JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Decentralized Cloud Storage using Blockchain

Kshitij Naranje[1], Megha Pallewar[2], Siddhant Kotambe[3], Ajay Ramgirwar[4]

Department of E&TC, SKNCOE, SPPU, Pune

Abstract— **Today, the requirement of each cloud user is not the same as it used to be, some users need better storage capacity, some need lower storage with better plans hence this paper is the complete solution of unique cloud storage which is completely decentralized to provide utmost transparency with peer-to-peer systems. The major security problem with the existing system is that it is unidirectional, hence the user can only rent the storage from the big service providers. Instead of that one can develop an ecosystem in which some users could put their unused resources on rent and others could rent them. Initially, a huge chunk of the amount in buying the resources is not invested to start extreme servers at one point and pile up all the user data in a single space, which would reasonably reduce the security of the system and, also this huge investment upfront, so to get this thing up a better solution based on Blockchain Technology.**

Keywords—**Decentralization, Peer-to-Peer, Cloud Storage, Blockchain Technology, Storage and Security.**

I. INTRODUCTION

Recent advancements in data processing technologies interest ordinary consumers seeking improved data storage. Cloud computing is used as a system for cloud customers. Depending on their location, cloud users have access to distribute or trade data at any time and from any site. As we progress into the "technology age," we can see an enormous increment, pace, and diversity of material on the internet. Data can come from various sources, including mobile devices, archives, sensors, and social networks.

Cloud storage systems enable users to access massive amounts of storage at a cheaper price. At present, most of the cloud storage companies at home and abroad still provide their own centralized storage space and do not meet the requirements for storage resource integration and distributed storage. The paper compares and analyses the system performance of the centralized storage scheme, multi-centr`1234567890-e storage scheme based on genetic algorithm, network delay and security analysis of distributed P2P storage scheme based on blockchain, and draws conclusions: based on blockchain, the p2p storage scheme has significant improvements in system performance over the two conventional storage schemes described above.

Cloud computing has achieved substantial appeal with the expansion of communication and information technologies. AWS, Microsoft Azure, and Google Cloud Platform (GCP) are three cloud computing platforms. On-demand network access to a shared pool of computer resources includes storage, networking, computing, and security. A lot of firms employ cloud computing to store a significant amount of data remotely instead of maintaining it on local equipment. The services supplied by the cloud demand extensive bandwidth and high-speed Internet, which restricts their adoption by many end-users. Similarly, vendor lock-in is a problem with cloud computing, and moving data across cloud services is challenging. Recently, decentralized storage technology has been established for storing data safely without third-party aid. One of its applications is the DFS, which stores data chunks on multiple peers across the network. Other implementations include IPFS, SWARM, and SIA. The interplanetary file system is a peer-to-peer network that stores large amounts of data without relying on central servers. IPFS leverages the notion of storing data based on content-based-addressing. It breaks data into fixed-size pieces, distributes them throughout the whole network, and then generates a hash table. Current cloud customers can now store data locally, giving them more control over the data.

Security is a serious worry for sensitive and private data. Authorization or access control policies allow you to specify who has access to which resources based on certain attributes or roles. Amazon, for example, provides an Identity and Access Management (IAM) service to establish permission policies. Migrating private or sensitive data from the cloud to the DFS is not practicable until we can move the authorization policies, connected with the data on the cloud, to the DFS. Because current DFS implementations like IPFS and Sia lack permission policy definition methods, data cannot be moved from the cloud. The blockchain is another decentralized storage system that stores data in a sequence of blocks connected by cryptographic hashing of previous blocks. To our knowledge, no solution exists for transferring data and authorization policies from the cloud to DFS. We have mapped our recommended technique to move data from User's disk to Web3 cloud storage where the transaction details are stored in a locally created blockchain.

The data uploaded is managed and securely stored at web3 cloud storage and the transactions i.e., uploading, displaying, and sharing are occurring using the Metamask and Hardhat node which creates the local blockchain.

II. LITERATURE SURVEY

To provide decentralized storage for all users using Blockchain. Data security issues, single point server failure, etc are some real-time defects in the current cloud storage platforms.

Table 1 Blockchain technology development

NO	TITLE	TECHNOLOGY USED	YEAR
[1]	Blockchain-based Decentralized Storage Scheme	Decentralization	2019
[2]	Architecture of the hyperledger blockchain fabric	Hyperledger	2016
[3]	Decentralized Utility- and Locality-Aware Replication for Heterogeneous DHT-Based P2P Cloud Storage Systems	Decentralization	2020
[4]	Cryptanalysis of integrity checking scheme for cloud data sharing	Cryptography	2020

With ever-growing technological advancement and shrinking size with more powerful devices, there has never been a better time for advancements in an information system made up entirely of distributed devices. Of course, we have the internet as an example. However, the internet itself maintains a general hierarchy of client-server and a lot of middlemen which may or may not be trusted. The devices grow, data grow and so do the need for physical as well as logical means to hold the data. With a new race for powerful organizations to gather as much data as possible for future manipulation and understanding of information on a gigantic scale, there has been an unprecedented search and storage of data like never before. Even on a personal scale, we associate data with our personal lives as digital data has never been more of our personal life's metadata like today. Hence, they say data is the new currency, data is the new knowledge. [1] [2] However, how do we store our personal data? We store it locally, we burn it into DVDs, we use cloud services, we store it as much as we can, and then leave the rest for trusted servers to put. We have come to an age where our crucial data - we store in some server's storage space provided by a company with a promise of security and integrity. People now pour more trust into such services than themselves to store our data with security and integrity. However, in every system with central authorities, there is a hierarchy of power and in this case, such misuse directly affects the crucial data we use in our lives. Giving the key to an entity of higher authority in a system cannot last long without an imminent risk. One cannot guarantee such authorities' replication and misuse of such data. However, with technological advancements, computation power, data transfer rates, and storage space is distributed to each and every people in the form of many devices. there need not be networks with central authorities and hierarchies to where we trust our data for safekeeping and transfer. Instead, we can do what we have been doing for the past decade now in completely distributed systems maintained by parties involved using the system, and with Blockchain technology, we can do this with trust. In the blockchain, we store the hashes of files - metadata and its hash, the transactions between users, whom the data belongs to, who is storing the data, which other parties are involved during the replication and storage process, and access control data. Encryptions with Asymmetric keys paired and shared secrets, we will implement a layer of security and restriction. Using such an approach, one can be sure that one's data is safe and not accessible and readable by undesirable parties.

Although blockchain technology has been developed more than 2 decades ago, its actual implementation in various technology fields is just blooming. There are a few examples of distributed databases using blockchain. Some of the most popular applications of blockchain in distributed database management are storj.io, bigchaindb, etc. We here discuss BigchainDB,Storj.io, Sia, and MaidSafe as it is more somewhat related to our project. BigchainDB: a scalable blockchain database that uses Blockchain technology to store the users' data in various nodes. BigchainDB inherits characteristics of modern distributed databases: linear scaling in throughput and capacity with the number of nodes, a full-featured NoSQL query language, eïnˇCˇ client querying, and permissioning. Being built on an existing distributed DB, it also inherits enterprise-hardened code for most of its codebase. [5] Storj aims to become a cloud storage platform that can't be censored or monitored, or have downtime. It is the first decentralized, end-to-end encrypted cloud storage that uses blockchain technology and cryptography to secure users' files.

III. METHODOLOGY

1. The solution we propose here is to establish a distributed database system that will store data in a peer-to-peer network such that there will be no central body with the right to use and modify clients' data.
2. The data will be shared in multiple chunks, and stored at different nodes. No single node will know what data and whose data they are storing. Even if an attacker hacks into any node and pulls data, it will only receive part of the data which is encrypted. So, it's efficiently hard to grab complete data in decrypted form by any attacker, thus is more secure than Cloud.
3. For the data storing service that the storage nodes (Postmen) of the network provider, will be rewarded, and the client will pay for that service. Furthermore, the client and Postman will be bound by the Smart Contracts stored in the Blockchain that will act as a proof and trust layer for data availability and storage. This way the network will sustain by a reward and compensation mechanism. The integrity of the data and trust of data storage is managed by using Blockchain.
4. In this project, by using Hardhat we created a local blockchain, with a default smart contract, and deploy it. By making updates in the smart contract, for the storage service with the upload, share, and display prompts, we connect this smart

contract with Metamask for accounts handling and then embed it with the react application, to display as a web application. This way all the parts simultaneously play their role in the secure working of this decentralized cloud storage.

5. The uploading of the file, is done in a manner that each upload is considered as a transaction on Ethereum-based Blockchain. Thus, it acts as a currency for the transactions of these files. Similarly, the sharing and displaying of the data is done, but here, the account with access and the main account with the files stored in it can view the content stored. Accounts other than the main account and the shared access accounts will have no access to the data.

To provide a transparent, reproducible, and scientific literature review of blockchain-based applications, the process suggested by Briner and Denyer (2012) as well as some features of the PRISMA statement (Moher et al., 2009) have been adopted. The overall methodological approach includes the following steps:

1. Identify the need for the review, prepare a proposal for the review, and develop the review protocol.
2. Identify the research, select the studies, assess the quality, take notes and extract data, and synthesize the data.
3. Report the results of the review.

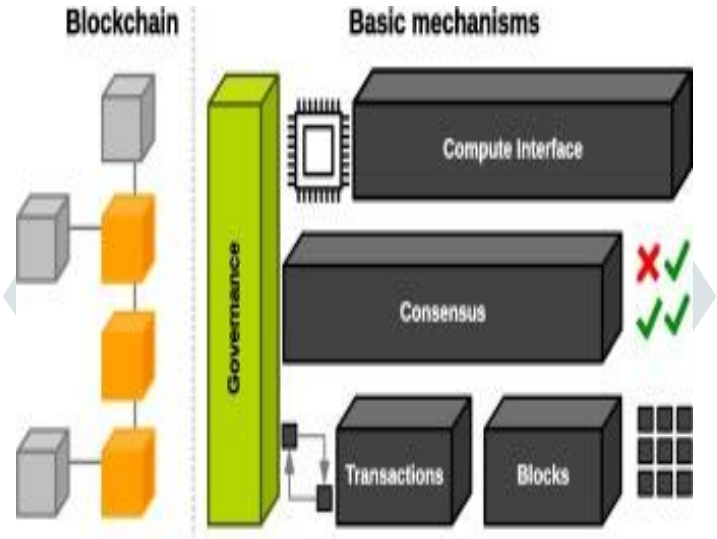

Fig. 1 Blockchain Mechanism

IV. FLOW-BLOCK DIAGRAM

The process of transaction i.e., initiating the upload or display of data taking place using the account created or handled by the user. Given the choice of either uploading the data or displaying the data, the user can interact with the created GUI. The data stored in the blockchain is stored in the form of small blocks which are connected to other small blocks on a node, thus multiple nodes happen to be present on a single server, providing working space.

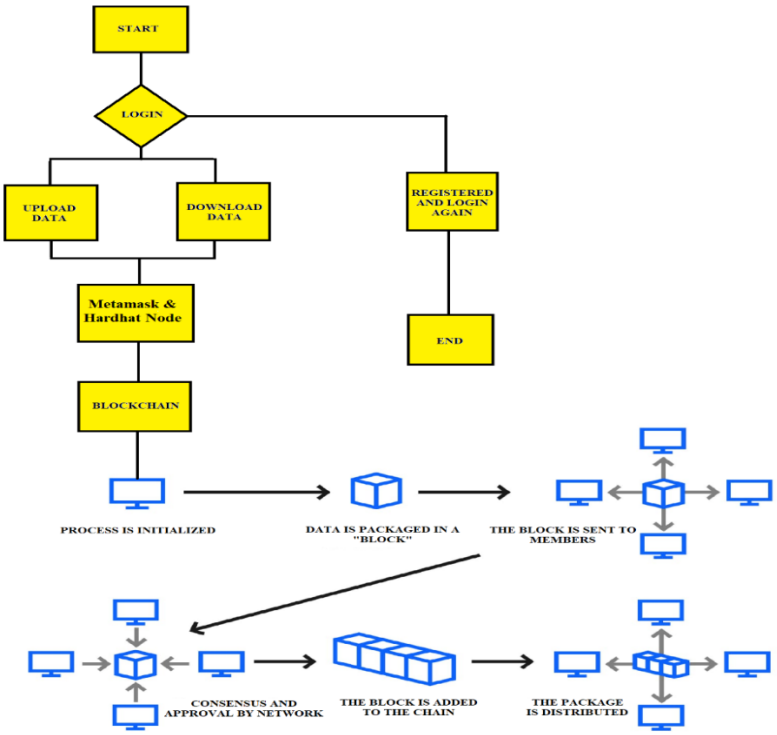

Fig. 2 Flow block diagram of Blockchain Process

V. SIMULATION RESULTS

Back-end Process UI

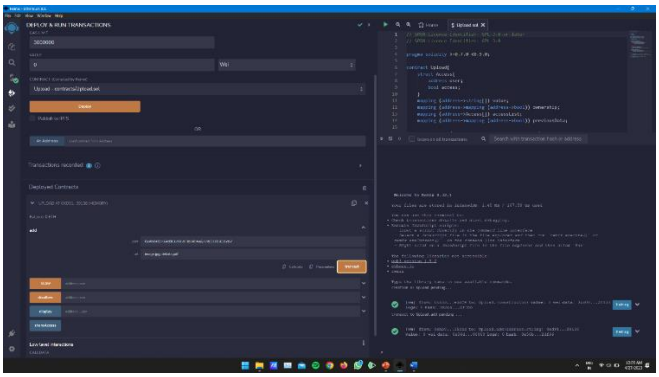

Fig.3 Backend process

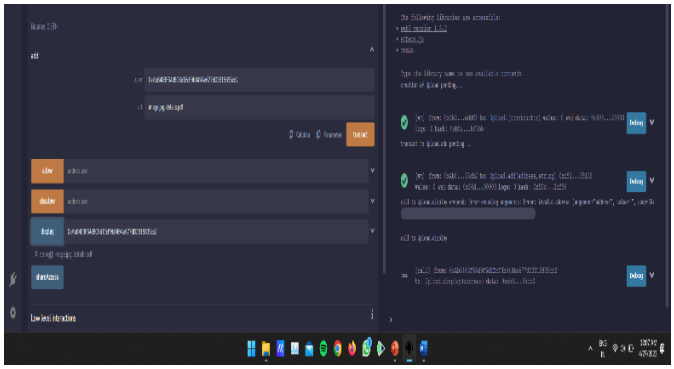

Fig. 4 Backend function invoking

Front-end UI

Fig. 5 Project UI

Fig. 6 FE-Uploading File

Fig. 7 FE-Transaction

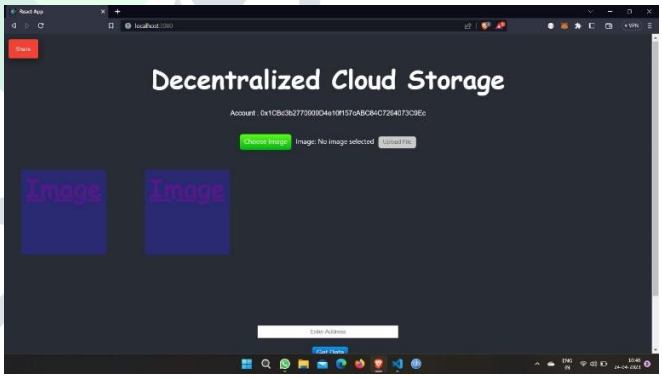

Fig. 8 File Uploaded

CONCLUSION

Cloud computing systems are popular for data sharing throughout many apps and network components. However, multiple copies of data follow different pathways to guarantee resilience, making it difficult for administrators to identify the origin of the assault, its impact, and its tool. The primary foundations of blockchain architecture are a combination of cryptography mechanisms and distributed public ledgers. This mixture enables the creation of any type of structure on a blockchain without causing any trust issues on the network. The same holds for blockchain-enabled cloud solutions. The blockchain Ethereum benefits the cloud by ensuring data provenance (verifying the data's source) and enabling cloud monitoring. If genuine data provenance exists in the cloud, with all data gathered on cloud servers, distributed data calculations, data transfers, and transactions, it would detect insider threats, replicate test findings, and identify the specific source of the system or network breach. Blockchain has developed a critical technique for ensuring security, particularly integrity, authenticity, and secrecy. These benefits prompted us to attempt to provide a security model using blockchain. We proposed a model for data storage security in cloud computing by using the blockchain Ethereum.

The developed system encrypted data using the ECC encryption algorithm, assuring the secrecy of the user's data. The IPFS protocol distributed and stored this encrypted data among network peers. The model addressed privacy and security issues associated with centralized cloud storage. Moreover, it provided a platform for peers to rent out underused storage and earn currency in the form of exchange, optimizing storage resource usage. The gap addressed was the amount of time taken to upload files, as determined by file size and the availability of peers. The time taken to upload a file grew proportional to its size.

This proposed system provided a distributed model for a cloud access control system that employs role-based access control. For available resources, we leveraged ECC encryption and Ethereum BC smart contracts. This then improved data security by encrypting and distributing data across different peers in the system.

ACKNOWLEDGMENT

At the outset, we would like to acknowledge our grateful thanks to our Project Guide Prof. M. G. Pallewar from the Department of Electronics and Telecommunication for her valuable guidance and suggestion regarding our project "Decentralized Cloud Storage using Blockchain". We would like to thank Prof/Dr. S. K. Jagtap, Head of the Electronics and Telecommunication department for her great moral support.
Last but not least, we would like to thank our staff and friends for their keen advice and support.

REFERENCES

[1] Li Dagang et al., "A Secure Data-Sharing Protocol Under Blockchain-Based Decentralized Storage Architecture", *IEEE Networking Letters*, vol. 1.1, pp. 30-33, 2019.
[2] D. Sivaganesan, "Blockchain enable Internet of Things", *Journal of Information Technology*, vol. 1.01, pp. 1-8, 2019.
[3] Meet Shah, Mohammedhasan Shaikh, Grinal Tuscano, "Decentralized Cloud Storage Using Blockchain", *IEEE Xplore*, 10.1109/ICOEI48184.2020.9143004 June 2020.
[4] Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2521–2549.
[5] J. Xue, C. Xu and L. Bai, "DStore: A distributed system for outsourced data storage and retrieval", *Future Gener. Comput. Syst.*, vol. 99, pp. 106-114, 2019.
[6] Y. Zhang, C. Xu, J. Zhao, X. Zhang and J. Wen, "Cryptanalysis of an integrity checking scheme for cloud data sharing", *J. Inf. Secur. Appl.*, vol. 23, pp. 68-73, 2020.
[7] Wassim Jerbi, Abderrahmen Guermazi and Hafedh Trabelsi, "Orphan node connected management in multi-hop clustering-based routing protocols for wireless sensor networks", *International Journal of Interdisciplinary Telecommunications and Networking*, vol. 11, no. 4, pp. l, October- December 2019.
[8] Wassim Jerbi, Omar Cheikhrouhou, Abderrahmen Guermazi, Habib Hamam and Hafedh Trabelsi, "A Blockchain based Authentication Scheme for Mobile Data Collector in IoT", *17th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 929-934, 2021.
[9] W Jerbi, O Cheikhrouhou, A Guermazi, M Baz and H. Trabelsi, "BSI: Blockchain to secure routing protocol in Internet of Things", *Concurrency Computat PractExper*, pp. e6794, 2021.
[10] G. Richa, Shalom, "Blockchain Decentralized Cloud", DOI:https://doi.org/10.22214/ijraset.2022.46810, September, 2022
[11] D. Vorick and L. Champine, "Sia: Simple decentralized storage", *Nebulous Inc*, 2014.
[12] Dhruv Doshi, Satvik Khara, "Blockchain-Based Decentralized Storage", *International Conference on Mobile Computing and Sustainable Informatics (pp.563-569)*, DOI:10.1007/978-030-49795-8 54, January 2021.
[13] Y. Hassanzadeh-Nazarabadi, A. Küpçü , O. Ozkasap, "Decentralized Utility- and Locality-Aware Replication for Heterogeneous DHT-Based P2P Cloud Storage Systems", 2020.
[14] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad and M.H. Rehman, "Decentralized Document Version Control using Ethereum Blockchain and IPFS", *Comput. & Elect. Eng.*, vol. 76, pp. 183-197, Mar. 2019.