The Scientific Temper (2023) Vol. 14 (3): 806-810
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2023.14.3.37
https://scientifictemper.com/

RESEARCH ARTICLE

An implementation of secure storage using blockchain technology on cloud environment

I. Bhuvaneshwarri*, M. N. Sudha

Abstract

Data generation and consumption have significantly increased recently, necessitating the need for secure and dependable file storage solutions. The vulnerability of current centralized storage solutions to data breaches and hackers compromises the security and integrity of user data. These problems may have a workable solution in a decentralized file storage system. In order to offer a secure and dependable storage solution, this paper proposes a blockchain-based file storage (BBFS) system that takes advantage of features like immutability, transparency, and security. Any user can upload unlimited files (one at a time) with this proposed system. Users can download and access those files on their machines as well as all other peers. As soon as a peer uploads a file, it is placed in a block along with the user name, file size, and file information. It is not possible to change or remove these blocks because they are added to the current blockchain. These blocks can be connected with cloud storage, giving users a safe place to store and access their files that cannot be altered. By integrating this proposed system with cloud storage, customers can take advantage of the scalability and security of cloud services as well as the immutability and security of blockchain. The proposed system addresses the cost and scalability problems that make to be widely applicable.

Keywords: Blockchain technology, Cloud environment, Implementation, Secure storage.

Introduction

Blockchain technology has gained traction across a number of sectors, and file storage is one of its most exciting potential uses. It is possible to build a more reliable, decentralized, and effective method for storing and sharing data by merging blockchain with cloud storage. Files are kept on centralized servers by traditional cloud storage providers, which makes them susceptible to downtime, hacking, and data breaches. The distribution of files across a network of computers via BBFS, in contrast, makes it far more difficult for hackers to access and alter the data. Users can take advantage of the positivity of both technologies by integrating cloud-based file storage with blockchain technology. They may take advantage of blockchain's decentralized and tamper-proof features while storing and accessing files safely and conveniently in the cloud. Businesses and people who need to keep sensitive information, such as bank records, contracts, and intellectual property, may find this to be particularly helpful. In general, cloud-based and blockchain-based file storage has the potential to completely change the way of distributing and saving data. The set of nodes is used to store data and do transactions in a decentralized manner. Each node has a copy of the blockchain that is updated in real-time by a consensus mechanism. As a result, it is almost impossible to change the data or compromise the system without access to the majority of the nodes. The system that is suggested in this study combines the benefits of both approaches by fusing blockchain technology with cloud storage. Available blockchain-based file storage choices include Filecoin, Storj, and Sia. Users of these services use cryptocurrency to pay for storage and bandwidth, and data is stored and retrieved utilizing decentralized networks of nodes. Some cloud service providers, including Microsoft Azure, are looking into blockchain technology for cloud management and storage. Finally, the suggested approach to cloud integration with blockchain-based file storage has the potential to revolutionize the access, sharing, and storage of data.

Department of Information Technology, Government College of Engineering, Erode, Vasavi College post, Erode, India.

***Corresponding Author:** I. Bhuvaneshwarri, Department of Information Technology, Government College of Engineering, Erode, Vasavi College post, Erode, India, E-Mail: ibw@gcee.ac.in

How to cite this article: Bhuvaneshwarri, I., Sudha, M.N. (2023). An implementation of secure storage using blockchain technology on cloud environment. The Scientific Temper, **14**(3): 806-810.

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.3.37

Source of support: Nil

Conflict of interest: None.

Received: 12/07/2023 **Accepted:** 10/08/2023 **Published** : 25/09/2023

Related Work

With the help of the blockchain data structure, digital data is safely saved. Blockchain is an open ledger that is accessible to multiple people at once. A blockchain is used to store all types of digital data, including transactional data, files, communications, and more. The consensus method, block mining, block validation, and other features are all part of a successful blockchain implementation. Large storage providers are the only sources of cloud storage. These storage companies handle the data transactions for storing, sending, and receiving data from an organization as reliable third parties.

According to Bhosale *et al.* (2019), this type of paradigm raises a variety of difficulties, including high operational costs, data accessibility, and data security. An open source software project called Metadisk aims to conceptually demonstrate how cloud storage services might be made more efficient, safe, and decentralized. It offers a framework for the prototyping of a totally decentralized network.

The main goal of Metadisk is to offer a reliable testing environment for the Storj peer-to-peer cloud storage network (Wilkinson *et al.*, 2014). Its ultimate goal is to offer a collection of tools that will make it simpler for Storj to interact with established platforms and users. Before any data is transferred from a client's PC to the cloud, it must first be encrypted, including filename, date, and other metadata. Politics or the law cannot be used as a centralized point of attack. All incentive payments will be automated and made in an anonymous cryptocurrency to both resource producers and consumers. It's time for the cloud to fully materialize as a collection of countless resource droplets that are continuously added to and removed from as the cloud moves and changes shape. The amount of data kept in computer settings has dramatically grown in recent years. Due to the volume expansion, it has become exceedingly challenging to store and handle a lot of data on a single server. Distributed storage technologies are being employed to fix issues with scalability and high availability on a single server. Utilizing related administrative techniques, distributed storage solutions advance the handling and serving of data over several nodes. Later, new storage infrastructures were created by implementing distributed storage strategies on fresh blockchain technology. However, a framework for analysing solutions that use this novel distributed blockchain technology is lacking in the literature. To the best of our knowledge, we outline the first classification and taxonomy of blockchain-based distributed storage technologies in this article. In addition, if the network or any of the storage nodes fail, it will have an impact on the entire architecture. As a result, the single point of failure issue may affect the entire NAS network in which the storage nodes are situated.

Due to NAS nodes' poor failure tolerance, the storage infrastructure is insufficient. The proposed taxonomy is used to investigate, compare, and assess the state-of-the-art solutions (Cangir *et al.*, 2021).

Li et. al, 2021 have developed secure P2P cloud storage with better reduced transmission delay. Nguyen *et al.*, (2019) developed a technique for ensuring data interchange reliability on mobile clouds while protecting sensitive health information from potential threats. When compared to previous data sharing models, the system evaluation and security analysis show performance gains in lightweight access control architecture, minimum network latency with high security and data privacy levels. The ChainFS on Ethereum and fuse based file system, as well as close integration with FUSE clients and Amazon S3 cloud storage. The system performance is measured and showed that it has a low overhead (Tang et al, 2018). The blockchain based secure storage system for healthcare system also developed (Xi *et al.*, 2022).

Existing System and its Drawbacks

The decentralized file storage system stores and retrieves files via a network built on the blockchain. Users can charge others to use their extra storage space. The inter planetary file system (IPFS), a peer-to-peer file sharing protocol, is the foundation for the blockchan platform. This blockchain based platform provides decentralised file storage. Users can safely store files on a distributed network of nodes. The software combines erasure coding and end-to-end encryption to make sure that files are safe and accessible. Blockchain workbench enables users to create and deploy blockchain applications, and it enables users to store and manage files on the blockchain. Other cloud services like Azure Storage and Azure Functions can be linked with these solutions. In this paper, file of information is created in blockchain, enabling users to upload or download any sort of file via a publicly accessible website. It ensures that the block is kept secret by using the SHA256 cryptographic technique. Proof of work is used as a consensus technique, requiring miners to crack any cryptographic conundrum before they can publish a new block on the chain. In the proposed application, to solve a challenge by finding a hash value that begins with three 0s. Finding the most appropriate system requires investigation and comparison of the many features and pricing structures offered by these systems. The shortcomings of the current system are,

- Running time of the insertion and other block-operations can be slow because it holds too much data to process;
- It is expensive and takes more resources to maintain.
- In this case, off-chain blockchain can be used to address on-chain blockchain problems.

Proposed System

Other cloud services like Azure storage and Azure functions can be linked with these solutions. In this paper, a file is created as a block in a blockchain as part of this paper,

enabling users to upload or download any sort of file via a publicly accessible website. It ensures that the block is kept secret by using the SHA256 cryptographic technique. Proof of work is used as a consensus technique, requiring miners to crack any cryptographic conundrum before they can publish a new block on the chain. In this paper, to solve a challenge by finding a hash value that begins with three 0s. Finding the most appropriate system requires investigation and comparison of the many features and pricing structures offered by these systems. The cloud storage system must provide the infrastructure for the system's storage. Any cloud storage service, including Amazon S3, Microsoft Azure, and Google Cloud Storage, can be incorporated into the system's design. The system gains advantages in terms of scalability, dependability, and performance with the incorporation of cloud technologies. The user produces a transaction that includes the file hash and metadata like the file name, size, and type in to upload a file to the system. The transaction is subsequently broadcast to all network nodes for confirmation and verification. The file is encrypted and sent to the cloud storage server after confirming the transaction. The file encryption key is kept on the blockchain network to maintain its security. The following are some benefits of the suggested system:

- Information is contained in safe blocks, which can increase the security of on-chain blockchain.
- Information can be easily restored in the event of a system breakdown.
- More dependable and usable.

System Specification

Hardware refers to the actual parts of the computer, such as the motherboard, hard drives, RAM, and processor. The executors of the commands given by software programmes are hardware devices.

Platform	: Windows 10, Windows 11
Processor	: INTEL
Pentium RAM Capacity	: 8 GB
RAM Hard disk	: 50 GB

The software requirements are: Flask,Numpy,Requests and Werkzeug.

System Architecture

The entire system architecture has the following steps (Figure 1):

- User initially send the request for apply for admission to the middleman.
- Based on the user's admission request, the middleman sends the agreement to admission.
- The next step is the user to send the encrypted data to the middleman.
- The middleman distributes the file data blocks to each storage user.
- The user then issues an integrity challenge to the storage provider.

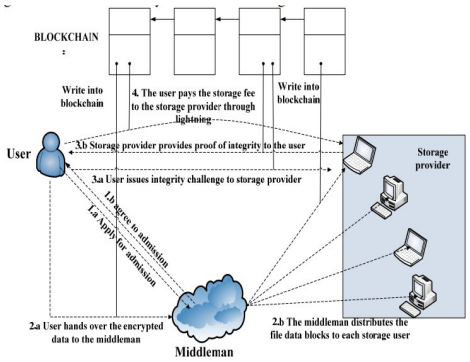

Figure 1: System architecture of the proposed system

Sources: "Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum" by Nabeel Khan, Hana Aljoaey, Mujahid Tabassum, Ali Farzamnia, Tripti Sharma and Yew Hoe Tung in MDPI

- Then the storage provider provides proof of integrity to the user.
- The user pays the storage fee to the storage provider through lightning.
- Finally, the user writes the information securely onto the blockchain blocks.

Procedural Diagram

The procedural steps in the proposed system is depicted in the Figure 2 are as follows:

- Initially, the user chooses a blockchain platform.
- The user develop a user interface.
- Creation of a smart contract.
- The user performs authentication and authorization.
- Integration with the cloud environment.
- The user creates the blockchain and upload the files in the blockchain.
- The files created are stored under the blocks.
- Upload the blocks into the cloud.
- Implement encryption and access control.
- Test and deploy the proposed system.

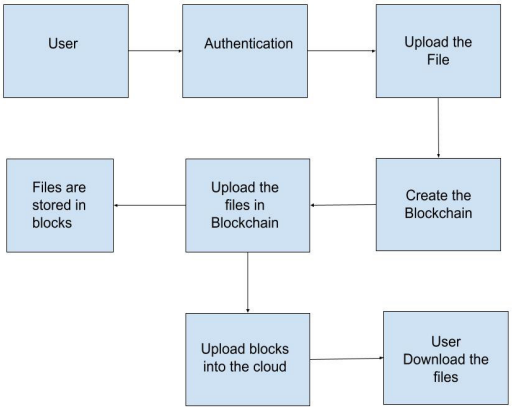

Figure 2: Procedural steps in the propsosed system

Table 1: Comparison between traditional and blockchain based secure storage

Traditional secure storage	*Blockchain-based secure storage*
Belongs to single-ownership	Blockchain establishes with more nodes each owner is different
Mutable in nature	Blockchain is immutable in nature
External security mechanisms are used to provide security to storage	Built in secure system
There is no link between previous block of storage with current block	There is link between previous block of storage with current block through hash values
Nonce value is not used	Nonce value is used

Comparison between Storage Systems

The comparison between traditional storage system and blockchain based secure storage system is given in the Table 1.

Results and Discussion

The suggested solution in this research employs blockchain technology to provide secure distributed data storage. The system enables the user to upload data via the IPFS, which distributes data content to cloud nodes at the global level network and ensures data availability by retrieving data files via Uniform Resource Locators (URLs) based on the hash values of the files uploaded to IPFS. As a result, only the person with the hash value of the data uploaded to the IPFS network can access the file. The suggested solution protects data privacy by assuring the immutability of the blockchain and storing it on a distributed global network. The speed of accessing data from traditional secure storage versus blockchain with 5 nodes is depicted in Figure 3.

Figure 3 shows that the accessing speed of the blockchain with 5 distributed nodes outperforms the traditional secure storage. The proposed system is built with smart contracts, Ganache Blockchain was tested on the Ethereum blockchain platform. A web application that provides an interface for non-technical users as well as an underlying application programming interface (API) for native apps and feature additions was also built. Financial transactions are conducted via cryptocurrency, and trust is established between client and host via cloud storage. A user interface and smart contract are created using blockchain technology. Authentication and authorization ensure the security of file storage. The files are immutable and are written beneath the blocks. The blocks are then added to the blockchain and

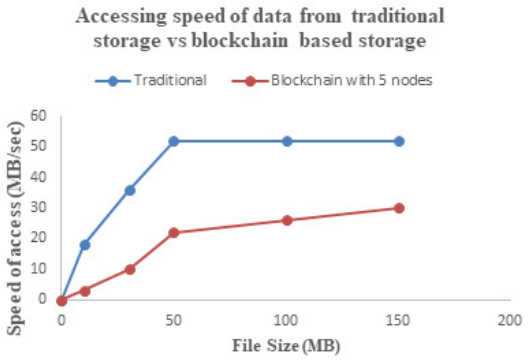

Figure 3: Accessing speed of data from traditional versus secure blockchain storage

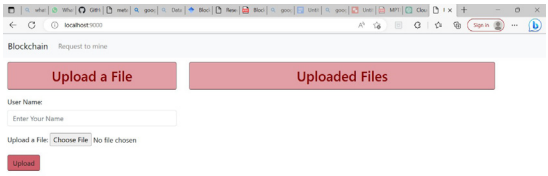

Figure 4: User interface for uploading a file

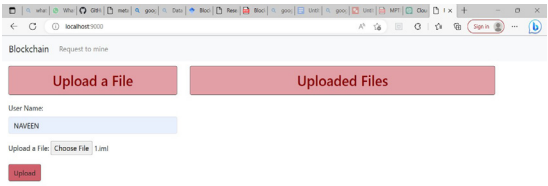

Figure 5: Select file for uploading

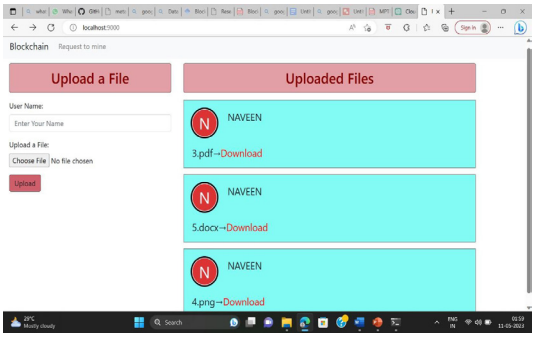

Figure 6: Select files for downloading

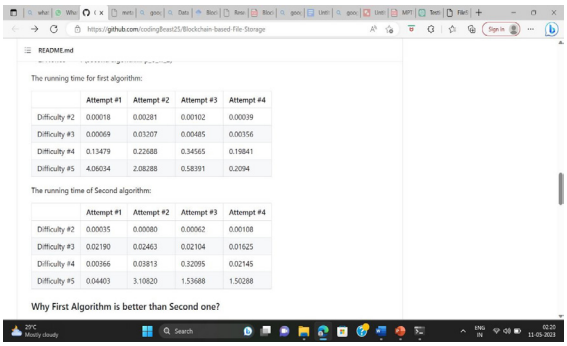

Figure 7: Display file content after downloading

uploaded to the cloud. After completing the authentication and authorization mechanism, the user wishes to download files from the cloud. The sample output screenshots are given in Figures 4 to 7.

Conclusions and Future Work

The proposed system demonstrated the feasibility of using blockchain technology for secure and decentralized file storage. Compared to traditional centralized file storage solutions, the system provides several benefits, including increased security, immutability, and transparency. It identified some challenges and limitations of the existing system, such as scalability issues and potential regulatory hurdles. This paper addresses the above-mentioned challenges and improves the system's usability and scalability. This paper also has implications for various industries, such as healthcare, finance, and government, where secure and tamper-proof data storage is critical. Overall, the conclusion of this paper should provide a clear and concise summary of the proposed system's main findings and contributions, highlighting the potential impact of the proposed system on the broader community. The current blockchain technology has scalability limitations, and the file storage system needs to accommodate increasing amounts of data. Our future work could explore different blockchain-based storage solutions or combine blockchain technology with other technologies to enhance scalability. BBFSneed to be interoperable with other systems to ensure data exchange and integration.It would investigate standardizing data formats and APIs to enhance interoperability. The success of the BBFS project largely depends on its usability and user experience. Future work could focus on designing and developing user-friendly interfaces and applications that allow users to interact with the system easily. As blockchain technology evolves, regulations around it will also change. Future work could focus on studying regulations related to BBFS and ensuring compliance with them. The blockchain-based file storage system can be integrated with other blockchain applications such as smart contracts, digital identity management, and supply chain management. Future work could focus on exploring the potential benefits of such integrations.

Acknowledgment

We are thankful to the management for conducting this collaborative study.

References

Bhosale, K, Akbarabbas, K, Deepak, J, Sankhe, A. (2019). Blockchain based secure data storage. International Research Journal of Engineering and Technology (IRJET), 6(3):5058-5061.

Bhuvaneshwarri, I (2023). Blockchain Technology based Secured Framework for Healthcare Systems. Gradiva Review Journal, 9(6): 944-950.

Bhuvaneshwarri, I (2023). Determination of factors affecting stock market analysis during war, pandemic period using rough set and scalable future stock market price prediction model. Gradiva Review Journal , 9(6): 1137-1143.

Cangir, O,F, Cankur, O, Ozsoy, A. (2021). A taxonomy for blockchain based distributed storage technologies. Information processing & management, 58(5):102627.

Li, J, Wu,J, Chen, L. (2018). Block-secure: Blockchain based scheme for secure P2P cloud storage. Information Sciences, 465:219-231.

Nguyen, D.C, Pathirana, P.N, Ding, M, Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE access. 7: 66792-66806.

Tang, Y, Zou, Q, Chen, J, Li, K, Kamhoua, C.A, Kwiat, K, Njilla, L.(2018). ChainFS: Blockchain-secured cloud storage. In proceedings of 11th international conference on cloud computing (CLOUD), IEEE, 987-990.

Wilkinson, S, Lowry, J, Boshevski, T. (2014). Metadisk a blockchain-based decentralized file storage application. Storj Labs Inc., Technical Report, hal.,1(11).

Xi, P, Zhang, X, Wang, L, Liu, W, Peng, S. (2022). A review of Blockchain-based secure sharing of healthcare data. Applied Sciences. 12(15):7912.

Zhang, Y, Xu,C, Cheng,N. (2019). An Accurate Blockchain-Based Time- stamping scheme for Cloud Storage. IEEE Transactions on Services Computing, 13(2):216-229.