DATA SECURITY AND ACCESS CONTROL SYSTEM BASED ON BLOCKCHAIN USING CLOUD

Sagar Gangwani
MIT School Of Engineering
MIT ADT University
Pune, India
sagarrgangwani@gmail.com

Prof. Reetika Kerketta
MIT School Of Engineering
MIT ADT University
Pune, India
reetika.kerketta@mituniversity.edu.in

Abstract: ***Today, major storage providers are the only sources of cloud storage. These storage companies take on the role of unreliable third parties who handle data in order to transfer, store, and receive data from a business. Numerous problems exist with this system, including excessive operational costs, subpar software, and data security. In this study, we provide a multi-user access control system concept for databases that make use of blockchain technology to provide reliable, distributed data processing. Using a web interface, the data owner can upload the data to the system. As a result, the folder can only be accessed by the user who has the secret key to the data that has been encrypted and uploaded to the Cloud.*** **Actually, by maintaining the blockchain's integrity and consistency while processing it on the cloud, the technology enhances data privacy. We designed a safe, blockchain-based data storage and access control solution to increase the security of cloud storage.**

Keywords **– Blockchain, Cloud Storage, Encryption, Decryption, Security, Distributed**

I. INTRODUCTION

In the modern day, maintaining enormous volumes of data for huge companies that operate abroad has proven difficult. Because cloud storage provides better archiving, distribution, and upload capabilities, many firms have switched to it. Maintaining data confidentiality and integrity while also assisting with data security are the main concerns that cloud computing needs to cope with. Most people decide to save their personal information in the cloud. However, there are a few security and copyright issues with the information. The main problem with sending data to an outside environment is that someone other than the owner can access it. Cloud service providers do not offer the level of security and privacy necessary for effective data security and privacy.

The technical solutions, policies, and practices you put in place to safeguard cloud-based systems and apps, along with the data they contain and the user access to them, are collectively referred to as cloud data security. Data confidentiality, integrity, and availability, commonly referred to as the "CIA trinity," are the fundamental tenets of information security and data governance.

Confidentiality: preventing unwanted access to and disclosure of the data Integrity: preventing illegal data change to ensure its reliability.

Availability: ensuring the data is fully available and accessible when it's needed

The blockchain keeps track of all information exchanged during transactions, and nearly no one can alter the data after it has been entered. As a result, compared to other security methods, blockchain technology is easier to use and more efficient.

This study provides a system that employs the Blockchain-based Secure Data Storage and Access System to provide data storage in order to address this issue. Therefore, we suggest that Blockchain be employed as a reliable Smart contracts use computer protocols to automate functions, cutting down on the amount of time needed for various corporate processes. The automated agreements reduce the possibility of third-party manipulation by eliminating the requirement that brokers or other middlemen confirm the already signed legal contracts. environment to strengthen the security of cloud storage and guard against exploitation attacks.

Blockchain is a peer-to-peer network that records transactions in a decentralised, tamper-proof electronic ledger. All network users contribute to the ledger, which records all data sent between nodes in a sequential chain of blocks linked by cryptographic hashes.

II. ADVANTAGES OF BLOCKCHAIN

Transactions that are approved and sent over the network enable the immutability of the Blockchain. Once a transaction is connected to the Blockchain, it will be impossible to change or remove it. It also depends on the type of system used: a centralised system can be changed or deleted because only one person makes the decision. In contrast, each device in the Blockchain network duplicates the transaction connected to the Blockchain if the system is distributed, such as the Blockchain. As a result of this advantage, Blockchain technology is unchangeable and unbreakable.

Transparency on the blockchain is a feature that develops at the copying stage of a transaction. Each transaction is recorded on a machine in the Blockchain network, as was already said. Since every member has access to all transactions, the Blockchain is transparent in that all activity is accessible to all users.

SMART CONTRACT:

The conditions of a contract between two dishonest people can be created, implemented, and enforced using a smart contract, which is a programme that runs on the blockchain. Fundamentally, it operates on its ownA smart contract's primary goal is to dynamically enforce its terms once the predetermined criteria have been met. As a result, it has lower

transaction costs when compared to conventional services that demand the execution of the contract by a reliable third party. A variety of blockchain technologies, most notably Ethereum, can be used to create smart contracts. This is because the Turing-completeness property of the Ethereum platform permits the development of more intricate and customisable contracts.

III. RELATED WORK

There are many security mechanisms that have been put forth by various researchers. In this section, we present a review of the literature on the subject.

"Blockchain-based System for Secure Data Storage with Private Keyword Search" was developed in 2017. Blockchain technology was used by Hoang Giang Do and Wee Keong Ng to present a system that offers a secure distributed data storage system with keyword search functionality. These systems enable users to spread data content across cloud nodes, upload data in encrypted form, and employ cryptographic techniques to guarantee data availability. Once a particular file has been pulled from the data repository, it must be encrypted in order to be accessed. The aggregate key is only accessible to certain individuals, but the trapdoor key for a particular community is made available to everyone.[11]

In 2018, "A Blockchain-Based Access Control System for Cloud Storage" presented by Ilya Sukhodolskiy and Sergey Zapechnikov suggested a blockchain-based user access framework for cloud storage. This gives a framework for recovering data stored in shaky environments, such cloud storage. For instance, the metadata identifying the file will be accessible on the blockchain, while the data, such as multimedia files, documents, and so forth, will be safely stored on the cloud. A blockchain will encrypt and restrict access to the anonymous data it stores before processing it. The client who wishes to view a file must be compliant with the access policy and possess the key necessary to unlock and decrypt it. The decryption keys are provided by the owner of the information. Blockchain and smart contracts ensure the adaptability of access policies, other stakeholders' ability to modify access policies without requiring additional security measures to keep user keys unchanged, security and privacy of all transaction data, facts that are accepted and rejected and the impossibility to edit and modify these data. [8]

In 2019, "Blockchain based Secure Data Storage and Access Control System using Cloud" is published by Shubham Desai and Omkar Deshmukh all have describe a multi-user access control system for databases that uses blockchain technology to deliver robust, distributed data processing. Finally, by processing the blockchain in the cloud, the technology promotes data privacy. retaining the blockchain's immutability. To improve the security of cloud storage, this proposes a secure, blockchain-based data storage and access management system.[5]

In 2020, "Evolutionary survey on data security in cloud computing using blockchain" is published by S.Prianga, R. Sagana, and E. Sharon. They conduct a survey on security challenges, highlighting the effectiveness of security as it relates to cloud computing and blockchain technology. A detailed understanding of a PoW–based blockchain model leveraging blockchain technology is also included in this survey. The goal of this project is to provide a comprehensive overview of blockchain technology, which is rapidly gaining popularity.[3]

Mrs. Rohini Pise and Dr. Sonali Patil proposed that decentralized cloud storage be linked with blockchain technology to better data security and storage procedures in their paper "Enhancing Security of Data in Cloud Storage using Decentralized Block chain" released in 2021. It successfully prevents data from being changed or deleted in part. The data stored there is connected through the chain of blocks that makes up blockchain. As a result, there's a lower chance of data manipulation. This is done using the SHA-512 hashing technique.[2]

Summary

Following are a few of the challenges or problems that were found when reading and evaluating the study articles:

- Some Papers primarily focused on data confidentiality, neglecting to include integrity, non-repudiation, and authenticity. How security mechanism make secure the cloud data storage
- Few of the papers were of a theoretical nature, suggesting that no work on a real-world application was done.
- In other papers, the proposed technique appears to be dependable, but it appears to be strange, convoluted, and difficult to execute.
- Some proposed techniques, such as Access Control and Data Confidentiality, were also not experimentally proven (ACDC). How the ACDC make more secure cloud data storage using various security mechanism.

IV. SOLUTION METHODOLOGY

One of the most significant and useful technologies in the world today is cloud computing. A digital storage option known as cloud storage keeps data safely on numerous servers spread out throughout the globe. Local storage is being directly competed with by the growing popularity of cloud storage in recent years. For many different third-party service providers today, cloud computing has emerged as a promising computing paradigm. Data owners can store their data in the cloud and offer access to businesses who need it thanks to the cloud's provision of a data storage solution. [9]

While cloud computing has numerous advantages, it also comes with a slew of security concerns. The following are some security concerns around cloud storage:

a. Data PrivacyNobody wants their data to be viewed without their consent. Privacy is the capacity of an individual or a group to keep themselves apart or to selectively reveal information about themselves. Additionally, when data is

kept and managed on the cloud, users have control over it, preventing theft, criminal use, and unauthorised sales. This seems easy to maintain if you keep your data locally, but what about the other cloud? It could be challenging to ascertain how open it is as your personal information is stored somewhere.

b. Lack of Control: You greatly reduce your worry when you rely on a third party to store your data for you. This, however, has two disadvantages. On the one hand, you won't have to deal with the data; on the other, someone else will. If something goes wrong with your data, such as a power outage or a ransomware attack, you won't be able to access it. You're completely reliant on your service provider to handle these issues. Your data grows more harmful the longer it is exposed to the elements.

C. Data Leakage: Making sure that no one from outside the firm tries to access documents is a key part of cloud data storage. The intention is to prevent the information from being disclosed to anyone outside the company. Data leakage is a serious issue since external sources have access to sensitive or private information.

d. Data Breaches: These are the effects of an assault or the carelessness and mistake of a worker. This is the main area of worry for cloud systems. Implementation errors or inadequate safety precautions can also result in information leaks. Employees' own computers or laptops can be used to log into cloud services, exposing the system open to malicious assaults. Examples of data that shouldn't be made public include private medical information, financial information, secret information, and proprietary information.

To address the above - mentioned security concerns, I propose a "Blockchain-based secure data storage and access control system" paradigm. Blockchain technology is employed in this model to improve the security of cloud data. The access URLs for the articles will be kept on the blockchain. The owner of the data will first encrypt the papers before sending them to the cloud. The documents will be encrypted using the AES-256 encryption method. These documents can be decoded using the aggregate key supplied by the data owner.

The user must first authenticate their identity before they can access data saved in the cloud. After verification, the user does a keyword search on the required file to look for any number of documents. The public trapdoor key for each file will only be available to users who have been given permission by the data owner. The user will ask the information owner for access to the data stored there if they find the requested file in the cloud. When an information owner receives a request, he or she provides the aggregate key or hash keys to the user who asked for access to the information. The user can now use the aggregate key to access the blockchain link.

AES-256: AES is a symmetric key key cypher. As a result, the secret key, which is required for both encryption and decryption, must be copied by both the sender and the recipient of the material. As a block cypher, AES is also categorised. The information that has to be encrypted (sometimes referred to as plaintext) is separated into units called blocks in this sort of encryption. Data is separated into a four-by-four array holding 16 bytes in the 128-bit block size of AES. Because each byte is eight bits long, each block has a total of 128 bits. Both the plaintext and the encrypted data are 128 bits in size, which is the same as the plaintext.

This is simply a Graphical representation of access control system model steps. As the steps are displayed sequentially, it is widely used to represent the flow of algorithms, workflows, or processes. It demonstrates the access control system model's step-by-step execution method.

This model shows the how the blockchain technology is used to secure the cloud data storage using access control system. This model demonstrates how crucial a role blockchain plays in securing cloud computing.

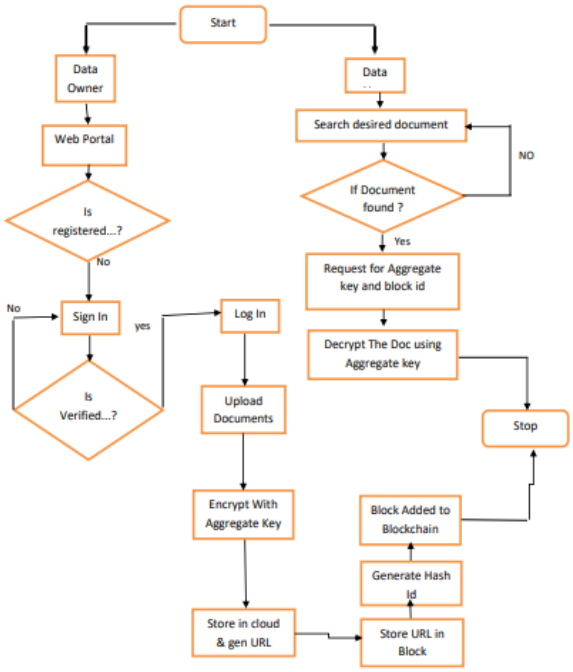

Fig 4.1 Blockchain based Access Control System Model for Data Security

Key cypher AES uses symmetric keys. As a result, both the sender and the recipient of the data require a copy of the secret key, which is used for both encryption and decryption. AES is likewise categorised as a block cypher. The information that has to be encrypted (sometimes referred to as plaintext) is separated into units called blocks in this sort of encryption. Data is separated into a four-by-four array holding 16 bytes in the 128-bit block size of AES. Each block has a total of 128 bits because each byte is eight bits long. The plaintext and encrypted data have the same size: 128 bits of plaintext equal 128 bits of ciphertext.

The Text File Size in MBytes	AES (256 bit)	DES (56-bit)	Blowfish (448-bit)
Text File(2.5MB)	40.5	16.2	10.7
Text file(4.3MB)	71.07	28.2	17.66
Text File(5.6MB)	90.63	36.2	22.53
Text File(7.3MB)	118.17	47.2	29.37
Average Time	80.09	31.95	20.06

V. ENCRYPTION ALGPRITHM COMPARISON

Three text files (2.5mb,4.3mb,5.6mb,7.3mb) were utilized to generate three experimental outcomes, with five cryptographic methods (AES-256, DES-56, Blowfish-448) being employed in each experiment. Each algorithm's performance was assessed in terms of speed, memory file size, and throughput.

Table 5.1: The Time Evaluation of various cryptography techniques using various text files. [5]

$$\text{Throughput} = \frac{Total\ Text\ Files\ Size\ in\ (MB)}{Total\ Evaluation\ Time\ of\ Algorithm\ in\ (ms)}$$

The total average time and Throughput	AES (256-bit)	DES (56-bit)	Blowfish (448-bit)
Total Average Time	80.09	31.95	20.06
Throughput	0.23	0.59	0.95

Table 5.2 The Time Evaluation of various cryptography techniques using various text files. [5]

Any cryptography algorithm's encryption time is the time it takes for the encryption technique to transform plain text to cypher text Encryption is used.
The throughput of any encryption process is calculated as the entire amount of time it takes to complete it. plaintext encrypted (in bytes) divided by encryption time (in ms).
In terms of processing time, table 1 demonstrated the superiority of AES over other algorithms. After AES, DES is the better algorithm since it takes less time to assess than other algorithms.

For various data input sizes, the performance execution times for the algorithms DES, AES, and Blowfish are shown in Fig 6.1.1 Blowfish has the worst execution, as is evident. AES is first used across all input sizes, then DES.
The speed of the algorithm during the encryption and decryption processes, Blowfish works fast due to its bulk encryption and decryption.as effective as AES.

Blowfish was not subject to legal protection, which explains why it was so widely used. The block size of Blowfish is 64 bits, while AES is 128 bits. Small block size can be a severe security issue; Blowfish is more vulnerable to attacks as a result of its small block size. The throughput of each algorithm when evaluating the same text files was shown in table 2.

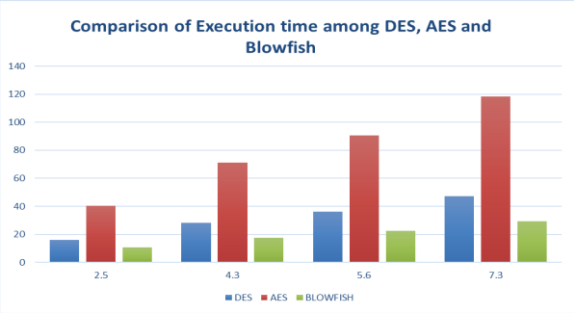

Fig 5.1 Comparison of Encryption Algorithm

As the throughput of a cryptographic technique increases, the power consumption of that technique decreases due to the reduction in time spent encrypting and decrypting data.[13].

VI. FUTURE SCOPE & CONCLUSION

The suggested approach offers a secure cloud storage system prototype built on a blockchain. The suggested method safeguards data held in an unreliable setting. A few security techniques with the right level of time complexity, usability, and effectiveness were selected for the system's implementation.

Because the data will be stored on the cloud, only the blockchain will have access to the file location information. The information stored on the blockchain is open to the public, access to it is restricted, and it is encrypted before being transported to the cloud. The access policies must be accepted by users before they may read a file. Before being downloaded, a particular file from the document pool is decrypted using the aggregate key supplied by the data owner.

The AES-256 encryption technique, along with a fixed-length cypher text and key, are used in the suggested system to boost the system's effectiveness. Blockchain is used by the system to store the links to cloud-based, encrypted documents. As a result, the proposed approach presents a workable substitute for the existing cloud storage techniques.

The most important and practical technology of the present day is cloud computing. Even while cloud computing has numerous advantages, there are unavoidable security

concerns.

Data privacy, lack of control, data leakage, data breaches, system vulnerabilities, and so on are all issues that need to be addressed. To address the above - mentioned security concerns, I propose a "Blockchain-based secure data storage and access control system" architecture

References

[1] "Performance Analysis of Data Encryption Algorithm", http://www.cse.wustl.edu/~jain/cse567-06/encryption_perf.html.

[2] Mrs. Rohini Pise and Dr. Sonali Patil "Enhancing Security of Data in Cloud Storage using Decentralised Blockchain", ICICV 2021

[3] S. Prianga R. Sagana and E. Sharon, "Evolutionary survey on data security in cloud computing using blockchain", vol. 6, no. 4, pp. 4396–4401, 2020

[4] Shuaib, M. Samad, A. Alam S., and Siddiqui. S. T. 2019. Why Adopting Cloud Is Still a Challenge?—A Review on Issues and Challenges for Cloud Migration. Ambient Communications and Computer Systems: Advances in Intelligent Systems and Computing, vol 904. Springer, Singapore: RACCCS-2018, 387.

[5] Shubham Desai and Omkar Deshmukh "Blockchain based Secure Data Storage and Access Control System using Cloud", IEEE 2019

[6] A. VatankhahBarenji, H. Guo, Z. Tian, Z. Li, W. M. Wang, and G. Q. Huang, ''Blockchain-based cloud manufacturing: Decentralization,'' 2019, arXiv:1901.10403. [Online]. Available: http://arxiv.org/ abs/1901.10403

[7] JulijaGolosova, Andrejs Romanovs, "The Advantages and Disadvantages of the Blockchain Technology", IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018.

[8] Ilya Sukhodolskiy, Sergey Zapechnikov, "A BlockchainBased Access Control System for Cloud Storage," IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2018.

[9] M. K. R. Ingole and M. S. Yamde, ''Blockchain technology in cloud computing: A systematic review,'' Sipna College Eng. Technol., Maharashtra, India, Tech. Rep., 2018

[10] Shuaib, M. Samad, A. and Siddiqui. S. T. 2017. Multi-layer security analysis of hybrid Cloud. In 6th international conference on system modeling & advancement in research trends, 526-531

[11] Hoang Giang Do and Wee Keong Ng "Blockchain-based System for Secure Data Storage with Private Keyword Search", IEEE 2017

[12] khodolskiy I. A., Zapechnikov S. V. An access control model for cloud storage using attribute-based encryption. In Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian (pp. 578-581). IEEE.

[13] Zibin Zheng, ShaoanXie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE International Conference on Big Data (Bigdata Congress), 2017.

[14] G. Zyskind, O. Nathan et al., "Decentralizing privacy: Using blockchain to protect personal data," in Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015, pp. 180–184.

[15] IBM, what is Cloud Computing —, https://www.ibm.com/cloudcomputing/learn-more/what-is-cloudcomputing.