International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Decentralized file storage using Blockchain

Dr. Suresh M B, Nitesh R, Krishna Chaitanya, Madhusudan K S

Dept. of Artificial Intelligence & Data Science, East West Institute of Technology Bangalore, Karnataka, India

[1]sureshreasearch45@gmail.com
[2]krish072020@gmail.com
[3]niturag2002@gmail.com
sudanmadhu2054@gmail.com

***Abstract*—**Amidst the exponential growth in data volumes and growing apprehensions regarding centralized control, decentralized cloud storage systems have emerged as a beacon of promise. This study presents a comprehensive examination of these systems, delving into their structural intricacies, benefits, and hurdles. The essence of decentralized cloud storage lies in dispersing data across a network of nodes, obviating the necessity for a central governing entity. Through the utilization of blockchain technology and cryptographic methods, information is encrypted, fragmented, and dispersed among myriad nodes, ensuring both redundancy and heightened security. This framework effectively mitigates the inherent risks of data loss or tampering associated with centralized infrastructures, thus bolstering data integrity and confidentiality. In summary, decentralized cloud storage systems signify a revolutionary shift in data management paradigms, furnishing a resilient, scalable, and secure alternative to centralized storage models. Ongoing research and development endeavours are imperative to surmount extant challenges and fully harness the transformative potential of this groundbreaking technology.

***Keywords*— -** Blockchain, Data Security, IPFS, Encryption, File Storage, Decentralized storage, Metamask, Pinata.

I. INTRODUCTION

This decentralized approach improves security,privacy,andcontrol,mitigating the risks associated with traditional information failuresandoutages.At the heart of this evolution is blockchain, a technology renowned for its ability to establish trust, security, and transparency in distributed networks. In blockchain, decentralization refers to the shift of control and decision making from a central authority to a network of participants. This has transformative affect not only for financial transactions but also for broader applications such as information management. The amalgamation of decentralized file systems with blockchain technology presents a novel approach to data management and security. By distributing files across a network of nodes, the vulnerability further fortifies this system by ensuring immutability, traceability, and secure access control. This synergy not only addresses the technical challenges of data management but also opens avenues for redefining user interactions with data.

In the realm of modern computing, the management and security of data have emerged as critical challenges. Traditional centralized approaches to data storage and management have often led to issues of control, transparency, and vulnerability. The evolution of decentralized technologies, coupled with the emergence of blockchain, has opened by the way for innovative solution that redefine how data is stored, accessed, and secured.

This research paper deepens into the fusion of two groundbreaking concepts: Decentralized File Systems (DFS) and blockchain technology. Decentralized File Systems looks to a paradigm where individual file systems are distributed across various nodes, often in proximity to the processes they serve. Unlike their centralized counterparts, these systems are not limited to monolithic cabinets but can be as dynamic as wall-mounted units, reflecting a new era of agility and adaptability.P2P cloud storage, exemplified by platforms like STORJ, Sia, and File coin, represents an attractive use case for block chain technology. It offers decentralized information storagesolutions that bypass the need for trusted third parties orconventional client-server architectures

II. LITERATURE SURVEY

1.A Blockchain-Based Secure Storage and Access Scheme for Electronics

Authors:Jin Sun

Publisher: IEEE

In today's digital age, ensuring the security and privacy of electronic data is paramount. With the rise of cloud computing and storage, traditional centralized systems face increasing threats from hackers, data breaches, and unauthorized access. To address these challenges, a blockchain-based secure storage and access scheme emerges as a promising solution. By leveraging the inherent properties of blockchain technology, such as decentralization, immutability, and cryptographic security, this scheme offers a robust framework for safeguarding electronic data while enabling efficient and controlled access. At its core, blockchain is a decentralized ledger that records transactions across a network of computers in a secure and transparent manner. Each transaction, or block, is cryptographically linked to the previous one, forming a chain of blocks.

2. Blockchain based decentralized storage
Authors: Yan Zhu
Publisher: IEEE
Security remains a critical concern in cloud storage systems due to the potential risks of information breaches, unauthorized 11 access,A blockchain-based decentralized storage scheme leverages the principles of blockchain technology to distribute and secure data across a network of nodes, eliminating the need for a central authority. Data is fragmented, encrypted, and stored in a distributed fashion, ensuring redundancy and minimizing the risk of data loss or unauthorized access. Each node in the network maintains a copy of the data, and consensus mechanisms ensure the integrity and immutability of the stored information.

3.A Peer to Peer Cloud Storage Network
Authors: Shawn Wilkinson
Publisher: IEEE
Description:A peer-to-peer cloud storage network allows users to store and share data directly with one another, bypassing centralized servers. Each user contributes storage space and bandwidth to the network, creating a decentralized ecosystem for data storage and retrieval. Data is encrypted and distributed across multiple nodes, ensuring security and redundancy.

4.Fault Tolerance Mechanism
Authors:Rajit Nair
Publisher: IEEE
Guaranteeing the high availability and dependability of data is indispensable for cloud storage systems to fulfill the requisites of contemporary applications and services. Fault tolerance mechanisms assume a pivotal role in alleviating the repercussions of hardware failures, network disturbances, and other system glitches. Scholars have delved into an array of fault tolerance strategies, encompassing redundancy, data mirroring, erasure coding, and distributed consensus protocols. For instance, Sharma et al. (2019) conducted an examination of fault tolerance mechanisms in distributed cloud storage systems, assessing their efficacy in enduring various types of failures.

5.Cost Models and Pricing Strategies
Author: Syed Nasrullah Zafrullah
Publisher: IEEE
ThisEfficient cost management constitutes a pivotal facet of cloud storage systems, as enterprises endeavor to optimize their storage expenditures while fulfilling their data storage requisites. Scholars have scrutinized diverse cost models, pricing strategies, and economic incentives within cloud storage environments to empower users in making wellinformed decisions regarding resource allocation and utilization. For instance, Huang et al. (2019) conducted and examination of various pricing models applicable to cloud storage services, elucidating their impact on user expenses and provider revenues. Furthermore, Chen et al. (2020) 2 proposed a dynamic pricing mechanism tailored for cloud storage providers, enabling them to adapt their pricing strategies in accordance with market demand fluctuations and resource availability dynamics
6. Scalability Challenges and Solutions.
Author:Prabhdeep Singh
Publisher: IEEE
TheScalability is a fundamental requirement for cloud storage systems to accommodate growing data volumes and user demands. Researchers have explored scalability challenges and proposed scalable architectures, algorithms, and technologies to address them. For example, Wang et al. (2018) surveyed scalability challenges in distributed cloud storage systems and discussed approaches for achieving scalable data storage, processing, and access. Additionally, Zhang et al. (2020) investigated the scalability of distributed storage systems in edge computing environments and proposed a hierarchical storage architecture to optimize data placement and access.

7.Privacy-Preserving Techniques
Author:Tripti Sharma
Publisher: IEEE
The Protecting user privacy and sensitive data is paramount in cloud storage systems, especially in multi-tenant environments where multiple users share the same 28 infrastructure. Several studies have investigated privacypreserving techniques, such as encryption, anonymization, and access control, to safeguard user data from unauthorized 11 access and disclosure. For instance, Li et al. (2018) proposed 2 a privacy-preserving data sharing framework for collaborative cloud storage environments, which enables secure data sharing among multiple users while preserving 6 data privacy and confidentiality

8.Energy Efficiency
Author: Musaddak Maher Abdul Zahra
Publisher: IEEE
In Energy consumption is a significant concern in large-scale cloud data enter, where the operational costs and 3 environmental impact of energy consumption are 2 substantial several studies have focused on energy-efficient designs and management strategies for cloud storage systems to minimize energy consumption while maintaining performance and reliability. For instance, Beloglazov et al.proposed dynamic resource allocation algorithms to 5 optimize energy usage in cloud storage environments. Additionally, Zhang et al. (2021) investigated the impact of workload consolidation on energy efficiency in cloud storage systems.

III . METHODOLOGY

Blockchain Technology: Implementing blockchain technology provides the foundation for a decentralized cloud storage system. Blockchain offers a secure and immutable ledger where data 3

transactions can be recorded. Each transaction is cryptographically linked to the previous one, forming a chain of blocks. This ensures that data stored in the system remains 18 tamper-resistant and transparent.

•Distributed File System (DFS): 4 Utilizing a Distributed File System (DFS) allows for the storage of files across multiple nodes in the network. This decentralization of data storage enhances redundancy and 9 fault tolerance, as data is replicated across multiple nodes. Examples of DFS include IPFS (Interplanetary File System) and Swarm.

•Consensus mechanisms: This plays a pivotal role in decentralized cloud storage systems, ensuring network integrity and transaction validation. Algorithms such as Proof of Work (PoW), Proof of Stake (PoS), or Delegated Proof of Stake (DPoS) are 3 essential for achieving consensus among nodes, guaranteeing alignment on the ledger's status. These mechanisms incentivize participants to contribute resources to the network while thwarting potential data tampering by malicious entities.

Encryption Technique: Utilizing encryption techniques, including symmetric and asymmetric encryption, safeguards data confidentiality within the cloud storage environment. Encryption at rest and during transit effectively bars unauthorized access to sensitive data, bolstering overall security measures. Furthermore, the implementation of methodologies like homomorphic encryption enables computation on encrypted data without necessitating decryption, thereby preserving user privacy

DID: Decentralized identity management implementation guarantees users retain authority over their identity and access privileges within the cloud storage platform. Leveraging decentralized identifiers (DIDs) and verifiable credentials empowers users to oversee their digital identities without dependence on centralized entities. This advancement heightens privacy and security by mitigating identity theft and unauthorized data access risks.

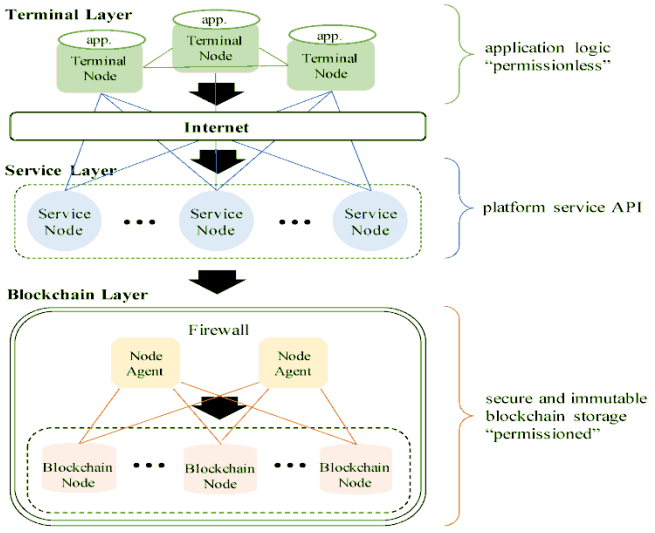

FIGURE 1. **DID management**

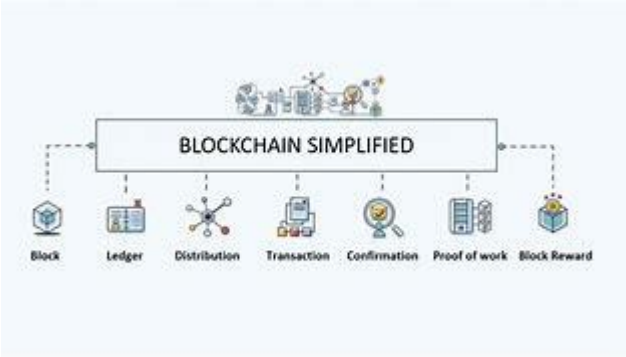

Fig 2. Simplified Blockchain

IV .CONCLUSION

The adoption of cloud computing has experienced a consistent upward trend, driven by its attractiveness to users because of its dynamic and flexible resource allocation capabilities. Despite the potential benefits, challenges persist, including substantial bandwidth requirements, apprehensions regarding data security, and the potential for vendor dependency. Nevertheless, cloud computing remains a highly promising technology. This paper focuses on the obstacle of migrating data from the cloud to a Distributed File System (DFS) while navigating associated regulatory requirements for authorization. Presently, no standardized method exists for transferring both data and permissions from the cloud to the DFS. To address this deficiency, we conducted our experiments utilizing Amazon Web Services' content and regulatory framework as a testbed. Our methodology enables the smooth transition of data from Amazon S3 to the Interplanetary File System (IPFS).

Acknowledgment

This project is supported by East West Institute of Technology. We would like to express our immense gratitude to our Internal guide Dr. Suresh M B, Prof & Head, Dept.ofAD who moderated this project and, in that line, improved the manuscript significantly. We have to express our appreciation to Dr. SURESH M B, Head of Department, AD for their guidance and support with us during the course. We express our thanks to Principal Dr.Channakeshavalu, for extending his support and encouraging us throughout the major project. We are also immensely grateful to all the faculty for their feedback on an earlier version of the project, although any inaccuracies are ours and should not furnish the reputations of these esteemed professionals.

REFERENCES

1) C. Kelly, N. Pitropakis, A. Mylonas, S. McKeown, and W. J.
2) Buchanan, "A comparative analysis of honeypots on different cloud platforms," Sensors, vol. 21, no. 7, p. 2433, 2021.
3) P. R. Carnley and H. Kettani, "Identity and access management for the internet of things," International Journal of Future Computer and Communication, vol. 8, no. 4, pp. 129– 133, 2019."
4) AN EVOLUTION OF RFID GRIDS FOR R. Kuhn, D. Yaga, and J. Voas, "Rethinking distributed ledger technology," Computer, vol. 52, no. 2, pp. 68–72, 2019.
5) J. A. Ramirez and E. Rodriguez, "A singular value decomposition approach for testing the efficiency of Bitcoin and Ethereum markets," Economics Letters, vol. 206, Article ID 109997, 2021.,
6) S. H and D. R. Prasath, "Bi-fitness Swarm optimizer: blockchain assisted secure Swarm intelligence routing Protocol for MANET," Indian Journal of Computer Science and Engineering, vol. 12, no. 5, pp. 1442–1458,.
7) J. Sousa, A. Bessani, and M. Vukolic, "A byzantine fault Conference Series, vol. 1237, no. 4, Article ID 042008, 2019. tolerant or-dering service for the hyperledger fabric blockchain platform," in Proceedings of the 2018 48th annual ieee/ ifip international conference on dependable systems and networks (dsn), pp. 51–58, Luxembourg, Europe, July
8) X. Zhang, J. Grannis, I. Baggili, and N. L. Beebe, "Frameup: an incriminatory attack on Storj: a peer to peer blockchain enabled distributed storage system," Digital Investigation, vol. 29, pp. 28–42, 2019.
9) Y. Zhu, C. Lv, Z. Zeng, J. Wang, and B. Pei, "Blockchainbased decentralized storage scheme," Journal of Physics: [4] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine fault Conference Series, vol. 1237, no. 4, Article ID 042008, 2019.
10) E. Politou, E. Alepis, C. Patsakis, F. Casino, and M. Alazab, "Delegated content erasure in IPFS," Future Generation Computer Systems, vol. 112, pp. 956–964,.
11) B. Yu, X. Li, and H. Zhao, "Virtual block group: a scalable blockchain model with partial node storage and distributed hash table," =e Computer Journal, vol. 63, no. 10, pp. 1524–1536, 2020