" button next to a file listed in the "**Your Files**" section, a popup modal appears. This modal prompts the user to enter the email address of the recipient they wish to share the file with. The modal contains an input field for entering the email, an "**OK**" button to confirm the action and proceed with sharing, and a "Cancel" button to abort the process. This feature ensures controlled sharing of files by requiring the recipient's email, likely sending them a secure link or access details via email.

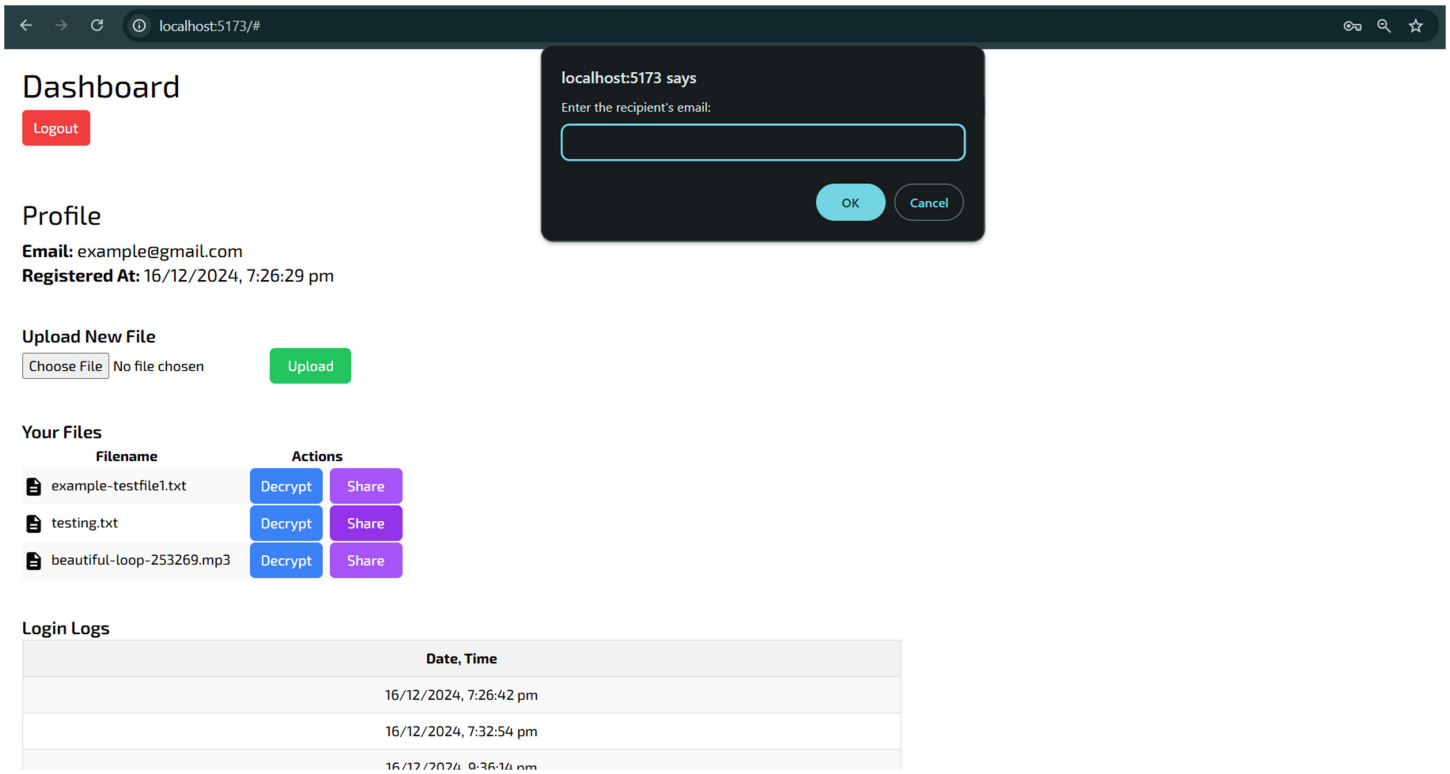

Fig 4.9.1: Sharing files Functionality

4.10 File Decryption

Fig 4.9.1 describes that after uploading a file to the platform, users can utilize the "Decrypt" option available in the "Your Files" section to decrypt an encrypted file. Once the decryption process is successfully completed, a popup notification appears with the message "File decrypted successfully!" and an "OK" button to confirm and close the notification and stores the decrypted file to the downloads. This feature ensures that encrypted files can be securely converted back to their readable form. The decryption process is seamless, providing users with instant feedback and easy access to the decrypted content.

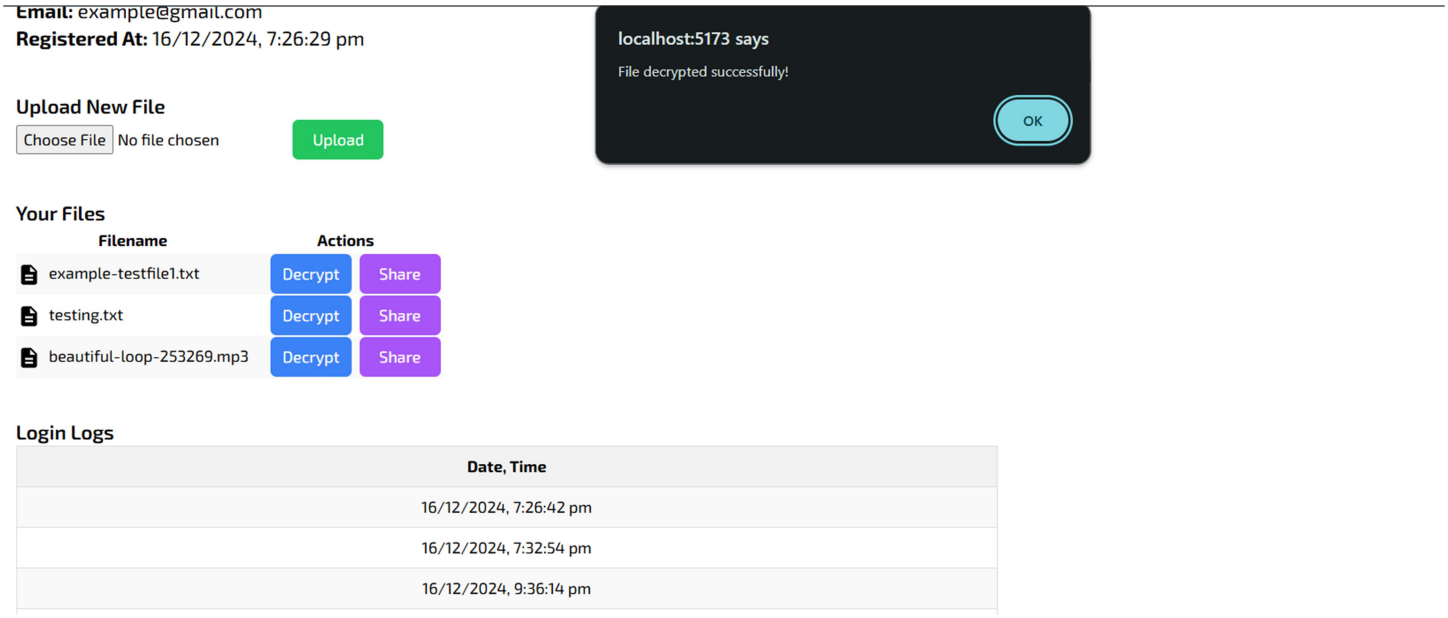

Fig 4.10.1: File Decryption

CONCLUSION

This project showcases the transformative potential of blockchain technology in addressing key challenges related to secure data sharing. By integrating blockchain's decentralized and tamper-proof architecture, the system ensures that data transactions are transparent, immutable, and verifiable, providing an auditable trail for accountability. The use of decentralized storage eliminates reliance on a single point of failure, enhancing data availability and resilience against breaches. Additionally, the incorporation of encryption safeguards sensitive data, ensuring that only authorized parties can access it while maintaining privacy and confidentiality. Together, these elements work in harmony to create a robust platform that tackles privacy, security, and integrity concerns, setting a foundation for trustworthy, efficient, and secure data-sharing mechanisms across multiple parties. This approach highlights how blockchain can revolutionize data sharing by fostering trust and transparency in a decentralized manner.

REFERENCES

[I] "A Security-Oriented Data-Sharing Scheme Based on Blockchain" (2023), published in Applied Sciences by MDPI, authored by Wei Zhou et al.
https://www.mdpi.com/2076-3417/14/16/7034

[II] "Blockchain-Based Secure Data Sharing Algorithms for Cognitive Decision Management" (2023), published in Cognitive Decision Sciences on ResearchGate, authored by Rajesh Kumar et al.
https://www.researchgate.net/publication/380662728_A_blockchainbased_secure_framework_for_data_management

[III] "A Blockchain-Based Traceable and Secure Data-Sharing Scheme" (2023), published in PeerJ Computer Science by PeerJ, authored by Xin Chen et al.
https://peerj.com/articles/cs-1337/

[IV] "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain" by Randhir Kumar and Rakesh Tripathi, and published in 2019.
https://ieeexplore.ieee.org/document/8777563