International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

Blockchain based Data Security and Access Control System using Cloud

Sagar Gangwani
MIT School of Engineering
MIT ADT University
Pune, India

Prof. Reetika Kerketta
MIT School of Engineering
MIT ADT University
Pune, India

Abstract— **Currently, cloud storage is totally reliant on big storage companies. These storage companies serve as untrustworthy third parties who process data in order to store, send, and receive data from a company. This system has a number of issues, with high operational expenses, poor data security and software quality. That is research, I'm outlining the idea of a blockchain-based database multi-user access control system deliver robust, distributed data processing. The data owner can upload the data to the system using a web interface. As a result, only the user who possesses the secret key to the material that has been encrypted and uploaded to the folder is accessible via cloud. As a result, cloud computing has been widely used in many facets of the IT sector. It has emerged as a critical technology to meet infrastructure and data service requirements at low cost, with little effort, and with a high level of scalability. Although the adoption of cloud computing has grown quickly, issues about information security have not yet been entirely addressed. Cloud Computing's expansion is still somewhat constrained by information security issues that need to be addressed. Blockchain has also become a crucial security tool, particularly in terms of integrity, authenticity, and confidentiality. Actually, the technology supports data privacy by maintaining the integrity and consistency of the blockchain by processing it in the cloud. To improve the security of cloud storage, we presented a secure, blockchain-based data storage and access management system.**

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

I. INTRODUCTION

Cloud computing is a new technology that has recently drawn a lot of interest from both business and academia. By using cloud computing, users can access many types of software's internet services without having to purchase or install them on their computers. possess a computer. According to the National Institute of Standards and Technology, cloud computing (NIST). access across a network to a common pool of adaptable computer resources is a paradigm for delivering useful, on-demand information.

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. The content does have some copyright and security issues, though. The fact that data can be accessed by someone outside the owner is the main issue with sending data to an external environment. Providers of cloud services do not provide the level of security and privacy required for efficient data security and privacy. The introduction of a decentralised cloud storage network offers several advantages over data center-based storage. Similar to conventional methods, decentralised cloud storage networks ensure data security by using client-side encryption. However, handling encrypted data comes with a variety of challenges, with data usability being the most important. More specifically, the data owner should be able to authorise others to access remotely encrypted data and extract useful but unfinished material. Obtaining the entire collection of data, filtering it, and then providing the relevant portions to the authorised client is one simple strategy.. However, the significant cost to the consumer renders that alternative unworkable and goes against the purpose of outsourcing data.

Data security is a top concern for consumers interested in cloud computing. This technology needs the right security concepts and practises to soothe users' concerns. Most users of cloud services are concerned that their personal information might be moved to other cloud service providers or utilised for unrelated purposes. 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.

To address this issue, this study offers a system that uses the Blockchain-based Secure Data Storage and Access System to provide data storage. As a result, We suggest using Blockchain as a reliable platform for smart contracts, which employ computer protocols to automate jobs and cut down on the time required for various business 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. The ledger, which is shared by all network participants, keeps track of all transactional data between nodes in an ordered chain of cryptographic hash-linked blocks.

II. ADVANTAGES OF BLOCKCHAIN

Transactions that are approved and sent over the network enable the immutability of the Blockchain. A transaction cannot be changed or removed after it has been added to the Blockchain. It also relies on the system type being utilised; a central system, for example, can be modified or eliminated as just 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. Blockchain technology is unchangeable and indestructible as a result of this feature. Transparency on the blockchain is a feature that develops throughout the transaction copying phase. 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 METHDOLOGY

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 keep their information in the cloud and offer access to organisations who need it thanks to a data storage option made available by the cloud. [9]

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. Today, a variety of outside service providers are considering using cloud computing as their computing paradigm. Data owners can store their data on the cloud and grant access to businesses who need it since the cloud provides a solution for data storage.

To address the security issues with cloud data storage and guarantee the confidentiality, integrity, and availability of the cloud data, I propose the Blockchain Based Data Security and Access Control System Using Cloud. The following activities will occur in my model.

- Step I: To gain access to the cloud-based access control system, each data user or data owner must first complete the entire registration and verification process. The email is used to carry out the verification process.
- Step 2: The data owner has access to the data owner dashboard following successful registration and authentication. Here, the data owner can encrypt a file using the AES-256 encryption technique and upload the encrypted file to the cloud.
- Step 3: The access link to the encrypted file and the private key needed to decrypt it are stored in the block when the encrypted file has been successfully uploaded to the cloud.Do not confuse "imply" and "infer."
- Step 4: Upon the link's storage on the block, each block's hash id is generated, and the block is then stored on the blockchain
- Step5: If the data user wants to access any file, proceed to. The user uses the search bar to look for the document.
- Step 6: If the user locates the requested file in the cloud, he or she will ask the information owner for permission to view the data that is kept there.
- Step 7: The user receives the hash key/id necessary to obtain the access link and private key of the data owner's uploaded encrypted file if the data owner approves the data user request and meets the conditions established by the smart contract.
- Step 8: After receiving a request, the owner of the information provides the aggregate key or hash keys to the user who made the request for access to the information. The user can now use the aggregate key to access the blockchain link. An excellent style manual for science writers is [7].

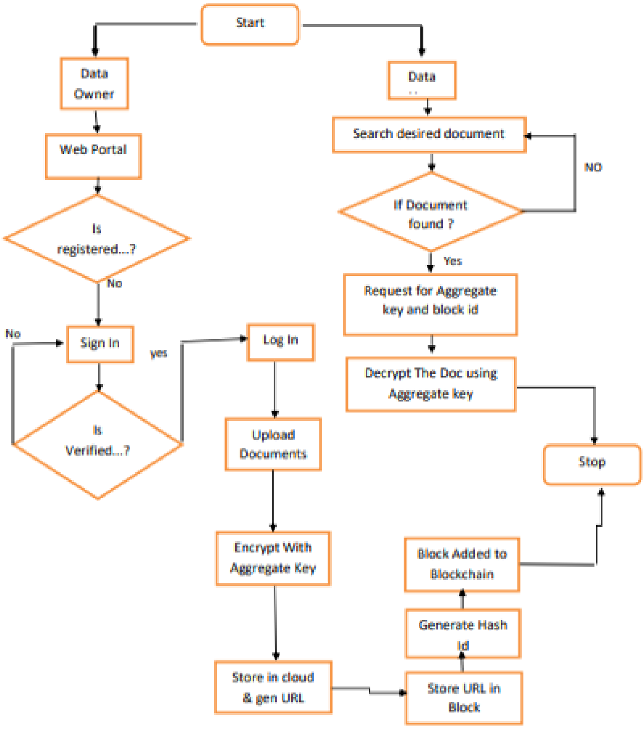


Fig 4.1. Blockchain based Access Control System for cloud data security

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.

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.

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.

V. RESULTS AND DISCUSSIONS

5.1 Encryption Algorithm Comparison for Cloud Data Security

The biggest concern of keeping and moving sensitive information online, when it is no longer limited within physical borders, is security.

Cryptography is a fundamental, effective, and efficient component that enable secure communication between the various entities by conveying unknowable information that can only be accessed by authorised recipients. Selecting the appropriate cryptographic method is crucial for secure communication that offers increased security, precision, and effectiveness.

The evaluation parameters like encryption and decryption time, memory, avalanche effect, throughput, correlation assessment, and entropy are the main topics of discussion and results demonstration for these algorithms because they demonstrate a higher level of security, confidentiality, integrity, and dependability for secure communication. According to performance evaluation, the findings of Blowfish, AES, and DES provide superior security depending on resource availability.

A. Symmetric Key Encryption:

When using symmetric key (secret key) encryption, the same key is utilised for both encrypting and decrypting a communication. Only those parties who are permitted to send and receive communications know the encryption and decryption keys. The overall communication security is increased by providing unique keys to each party. The secrecy of the encryption and decryption keys determines how strong symmetric key encryption is. The two types of symmetric encryption algorithms are block cypher and stream cypher. The block cypher can also be further divided into binary and non-binary block cypher depending on the results of the message, keys, and ciphertext. The binary block cypher has defined the message bit size as 64, 128, 192, and 256, but the non-binary block cypher has not created a standard that is dependent on the implementation of the cypher.

B. Asymmetric Key Encryption:

Different keys are used for the message's encryption and decryption in the asymmetric key encryption method, also known as public key encryption. The communication can be encrypted using the encryption key, which is often referred to as the public key. The communication can be decrypted using the decryption key, often known as a secret or private key. When combined with a digital signature, asymmetric key encryption's strength can be made available to users through message authentication detection. RSA the Diffie-Hellman algorithm, and other asymmetric encryption algorithms are examples. depicts the elements of an asymmetric block cypher.

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

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

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]

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.

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. The performance execution times for the algorithms DES, AES, and Blowfish are displayed in Fig. 5.1.1 for a range of data input sizes. Blowfish has the worst execution, as is evident. AES is first used across all input sizes, then DES.

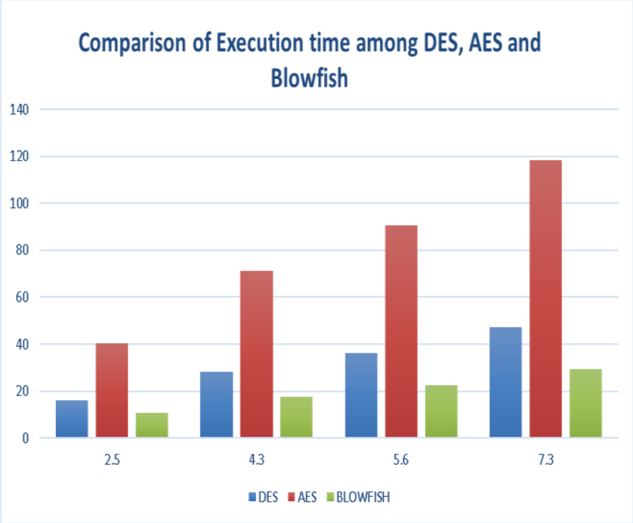


Fig 5.1.1 Comparison of Encryption Algorithm for data security

Fig. 5.1.1 displays the performance execution times for the algorithms DES, AES, and Blowfish for a range of data input sizes. 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, Due to its mass encryption and decoding, blowfish operates quickly. Block sizes in Blowfish are 64 bits. Even if it is implemented in software faster than AES, AES still outperforms it in terms of security. The lack of legal protection for blowfish accounts for its widespread use. Blowfish uses blocks of 64 bits, whereas AES uses blocks of 128 bits. Small block size can pose serious security risks; because of its small block size, Blowfish is more susceptible to assaults.

The throughput of each algorithm when evaluating the same text files was shown in table 2. 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]. Table 2 displays the throughput of each algorithm when analysing the same text files. Because less time is spent encrypting and decrypting data, the power consumption of a cryptographic technology lowers as throughput rises.

The step wise execution of the Blockchain based Access Control System model using cloud is shown using the below figures.

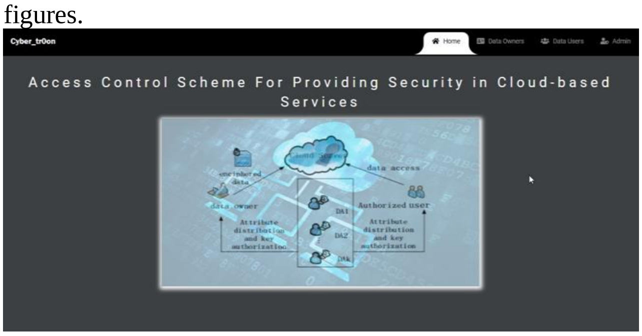

Cyber_tr0on
Home
Data Owners
Data Users
Admin
Access Control Scheme For Providing Security in Cloud-based Services
Cloud Server
data access
encinhered data
data owner
Authorized user
Attribute distribution and key authorization
DA1
DA2
DAk
Attribute distribution and key authorization

Fig 5.1.2: Access Control System Dashboard

Step1: It shows the welcome page of a cloud-based access control system built on the blockchain theory, which introduces itself to new visitors and provides connections to the next page for the data user, data owner, and admin.

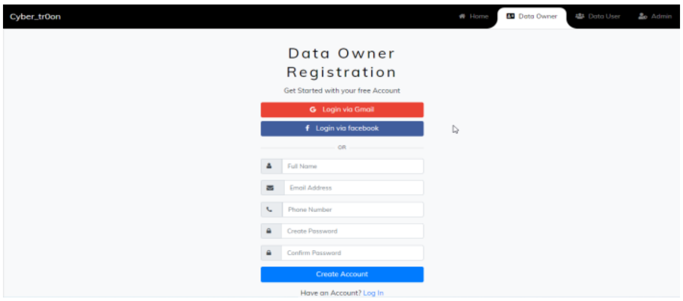


Fig 5.1.3: Data Owner Registration/Login Page

Step2: Next it shows the data owner/data user registration/login page, where the owner/user can finish signing up and utilising credentials to verify their identities

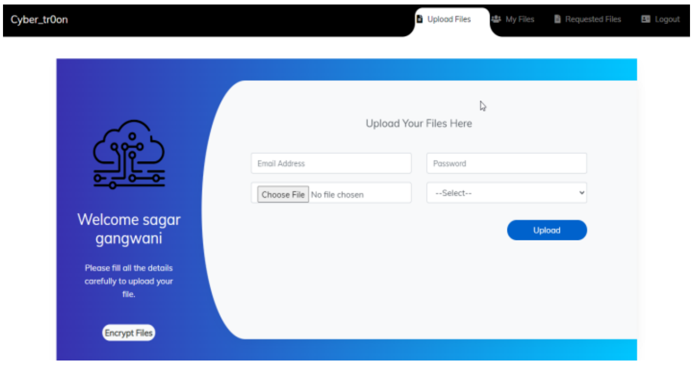
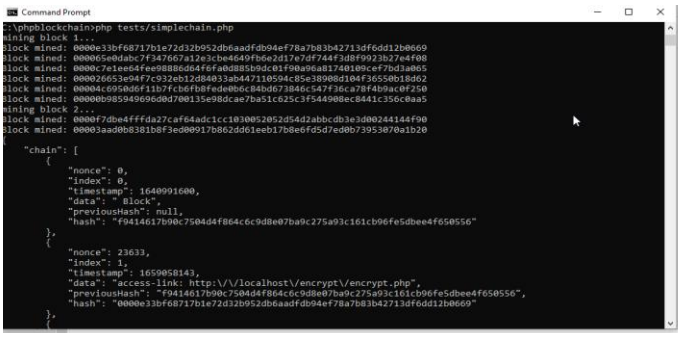


Fig 5.1.4: Data Owner Upload Files Panel

Step3: After successfully registration and verification data owner go to the dashboard panel, from which he or she can choose a file, enter information, and upload the encrypted file to the cloud.

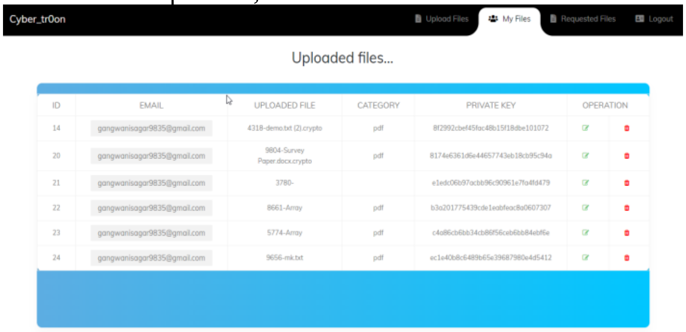


```
:\phpblockchain>php tests/simplechain.php
mining block 1...
Block mined: 0000e33bf68717b1e72d32b952db6aadfdb94ef78a7b83b42713df6dd12b0669
Block mined: 000065e0dabc7f347667a12e3cbe4649fb6e2d17e7df744f3d8f9923b27e4f08
Block mined: 0000c7e1ee64fee98886d64f6fa0d885b9dc01f90a96a81740109cef7bd3a065
Block mined: 000026653e94f7c932eb12d84033ab447110594c85e38908d104f36550b18d62
Block mined: 00004c6950d6f11b7fcb6fb8fede0b6c84bd673846c547f36ca78f4b9ac0f250
Block mined: 00000b985949696d0d700135e98dcae7ba51c625c3f544908ec8441c356c0aa5
mining block 2...
Block mined: 0000f7dbe4fffda27caf64adc1cc1030052052d54d2abbcdb3e3d00244144f90
Block mined: 00003aad0b8381b8f3ed00917b862dd61eeb17b8e6fd5d7ed0b73953070a1b20
{
    "chain": [
        {
            "nonce": 0,
            "index": 0,
            "timestamp": 1640991600,
            "data": " Block",
            "previousHash": null,
            "hash": "f9414617b90c7504d4f864c6c9d8e07ba9c275a93c161cb96fe5dbee4f650556"
        },
        {
            "nonce": 23633,
            "index": 1,
            "timestamp": 1659058143,
            "data": "access-link: http:\/\/localhost\/encrypt\/encrypt.php",
            "previousHash": "f9414617b90c7504d4f864c6c9d8e07ba9c275a93c161cb96fe5dbee4f650556",
            "hash": "0000e33bf68717b1e72d32b952db6aadfdb94ef78a7b83b42713df6dd12b0669"
        },
        {
```

Fig.5.1.5 Access link and Private key Store on Block

Step4: After successfully uploading file to the cloud the access link and private key of that file is store on the block and generating the hash id of that block.

Step 5: Once the file is successfully uploading the uploaded files panel for the data owner displays a list of all the files that the owner has uploaded,

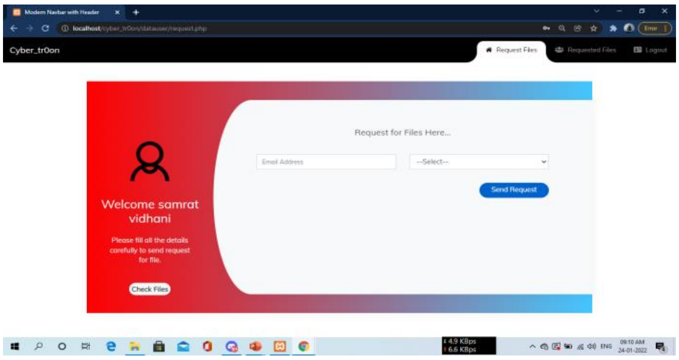


Uploaded files...

ID	EMAIL	UPLOADED FILE	CATEGORY	PRIVATE KEY	OPERATION	
14	gangwanisagar9835@gmail.com	4318-demo.txt (2).crypto	pdf	8f2992cbef45fac48b15f18dbe101072	✎	🗑
20	gangwanisagar9835@gmail.com	9804-Survey Paper.docx.crypto	pdf	8174e6361d6e44657743eb18cb95c94a	✎	🗑
21	gangwanisagar9835@gmail.com	3780-		e1edc06b97acbb96c90961e7fa4fd479	✎	🗑
22	gangwanisagar9835@gmail.com	8661-Array	pdf	b3a201775439cde1eabfeac8a0607307	✎	🗑
23	gangwanisagar9835@gmail.com	5774-Array	pdf	c4a86cb6bb34cb86f56ceb6bb84ebf6e	✎	🗑
24	gangwanisagar9835@gmail.com	9656-mk.txt	pdf	ec1e40b8c6489b65e39687980e4d5412	✎	🗑

Fig 5.1.6: Data Owner Uploaded Files Panel

Together with all the necessary details including the owner's email address and files that have been uploaded along with private keys.



Request for Files Here...

Email Address

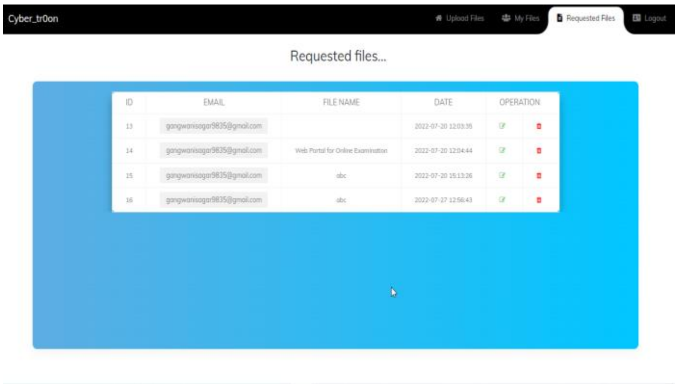
--Select--

Welcome samrat vidhani

Please fill all the details carefully to send request for file.

Fig 5.1.7: Data User Request files panel

Step 6: By entering their email address and choosing the file they wish to access in the Data User Request File window, data users can request access to a file from a data owner.



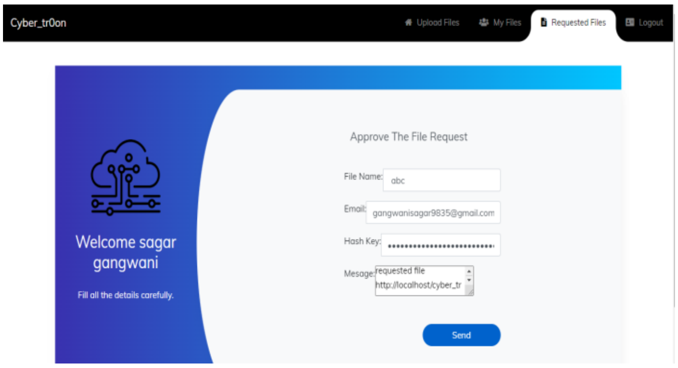
Requested files...

ID	EMAIL	FILE NAME	DATE	OPERATION	
13	gangwanisagar9835@gmail.com		2022-07-20 12:03:35	✎	🗑
14	gangwanisagar9835@gmail.com	Web Portal for Online Examination	2022-07-20 12:04:44	✎	🗑
15	gangwanisagar9835@gmail.com	abc	2022-07-20 15:13:26	✎	🗑
16	gangwanisagar9835@gmail.com	abc	2022-07-27 12:56:43	✎	🗑

Fig 5.1.8: Data Owner Requested File Panel

Step 7: In this panel data owner see the list of all the requested file along with user's email address, the file name they wish to see, and the date of the request, through which data owner give approval to user to access the document.

Step 8: After getting the approval from the data owner user get the email along with file name, hash key to access the file decryption link, access link and decryption key about the file user have requested.



Approve The File Request

File Name: abc

Email: gangwanisagar9835@gmail.com

Hash Key: •••••••••••••••••••••••••

Mesage: requested file
http://localhost/cyber_tr

Welcome sagar gangwani

Fill all the details carefully.

Fig 5.1.9: Data Owner Requested File Approval Panel

IV. FUTURE SCOPE AND CONCLUSIONS

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/