SecuraVault: A secured blockchain based cloud storage system

Shruti Srivastava, *Harsh Mishra, Anshika Jaiswal,

Anish Maurya

Department of Computer Science and Engineering, UIT Naini, Prayagraj

shrutiuim@gmail.com, harshmishra2080@gmail.com, janshika2323@gmail.com, anishmaurya088@gmail.com

*Corresponding Author

ABSTRACT

These days, cloud computing is everything for data access, but it often falls short due to significant issues with accessibility and security—challenges that stem from the centralized nature of traditional cloud solutions. This research article introduces Securavault, an innovative approach that leverages blockchain technology to tackle these problems in a decentralized environment. With Securavault, users can upload, download, and access their files anytime, anywhere, giving them greater independence and control over their private information. The platform makes use of the Interplanetary File System (IPFS) protocol and the Pinata API for efficient data storage and retrieval, while MongoDB helps keep user records organized.

Keywords: Decentralized Storage, Blockchain Security, Interplanetary File System (IPFS), Smart Contracts, Data Integrity, Privacy Preservation in blockchain, Cryptographic Encryption, Cryptocurrency, Crypto Wallets, MetaMask Wallet.

1. INTRODUCTION

Introduction The way digital data managed and stored has changed drastically over the last few years, moving from relational database to more complex cloud storage solutions. Relational databases offer a structured way with efficient query 1 capabilities. But as the amount of data generated by user (individuals or organizations) increases, the limitations of relational database become clear. These problems include challenges with scalability, high maintenance costs, and vulnerability to data loss. In response, cloud storage became a strong alternative, providing better scalability, accessibility etc. But despite these benefits, it increases the concerns around data security, privacy and potential misuse of user's data. These concerns have led to some major risks like unauthorized access, data breaches etc. The dependence of a centralized cloud storage system has decreased the trust of users and has put into focus the urgent need for a more secure and transparent way of data management that gives the user back control over his information. In this paper, we present Securavault, a decentralized storage system using blockchain technology to provide secure, transparent, user-centric data storage.[1] The primary goal of this project is countering what is lacking in conventional storage and cloud storage by implementing secure data uploading, downloading, and management through the Interplanetary File System (IPFS) protocol and using the Pinata API while keeping users' privacy unbroken.[3] SecuraVault is created to offer users a comprehensive platform where they can securely authenticate their account using Crypto Wallet ensuring a seamless and secure login process. Once logged in, users can upload, save their data or file through the platform. Users can upload as many files as they want but for every file there will be a transaction fee. [8] Each file upload will require a transaction fee, processed through the blockchain to maintain full security and transparency of the Data. Uploaded data will be securely stored on the nodes of the blockchain with their IPFS Hash Addresses. The purpose of developing SecuraVault includes building a good interface with the user for better User Experience, saving data on the blockchain network and implementing transaction management using smart contracts. File upload is done using the IPFS and Pinata API. In conclusion, Securavault targets to convert data management through operating the power of blockchain technology, while favouring user empowerment and security of user data. While

understanding the key challenges faced by traditional and cloud storage systems, Securavault attempts to create a secure, transparent environment for managing digital data, ultimately rebuilding user trust in the digital world.[2]

1.1 Interplanetary File System:

Interplanetary File System is a decentralized peer to peer network for storing, sharing and accessing files over a network. It is designed to be a stronger alternative option to traditional centralized file storage systems. IPFS uses a content address system also known as CID, where each file is identified by it. CID is also called IPFS Hash. Content is distributed across network of nodes of blockchain rather than just stored on a single server. Users can access files by their content identifier and can share it with others. IPFS is stronger to attacks because there is no single point of failure in it. It is highly scalable, making it ideal for storing large files and it is also decentralized.

1.2 Pinata API:

Pinata is a web application which provides user ability to store, manage and retrieve their digital assets on the IPFS network. It provides an easy: to use interface and tools for developers to upload and manage files on the IPFS network. The integration will increase the overall user experience as well as security and integrity of the data storage.

1.3 MetaMask:

MetaMask is one of the most well-known crypto wallets and an entrance to blockchain applications, letting users manage digital assets and seamlessly interact with decentralized applications (DApps). MetaMask is both a browser extension and a mobile app, allowing the user to create and manage their very own cryptocurrency wallet [9].

2. METHODOLOGY

This chapter outlines the methodology employed for realizing the project, including the flowchart of the platform. The whole methodology was divided into 4 parts.

2.1 User Authentication:



Figure 1 User Authentication

To check the authentication of the user, user first login on this platform using MetaMask. When the user successfully logged in at the same time an encryption key is generated and stored in the database for later use. After that there is an option to upload files to the blockchain using the IPFS protocol and Pinata API. This initial

step is essential as it establishes a steady connection between the user and the platform, ensures that the authorized person can easily access their data and can easily manipulate them.

2.2 Data Encryption and Upload:



After logging into the platform then the user selects files to upload to the blockchain. 4 To do that it first uploads data on the server, then server encrypts the data and sends to Pinata using IPFS protocol and generates a CID, Content Identifier, which then sends back to the server and from server sends back to the user and saves the CID into the Smart Contract. The encryption which is used for encrypting the data is AES-256 CBC.[5]

2.3 CID Generation and Smart Contract Interaction:

When the data or file is uploaded on the blockchain a CID is generated also known as IPFS hash. This CID serves as a unique reference to the uploaded data which is also used for retrieving it. This CID is stored in a Smart Contract that can only be accessed by the used with the help of their Crypto Wallet.[4]

2.4 Data Retrieval and Decryption:



Figure 3 Data Retrieval and Decryption

When user logs on to the platform, they can easily find their uploaded data or files just below the upload option. But on the server end when the user logs in their encryption key as well as CIDs of all the uploaded files are shared to the nodes using Pinata and IPFS and by doing that all the uploaded files can be seen. This proposed answer now not handiest complements the safety and transparency of facts management but additionally empowers customers via imparting them with manipulation over their information. By leveraging cutting: edge technology which includes blockchain, IPFS, and the Pinata API, Securavault efficaciously addresses the vital challenges related to traditional and cloud storage solutions. The result is a secure, decentralized, and consumer: centric surroundings for digital records management that fosters consideration and confidence amongst customers, ultimately remodelling the manner people and corporations take care of their sensitive facts.

3. Literature Review

To analyse the effectiveness of our proposed system, we looked through various research papers focusing on secure cloud storage using blockchain technology. These analyses were very critical in understanding the different frameworks which enabled us to change our project goals and design accordingly. To develop our system, there are several relevant areas that must be mastered, such as blockchain technology, cloud storage, and smart contracts. While researching on the internet, we came across a particular study regarding the application of blockchain technology in secure storage. One of the most remarkable studies was on Decentralized Cloud Storage Using Blockchain, which discussed the employment of IPFS, AES-256 encryption, and smart contracts on the blockchain. We pointed out in our paper the IPFS scalability issues and the missing focus on the user: friendly interface that made us take these aspects into consideration in our design. Another study on Secure Storage Using Blockchain Technology on Cloud Environment which partially covers our case has placed the cloud storage in the blockchain and used SHA256 and Proof-of-Work. This method showed problems with user: friendly interface and proper scalability, leading us to switch our approach to less complex and more user: friendly in our project.[6] In addition, the study Securer Distributed Cloud Storage Based on the Blockchain and Smart Contracts stresses the use of blockchain configuring as data structure and RSA encryption. The research illuminated the level of security granted by integrating blockchain; but it also pointed out the need for more user accessibility and evaluative mechanisms that we aim to address in our project. Through participating in these projects and several others, we have garnered immense experience in developing a secure and efficient cloud storage system using blockchain technology. Knowing the research gaps has played a very vital role in refining our approach, ensuring that our project meets not only the security requirements but also an intuitive experience for all the users.[7]

4. RESULT AND ANALYSIS

This section presents the results obtained from the implemented system and describes the various test cases used for its evaluation. The following sections elaborate on the different tests performed and provide detailed information about the corresponding outcomes.

4.1 Test Objectives:

• All input fields must function correctly, and handle user entries as intended.

• Page transitions should be properly triggered through the specified links or navigation elements.

• There should be no noticeable delays or lags when rendering screens, displaying messages, or providing responses to user inputs.

4.2 Features Tested:

• Verify that all user inputs conform to the expected data formats and validation rules.

• Confirm that all navigational links and buttons correctly redirect the user to their intended destination pages or sections.

4.3 Results:

All tests conducted have produced positive results, demonstrating the proposed platform's ability to upload files on the blockchain. By using the IPFS protocol the platform store the files uploaded by the SecuraVault user to the blockchain and can be accessed by using its IPFS hash or CID (Content Identification)



Figure 5 Home Page



Figure 6 File Upload and Download

	This guide	welcome to s will help you navigate o	and use our website effect	ively.	
1 Uploading					
	To up	pload a file to the block	chain, follow these steps:		
Click on the "Upload	d" button on the home	epage.			
Select the file you w	ant to upload from yo	our device.			
Click "Upload" to up Pay the Fees.	load the file.				
You will see a confir	mation message onc	e the upload is success	stul.		
Viewing U	ploaded Files				
	You can se	ee all your uploaded file	es down below when you s	scroll	
	upport				
D Contact Si	upport .		ion or bours quantiane:		
	I	you encounter any issu	les or nave questions:		
Contact us for	any problems.				

Figure 7 User Guide

5. CONCLUSION AND FUTURE WORK

5.1 Future Work:

• Implement Parallel Processing for Downloading and Uploading Files: Enhancing performance through permitting simultaneous file transfers, decreasing ready times and enhancing user enjoy.

• Implement Features like Filters and Search: Enabling users to effortlessly locate and control their documents via superior filtering alternatives and seek competencies, improving usability.

• Implement More Security Options: Introducing signals to inform customers of unauthorized account get admission to, enhancing normal security and person self: assurance.

• Support to Use Other Cryptocurrencies: Expanding the range of cryptocurrencies time-honoured for transactions, growing flexibility and user adoption whilst catering to numerous person options.

• Improve Performance Speed: Optimizing device structure and protocols to reduce latency at some stage in records get admission to and switch, main to a smoother user experience.

• Decrease Transaction Fees: Finding ways to limit charges related to transactions, making the platform more attractive to customers and encouraging higher volumes of transactions.

5.2 Limitation:

• Data Upload Speed is Low: Current speeds may additionally avoid consumer levelling in and productivity, especially in information heavy operations.

Low File Organization: Inefficient management features can cause frustration and problems in locating files fast.
Not Possible to Upload Large Files: File size restrictions restrict usability for users needing to keep massive media documents or enormous datasets.

• Transaction Fees are High: Elevated transaction prices may deter customers, necessitating an overview of the rate shape to beautify competitiveness.

• No Security for Database that Stores Encryption Key: Lack of security features for the database puts touchy records at hazard.

The modern offerings are geared towards person customers, which may not meet the desires of groups in search of complete facts answers. These limitations emphasize the challenges and areas for development that want to be addressed for better consumer pride and operational efficiency

6. REFERENCE

[1] Sharma, P., Jindal, R., & Borah, M. D. (2021). Blockchain-based decentralized architecture for cloud storage system. Journal of Information Security and Appli cations, 62, 102970.

[2] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067

[3] Bieri, C. (2021). An overview into the InterPlanetary File System (IPFS): use cases, advantages, and drawbacks. Communication Systems XIV, 28.

[4] Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Gen eration Computer Systems, 105, 475-491.

[5] Sivathanu, G., Wright, C. P., & Zadok, E. (2005, November). Ensuring data integrity in storage: Techniques and applications. In Proceedings of the 2005 ACM workshop on Storage security and survivability (pp. 26-36).

[6] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. Ieee Access, 7, 164908-164940.

[7] Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., & Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. International Journal of Advanced Computer Science and Applications, 8(11).

[8] Albayati, H., Kim, S. K., & Rho, J. J. (2021). A study on the use of cryptocurrency wallets from a user experience perspective. Human behavior and emerging technologies, 3(5), 720-738.

[9] Choi, N., & Kim, H. (2019). A Blockchain-based user authentication model using MetaMask. Journal of Internet Computing and Services, 20(6), 119-127.

[10] Foster, I., Kesselman, C., Nick, J., Tuecke, S.: The physiology of the grid: an open grid services architecture for distributed systems integration. Technical report, Global Grid Forum(2002)