IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12485

BLOCKCHAIN BASED SECURE FILE STORAGE AND SHARING USING DECENTRALIZED APPROACH

Dr.P.Maragathavalli[1], Mr. Bhuvanesh .D[2], Mr. Manikandan .S[3], Mr. Syed Abdul Kareem[4]

Assistant Professor, Information Technology, Puducherry Technological University, Puducherry, India.[1]

B. Tech Student, Information Technology, Puducherry Technological University, Puducherry, India.[2-4]

Abstract: These days, instead of using local storage devices, cloud storage is used to store and retrieve data. Cloud storage is based on the internet and provides data that is more dependable, safe, and readily available. Nonetheless, the information is crucial and shouldn't be shared with anyone not authorised. On the cloud, there is a lot of data that needs to be secured against unauthorised access. A variety of algorithms are employed to protect the security and privacy of data. Every system aims to achieve availability, confidentiality, and integrity (CIA). Nevertheless, these CIA features are not offered by the current centralised cloud storage. Decentralized cloud storage and blockchain technology are thus utilised to increase the security of data and storing methods. It efficiently aids in preventing data from being altered or having a portion of it deleted. A chain of blocks connects the data contained in blockchain to one another. Each block has a hash value that is saved in the following block. Consequently, it lessens the likelihood of data alteration. The SHA-3 Hashing algorithm is employed for this.

Keywords: Web 3.0, Blockchain, DApp, SHA 3, Two fish, Ethereum, Decentralization.

I.INTRODUCTION

Blockchain is a chain of blocks that is constantly expanding and contains immutable records that are connected and secured using cryptographic concepts. Each block has a pointer to the following block, a timestamp, and transactional information. Blockchains are impervious to data tampering. It can be used in a variety of industries where data needs to be permanently preserved and made accessible to all network users. Blockchain can maintain trust, transaction transparency, and task decentralisation in any system when it is applied.

II.MOTIVATION

Our main goal is to create a Blockchain-based system that can store user data in a distributed, decentralized database across a peer-to-peer network. Our objectives can be pointed as:

• To develop a system that can be implemented in real world to store users' data in network considering more safety, availability and backup.

• To decentralize the storage mechanism of database and remove the sole right of any private company over user data.

• To contribute the development of a viable, practical product based upon the Blockchain technology. Also, to implement the techniques and benefits of using Blockchain in existing system.

III.LITERATURE SURVEY

[1] Journal on Future Generation Computer Systems 141 (2023) 197–204: A peer-to-peer file storage and sharing system based on consortium blockchain.

[2] Journal of King Saud University – Computer and Information Sciences, ScienceDirect-2022: Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12485

[3] S. Wang et al.: Secure Cloud Storage Framework with Access Control Based on Blockchain, IEEE-2021: Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing.

[4] Journal on Intelligent Communication Technologies and Virtual Mobile Networks. IEEE-2021: Enhancing Security of Data in Cloud Storage using Decentralized Blockchain.

IV.LIMITATIONS IN THE EXISTING SYSTEM

- The majority of cloud computing systems in use today are centralized, meaning that many resources are gathered in one location for users to hire and store their data on. One of its flaws is that there is only one encryption and decryption secret as shown below in the figure.

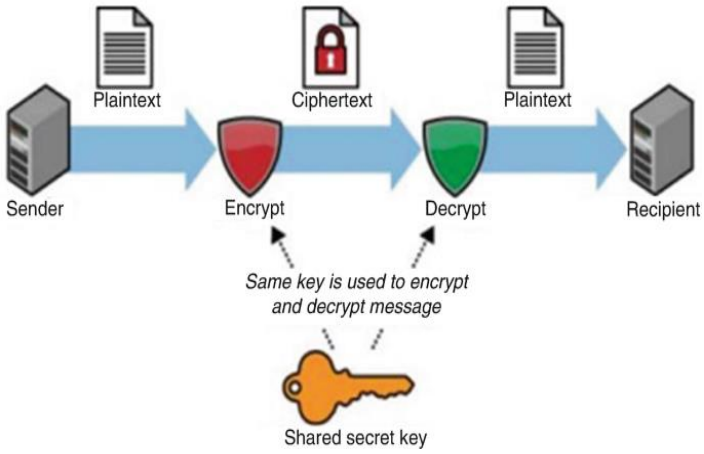

Fig 1. Centralized approach for the cloud storage

- If the encryption key was lost, anyone might access the data by decrypting it. Additionally, there are significant upfront expenditures associated with deploying the system, which raises the cost of rent. However, the highest level of data security cannot be ensured due to these higher rent prices.

- It uses SHA-1 and SHA-2 and AES algorithm for encryption which are older techniques.

V.PROPOSED SYSTEM

DECENTRALIZED APPROACH

The distributed network: peer to peer network, which is built on the blockchain system and is further explained, is the suggested solution for the issue. The accompanying figure, which illustrates how cloud decentralisation would operate on peer networks, is used as a basic overview. The three main duties are to encrypt the file, break it up into smaller pieces, and keep a blockchain-based log file as a record of the system. With this method, it is easier to have highly redundant data bytes, which improves security divisions.

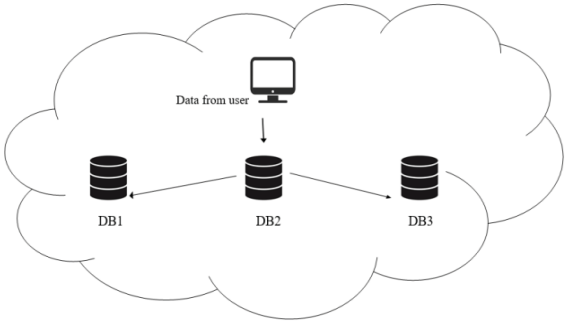

Fig 2. Decentralized approach for the cloud storage.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12485

- **SHA-3:** the most recent iteration of the Secure Hash Algorithm family, has a number of benefits over SHA-256. The following are some advantages of using SHA-3 for safe cloud storage in blockchain rather than SHA-256:

- **Improved Security:** Because SHA-3 employs a more intricate and unpredictable hash function than SHA-256, it is intended to offer greater security. This increases its protection against assaults like collisions and preimages that could jeopardise the confidentiality of the data saved in the blockchain.

- **Increased Flexibility:** Since it allows a variety of hash sizes, SHA-3 is more adaptable than SHA-256 and can be used for applications with a variety of security needs.

- **Better Performance:** SHA-3 is faster than SHA-256 in certain scenarios, such as when dealing with large data sets or when hardware acceleration is used.

- **Twofish:** Two fish is a symmetric encryption algorithm that is similar to AES and is considered to be one of its closest competitors. Two fish has a larger block size and a more complex structure compared to AES, making it more secure.

VI. FLOW DIAGRAM OF A PROPOSED SYSTEM

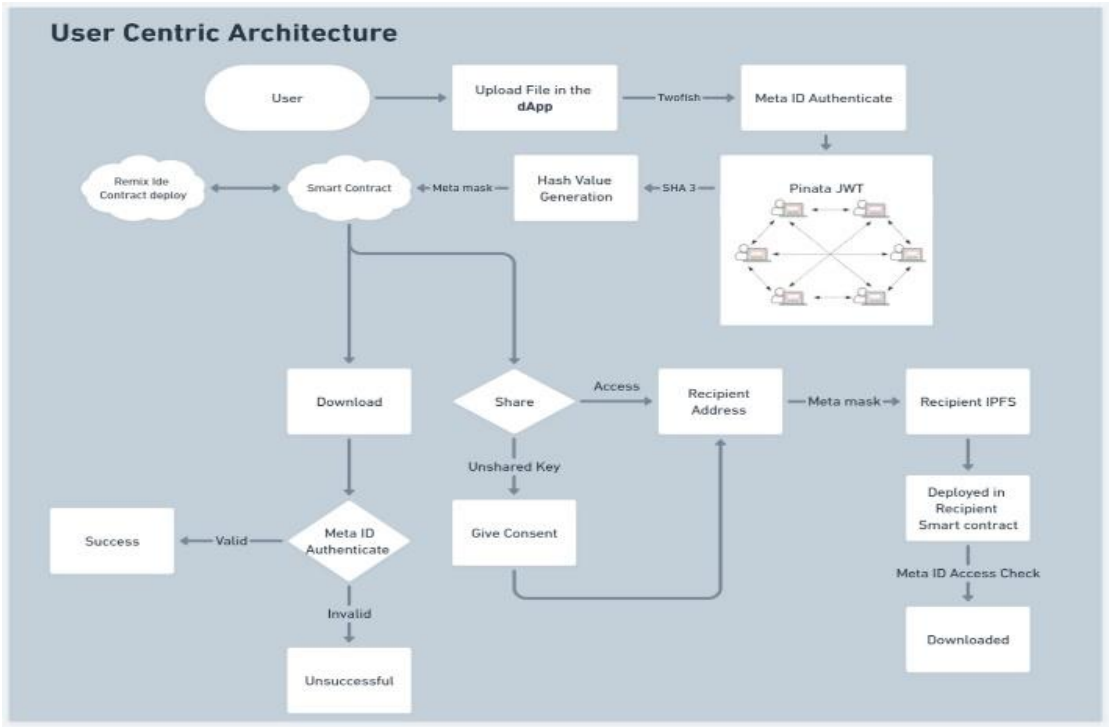

Fig 3. Detailed design diagram of proposed system

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12485

VII. EXPERIMENTAL RESULTS

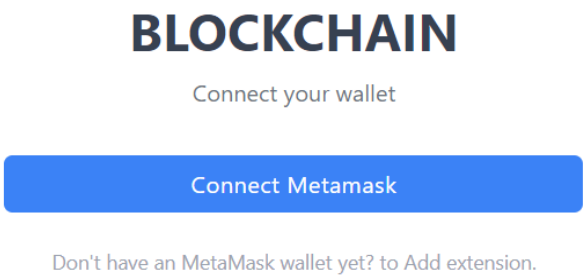

Fig:4 To connect MetaMask with Blockchain

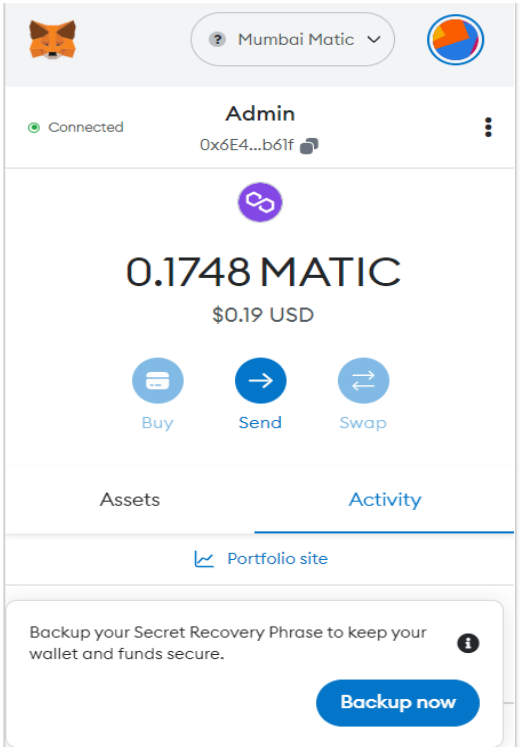

Fig: 5 MetaMask account for various users.

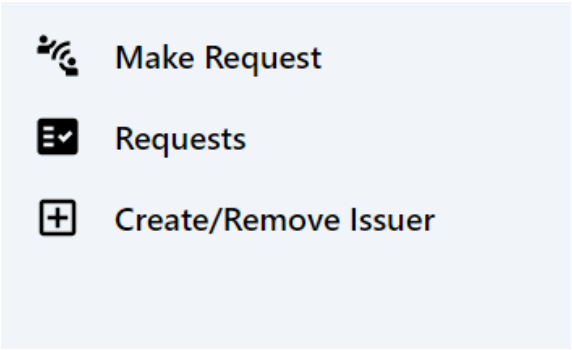

Fig: 6 Dashboard for Admin

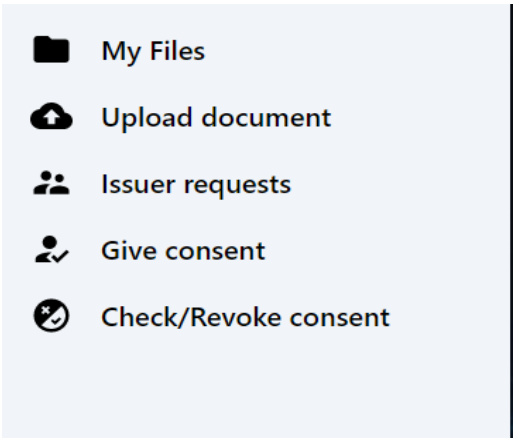

Fig:7 Dashboard for User

CONCLUSION

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12485

The major problem with an existing cloud service provider is the mediator and centralized system which could be solved by including blockchain and having peer to peer decentralized systems and implementing specialized algorithms for encryption and decryption of the data and generation of the public and private keys. The algorithms used to implement the system model is efficient and required less time and give high security for the data which is being stored on cloud. This kind of architecture makes the system more robust and resistant to different security attacks which are performed by unauthorized users who try to steal and disclose the information in data files of user for their benefits.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy (SP), May 2020, pp. 321–334.
[2] Wei, W. Liu, and X. Hu, ‘‘Secure and efficient attribute-based access control for multiauthority cloud storage,’’ IEEE Syst. J., vol. 12, no. 2, pp. 1731–1742, Jun. 2021.
[3] Alizadeh, M., Andersson, K., Schelén, O., 2020. Efficient Decentralized Data Storage Based on Public Blockchain and IPFS. 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020. IEEE, 1-8.
[4] Almehmadi, E., Gutub, A., 2021. Novel arabic e-text watermarking supporting partial dishonesty based on counting-based secret sharing. Arab. J. Sci. Eng. https://doi.org/10.1007/s13369-021-06200-7.
[5] Al-Shaarani, F., Gutub, A., 2021a. Securing matrix counting-based secret-sharing involving crypto steganography. J. King Saud Univ. – Comput. Inf. Sci. https:// doi.org/10.1016/j.jksuci.2021.09.009.
[6] Y. Du, H. Duan, A. Zhou, C. Wang, M. H. Au, and Q. Wang, “Towards privacy-assured and lightweight on-chain auditing of decentralized storage,” in Proc. of IEEE ICDCS, 2020
[7] Rouhani, S., Deters, R., 2019. Blockchain based access control systems: State of the art and challenges. IEEE/WIC/ACM International Conference on Web Intelligence, 2019. 423-428.
[8] Salman, T., Zolanvari, M., Erbad, A., Jain, R., Samaka, M., 2018. Security services using blockchains: A state of the art survey. IEEE Commun. Surv. Tutorials 21, 858– 880.
[9] Sandor, V.K.A., Lin, Y., Li, X., Lin, F., Zhang, S., 2019. Efficient decentralized multiauthority attribute based encryption for mobile cloud data storage. J. Netw. Comput. Appl. 129, 25–36.

