IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 2, February 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202056 |

Decentralized and Privacy-Preserving Public Auditing for Cloud Storage Based on Blockchain

Bhushan Munjal [1] , Vaishnavi Shete [2] , Amruta Daspute [3]

U.G. Student, Department of Computer Engineering, Vishwabharti Engineering College, Ahmednagar, Maharashtra, India [1]

Department of Computer Engineering, Vishwabharti Engineering College, Ahmednagar, Maharashtra, India [2]

ABSTRACT: Cloud storage is a service model in which data is transmitted and stored on remote storage systems, where it is maintained, managed, backed up and made available to users over a network --typically, the internet. Users generally pay for their cloud data storage on a per-consumption, monthly rate. Blockchain is touted for its capability to improve the trust and straightforwardness of information based exchanges among people and associations. The innovation offers guarantee when deliberately applied in the correct settings. Customarily, associations working their own, singular IT frameworks trying to team up must deal with difficulties including compromise of data, recognizing a solitary wellspring of truth, and encouraging responsibility. Blockchain innovation tends to these difficulties by giving a specialized establishment that underpins the execution of shared business forms such that no single substance controls the whole framework. Government has a characteristic need to assemble, support, and ensure open trust in data and frameworks. In certain circumstances, blockchain may help improve this trust.

KEYWORDS: BLOCKCHAIN, PUBLIC VERIFICATION, DECENTRALIZED PUBLIC AUDITING.

I. INTRODUCTION

Blockchain is touted for its capability to improve the trust and straightforwardness of information based exchanges among people and associations. The innovation offers guarantee when deliberately applied in the correct settings. Customarily, associations working their own, singular IT frameworks trying to team up must deal with difficulties including compromise of data, recognizing a solitary wellspring of truth, and encouraging responsibility. Blockchain innovation tends to these difficulties by giving a specialized establishment that underpins the execution of shared business forms such that no single substance controls the whole framework. Government has a characteristic need to assemble, support, and ensure open trust in data and frameworks. In certain circumstances, blockchain may help improve this trust. The security of most auditing schemes is based on the assumption that the TPA is honest and trustworthy however, in practice, the TPA does not always act as expected. What is worse, the TPA has total control to fabricate audit results without disincentive. Such undetected mistakes can be avoided by publishing all information related to auditing, although this is hard to realize in the TPA-based framework. In this report, we offer a promising solution to the above problems. We propose a blockchainbased auditing framework in which the audit is performed by multiple auditors (who are selected randomly from local users) with the help of a smart contract. The proposed framework has the following dominance. a) Fault-tolerance: the audit is not affected even when a portion of auditors malfunction or are controlled by attackers. b) Transparency: both auditing rules and auditing processes are stored on the blockchain and so are publicly accessible. As a further step, we build a decentralized auditing system called Audinet based on the proposed framework. Audinet consists of three parts: a) auditor election, which is an algorithm that selects a random subset of local users as auditors with a bias towards users with more data stored.

II. RELATED WORK

A blockchain is a type of distributed ledger technology (DLT) that consists of growing lists of records, called blocks, that are securely linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves).

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202056 |

Transactions processed over a blockchain could be settled within a matter of seconds and reduce (or eliminate) banking transfer fees. Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network. A blockchain database stores data in blocks that are linked together in a chain. The data is chronologically consistent because you cannot delete or modify the chain without consensus from the network. As a result, you can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts, and other transactions. The system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of these transactions.

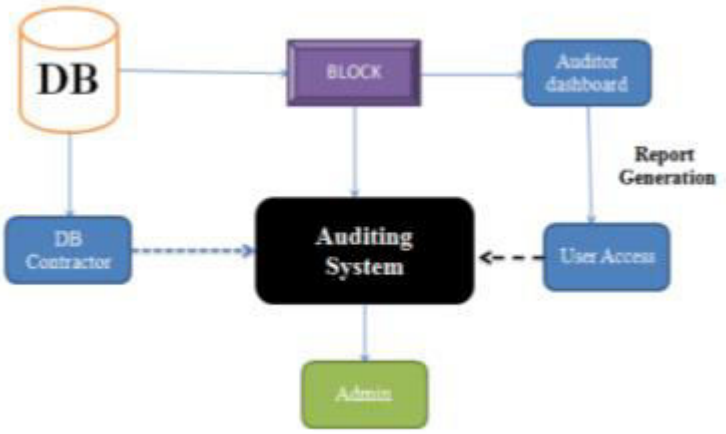
III. PUBLIC VERIFICATION

Customary social database the board arrangements (for example Prophet and SQL), sent universally across a huge number of uses, have one significant operational imperative – the administration of information is performed by a couple of substances who must be trusted. Disseminated Ledger Technologies (DLT, normally alluded to as blockchain), an option compositional way to deal with overseeing information, and evacuates the requirement for a confided in power to store and offer an unendingly developing arrangement of information. To maintain transparency and security at every stage. Like order to create a audit procedure that is incorruptible, system should provide an immutable environment for audit tracking. Also Utilization of transaction.

IV. PROPOSED SYSTEM

Figures shows the results of text detection from an image and inpainting by using exemplar based Inpainting algorithm. Figs. 2, 3, 4 (a) shows the original image. (b) is the image obtained by applying first set of criteria. All objects whose area greater than 10000 and filled area greater than 8000 are eliminated and major axis lengths are in between 20 to 3000 are considered to be text. Still, some small non-text objects are detected.

V. SYSTEM ARCHITECTURE



VI. CONCLUSION

In this report, we initially design a decentralized and privacy preserving public auditing scheme, which is secure against the procrastinating third-party auditor and malicious cloud server. Our scheme utilizes two components to generate unpredicted challenge messages. One is generated by the auditor, and the other is a series of decentralized block hashes. Our scheme could resist against the procrastinating auditor, and a malicious cloud server could not retrieve or guess the challenge message ahead of the audit time.Furthermore, our scheme provides better protection of user privacy during the process of verification of the audit response from the cloud server. We analyzed our scheme to

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202056 |

show that it is secure, and conducted a comprehensive performance analysis, showing that our scheme has low communication overhead and is efficient in terms of computation overhead.

REFERENCES

[1] E. Azhir, N. J. Navimipour, M. Hosseinzadeh, A. Sharifi, and A. Darwesh, "Query optimization mechanisms in the cloud environments: A systematic study," Int. J. Commun. Syst., vol. 32, no. 8, May 2019, Art. no. e3940.
[2] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," J. Netw. Comput. Appl., vol. 79, pp. 88–115, Feb. 2017.
[3] Y. Shin, D. Koo, and J. Hur, "A survey of secure data deduplication schemes for cloud storage systems," ACM Comput. Surveys, vol. 49, no. 4, pp. 1–38, Feb. 2017.
[4] M. Du, Q. Wang, M. He, and J. Weng, "Privacy-preserving indexing and query processing for secure dynamic cloud storage," IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2320–2332, Sep. 2018.
[5] N. Kaaniche and M. Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," Comput. Commun., vol. 111, pp. 120–141, Oct. 2017.
[6] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," Inf. Sci., vol. 387, pp. 103–115, May 2017.
[7] N. A. Kofahi and A. R. Al-Rabadi, "Identifying the top threats in cloud computing and its suggested solutions: A survey," Adv. Netw., vol. 6, no. 1, pp. 1–13, 2018.
[8] A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. 14th ACM Conf.Comput. Commun. Secur. CCS, 2007, pp.
[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. CCS, 2007, pp. 598–609.
[10] B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Trans. Services Comput., vol. 8, no. 1, pp. 92–106, Jan. 2015.
[11] J. Yuan and S. Yu, "Public integrity auditing for dynamic data sharing with multiuser modification," IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1717–1726, Aug. 2015.
[12] T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Trans. Comput., vol. 65, no. 8, pp. 2363–2373, Aug. 2016.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details