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 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

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: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305262 |

Data Integrity Audit Scheme Based on Block Chain Expansion with File Prediction

Dr. G. Kavitha, G. Raghul, Dr. G. Kalaimani

Professor & HOD, Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Assistant Professor, Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Professor, Department of CSE, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India

ABSTRACT: With the large-scale application of cloud storage, how to ensure cloud data integrity has become an important issue. Although many methods have been proposed, they still have their limitations. This paper improves some defects of the previous methods and proposes an efficient cloud data integrity verification scheme based on blockchain. In this paper, we proposed a lattice signature algorithm to resist quantum computing and introduced cuckoo filter to simplify the computational overhead of the user verification phase. Finally, the decentralized blockchain network is introduced to replace traditional centralized audit to publicize and authenticate the verification results, which improves the transparency and the security of this scheme. Security analysis shows that our scheme can resist malicious attacks and experimental results show that our scheme has high efficiency, especially in the user verification phase.

KEYWORDS: Security; data integrity; blockchain; distributed, system; congestion; intelligent agent.

I. INTRODUCTION

With lots of applications deployed in the cloud, user data are also collected centrally and handed over to the cloud. Cloud computing provides users with shared computing resources and storage resources and has multiple deployment models like private cloud, community cloud, public cloud, and hybrid cloud [1]. For users, storing data in the cloud can bring many benefits, such as reducing hardware investment costs, reducing the local storage burden, and supporting remote access. However, while cloud storage brings convenience, it also brings corresponding challenges. Highly centralized data and complex computing environments make user data subject to multiple threats [2]. Compared to traditional data centers, the cloud has more complex systems. The numerous components make the cloud more likely to be attacked. As the complexity of the systems increases, so do the vulnerabilities of the systems. Secondly, multitenants share cloud computing resources, making data more vulnerable to be damaged. In the cloud computing environment, the customized resources between tenants are usually isolated by adopting a logical method. A malicious attacker may pretend to be a tenant to launch an internal attack, violating other users' data. Finally, cloud service providers may deliberately hide that user data are corrupted or store data that users rarely access offline. Considering the large-scale outsourcing data and limited computing power, verifying outsourcing data integrity has become a vital issue in cloud storage.

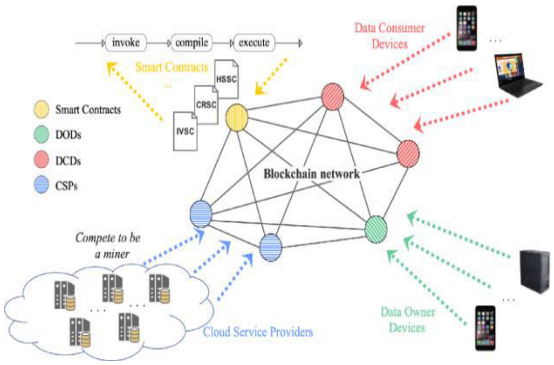

Fig 1: Blockchain Based Data Integrity Verification

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305262 |

The root problem of cloud data security lies in the trust between the cloud service provider (CSP) and the user. Failure of cloud devices, external attacks, or even the snooping of user data by the CSPs may result in leakage, loss, and damage of user data. On the other hand, even if user data is destroyed, users may not achieve effective accountability, and the CSP will evade responsibility and not recognize it. Therefore, the essence of the problem lies in the lack of trust between the two sides. Once problems occur, it is difficult for the challenged party to provide the basis agreed by both sides.

The traditional solution is to introduce a third-party auditor (TPA) to form a three-party authentication model [3], as shown in Figure 1. But there are still problems in this way, which cannot guarantee that the TPA will not cooperate with the other party to cheat for interests or other reasons. However, the emergence of blockchain provides a new solution to this problem. Blockchain is a type of chain structure that combines data blocks in chronological order, and it is a tamper-proof and nonforgeable distributed ledger guaranteed by cryptography [4]. All blockchain participants maintain the blockchain's node information, so all information on the blockchain is open and transparent. Once the information is released, it is permanently retained and cannot be tampered with. The open verification and tamper-proof features of the blockchain enable it to act as a trusted third party to address users' concerns in the cloud computing environment, and all results can be published to the blockchain for authentication and maintained by all users of the blockchain. Therefore, integrating the blockchain into cloud computing, using the blockchain's advantages to solve the disadvantages of the cloud computing environment, can more effectively provide users with data security.

II. RELATED WORK

With the rapid development of the Internet, there are more and more new hot areas, such as, Internet of Things (IoT), and cloud computing, which have spawned a lot of related research. In the field of cloud computing, there are some researches on the verification of data integrity, as well as data retrieval [8], image retrieval [9, 10], and so on. This section mainly introduces some related work on the cloud data integrity verification, lattice signature, and blockchain involved in this paper. With the popularization of cloud storage, many scholars pay attention to remote data integrity audit. Cloud storage integrity verification refers to how users verify the integrity and availability of data stored in the cloud. To solve the security risks brought by cloud storage, many solutions have been proposed to ensure data integrity. At present, data integrity verification schemes can be divided into two categories: Provable Data Possession (PDP) schemes and Proofs of Retrievability (POR) schemes. The PDP schemes use the "challenge-response" mechanism to verify whether the user's data is correctly stored in the cloud; the POR schemes can recover some lost or damaged data. Besides, referring to the verifier's identity, the verification scheme can be divided into private verification scheme and public verification scheme. Compared with private verification, public verification with TPA better supports public audit, dynamic update, and efficient verification.

proposed a PDP scheme for the first time in consideration of public audit based on the challenge-response mode, using RSA algorithm to generate key pairs and using trusted third-party audit to verify data integrity instead of users. The CSP only needs to return the label information of the file block to verify the integrity of the file, reducing the computational and communication overhead of the data verification process. However, this scheme does not support the dynamic update operation of data. In order to support dynamic auditing of data, proposed an extensible PDP. This scheme first calculates a limited number of verification tokens, and each token is linked to some data blocks, thereby ensuring that the scheme can support the modification of data in a prescribed manner, but the number of verifications and data updates performed by the verifier is limited, and only additional operations are supported. Each update requires recreating the remaining verification tokens.

proposed an algorithm for detecting data verification results to resist counterfeit fraud attacks from untrusted verification results. The algorithm performs cross-validation by establishing a dual evidence mode of integrity verification proof and incredible check proof. Integrity verification proof is used to check the integrity of the data, and incredible check proof is used to determine the correctness of the data verification results, but the introduction of secondary verification evidence to cross-check verification results increases the computation and storage overhead. Shen et al. [20] proposed a new data integrity verification scheme that enables files in cloud storage to be shared securely without affecting privacy and integrity verification.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305262 |

III. METHODS

A third-party audit platform between the user and the CSP is responsible for forwarding and recording the user and the CSP interactions during the data integrity verification process. When users dispute with CSP, the blockchain's records can be submitted to the arbitration institution as valid evidence. All participants jointly maintain the blockchain network, and the behavior of users and CSP is jointly monitored to ensure the system's normal operation.

Generally speaking, files are not immutable after being uploaded by users. In practical applications, users will need to update files, such as add, delete, and modify. So, we use MHT to support dynamic operation. Simultaneously, the proposed scheme reduces the complexity of the verification process by introducing cuckoo filter, so the dynamic operation of the scheme involves two parts. The first part is the update operation of MHT, and the second part is the update operation of the cuckoo filter.

In 2016, NIST (National Institute of Standards and Technology) released "Report on postquantum cryptography". According to the report, due to the rapid development of quantum computing technology, most existing public-key cryptographic standards will no longer be secure under quantum computing. Up to now, there is no effective polynomial time algorithm that can solve the difficult problem based on lattice, so the cryptosystem based on lattice can effectively resist quantum attacks. Therefore, our proposed scheme meets the security requirements of postquantum cryptography. Then, we will analyze the security of the proposed scheme.

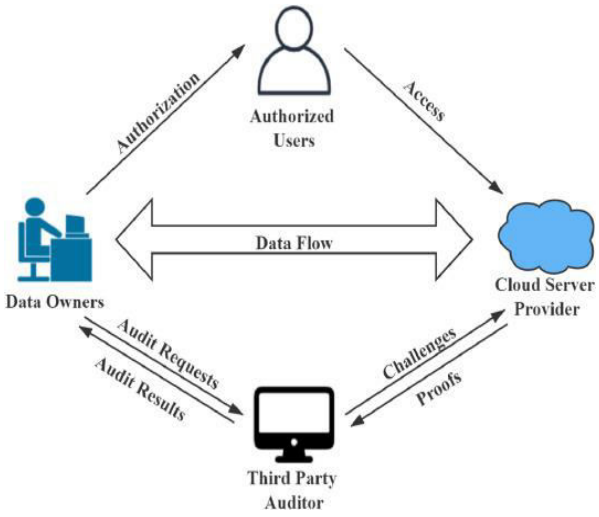

Fig 2: blockchain-based integrity auditing for cloud data

Blockchain is a decentralized and untrusted distributed shared ledger system that combines data blocks in a chronological order to form a specific data structure. It is cryptographically guaranteed to be tamper-proof and unforgeable. From a data perspective, blockchain is a distributed database that cannot be changed in practice. Traditional distributed databases only maintain data at a central server node, and other nodes store only data backups. The data storage on the blockchain is completely distributed; that is, all nodes jointly participate in data maintenance. The tampered or destroyed data of a single node will not affect the data stored in the blockchain. Only more than 51% of the nodes jointly launching an attack can change the data on the blockchain. Therefore, the data on the blockchain can be considered immutable to achieve secure storage of the data.

On the other hand, since the blockchain runs automatically, there is no problem with procrastinating auditors, and it is impossible to collude with CSP. Therefore, when users have disputes with CSP, the records on the blockchain can be used as valid evidence. Simultaneously, by replacing TPA with blockchain, users' sensitive private information is accessible only to themselves, which can avoid obtaining users' privacy information during the TPA verification process and guarantee the users' privacy security. In conclusion, using blockchain as the third-party authentication platform can ensure availability, security, efficiency, and user privacy.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305262 |

IV. RESULT ANALYSIS

The algorithm and cuckoo filter are conducted by C programming language with the pairing-based cryptography (PBC) library version 0.5.14, GNU multiple precision arithmetic (GMP) library version 6.2.0, and the Openssl version 1.0.2n. The security parameter of the lattice signature is set to bits. The size of the file to be signed is all 1 MB. All experimental data are the average result of 100 experiments. The blockchain network is conducted on Hyperledger Fabric. Hyperledger Fabric is a leading open source, general-purpose blockchain structure built for enterprises. Since Hyperledger does not require mining, it does not require strong hardware support, nor consume resources, and its allowable transactions per minute are much greater than Ethereum.

The comparison result of the proof generation time. There is a linear relationship between the proof generation time and the number of challenging blocks. Like the signature generation process, the BLS signature needs to calculate an exponential operation, a hash operation, and a bilinear mapping operation. However, the computational overhead of the ZSS signature in the proof generation stage is higher than that of the BLS signature, since although the ZSS signature does not involve exponential calculations, the amount of data to be calculated is much larger, so it takes the most time. In our scheme, the proof generation stage only involves multiplication, hash, and modulus operations, and the amount of data to be calculated is small, so our scheme has better performance.

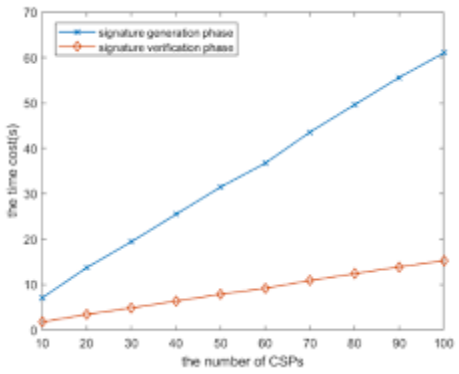

Fig 3: Result Analysis

Then we simulate the performance of the three schemes in the verification phase. Besides, we also compare the performance of our scheme in the verification phase without the cuckoo filter. The comparison result is shown in Figure 11. The BLS signature has the worst performance due to the need to calculate many exponential operations. Without the cuckoo filter, our scheme's performance is worse than the ZSS signature, since the ZSS signature has only bilinear mapping operations in the verification phase, and only a series of addition and multiplication operations are calculated. However, with the introduction of the cuckoo filter, the complex signature verification process is simplified to a simple cuckoo filter lookup process; the verification process only takes a few milliseconds, which is much lower than other methods. When users want to verify the data integrity, they only need to perform a lookup operation of the cuckoo filter to verify whether the signatures returned by the CSP are in the filter.

V. CONCLUSION

With the rapid popularity of cloud storage and the rapid expansion of data on the cloud, ensuring the integrity of the data on the cloud has also become a classic topic. In this paper, we propose an efficient cloud data integrity verification scheme based on blockchain. In our scheme, we use the blockchain network to solve some shortcomings of the traditional centralized audit and improve the efficiency and security of the scheme. On the other hand, based on the assumption of SIS problem, our scheme can resist the threat of quantum computing, and by combining lattice signature and cuckoo filter, we also simplify the user verification process, solving part of the problem of the insufficient computing power of users. The proposed scheme's performance is evaluated, and the result shows that the scheme is provably efficient. In future work, the closer combination of blockchain and integrity verification scheme needs to be explored and more comprehensive characteristics of the scheme need to be satisfied.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305262 |

REFERENCES

1. S. Nepal, S. Chen, J. Yao, and D. Thilakanathan, "DIaaS: Data Integrity as a Service in the Cloud," in Proceedings of the 2011 IEEE 4th International Conference on Cloud Computing, pp. 308–315, IEEE, Washington, DC, USA, 2011.
   View at: Google Scholar
2. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 199–212, ACM, New York, NY, USA, 2009.
   View at: Google Scholar
3. G. Ateniese, R. Burns, R. Curtmola et al., "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 598–609, ACM, New York, NY, USA, 2007.
   View at: Google Scholar
4. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: beyond bitcoin," Applied Innovation, vol. 71, no. 2, pp. 6–10, 2016.
   View at: Google Scholar
5. W. S. H. M. W. Ahmad, N. A. M. Radzi, F. S. Samidi et al., "5G technology: towards dynamic spectrum sharing using cognitive radio networks," IEEE Access, vol. 8, pp. 14460–14488, 2020.
   View at: Publisher Site | Google Scholar
6. J. Su, R. Xu, S. Yu, B. Wang, and J. Wang, "Idle slots skipped mechanism based tag identification algorithm with enhanced collision detection," KSII Transactions on Internet and Information Systems, vol. 14, no. 5, pp. 2294–2309, 2020.
   View at: Google Scholar
7. J. Su, R. Xu, S. Yu, B. Wang, and J. Wang, "Redundant rule detection for software-defined networking," KSII Transactions on Internet and Information Systems, vol. 14, no. 6, pp. 2735–2751, 2020.
   View at: Google Scholar
8. X. Jiang, J. Yu, J. Yan, and R. Hao, "Enabling efficient and verifiable multi-keyword ranked search over encrypted cloud data," Information Sciences, vol. 403-404, pp. 22–41, 2017.
   View at: Publisher Site | Google Scholar
9. Z. Zhou, Q. M. J. Wu, Y. Yang, and X. Sun, "Region-level visual consistency verification for large-scale partial-duplicate image search," ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 16, no. 2, pp. 1–25, 2020.
   View at: Publisher Site | Google Scholar
10. Z. Zhou, Y. Mu, and Q. M. J. Wu, "Coverless image steganography using partial-duplicate image retrieval," Soft Computing, vol. 23, no. 13, pp. 4927–4938, 2019.
    View at: Publisher Site | Google Scholar
11. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, pp. 1–10, ACM, New York, NY, USA, 2008.
    View at: Google Scholar
12. C. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," ACM Transactions on Information and System Security, vol. 17, no. 4, pp. 1–29, 2015.
    View at: Publisher Site | Google Scholar
13. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.
    View at: Publisher Site | Google Scholar
14. E. Zhou, Z. Li, H. Guo, and Y. Jia, "An improved data integrity verification scheme in cloud storage system," Acta Electronica Sinica, vol. 42, no. 1, pp. 150–154, 2014.
    View at: Google Scholar
15. Y. Zhu, H. Wang, Z. Hu et al., "Dynamic audit services for integrity verification of outsourced storages in clouds," in Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 1550–1557, ACM, New York, NY, USA, 2011.
    View at: Google Scholar

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details