IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

BLOCKCHAIN-BASED DECENTRALIZED SECURE CLOUD STORAGE

T ANIL KUMAR[1], A KIRAN SAI[2], A DHANASEKHAR REDDY[3], K PAVANI[4]
[1]Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: anil.thumburu@gmail.com
[2]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: kiransai9141@gmail.com
[3]Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: dhanasekhar918@gmail.com
[4]Assistant Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email:kothapavani1990@gmail.com

Abstract: In spite of the fact that cloud storage is one of the most outstanding ways of putting away a lot of information, distributed computing's brought together capacity model is unreliable. Blockchain, then again, is a decentralized cloud storage arrangement that ensures data security. Any web associated registering hub might join and make peer organizations to amplify the utilization of accessible assets. Blockchain is a changeless conveyed shared framework on the grounds that each hub in the organization keeps a duplicate of the blockchain. Utilizing the IPFS (InterPlanetary File System) convention, the client's document is encoded and put away among many companions in the organization in the proposed framework. Hashing is made by IPFS. The record way is shown by the hash esteem, which is kept on the blockchain. The decentralized safe data storage, high information accessibility, and compelling storage asset use are the principal subjects of this article.

Index terms *- Blockchain, Data Security, IPFS, Encryption, Smart Contract, Cloud Storage.*

1. INTRODUCTION

A Forbes article[1] states that cloud storage solutions are essential due to the enormous amount of data created every day—2.5 quintillion bytes. The previous two years alone have seen the emergence of an astounding 90% of the world's data, underscoring the need for scalable storage solutions. Still, there are a number of issues with the current storage architecture, which is typified by computer companies' centralized repositories.

Centralized storage systems are the main source of security vulnerabilities. Since all the data is in one place, hackers may access sensitive data without restriction if they compromise the server, which opens the door to possible theft or modification. Furthermore, third parties often use this centralized pool for analytics and marketing initiatives, which raises questions about data sovereignty and permission and compromises user privacy.[14]

Centralized storage models are inefficient financially. Regardless of their real storage demands, users frequently sign up for fixed plans, which results in wasteful spending and less flexibility. As such, there is a mismatch between the price structure and the patterns of consumption, which negatively impacts both customer pleasure and economic sustainability.

Scalability also shows up as a crucial concern. The centralized paradigm is unable to keep up with the increasing amount of data required, which hinders

ISSN 2347–3657

Volume 12, Issue 3, 2024

its flexibility in responding to changing needs. Because of this, consumers are unable to access more storage space, which impedes development and innovation.[16]

The idea of zero trust, made possible by blockchain technology, presents a strong counterargument to these difficulties. Zero trust allows for the distribution of trust among participating entities by promoting a decentralized ecosystem that eliminates reliance on a single authority. As a result, transactions take place with more openness and security, which lessens the weaknesses present in centralized systems.

In summary, even if the amount of data is growing exponentially, strong storage solutions are still needed, and the existing centralized paradigm is unable to handle important issues like security, privacy, affordability, and scalability. Adopting zero trust and blockchain technology offers a viable path toward transforming data storage and promoting a decentralized environment where security, privacy, and adaptability are given top priority.

2. LITERATURE SURVEY

Zhe, D. "Study on Data Security Policy Based On Cloud Storage" [2] examines data security rules in cloud storage settings. It is likely that the study looks at different methods of protecting data in cloud storage systems, taking into account things like access control, encryption, and authentication methods.[18]

[3] In their work "Data security in cloud computing using AES under HEROKU cloud," Lee, B. H., Dewi, E. K., & Wajdi, M. F. most likely look at how to use the Advanced Encryption Standard (AES) to improve data security in cloud computing settings. The effectiveness of AES encryption in safeguarding data kept on the HEROKU cloud platform may be the main topic of this study.

[7] In the whitepaper "Next Generation Smart Contract and Decentralized Application Platform," V. Buterin presents the Ethereum platform, which facilitates the development and implementation of DApps and smart contracts. The article probably goes over Ethereum's features and design, highlighting how it may be used to make transactions safe and transparent.

[8] Ruj, S. et al., in their article “BlockStore: A Secure Distributed Storage Framework on the Blockchain”, BlockStore is a distributed storage framework based on the blockchain infrastructure. The design and implementation of BlockStore may be examined in this study, with an emphasis on the aspects that guarantee data security and integrity in a decentralized storage system.

[9] The IPFS is introduced in "IPFS - Content Addressed, Versioned, P2P File System," by J. Benet. IPFS's decentralized, content-addressed file storage and sharing methodology is likely highlighted in the paper's overview of the protocol's fundamentals.

[10] In "Meta-Key: A Secure Data-Sharing Protocol Under Blockchain-Based Decentralized Storage Architecture," Li, D., et al. provide a safe protocol for data sharing in decentralized storage systems that are based on blockchain technology. The design and execution of Meta-Key may be covered in detail in this study, with an emphasis on the mechanisms that make sure participant data sharing is safe and effective.

[11] As part of the International Workshop on Blockchain-Oriented Software Engineering

(IWBOSE), Wohrer, M. and Zdun, U. spoke on "Smart Contracts: Security Patterns and Robustness in the Ethereum Ecosystem." This study will likely explore security trends and best practices for creating smart contracts using Solidity, the programming language used to create Ethereum smart contracts.

[12] UCCT has an analysis of "SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN" by V. Sum. This research may look at the diverse privacy and security features made possible by blockchain technology, showcasing their uses and advantages across a range of industries.

Sivagenesan, D., in his article “BLOCK CHAIN ENABLED INTERNET OF THINGS” published in the Journal of Information Technology, explores the integration of blockchain technology into the Internet of Things (IoT). The study probably covers how blockchain technology might improve IoT system security, privacy, and interoperability by facilitating reliable transactions and data transfers.

3. METHODOLOGY

i) Proposed Work:

This venture uses cloud services and blockchain technology to securely store client data. The plan is to divide the user file into blocks, encrypt each block separately using the AES algorithm, and then store each block at different IPFS server nodes. IPFS will return the memory address of the saved block, and the blockchain will store this address. In order to retrieve all file blocks, the application will gather all of the Blockchain's block addresses during the download and use those addresses to submit a request to IPFS. The client will be able to decode and download the file blocks when all of the blocks have been acquired and merged.

ii) System Architecture:

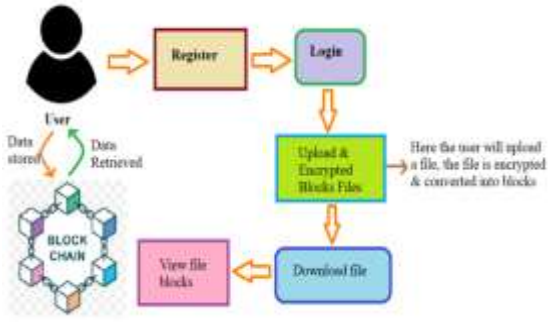

Fig 1 Proposed Architecture

A distributed database called a blockchain makes it possible to store data in a transparent and safe manner. Data blocks are connected in a chronological chain, with a hash of the preceding block included in every block. Because any effort to alter a block would alter its hash and end the chain, this produces a record that is impenetrable to tampering.

The block chain and user interaction are the two primary elements depicted in the diagram.

The rectangular blocks with the name "Block" make up the block chain. "Block Chain" is printed in writing above these blocks. The data in each block is encrypted in accordance with the diagram.

On the diagram's left side is a representation of user interaction. At the top are two text boxes with the labels "Login" and "Register". There is a section underneath these boxes with the caption "Data" and two arrows. The "Retrieved" arrow points up, whereas the "Uploaded" arrow points down. This implies that users will be able to upload and retrieve data to engage with the blockchain.[20]

iii) Modules:

ISSN 2347–3657

Volume 12, Issue 3, 2024

To implement the aforeimented project we used the following modules. They are:

1. Register
2. Login
3. Upload & Encrypted Blocks Files
4. Download File
5. View File Blocks

iv) Module Description:

1. Register:

Users may establish accounts via the "Register" module by entering personal data such their email address, password, and username. User account credentials are immutable and resistant to tampering because to the secure blockchain storage of user data upon registration. Users can create an account on the system with this module, which is necessary for data management and safe access.

2. Login:

By inputting their login credentials (password and username), registered users can access their accounts using the "Login" module.Users may access their saved files and personal data after successfully authenticating, guaranteeing that only those with permission can access and handle their data.

3. Upload & Encrypted Blocks Files:

Users can upload files to the cloud storage system using this module. To protect data confidentially, the uploaded files are split up into smaller blocks, and each block is encrypted using the AES method.Data security and availability are improved by distributing and storing these encrypted blocks on IPFS nodes.Furthermore, the blockchain stores pertinent data for tracking and retrieval reasons regarding the submitted files and their encrypted blocks.

4. Download File:

Users can access and download saved files from the cloud storage system using the "Download File" module. When a user chooses a file to download, the system searches IPFS nodes for the relevant encrypted blocks. After reassembling the original file from these blocks and decrypting them with the proper keys, the user is given the option to download it. When needed, this module makes sure users may safely access the data they have stored.

5. View File Blocks:

Users may examine an overview of their uploaded files and the data blocks that go with them by using the "View File Blocks" module. The memory addresses (also known as hash codes) of the blocks containing the files that they own are visible to users. Transparency and control over the data dissemination and storage process are provided by this perspective.

v) Blockchain Integration:

The memory addresses (hash codes) of the encrypted data blocks produced during the file upload procedure are kept on blockchain.

All data transactions pertaining to user file uploads and downloads are recorded by blockchain.

Smart contracts written in Solidity are used to specify and carry out operations that allow information to be stored and retrieved on the blockchain, including user account information.[20]

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

4. EXPERIMENTAL RESULTS

Fig 2 home page

Fig 3 new user signup screen

Fig 4 signup process completed screen

Fig 5 user login screen

Fig 6 main page

Fig 7 upload file screen

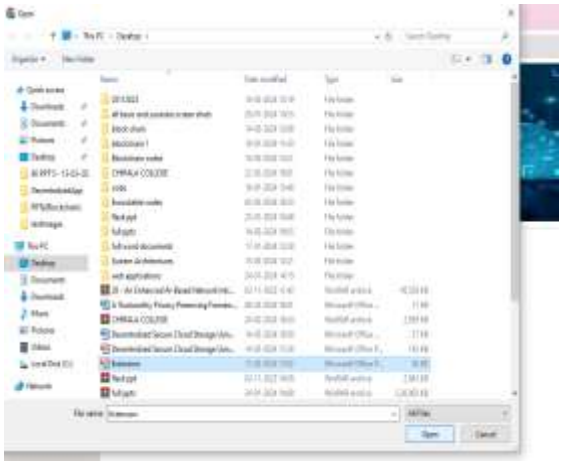

Fig 8 upload input file

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

Fig 9 submit screen

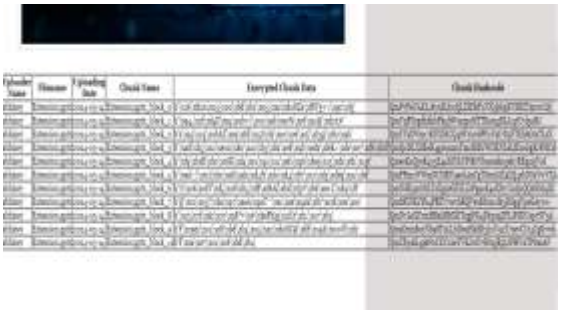

Fig 10 output screen

Fig 11 click here screen

Fig 12 downloaded screen

Fig 13 output screen

5. CONCLUSION

The proposed approach improves data security by distributing and encrypting data across multiple system peers. The implemented system encrypts data using 256-bit AES encryption technology to ensure confidentiality of user data. The IPFS protocol is then used to distribute and store the encrypted data across network peers. Our approach addresses privacy and security issues associated with centralized cloud storage while maximizing storage resource utilization by giving peers the opportunity to rent out unused storage and earn Bitcoin in return.[22]

6. FUTURE SCOPE

The proposed method improves data security by distributing and encrypting data across multiple system peers. The developed system encrypts data using 256-bit AES encryption technique to ensure

ISSN 2347–3657

Volume 12, Issue 3, 2024

the security of user data. The encrypted data is shared and stored among network peers using IPFS protocol. Our method addresses privacy and security issues associated with centralized cloud storage, while maximizing the utilization of storage resources by providing an opportunity to lend unused storage to peers and earn Bitcoin in return.

REFERENCES

[1] Bernard Marr, ”How Much Data Do We Create Every Day? The MindBlowing Stats Everyone Should Read.” Forbes, 2018.

[2] Zhe, Diao, ”Study on Data Security Policy Based On Cloud Storage” 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids) IEEE, 2017.

[3] Lee, Bih-Hwang, Ervin Kusuma Dewi, and Muhammad Farid Wajdi. ”Data security in cloud computing using AES under HEROKU cloud.” 2018 27th Wireless and Optical Communication Conference (WOCC). IEEE, 2018.

[4] Nakamoto, Satoshi,”Bitcoin: A peer-to-peer electronic cash system”, (2008). [5] Zyskind, Guy, and Oz Nathan,” privacy: Using blockchain to protect personal data”,IEEE Security and Privacy Workshops. IEEE, 2015.

[6] Cachin, Christian,” Architecture of the hyperledger blockchain fabric”, Workshop on distributed cryptocurrencies and consensus ledgers. Vol. 310. 2016.

[7] Buterin, Vitalik, ”A next-generation smart contract and decentralized application platform”, white paper (2014).

[8] Ruj, Sushmita, et al, ”BlockStore: A Secure Decentralized Storage Framework on Blockchain” 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). IEEE, 2018.

[9] Benet, Juan, “IPFS - Content Addressed, Versioned, P2P File System.” 2014. [10] Li, Dagang, et al. Meta-Key: ”A Secure Data-Sharing Protocol Under Blockchain-Based Decentralized Storage Architecture”, IEEE Networking Letters 1.1 (2019): 30-33.

[11] Wohrer, Maximilian, and Uwe Zdun,”a Smart contracts: security patterns in the ethereum ecosystem and solidity”, International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 2018.

[12] Sum, V. “SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN.” Journal of Ubiquitous Computing and Communication Technologies (UCCT) 1.01 (2019): 45-54

[13] Sivaganesan, D. “BLOCK CHAIN ENABLED INTERNET OF THINGS.” Journal of Information Technology 1.01 (2019): 1-8.

[14] G.Viswanath, “Hybrid encryption framework for securing big data storage in multi-cloud environment”, Evolutionary intelligence, vol.14, 2021, pp.691-698.

[15] Viswanath Gudditi, “Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage”, Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol.12, 2021, pp.545-552.

[16] Viswanath Gudditi, “A Smart Recommendation System for Medicine using Intelligent NLP Techniques”, 2022 International Conference on

ISSN 2347–3657

Volume 12, Issue 3, 2024

Automation, Computing and Renewable Systems (ICACRS), 2022, pp.1081-1084.

[17] G.Viswanath, "Enhancing power unbiased cooperative media access control protocol in manets", International Journal of Engineering Inventions, 2014, vol.4, pp.8-12.

[18] Viswanath G, "A Hybrid Particle Swarm Optimization and C4.5 for Network Intrusion Detection and Prevention System", 2024, International Journal of Computing, DOI: https://doi.org/10.47839/ijc.23.1.3442, vol.23, 2024, pp.109-115.

[19] G.Viswanath, "A Real Time online Food Ording application based DJANGO Restfull Framework", Juni Khyat, vol.13, 2023, pp.154-162.

[20] Gudditi Viswanath, "Distributed Utility-Based Energy Efficient Cooperative Medium Access Control in MANETS", 2014, International Journal of Engineering Inventions, vol.4, pp.08-12.

[21] G.Viswanath," A Real-Time Video Based Vehicle Classification, Detection And Counting System", 2023, Industrial Engineering Journal, vol.52, pp.474-480.

[22] G.Viswanath, "A Real- Time Case Scenario Based On Url Phishing Detection Through Login Urls ", 2023, Material Science Technology, vol.22, pp.103-108.

[23] Manmohan Singh,Susheel Kumar Tiwari, G. Swapna, Kirti Verma, Vikas Prasad, Vinod Patidar, Dharmendra Sharma and Hemant Mewada, "A Drug-Target Interaction Prediction Based on Supervised Probabilistic Classification" published in Journal of Computer Science, Available at: https://pdfs.semanticscholar.org/69ac/f07f2e756b79181e4f1e75f9e0f275a56b8e.pdf