Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

Data Integrity Auditing Method Using Blockchain Expansion Technology

RAFI SM [1], T SURESH [2]

[1] PG Scholar, Dept of CSE, Gokula Krishna College of Engineering, Sullurpeta, AP, India.

[2] Associate Professor, Dept of CSE, Gokula Krishna College of Engineering, Sullurpeta, AP, India.

ABSTRACT_ Although data integrity is an important issue, an increasing number of users are outsourcing data to the cloud. Researchers are increasingly turning to blockchain to replace third-party auditors due to its decentralization and immutability. A data integrity system based on blockchain expansion technology is proposed in this paper to address the high costs of maintaining the blockchain network and allowing users to create new blocks due to the rapid growth of blocks in the current blockchain technology's data integrity audit scheme. On the main chain and its subchains, smart contracts are implemented by users and cloud service providers (CSP). The sub-chain completes intensive and frequent computing work, and the sub-chain submits the sub-chain's computation results to the main chain periodically or as needed to guarantee their finality. To avoid affecting the user experience as a result of communication with the CSP during the audit, the concept of non-interactive audit is introduced. A reward pool mechanism is implemented to guarantee the safety of data. Exhaustive examination from angles, for example, capacity, clump evaluating and information consistency demonstrates the accuracy of the plan. Probes the Ethereum blockchain stage show the way that this plan can really lessen capacity and computational above.

1. INTRODUCTION

In today's primary [31] and backup [26], [39], and [42] storage systems, CHUNK-BASED deduplication is frequently used to save a lot of space. It stores just a solitary actual duplicate of copy pieces, while referring to all copy lumps to the actual duplicate by little size references. Deduplication has been shown to effectively reduce primary storage's storage space by 50% [31] and backup storage's storage space by up to 98 percent [39]. This spurs the wide organization of deduplication in different business distributed storage administrations (e.g., Dropbox, Google Drive, Bitcasa, Mozy, and Memopal) to diminish significant capacity costs [18]. To give classification ensures, scrambled deduplication [7], [8] adds an encryption layer to deduplication, to such an extent that each piece, prior to being composed to deduplicated capacity, is deterministically encoded through

symmetric-key encryption by a key got from the lump content (e.g., the key is set to be the cryptographic hash of piece content [14]). Because of this, we are able to apply deduplication to the encrypted chunks in order to save space because duplicate chunks still have the same content even after encryption. In order to effectively manage outsourced data in cloud storage, numerous studies (e.g., [5], [7], [25], [33], and [36]) have designed various encrypted deduplication schemes. A deduplicated storage system must maintain deduplication metadata in addition to storing non-duplicate data. Deduplication metadata can be divided into two categories. The system keeps a fingerprint index that tracks the fingerprints of all chunks that have already been stored to see if they are identical. Likewise, to permit a record to be reproduced, the framework keeps a document recipe that holds the mappings from the lumps in the record to the references of the relating physical copies.\

Deduplication metadata is famously known to cause high capacity above [11], [21], [30], particularly for the exceptionally repetitive responsibilities (e.g., reinforcements) as the metadata stockpiling above turns out to be more predominant. We argue in this work that encrypted deduplication keeps key metadata, such as key recipes that keep track of the chunk-to-key mappings that make it possible to decrypt individual files, which results in even higher metadata storage overhead. Key recipes must be managed separately from file recipes, encrypted using the master keys of file owners, and stored separately for each file owner because they contain sensitive key information. In actual deployment, encrypted deduplication's storage efficiency may be compromised by such a high metadata storage overhead.

2. LITERATURE SURVEY

1.H. Wang, D. He, A. Fu, Q. Li, and Q. Wang, ‘‘Provable data possession with outsourced data transfer,’’ IEEE Trans. Services Comput., vol. 14, no. 6, pp. 1929–1939, Nov. 2021.

Abstract:
With the rapid development of cloud computing, more and more enterprises would like to upload and store their data in the public cloud. When the parts of the business of an enterprise are purchased by another enterprise, the corresponding data will be transferred to the acquiring enterprise. For the usual case, how to outsource the computation cost of data transfer to the cloud? How to ensure the remote purchased data integrity? Thus, it is important to study provable data possession with outsourced data transfer (DT-PDP). In this paper, for the first time, we propose the novel concept: DT-PDP. By taking use of DT-PDP, the following three security requirements can be satisfied: (1) the other un-purchased data security of acquired enterprise can be ensured; (2) the purchased data

integrity and privacy can be ensured; (3) the data transferability's computation can be outsourced to the public cloud servers. For the security concept of DT-PDP, we give its motivation, system model and security model. Then, we design a concrete DT-PDP scheme based on the bilinear pairings. At last, we analyze the security, efficiency and flexibility of the concrete DT-PDP scheme. It shows that our scheme is provably secure and efficient.

2. J. Chang, B. Shao, Y. Ji, M. Xu, and R. Xue, ''Secure network coding from secure proof of retrievability,'' Sci. China Inf. Sci., vol. 64, no. 12, Dec. 2021, Art.no. 229301

Abstract

In recent years, storage-as-a-service has emerged as a commercial alternative for user's local data storage due to its features include less initial infrastructure setup, relief from maintenance overhead, and universal access to the data irrespective of the location and devices [5]. However, it also faces several security threats. One of the most serious threats is the integrity of user's stored data. In particular, when storing the data file to a cloud service provider (CSP), a user (or data owner) will delete it from his/her local devices and hence lose local control of it. In this case, CSP may discard some user's rarely accessed data to save its space and earn more profit. Meanwhile, the CSP can lie about the fact. Obviously, it is extremely unfavorable for users. Proof of retrievability (PoR) protocol is just one of initial attempts to formulize the notion of "remotely and reliably checking data's integrity without downloading the whole data file".

3.N. Döttling and S. Garg, ''Identity-based encryption from the Diffie–Hellman assumption,'' J. ACM, vol. 68, no. 3, pp. 1–46, Mar. 2021

Abstract

We provide the first constructions of identity-based encryption and hierarchical identitybased encryption based on the hardness of the (Computational) Diffie-Hellman Problem (without use of groups with pairings) or Factoring. Our construction achieves the standard notion of identity-based encryption as considered by Boneh and Franklin [CRYPTO 2001]. We bypass known impossibility results using garbled circuits that make a non-black-box use of the underlying cryptographic primitives

3. PROPOSED SYSTEM

1) In the proposed framework, An information uprightness review convention in light of plasma brilliant agreements is proposed. This protocol has the potential to slow down the growth rate and reduce the storage pressure on the main chain by implementing plasma sub-chains, smart contracts, and smart contracts on the main chain and sub-chains. 2) A batch auditing scheme is proposed for the proposed system. This scheme can batch-process multiple audit tasks simultaneously. TPA audit protocol can be executed with low computational and communication overhead. To try not to influence the client experience because of the correspondence with the CSP

during the review cycle however much as could reasonably be expected, the idea of non-intuitive review is presented. For guaranteeing the rightness of the review, the award pool system is embraced, and the confirmation hub can get sensible prizes.

3) In the proposed framework, An examination of the security of the plan demonstrates the way that it can accomplish the normal security goals. Various trials on the ether block chain additionally showed the productivity and viability of the plan.

3.1 IMPLEMENTATION

Data Owner

In this module, the data owner uploads their encrypted data in the Cloud server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Upload File, View Files, Update File, Verify File's Block(Data Integrity Auditing).

Cloud

The Cloud manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the Server and then Server will decrypt them. The server will generate the aggregate key if the end user requests for file authorization to access and performs the following operations such as Login, View and Authorize User, View and Authorize Owner, View Files By Block chain, View All Transactions, Search Requests, Download Requests, View All Attackers, View File Rank Chart, View Time Delay Results, View Throughput Results.

User

In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and performing the following operations Register and Login, Search, Download, View Files, Search Request, Download Request.

TPA

Responsible for Login, View File's Meta Data, View Files & Generate Secret Key, CPU Speed.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

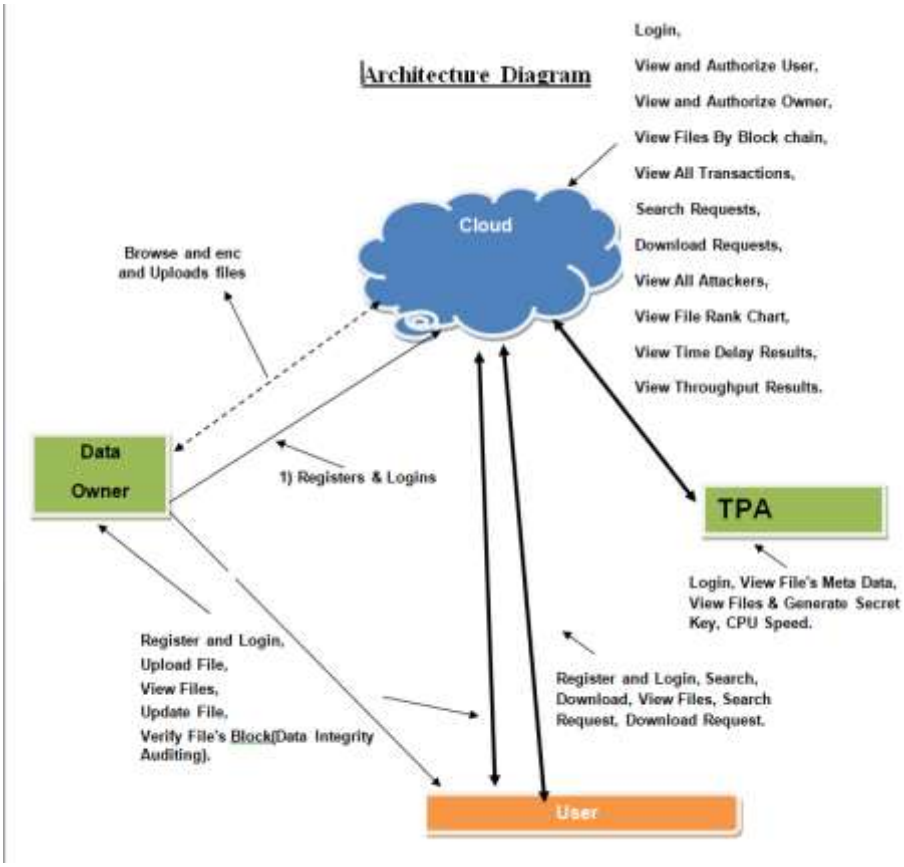
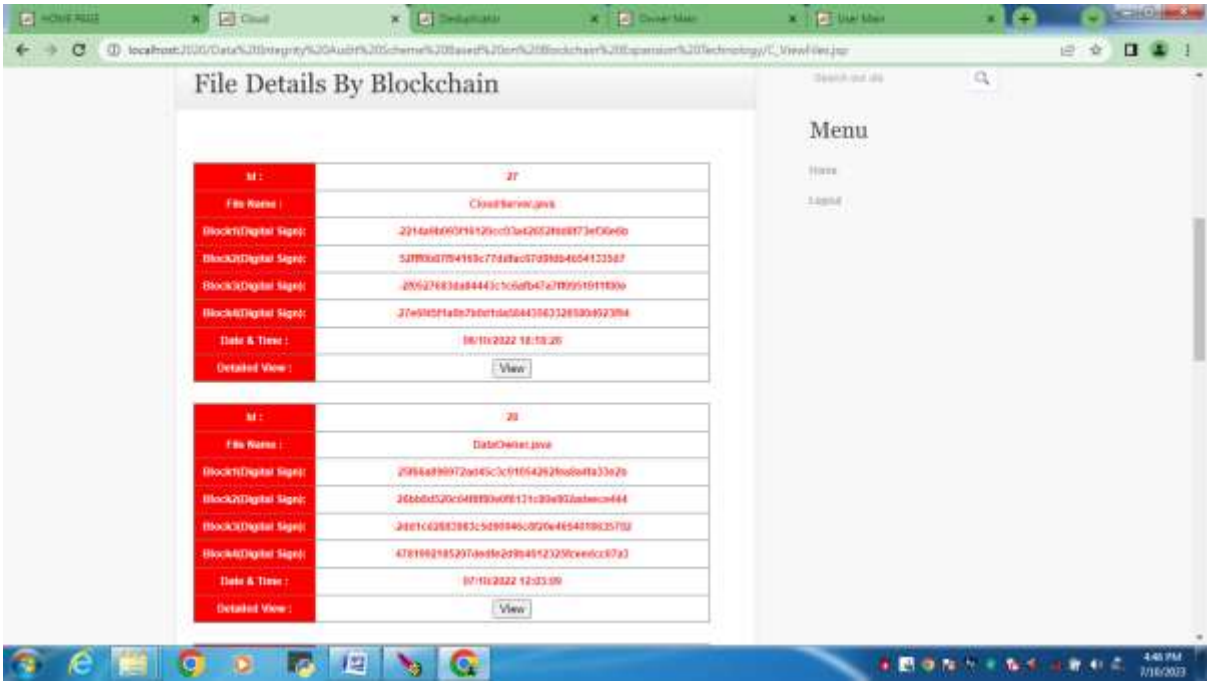


Fig 1: Architecture

4. RESULTS AND DISCUSSION



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

Fig 2:Uploaded data securely

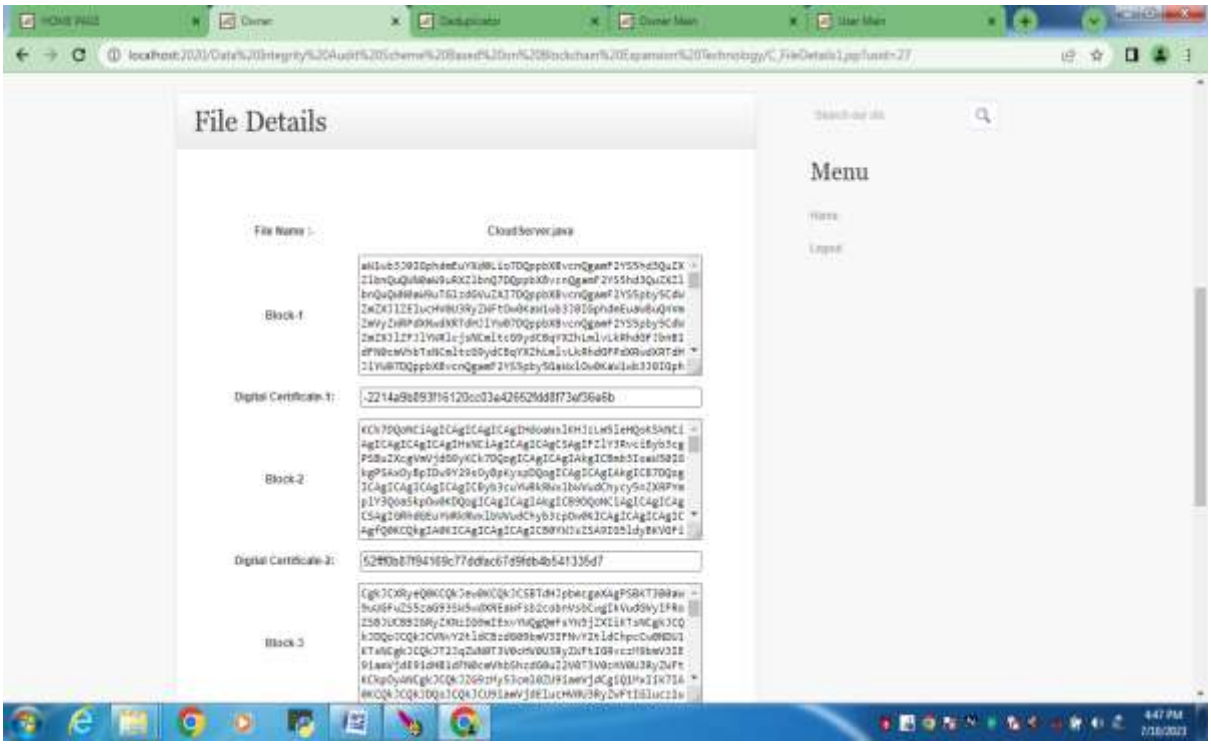


Fig 3:Encrypted data

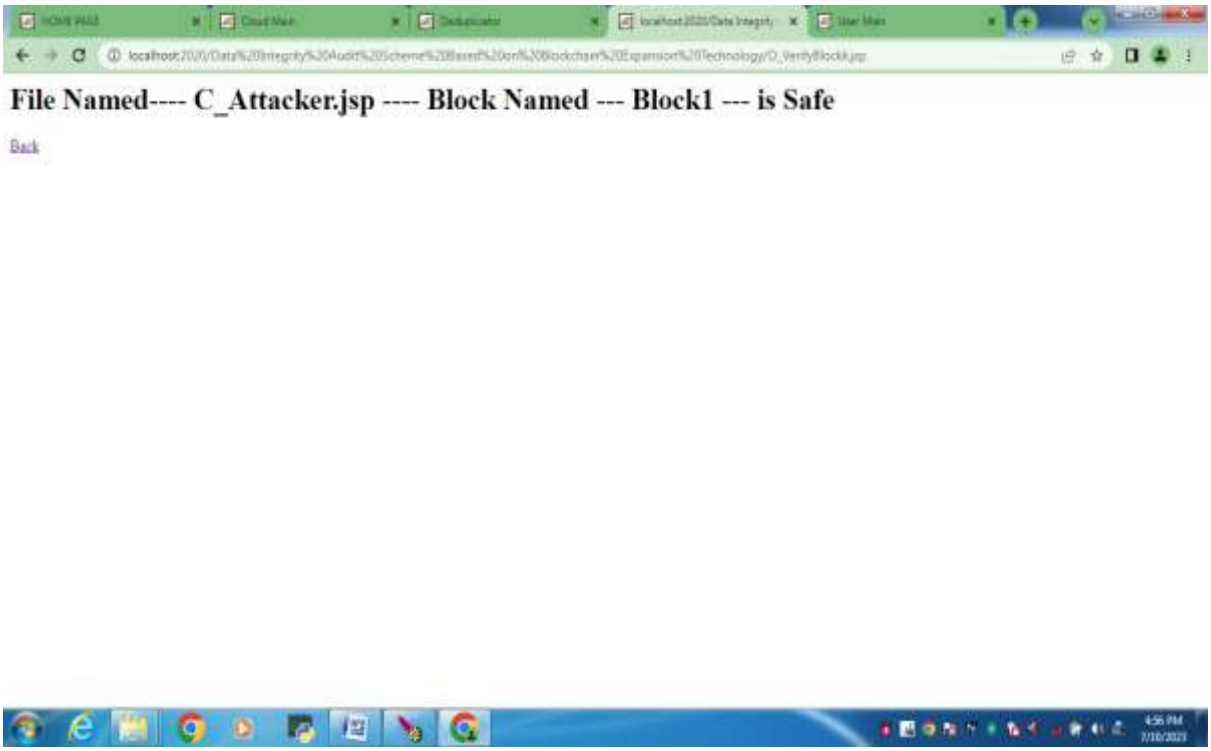


Fig 4:Data Integrity Checking

5. CONCLUSION

How can we ensure that users have access to all of their data stored on cloud servers as cloud computing and cloud storage technologies advance at an ever-increasing rate and the volume of data stored in cloud storage explodes? A data integrity plan based on block chain expansion technology is proposed in this article. We use the block chain network in our scheme to get around some of the problems with traditional auditing, making the scheme more efficient and secure. Additionally, we implement smart contracts on the main chain and plasma sub-chain, respectively. Through this convention, the capacity strain of the primary chain can be significantly decreased, the development rate can be dialed back, the capacity and computational above can be diminished, and the framework execution can be gotten to the next level. At the same time, the reward pool mechanism and the idea of a non-interactive audit are added to guarantee the audit's accuracy and prevent the smart contract platform and CSP from interacting during contract execution. As a result, the solution is able to achieve the anticipated security goals..

REFERENCES

[1] K. Hao, J. Xin, Z. Wang, and G. Wang, ``Outsourced data integrity veri_cation based on blockchain in untrusted environment," *World Wide Web*, vol. 23, no. 4, pp. 2215_2238, Jul. 2020.

[2] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, ``One secure data integrityveri_cation scheme for cloud storage," *Future Gener. Comput. Syst.*, vol. 96, pp. 376_385, Jul. 2019.

[3] H. Wang and J. Zhang, ``Blockchain based data integrity veri_cation for large-scaleIoT data," *IEEE Access*, vol. 7, pp. 164996_165006, 2019.

[4] Z. Miao, C. Ye, P. Yang, R. Liu, B. Liu, and Y. Chen, ``A scheme for electronic evidence sharing based on blockchain and proxy re-encryption," in*Proc. 4th Int. Conf. Blockchain Technol. Appl.*, Dec. 2021, pp. 11_16.

[5] F. Kefeng, L. Fei, Y. Haiyang, and Y. Zhen, ``A blockchain-based _exible data auditing scheme for the cloud service," *Chin. J. Electron.*, vol. 30, no. 6, pp. 1159_1166, Nov. 2021.

[6] K. He, J. Shi, C. Huang, and X. Hu, ``Blockchain based data integrity veri_cation for cloud storage with T-Merkle tree," in *Proc. Int. Conf. Algo-rithms Archit. Parallel Process.* Cham, Switzerland: Springer, Oct. 2020, pp. 65_80.

[7] Y. Lei, Z. Jia, Y. Yang, Y. Cheng, and J. Fu, ``A cloud data access authorization update scheme based on

blockchain," in *Proc. 3rd Int. Conf. Smart BlockChain (SmartBlock)*, Oct. 2020, pp. 33_38.

[8] Y. Yuan, J. Zhang, W. Xu, and Z. Li, ``Identity-based public data integrityveri_cation scheme in cloud storage system via blockchain," *J. Supercomput.*, vol. 78, pp. 8509_8530, Jan. 2022.

[9] S. Wang, D. Zhang, and Y. Zhang, ``Blockchain-based personal health records sharing scheme with data integrity veri_able," *IEEE Access*, vol. 7, pp. 102887_102901, 2019.

[10] A. Liu, Y. Wang, and X. Wang, ``Blockchain-based data-driven smart customization," in *Data-Driven Engineering Design*. Cham, Switzerland: Springer, 2022, pp. 89_107.

[11] K. Dhyani, J. Mishra, S. Paladhi, and I. S. Thaseen, ``A blockchain-based documentveri_cation system for employers," in *Proc. Int. Conf. Comput. Intell. Data Eng.* Singapore: Springer, 2022, pp. 123_137.

[12] K. Xu, W. Chen, and Y. Zhang, ``Blockchain-based integrity veri_cation of data migration in multi-cloud storage," *J. Phys., Conf. Ser.*, vol. 2132, no. 1, Dec. 2021, Art. no. 012031.