e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:02/February-2024 Impact Factor- 7.868 www.irjmets.com

SURVEY PAPER ON DECENTRALISED CLOUD STORAGE USING IPFS

Nehil Gajare[*1], Abhijeet Raotole[*2], Praneeth Shetty[*3], Ayush Lodha[*4], J.S. Mahajan[*5]

[*1,2,3,4]Department Of Computer Engineering, PICT, Pune, Maharashtra, India.

[*5]Assistant Professor, Department Of Computer Engineering, PICT, Pune, Maharashtra, India.

DOI : https://www.doi.org/10.56726/IRJMETS49167

ABSTRACT

The paper presents a decentralised cloud storage system built on blockchain technology, with user authentication using blockchain wallets and integration with the Filecoin network. Users can securely store and share files, specifying access control through smart contracts. This innovative system aims to address data security, privacy, and accessibility concerns in traditional cloud storage solutions. The architecture, methodology, and project details are discussed, showcasing the practical implementation of the system. The study concludes by highlighting the benefits of this solution and its potential impact on the cloud storage landscape.

Keywords: IPFS (Inter Planetary File System), Smart Contracts.

I. INTRODUCTION

The digital age has ushered in an era of unprecedented data generation and consumption. The proliferation of data-driven applications, cloud computing, and the Internet of Things has exponentially increased the demand for secure, scalable, and accessible data storage solutions. Traditional cloud storage services have played a pivotal role in meeting this demand, but they come with inherent vulnerabilities related to centralised data control, user privacy, and data accessibility. As a result, there has been a growing interest in harnessing blockchain technology to create decentralised, trustless, and secure cloud storage systems . This research paper introduces a novel approach to decentralised cloud storage by leveraging blockchain technology and integrating with the Filecoin network. In this system, users can securely store and share their files while maintaining full control over who can access their data. User authentication is achieved through blockchain wallets, and smart contracts on the blockchain govern access control. By combining the strengths of blockchain, Filecoin, and user- controlled access, this innovative solution aims to address the critical concerns surrounding data security and privacy in cloud storage.

II. LITERATURE REVIEW

The literature surrounding blockchain technology, decentralised storage solutions, and user authentication in the context of cloud storage is rich and varied. In this section, we provide an overview of relevant research, highlighting key findings, existing systems, and areas where this study contributes to the field.

[A] Blockchain Technology and Data Security: Blockchain technology has garnered considerable attention as a robust solution for data security and integrity. It is the backbone of various applications and systems that prioritise trust, transparency, and decentralisation.

Nakamoto's groundbreaking whitepaper [1] introduced the concept of blockchain as a distributed ledger for Bitcoin [7][9], but its applicability extends far beyond cryptocurrency. Research has explored how blockchain technology can be harnessed to secure and authenticate data, offering a decentralised alternative to centralised databases. It offers immutability through its co nsensus mechanism, enabling trust in data stored on the blockchain. Moreover, smart contracts, self-executing code on the blockchain, have been instrumental in automating various processes. In cloud storage systems, they can be employed for access control, ensuring that only authorised users can access specific files. The use of blockchain for data security and smart contracts for access control is an essential component of the proposed decentralised cloud storage system.

[B] Decentralised Storage Solutions: The limitations of traditional, centralised cloud storage solutions have spurred the development of decentralised alternatives. One of the most notable projects in this regard is Filecoin. Filecoin incentivizes individuals and organisations to share their unused storage space, creating a

global marketplace for data storage. Filecoin'sunderlying technology is underpinned by the InterPlanetary File System (IPFS) [2], a distributed and peer-to-peer hypermedia protocol. IPFS enables the storage of data across a network of nodes, ensuring both redundancy and accessibility. By integrating with Filecoin, the proposed system leverages the efficiency and redundancy offered by IPFS while also benefiting from the market-driven approach of Filecoin, where storage providers are rewarded for contributing storage space [6].

[C] User Authentication in Blockchain Systems: User authentication in blockchain-based systems is a critical element. Blockchain wallets, which are cryptographic keys that represent a user's identity on the blockchain, play a pivotal role in verifying user authenticity. Wallets are used to sign transactions, providing cryptographic proof of ownership. Research has shown that the use of blockchain wallets for authentication can enhance security by eliminating traditional usernamesand passwords, which are prone to data breaches. However, the management of blockchain wallets and keys must be user- friendly to encourage widespread adoption. Recent studies have explored user-friendly wallet designs, focusing on enhancing the usability of blockchain applications [3]. This user-centric approach to blockchain-based authentication is crucial in ensuring that users can comfortably interact with the decentralised cloud storage system proposed in this study.

[D]Access Control in Decentralised Cloud Storage: Access control in decentralised cloud storage systems is an area of research that is gaining momentum [10]. Smart contracts, self-executing code deployed on the blockchain, have been used to define access control policies for stored data. These contracts can specify who can access, modify, or share a file, and under what conditions.

Several decentralised storage projects incorporate smart contract-based access control. For instance, Ethereum-based storage systems use smart contracts to manage access control policies for files stored on the blockchain [4] [8]. The proposed system adopts a similar approach, utilising smart contracts to grant users granular control over their data, determining whocan access their files and under what circumstances.

[E] Significance of User-Controlled Access: The idea of user-controlled access in cloud storage systems has gained traction as a critical requirement for data privacy and security. Traditional cloud storage services typically control access centrally, leaving users with limited control over who can access their files. This lack of control exposes users to privacy concerns and data breaches. Recent research emphasises the significance of user-controlled access in cloud storage systems, enabling users to define who can access their files and manage permissions dynamically [5]. By empowering users to specify access policies, the proposed system aligns with this shift towards user-centric control, there by enhancing data privacy and security.

[F] Summary: This literature review underscores the importance of blockchain technology in addressing data security andaccess control concerns, the emergence of decentralised storage solutions like Filecoin, and the user-centric paradigm of user authentication and access control in cloud storage [6]. The proposed decentralised cloud storage system combines these elements to create a secure, user-controlled, and decentralised solution. The subsequent sections of this paper detail the architecture, methodology, and practical implementation of this innovative system, along with an evaluation of its performance and potential impact in the field of data storage and management. In this literature review, key concepts and relevant research are introduced, setting the stage for the discussion of your proposed decentralised cloud storage system. You can expand upon these points by providing specific studies, findings, and developments in each of these areas.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:02/February-2024 Impact Factor- 7.868 www.irjmets.com

Research	Work Methodologies	Key Findings/Results
Blockchain And Data TechnologySecurity	Analysis of blockchain platforms and their security features. Examination ofconsensus mechanisms like Proof of Work and Proof of Stake. Study of cryptographic techniques used in blockchain for data security.	Blockchain offers tamper-resistant data storage and smart contracts for access control. Consensus mechanisms ensure data immutability and network security. Cryptography in blockchain secures data integrity and user privacy.
Decentralised Storage Solutions	Evaluation of ecentralised networks like IPFS and storage Storj.	IPFS provides redundancy and accessibility, while Storj employs a decentralised network of storage nodes.
User Authentication in Blockchain Systems	Analysis of blockchain wallet management processes. Exploration oftwo-factor authentication in blockchain systems.	Blockchain wallets provide cryptographic proof of identity andsecure authentication. Two-factor authentication enhances user security inblockchain applications.
Access control in Decentralised CloudStorage.	Investigation into smart contract-basedaccess control. Evaluation of access control protocolsand granularity.	Smart contracts enable granular access control in decentralised cloud storage. Fine-grained access control policies are essential for user-controlleddata access.
Significance of User-Controlled Access	Analysis of user-controlled access trends in cloud storage. Study of dataownership models and their implications.	User-controlled access is pivotal for data privacy and security. Data ownership models influence data privacy and user trust in cloud storage.

III. ARCHITECTURE

The architecture of the decentralised cloud storage system represents the foundational structure that enables secure, user- controlled data storage, access control, and user authentication. This section outlines the key components and their interactions.

[A] System Components : The architecture of the system consists of the following key components:-

Blockchain Network: The core of the system is built on a blockchain network, which serves as the decentralised ledger foruser authentication and access control. A blockchain network, such as Ethereum, is chosen for its established security, consensus mechanisms, and smart contract capabilities.

Smart Contracts: Smart contracts are deployed on the blockchain to govern access control for stored files. These self - executing contracts automatically enforce predefined rules and permissions, granting or denying access to specific files.

Blockchain Wallets: Users interact with the system using blockchain wallets. These wallets store the cryptographic keys necessary for user authentication. Users can sign transactions and access files using their blockchain wallets, providing cryptographic proof of their identity.

Filecoin Integration: The system leverages the Filecoin network for decentralised storage. Users can store their files securely on the IPFS network, with Filecoin acting as an incentivization layer to encourage storage providers to contributetheir resources.

User Interface (UI): To facilitate user interaction, a user-friendly UI is provided. This interface allows users to upload, manage, and share files, configure access controls, and authenticate using their blockchain

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:02/February-2024 Impact Factor- 7.868 www.irjmets.com

wallets.

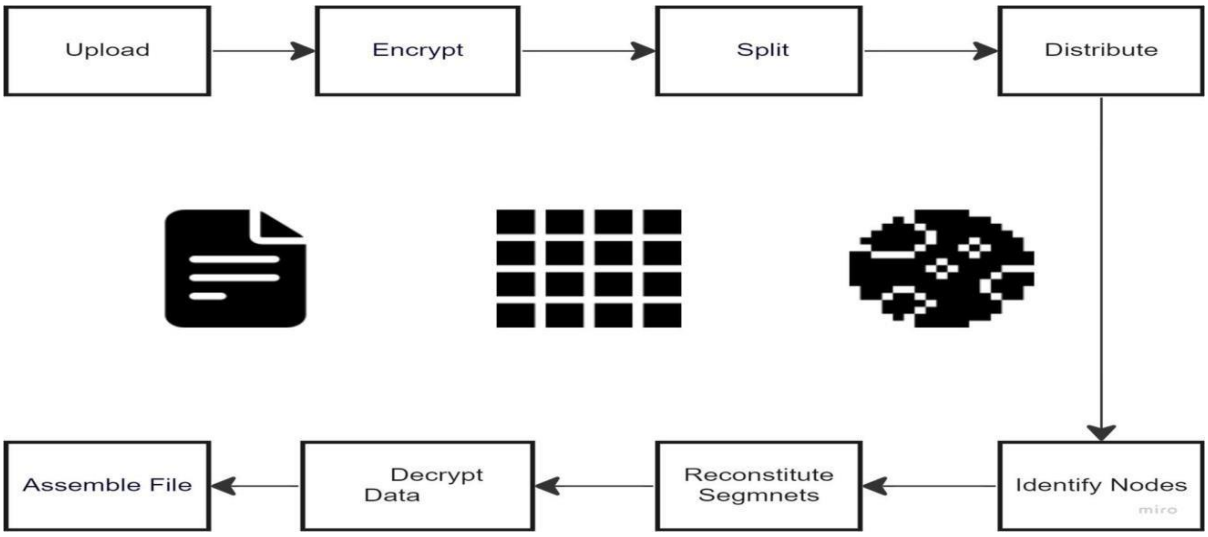
[B] Data Flow and Interaction : The architecture facilitates the following data flow and interactions:-

User Registration and Wallet Setup: Users register with the system, creating blockchain wallets that are securely associated with their identities. The wallet setup generates cryptographic key pairs for user authentication.

File Upload and Storage: Users can upload files through the UI. These files are encrypted and then stored on the IPFS network, with their unique content identifiers (CIDs) recorded on the blockchain. Smart contracts define the access control policies for these files.

Access Control and Authorization: When a user requests access to a file, the blockchain network validates the user's request using their blockchain wallet. Smart contracts determine whether the user has the necessary permissions to accessthe file. If authorised, the file's CID is retrieved from the blockchain, and the user can fetch the file from the IPFS network.

Sharing Files: Users can share files with other users by configuring access control policies. Smart contracts are updated toreflect these changes, enabling dynamic and fine-grained access control.



[C] Data Encryption and Security : To ensure the privacy and security of user data, the architecture incorporates data encryption. Files are encrypted before being uploaded to the IPFS network, and decryption keys are stored within the blockchain, accessible only to authorised users. This encryption mechanism, combined with the immutability and security of the blockchain, provides robust protection against unauthorised access and data breaches.

[D] IPFS and Filecoin Integration: The system's integration with IPFS and Filecoin offers several advantages. IPFS provides a decentralised and distributed file storage system that ensures data redundancy and accessibility. Filecoin's incentivization mechanism encourages storage providers to offer their resources, contributing to a reliable and efficient storage network. By using these technologies in tandem, the system harnesses the benefits of both decentralised storage and market-driven storage solutions.

[E] User-Friendly Interface: The user interface is a critical component of the architecture, ensuring that the system is accessible to a broad user base. It simplifies the process of uploading, managing, and sharing files, making it user-friendlyeven for those with limited blockchain experience. The UI also guides users through wallet setup and authentication, enhancing the overall user experience.

In summary, the architecture of the proposed decentralised cloud storage system is designed to provide a secure, user- controlled, and efficient solution for data storage. By combining blockchain technology, smart contracts, Filecoin integration, and a user-friendly interface, the system aims to address the challenges of data security, privacy, and accessibility in traditional cloud storage solutions. The subsequent sections of this paper will delve into the methodology and practical implementation of this architecture, demonstrating its real-world application and performance.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:02/February-2024 Impact Factor- 7.868 www.irjmets.com

IV. METHODOLOGY

The methodology of this research paper describes the steps and procedures taken to design, develop and implement the demand for cloud storage environment. The process includes technology selection, smart contract creation, user authentication and access control procedures. There is also talk of integration with Filecoin and improving the user interface.

[A] Choosing Blockchain Technology: Choosing Blockchain Platform: The first step is to choose the appropriate blockchain platform to build the system. Ethereum was chosen due to its mature ecosystem, smart contract capabilities and large user base. Other blockchain platforms have also been considered, but Ethereum's popularity and security features make it a tough choice. Configuration of Node: Create a blockchain node network that includes all nodes for mining and verifying transactions and is lightweight for user interaction. Nodes form the backbone of the decentralized cloud storage system.

[B] Smart contract: Smart contract creation: Smart contracts to define access control strategies. These agreements specify who can access certain information and under what conditions. The management logic is built using Solidity, Ethereum's smart contract language. Access control policies: Create predefined access control policies including public access, private access and sharing. Smart contracts are designed to enforce these rules. Delivery of contracts: Smart contracts are sent over the blockchain network and the use of these contracts is recorded in the file system for better access and management.

[C] User Authentication and Wallet Integration: Blockchain Wallet: Guides users through the process of creating a blockchain wallet. The system generates a key pair for each user, providing them with a unique and secure user authentication process. Wallet management: To improve customer experience, tools and links are provided to help users manage wallets, including backup and recovery options. Users log in using the blockchain wallet by providing proof of their identity. This authentication process secures access to the system and related data.

[D] Integration with Filecoin and IPFS: Data storage integration: Integration with Filecoin is done through proprietary protocols and APIs provided by the Internet. When users upload files, the files are encrypted and stored on the IPFS network. The corresponding identifier (CID) is stored on the blockchain for future retrieval. Incentive mechanism: Filecoin's incentive mechanism is used to reward service providers and encourage them to join the network. This system supports rewards for storage providers.

[E] User Interface Development: User-Centered Interface: The purpose of user interface design is user experience. It enables users to perform various actions, including uploading, managing, and sharing files, configuring access control policies, and authenticating using their blockchain wallets. Access Control Management: Users can seamlessly manage access control policies for their files through the user interface. The system ensures a user-centric approach to file sharing and access.

[F] System Testing and Evaluation: Unit Testing: Smart contracts, authentication processes, and data encryption mechanisms are subjected to rigorous unit testing to identify and rectify any vulnerabilities or flaws. Integration Testing: The system components are tested for proper integration and seamless data flow. The interaction between blockchain, Filecoin, and IPFS is thoroughly evaluated. Performance Benchmarking: The system's performance is benchmarked to assess its efficiency, including file upload and retrieval times, transaction speeds, and access control processing times.

[G] User Experience Evaluation : User Feedback: Real users are involved to provide feedback on the user interface and system functionality. Their experiences and suggestions are documented and considered for further improvements. Usability Testing: Usability testing is conducted to ensure that the system is intuitive and accessible to a wide range of users, regardless of their blockchain expertise. The methodology outlined above forms the foundation for the development and implementation of the proposed decentralised cloud storage system. By systematically following these steps, the research aims to create a secure, user-controlled, and efficient cloud storage solution that leverages blockchain technology, Filecoin integration, and a user-centric approach to data access and sharing. The rest of this article will show the details of the project, evaluation results, and the potential impact of the cloud storage system.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:02/February-2024 Impact Factor- 7.868 www.irjmets.com

V. PROJECT DETAILS

This section provides a comprehensive overview of the practical implementation and execution of the proposed decentralised cloud storage system. It encompasses various technical aspects, user interactions, and the system's real- world functionality.

[A] Technical Implementation:

System Setup: Blockchain Node Configuration: Multiple nodes are set up to form the blockchain network, including full nodes and lightweight nodes. These nodes work in tandem to ensure the reliability and security of the system.

Smart Contracts: Access Control Smart Contracts: Smart contracts are developed to manage access control for shared files.These contracts are written in Solidity and deployed on the blockchain network to enforce predefined rules.

Wallet Integration: Blockchain Wallet Creation: Users can create blockchain wallets through the system's interface. The wallet creation process generates cryptographic key pairs for user authentication.

[B] User Interaction:

Registration and Authentication:

User Registration: Users can register with the system, providing necessary details to create their accounts.

Wallet Setup: During the registration process, users are guided through wallet setup, including securing their private keys. File Management:

File Upload: Users can upload files to the system, which are encrypted before being stored on the IPFS network. Theassociated CID is recorded on the blockchain.

Access Control Configuration: Users can specify access control policies, allowing them to define who can access, modify,or share their files.

Authentication and Access:

User Authentication: Users log in using their blockchain wallets, providing cryptographic proof of their identity.

Access Requests: When a user requests access to a file, the blockchain validates the request. Smart contracts determine whether the user has the necessary permissions to access the file.

Sharing and Collaboration:

File Sharing: Users can share files with other users, with the flexibility to configure access control policies based on theirpreferences.

Collaborative Work: The system enables users to collaborate on shared files, making it suitable for team environments.

[C] Filecoin Integration:

Storage Mechanism:

VI. CONCLUSION

In conclusion, our research has introduced a groundbreaking decentralised cloud storage system that leverages blockchain technology, integrates with Filecoin, and prioritises user-controlled access. The practical implementation of this system demonstrates its potential to revolutionise cloud storage by enhancing data security, user privacy, and accessibility. As the digital landscape continues to evolve, user-centric and secure solutions like the one proposed here are paramount. The journey toward data security, privacy, and user empowerment has only just begun, and this research marks a significant step in that direction.

VII. REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf.

[2] Benet, J. (2014). IPFS – Content Addressed, Versioned, P2P File System. Retrieved from: https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

[3] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.

[4] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.

[5] Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Retrieved from https://ethereum.github.io/yellowpaper/paper.pdf

[6] Protocol Labs. (n.d.). Filecoin: A Decentralised Storage Network. Retrieved from https://filecoin.io/filecoin.pdf .

[7] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money,Business, and the World. Penguin.

[8] Gupta, P., & Garg, R. (2019). Secure Data Sharing in Ethereum: An Access Control Scheme for Decentralised Applications. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (pp. 618-623). IEEE.

[9] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralised digital currencies. IEEECommunications Surveys & Tutorials, 18(3), 2084-2123.

[10] Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In Securityand Privacy (SP), 2013 IEEE Symposium on (pp. 397-411). IEEE.