MANTECH Publications

Journal of Cloud Computing and Internet of Things
Volume 1, Issue 1, January-June, 2023

Block chain Based Cloud Storage System

Sarswati Apsingekar[1], Chaitrali Nakhate[2], Swamini Tarange[3], Siddharth Payghan[4]

Student [1,2,3,4]

Department of Computer Science Engineering

Indira College of Engineering & Management Parandwadi Tai Maval

Corresponding Author Email:- *saraswatiapsingekar@gmail.com [1]*

Abstract

An essential component of the cloud storage environment is data security. Preserving very important user data in the cloud is critical. The Interplanetary File System (IPFS) offers a content-addressable block storage format for storing and distributing files in a distributed environment. It is a version-controlled file system in a peer-to-peer architecture. We have developed a block chain-based architecture to share the file utilizing content-addressable block storage in the peer-to-peer paradigm in accordance with an IPFS feature. We've developed a distributed storage architecture based on block chain technology and IPFS that secures the resource's immutability, integrity, and availability in order to circumvent the availability, dependability, storage overhead, and other problems associated with centralized service providers. In this system, we store the file on IPFS and the transaction-level addressable content (hash) on the block chain. The issue of a centralized service provider's availability, dependability, and storage can be successfully resolved by our suggested plan.

Keywords: *IPFS, Cloud Storage Environment, block chain, peer-to-peer*

INTRODUCTION

Services are accessible 24/7 on a variety of platforms, so businesses do not need to keep internal storage. Despite the mentioned advantages, cloud storage has a number of drawbacks. They are preserving the privacy and accuracy of the data. Sensitive information may be present in data saved in the cloud. However, this is when problems with copyright are raised.

Anyone other than the owner of the data can access it because we are transferring it to an external environment. The most important factor to take into account when storing data on the cloud is security. Loud service providers, however, do not always guarantee a high level of security. With the aid of a Secure Data Storage and Access Solution based on Block chain, the system offered in this project will assist in resolving all the difficulties listed. By keeping track of user actions, Block chain in this study improves the security of the data stored in the cloud. Block chain will also protect the data from different threats.

Block chain technology is a promising development for the future. It can assist us in creating systems that are more dependable and safe. No of the sort of data, these solutions will work with it. In other words, we can utilize it for electronic papers, multimedia material, etc.

It is not a smart idea to keep this massive quantity of data directly on the block chain because doing so will raise block size and chain length. Therefore, the data that will enable us to detect document tampering will be recorded on the block chain along with the documents, which will be saved in the cloud.

MOTIVATION

The issue of keeping a vast amount of data is one that many organizations now face. Organizations have started using cloud storage as a way to store data in order to solve this problem. As a result, cloud-based services have grown during the past several years. These services provide features like sharing and data transfer, as well as remote user data storage on the cloud. The most important factor to take into account when storing data on the cloud is must have security. Loud service providers, however, do not always guarantee a high level of security.

PROBLEM DEFINATION

One of the most important technologies of the present century is block chain. It offers a remedy for problems with accountability, transparency, trust, and traceability. The authors of suggested a system to guarantee digital data rights administration. The permanent record of agreements between data owner and user is stored on a block chain. By agreeing to the terms and conditions stored in the block chain, a user requests the data from the owner. By utilizing block chain, the suggested method offers transparency, traceability, and fine-grained granularity over research data.

LITERATURE SURVEY

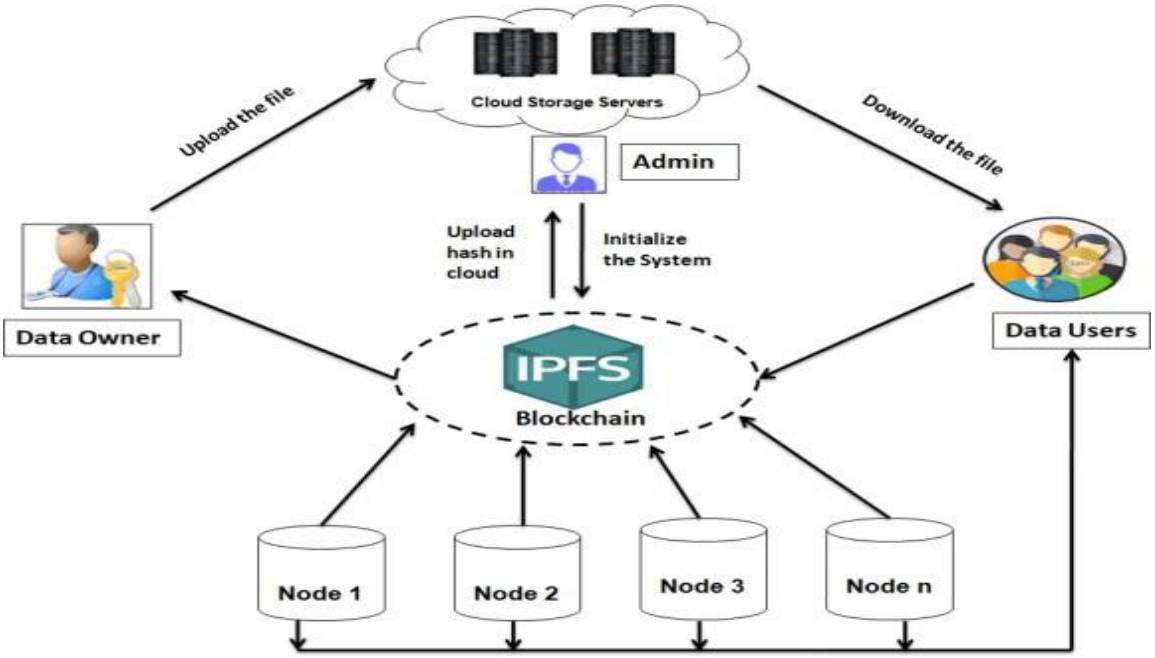
SR No	Title Of Paper	Year	Authors	Key Points	Limitations
1.	Block chain-Based Secure Data Storage and Access Control System using Cloud	2019	Shubham Desai, Rahul Shelke, Omkar Deshmukh, Harish Choudhary, Prof. S. S. Sambhare	Block chain, Cloud Storage, Smart Contract, Encryption, Decryption	It provides a model to access data stored in untrusted cloud storage. The data will be stored in cloud storage and the information identifying the file will only be available on the block chain.
2.	A Survey on the Security of Block chain Systems	2020	XiaoqiLia, PengJianga, Ting Chenb, XiapuLuoa,∗, Qiaoyan Wen	block chain, security, crypto currency, smart contract	We can't trust the cloud provider in every case.
3.	Research on Cloud Data Storage Technology and Its Architecture Implementation	2020	Kun Liu, Long-jiang Dong	Cloud Computing; Cloud Storage; Web Operating System; Distributed File System;	Technical security issues arising from adopting the cloud computing model such as XML-attacks, Browsers related attacks, and flooding attacks.
4.	Block chain Based Cloud Computing: Architecture and Research Challenges	2020	Ch. V. N. U. Bharathi murthy1, m. Lawanya shri1, SEIFEDINE KADRY 2, (senior member, IEEE), AND SANGSOON LIM	Cloud computing, Block chain technology, data security, decentralization, data	Security issues in SaaS In SaaS, the client has to depend on the vendor for proper security paradigms. The

				management.	provider must do the work to keep multiple users from seeing each other's data. So it becomes difficult to the user to ensure that right security measures are in place.
5.	'Machine Learning based Health Prediction System using IBM Cloud as PaaS,'	2019	A. A. Neloy, S. Alam, R. A. Bindu and N. J. Moni	Cloud Computing; Cloud Storage; Machine Learning; PaaS architecture;	PaaS is intended to enable developers to build their own applications on top of the platform. As a result it tends to be more extensible than SaaS, at the expense of customer-ready features. This tradeoff extends to security features and capabilities, where the built-in capabilities are less complete.
6.	'Proposed blockchain based healthcare system with an attributed based signature	2020	Su Q, Zhang R, Xue R, Li P	Blockchain, Healthcare System, Attribute-Based Signature, Privacy.;	Overloads the user node due to key related processing overhead.

	method for the revocation process'				
7.	A Blockchain based Secured Healthcare Framework	2020	Mohammad Tabrez ,FahadAlgarni, AlaaAbdElhamidRadwan, GoramMufareh M Alshmrani.	IoT, Blockchain, Cybersecurity, EHR	Limited availability of technical data
8.	Present blockchain based anonymous authantication with revocation method	2015	Yong Yu, Member, IEEE, Yanqi Zhao, Yannan Li, Student Member, IEEE, Xiaojiang Du, Senior Member, IEEE, Lianhai Wang and Mohsen Guizani, Fellow, IEEE	Smart Industry, Anonymous Credentials, Blockchain, Accumulator, Revocation.	Only specially designed for authentication process in smart industrial application.
9.	Suggest a proxy-assisted access control mechanism of cloud data for smart cities	2017	Fan K, Wang J, Wang X, Yang Y	Smart cities .Cloud computing .Attribute-based encryption .Revocation	Dependent on trusted certificate authority for the management of key related information.
10.	A smart-contract-based access control frame-work for cloud smart healthcare system.	2021	Saini Q, Zhu N, Singh Y, Xiang LG, Zhang Y	Access control, blockchain, cloud storage, ethereum, smart contracts, smart healthcare.	Lacks revocation procedure and suffers from scalability issues.

PROPOSED SYSTEM

System Architecture



A decentralized system based on block chain is proposed to address problems including single authority failure, internal employee data manipulation, communication overhead, and excessive processing overhead at the consumer side. Data access logs can be tracked via the block chain, enabling auditable access control management. In this research, a decentralized access model based on block chain technology is proposed as a secure and effective data transfer mechanism. Through the IPFS protocol, the idea of a decentralized block chain is put into practice. In Fig., the decentralized system model is mentioned. The data owner uploads the data to a cloud server in a decentralized system, and the block chain network generates the hash value of the file.

This cryptographic hash code is produced using the SHA256 key management method. The hash value is shared among network users that have permission to access the material. Data users with access rights have access to both the hash code and its original content. Because every time a modification is made to data, the block chain generates a new hash code representing the altered data, making it impossible for any other user or member of the decentralized network to alter the original data. Decentralized data access is therefore safer than centralized. The single point of failure issue is also resolved by

the decentralized system because block chains function as dispersed systems. Because there is no single authority in a block chain network and every node maintains a copy of every other node's data, data may be recovered quickly in the event of a failure

CONCLUSION

To address the issues of a single point of failure, data change by internal staff, excessive processing, and overhead during communication at the data consumer side, a decentralized system based on block chain is provided. The centralized system is changed by the advent of distributed IPFS technology based on block chains. The centre authority is no longer necessary to protect the distribution key against an attack. A distributed access control system with indirect data owner and data user interaction is constructed using IPFS. Because a block chain generates a new hash code for modified data each time it is changed, the original data on a decentralized network cannot be altered by any other users or members. Decentralized data access is therefore safer.

REFERENCES

1. Shubham Desai, Rahul Shelke, OmkarDeshmukh, Harish Choudhary, Prof. S. S. Sambhare "Block chain Based Secure Data Storage and Access Control System using Cloud" IEEE - ICCUBEA 2019.

2. Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solid it Maximilia006EWöhrer and UweZdun University of Vienna Faculty of Computer Science Währingerstraße 29, 1090 Vienna.

3. A Survey on the Security of Blockchain Systems XiaoqiLia, PengJianga, Ting Chenb, XiapuLuoa,∗, Qiaoyan Wen. Department of Computing, The Hong Kong Polytechnic University, Hong Kong SAR Center for Cyber security, University of Electronic Science and Technology of China, China State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China.

4. Xiaoqi Li, Peng Jiang, Ting Chen, XiapuLuo, QiaoyanWen,"A Survey on the Security of Blockchain Systems",beijing university China, 2018.

5. Rongzhi Wang, “Research on data security technology based on cloud storage”, 13th Global Congress on Manufacturing and Management, GCMM, 2016.

6. ZibinZheng, ShaoanXie, Hongning Dai, Xiangping Chen, and Huaimin Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE 6th International Congress on Big Data, 2017.

7. JulijaGolosova et.al. “The Advantages and Disadvantages of Blockchain Technology”, IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018.

8. MrAnup R. Nimje et.al. “Blockchain Attribute Based Encryption Techniques in Cloud Computing Security: An Overview” IJCTT Volume 4 ,Issue 3-2013.