International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

File Storage System Using Hybrid Cryptography on Cloud

Jyoti Birader[1]
Student
Computer Science & Technology
Usha Mittal Institute of Technology
Santacruz, Mumbai, India
jyotibiradar2002@gmail.com

Hrutika Thakur[2]
Student
Computer Science & Technology
Usha Mittal Institute of Technology
Santacruz, Mumbai, India
thakurhrutika2000@gmail.com

Najmin Shaikh[3]
Student
Computer Science & Technology
Usha Mittal Institute of Technology
Santacruz, Mumbai, India
nazminshaikh1012@gmail.com

Sonali Bodekar[4]
Assistant Professor
Computer Science & Technology
Usha Mittal Institute of Technology
Santacruz, Mumbai, India
sonali.bk86@gmail.com

Abstract — **One of the best places to store large amounts of data is in the cloud, however utilising a computer to manage a single cloud space is not secure. On the other hand, Blockchain is a cloud-based storage system that ensures data security. Any computer node connected to the Internet can join and build peer networks thus increasing utilization of resources. Blockchain is a distributed peer-to-peer system maintained by each node on the network, making it invariant. The user file is encrypted and distributed across a number of network peers in the proposed system utilising the IPFS (Inter Planetary File System) protocol. IPFS creates hash values. The path of the file is identified by the hash value, which is stored on the blockchain.**

Index Terms— **Cryptography, Cloud, Encryption, Decryption, File System, Security, Storage.**

I. INTRODUCTION

According to a study 2.5 quintillion data bytes are produced each day. Of all the data in the world more than 90 percent of the data produced in the last 2 years. With such huge data growth, cloud storage is needed to store data. Most of the data currently available online is stored in a single location and is stored by a handful of experienced technology companies and funds to build large data centres that can handle this huge data. The problem with this method is data security. Since this data is stored in a central way, if the attacker can gain access to the server he can easily view and edit the data.

Another problem with this method is the privacy of user data. In many cases, this data is used by third parties to analyse data and marketing purposes. Also, the costs incurred in storing data on central servers are high and often users have to pay for the entire system they have chosen even if they have used only a small portion of the storage space so it does not offer flexibility for the user to pay. only in what they use. Another problem is system scalability, it is difficult to measure a single storage system to meet a growing demand. With zero trust the two groups can trade in Blockchain. In this proposed system, we integrate the 3 algorithms with blockchain that are RSA, Blowfish and AES. We used the AES algorithm for file encryption and RSA for the text encryption and Blowfish for decryption. Our hybrid cloud is very safe because of these algorithms and blockchain. Our main goal is to store any file on IPFS securely and that file metadata will be stored on blockchain.

Blockchain is highly secure but using these algorithms we enhance the security level of our project. At the time of uploading a file, the file will be encrypted using the AES algorithm and the AES key will be encrypted by the RSA public key. This public key and encrypted text will be stored on the blockchain network. This encrypted file is also stored in IPFS server and hash value also stored in blockchain. While sharing a file to another user share all the file details to that user and while downloading these details is used. Firstly, the encrypted file will download to the local system and the AES key will be decrypted by the RSA private key and the file will be decrypted by that AES key and Blowfish key. This decrypted file is displayed to the user.

II. LITERATURE SURVEY

No	Title	Methodology	Limitation
1.	Secure storage and access of data in Cloud computing [1].	ECC (Elliptic Curve Cryptography) algorithm. Performs authentication, key generation, encryption and decryption.	Uses single key for encryption and decryption hence providing less security.

2.	Secure File Storage and File Sharing [2].	Separate servers are used for input, storage and output functions. Providing better security by keeping separate modules.	As three different servers are used there can be connectivity issues as well as synchronization problems.
3.	RSA Encryption and Digital Signature [3].	Use of RSA algorithm in combination with MD5 Digest to ensure data security on cloud.	RSA algorithm only provides key encryption and along with MD5 it provides single text encryption and not multiple text encryption.
4.	Survey Paper on Cloud Storage Security [4].	Using EFS, NTFS with cache for securing data files by using automatic cryptographic systems inbuilt in EFS.	As cryptographic systems are inbuilt in EFS, modifications for providing better security measures is difficult to implement.
5.	Use of Digital Signature with Diffie Hellman key exchange and AES encryption algorithm to enhance Data Security in Cloud Computing [5].	Use of Diffie Hellman for key exchange. Authentication provided by Digital Signature scheme and lastly files encrypted using AES.	Time consuming procedure as three different steps using different techniques are performed.

TABLE I: LITERATURE SURVEY

III. PROPOSED SYSTEM

Our proposed system is designed to provide a high security When user upload their data on cloud server for security of file in cloud computing source file is break into different parts for encryption of that file, we are using AES, RSA and Blowfish algorithm Because of this encryption, only authorized user can have access to their file So their files are safely saved on our server. For authorization first user needs to register on our system after that they will get login option by their username, password, birthdate, mobile number and mail id. then they will be able to login on server when user will login on the server. They will get an upload file option through which they will be able to upload any type of file (like jpg, xml)also they will have a share option there so if any user wants to share their file with others, they can share with them. For file share users need to type their username and receiver's username and their email id after that receiver will get the encryption key on their mail. When receivers will want to see their file, they will need to click on the receive file option and after that to open that file they will need to type that key which they will get on their mail. when they enter that key they will be able to open that particular file.

IV. ARCHITECTURE

A system's architecture is depicted in a diagram where the major components or functions are represented by blocks connected by lines that indicate their relationships.

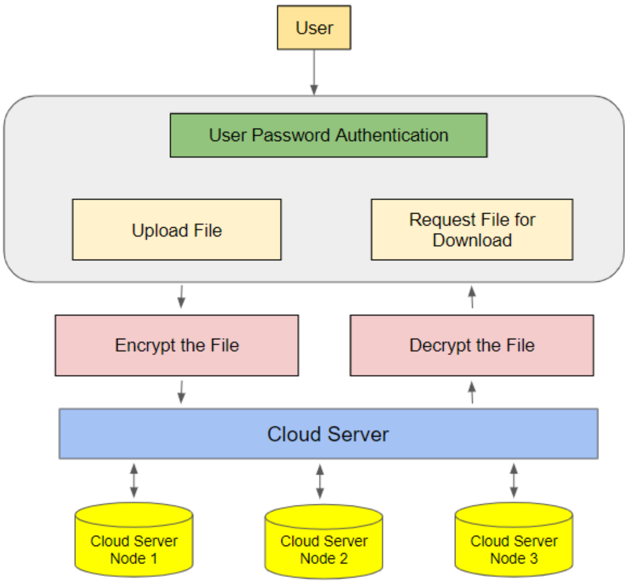


Fig. 1. Architecture

V. ALGORITHMS

A. *Blowfish Algorithm*

Blowfish algorithm is created by Bruce Schneier in 1993 it is the first symmetric encryption algorithm.it is alternative to DES encryption technique block size of the plain text is 64 bit which encrypt with variable length key 34-448 bits. The default key size is 128 bits, and no of rounds are 16.it is more secure algorithm and it execute in less memory it is faster than DES algorithm.

B. *AES Algorithm*

Advanced Encryption Standard is a symmetric- key algorithm that supports block length of 128 bit and can have a key size of 128, 192, and 256 bits. Data is encrypted and decrypted in blocks on each loop using keys that are 128 bits, 192 bits, or 256 bits, respectively. The entire AES algorithm is run in bytes rather than bits. Consequently, for the Advanced Encryption Standard, a block of 16 bytes equals 128 bits of plain data. To facilitate processing, a 4x4 matrix containing these 16 bytes is set up.

C. *RSA Algorithm*

One of the most well-liked and safe public-key (asymmetric) cryptographic techniques is RSA, or Rivest-Shamir-Adleman. The technique takes use of the fact that there is no effective way to factor very big (100-200 digit) values.

VI. FLOWCHART

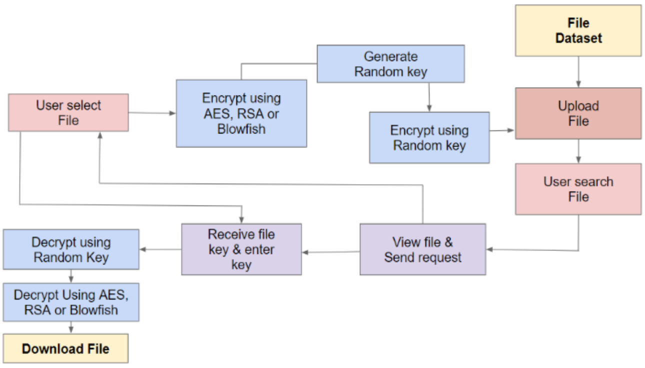
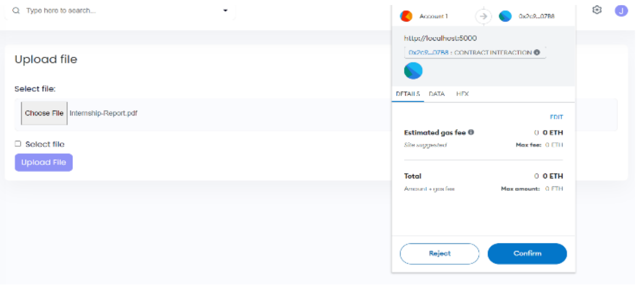


Fig. 2. Flowchart

VII. WORKFLOW

1. The user enters their information, including name, email address, phone number, password for the account, etc., to sign in if they are already registered or to sign up to register themselves.
2. The user then browses through local storage to choose the file that will be uploaded.
3. After the chosen file has been encrypted using the encryption algorithm, it is uploaded. The algorithms AES, RSA, and Blowfish are used to encrypt the file.
4. The user also has the choice of accessing and downloading the files they have posted or just viewing them. The decryption key is given to the user's email address provided at registration or sign-up when they choose a file to download.
5. The user can download either the original or decrypted file using this key.

VIII. RESULT ANALYSIS


Upload file

Select file: Choose File Internship-Report.pdf

□ Select file

Upload File

Account 1 → 0x2c9...07B8

http://localhost:5000

0x2c9...07B8 : CONTRACT INTERACTION

Estimated gas fee 0 ETH
Site suggested Max fee: 0 ETH

Total 0 ETH
Amount + gas fee Max amount: 0 ETH

Fig. 3

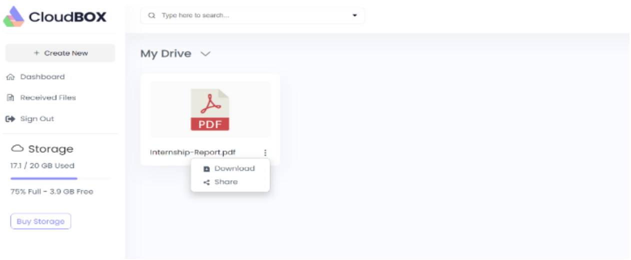
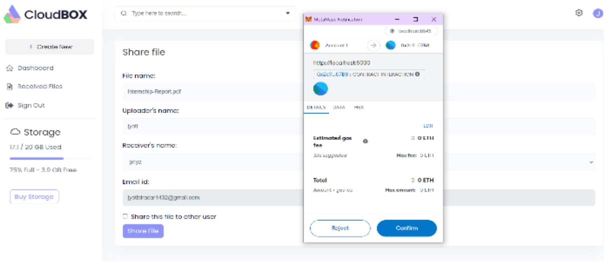


Fig. 4


Share file

File name: Internship-Report.pdf

Uploader's name: jyoti

Receiver's name: priya

Email id: jyotibiradar1432@gmail.com

□ Share this file to other user

Share File

MetaMask Notification

Account 1 → 0x2c9...07B8

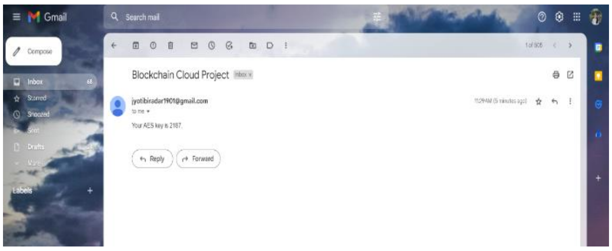
http://localhost:5000

0x2c9...07B8 : CONTRACT INTERACTION

Estimated gas fee 0 ETH
Site suggested Max fee: 0 ETH

Total 0 ETH
Amount + gas fee Max amount: 0 ETH

Fig. 5

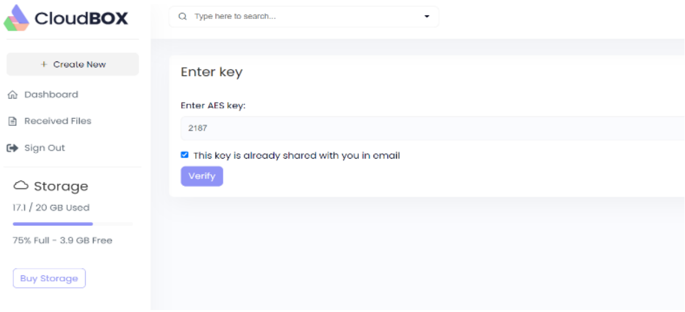

Blockchain Cloud Project Inbox

jyotibiradar1901@gmail.com
to me

11:29 AM (5 minutes ago)

Your AES key is 2187.

Fig. 6

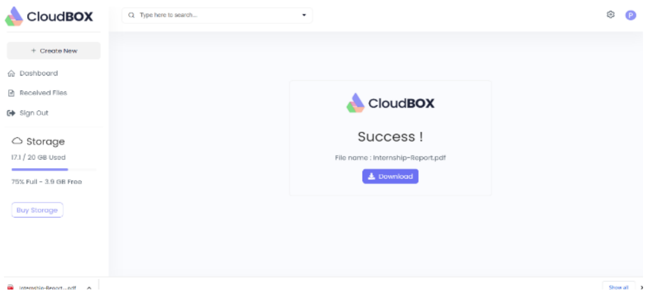

Enter key

Enter AES key: 2187

☑ This key is already shared with you in email

Verify

Fig. 7


CloudBOX

Success !

File name : Internship-Report.pdf

Download

Fig. 8

IX. FUTURE SCOPE

In the future, a flexible editing algorithm could compile files that can be accessed multiple times per user compared to the rarely accessible. This will help ensure that accessible files are always readily avail- able to the user whenever needed. Also, credit the program can be added to each of its assigned peers 100 credit default, based on the operating time of their system, and a few Successfully granted file access requesting that their credits receive you drawn or added. Peer-to-peer peers will be given the most important thing to keep data.

X. CONCLUSION

The proposed system improves data security by encoding and disseminating data to multiple peers in the system. The operating system uses the encryption algorithm to encrypt data that ensures the confidentiality of user data. The encrypted data is then transmitted and stored to peers on the network using the IPFS protocol. Our system not only solves the privacy and security of central cloud storage but also provides peers to rent their unused storage and receive cryptocurrency returns, thus maximizing the use of the storage facility.

XI. REFERENCES

[1] Kumar, A., Lee, B. G., Lee, H., Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).

[2] Rewagad, P., Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

[3] Ping, Z. L., Liang, S. Q., Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.

[4] Sunita Sharma,Amit Chugh:'Suvey Paper on Cloud Storage Security'. Rawal, B. S., Vivek, S. S. (2017).

[5] Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (SmartCloud).

[6] He Zhu , Yichuan Wang, Xinhong Hei, Wenjiang Ji, Li Zhang " A Blockchain-based Decentralized Cloud Resource Scheduling Architecture " International Conference on Networking and Network Applications, 2018.

[7] Nazmun Nahar, Farah Hasin and Kazi Abu Taher " Application of Blockchain for the Security of Decentralized Cloud Computing " International Conference on Information and Communication Technology, 2021.

[8] Mrs. Rohini Pise , Dr. Sonali Patil " Enhancing Security of Data in Cloud Storage using Decentralized Blockchain " Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, 2021.

[9] https://eduprojecttopics.com/product/secure-file-storage-on-cloud-using-hybridcryptography-pdf/

[10] https://link.springer.com/chapter/10.1007/978-981-15-0029-9$_1$

Personal Details

Hrutika Thakur

Dept : Computer Science and Technology

Jyoti Biradar

Dept : Computer Science and Technology

Najmin Shaikh

Dept : Computer Science and Technology