ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 3, March 2024

Blockchain-Based Automated Auditing Against Malicious Auditors for Data Integrity and Verification in Cloud Storage

[1] Kishore D, [2] Karthick S, [3] J. Sarojini Premalatha, M.E

[1] [2] [3] Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India

Corresponding Author Email: [1] 582kishore@gmail.com, [2] karthick081202@gmail.com

Abstract*— Users greatly benefit from the use of cloud storage services when it comes to data management. One of the numerous security issues it raises, however, is data integrity. A user may hire an auditor to check the data's integrity using public verification methods; however, current public verification systems are susceptible to auditors putting off verifications until the last minute. The majority of public verification techniques also have issues with certificate management as they are built on the PKI. Using blockchain technology, we provide the first certificateless public verification method (CPVPA) to combat auditors who procrastinate. The main concept is to have auditors record each verification result as a transaction on a blockchain. Users may ensure that auditors execute the verifications at the specified time by having them time-stamped when the appropriate transaction is entered into the blockchain; this is necessary due to the time-sensitivity of transactions on the blockchain. In addition, the certificate management problem is not an issue with CPVPA since it is based on certificateless cryptography. We establish that CPVPA is secure by presenting rigorous security proofs, and we show that it is efficient by doing a thorough performance assessment in addition an image or file recovery mechanism is included to improve the cloud storage system's general integrity and reliability.

Keywords: Data integrity, auditors procrastination, blockchain, certificateless public verification, file recovery.

I. INTRODUCTION

With the promise of cost savings and operational efficiency brought about by pay-as-you-go pricing and on-demand provisioning, more and more companies are moving their data, apps, and business operations to the cloud. Despite these clear benefits, many businesses still aren't willing to commit to cloud computing. Many people are wary of using cloud services because they have doubts about their safety, privacy, and dependability, and they aren't sure which cloud service providers to trust.

Cloud Service Certifications (CSC) have become an important tactic in reaction to these concerns. By building confidence and enhancing transparency in the cloud business, CSC plays a crucial role in resolving these challenges. Certifications for cloud services mainly aim to guarantee strict adherence to regulations and safety standards. With cloud services evolving in a constantly changing environment, it's reasonable to question the credibility of certifications with validity periods of more than one year.

Our proposed solution to this problem is to apply Continuous Auditing (CA) to certain certification requirements. We contend that certifications should be more trustworthy as continual auditing is essential for guaranteeing the continued security and dependability of cloud services. As a preventative step, regular auditing ensures that cloud services' dependability and security are continuously guaranteed.

While continuous auditing is becoming more important, it is still in its infancy when it comes to cloud services, and current approaches aren't always suitable for third-party audits. Our proposed conceptual Continuous Auditing architecture aims to fill this need. For continuous auditing of cloud services to be successful, this architecture details the key components and procedures that are required. Certification and continual auditing work hand in hand to help firms deal with urgent issues while also building confidence and reassuring stakeholders that their cloud infrastructure is reliable and secure

II. RELATED WORKS

[1] Kan Yang. An Effective and Secure Method for Dynamic Auditing of Data Stored in the Cloud.

Information kept by "data owners" on "cloud servers" is accessible to users, sometimes known as "data consumers," in a cloud computing setting. Having an unbiased auditing agency confirm the validity of cloud data is crucial, since data outsourcing has both advantages and new security issues. The auditing service cannot make use of some existing remote integrity testing methodologies because of the ever-changing nature of cloud data. These methodologies were developed for static archive content. An effective and secure dynamic auditing protocol is desirable for reassuring data owners about the proper storage of their data in the cloud. First, this research suggests an auditing protocol that is both efficient and protects users' privacy. Then, it builds an auditing

framework specifically for cloud storage systems. Then, by incorporating data dynamic processes into our auditing protocol, we use the efficiency and proven security of the random oracle architecture. Our auditing technique has been expanded to support batch auditing for several clouds and owners, without the need for a trusted organizer. The results of the simulations and analyses show that the auditing methods we proposed are secure and efficient, especially when it comes to reducing the computing cost for the auditor.

[2] Appearing on page 2 of the presentation are the authors Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou.

Privacy-Preserving Public Audits for Secure Online Data Storage.

The integrity of cloud storage shouldn't be a concern for customers; it ought to function similarly to local storage. Therefore, public cloud auditing is essential so that customers can rest comfortable knowing that TPAs are checking their outsourced data. To establish a reliable TPA, the auditing procedure must not endanger users' data privacy or hinder their internet access to an excessive degree. With the goal of easing public audits without compromising user privacy, this essay proposes a private cloud storage solution. To make things even better, we extend our result so that the TPA may audit several users simultaneously with ease. Extensive performance and security testing has shown that the proposed solutions are both highly efficient and provably safe.

[3] Wu Xiaodong, Yu Yong, Ni Jianbing, Zhang Kuan, and Shen Xuemin (Sherman) Li.

We can provide mobile crowd sensing job allocation and safe deduplication with fog computing.

Mobile crowd sensing allows a big number of individuals to combine their mobile devices to collect data for certain consumer groups. The involvement of mobile users is crucial to mobile crowd sensing. Increasing the number of participants allows us to collect more sensor data, but there is a chance that we will generate more duplicate data, which makes communication more difficult. Therefore, data deduplication, the process of removing duplicate data, is crucial for enhancing communication efficiency. Because sensor data is often encrypted, it is difficult to remove duplicates. This research presents a fog-based mobile crowd sensing platform for more precise task allocation. Depending on the user's mobility, fog nodes may distribute duties accordingly. Also, to boost communication efficiency and data secrecy, Finally, we demonstrate that both approaches provide secure data deduplication in an efficient manner.

[4] A data publish-subscribe service for cloud platforms that protects user privacy using attribute-keywords; Kan Yang, Kuan Zhang, Xiaohua Jia, M. Anwar Hasan, and Xuemin (Sherman) Shen b.

One excellent method for the selective distribution and reception of data is a data publish-subscribe service. The greatest platform for data publication and subscription is swiftly emerging as cloud computing, with to its inexpensive but strong storage and processing capabilities, handles the enormous volumes of data produced daily. However, cloud servers may care about users' interests in addition to the provided data. Here, we provide an attribute-keyword based data publish-subscribe AKPS approach for cloud platforms that protects user privacy.

Our approach involves encrypting published data using attribute-based encryption and outsourcing decryption. This lets publishers independently control data access while transferring the heavy lifting of decryption from subscribers' devices to the cloud server. This ensures that the published data is protected from both the cloud server and any other non-subscribers. To safeguard their interests, we provide a unique searchable encryption that subscribers may utilize to choose access the information that interests them. Unlike competing symmetric searchable encryption schemes, the AKPS ensures that no two subscribers or publishers will ever exchange secret keys, even if it permits a large number of subscribers and publishers. Furthermore, neither subscribers nor publishers may act as an agent for the other. In order to prevent their circumvention during the checking phase, the AKPS deftly links the two secrets that comprise the subscription policy and the access policy. Together, the cipher text and tags form one secret, while the subscription trapdoor and pre-decryption key form the other secret. In the random oracle model, the proposed AKPS method is effective and secure, as shown by the security proof and performance evaluation.

[5] Liu Xiulong, Wang Kun, Yu Jiahui, and Chao Yuan. A Proxy Re-Encryption Approach for Pre-Authentication-Based Big Data Environments.

As data volumes continue to grow, so does the demand for large-scale storage solutions. Information stored in the cloud may be readily shared throughout five distinct service providers. However, private data poses a big problem with big data 6 storage. transfer to just those users who have already been confirmed for certain attributes. An attribute-based authentication technique and a proxy conditional re-encryption multi-sharing mechanism are used in the pre-authentication method to ensure the security of data and attributes. Before re-encryption, this enables attribute authentication. After proving the system's resilience to many attacks, the research shows that the proposed pre-authentication approach might significantly boost the system's security.

III. EXISTING SYSTEM

Traditional auditing approaches have inherent limitations when it comes to handling data integrity and verification in cloud storage. It is common practice to have centralized auditing organizations or third-party service providers verify the data integrity using conventional methods. On the other hand, issues like collusion, weak points, or even a corrupted

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 3, March 2024

auditing institution are possible outcomes of these processes. Furthermore, manual auditing techniques may be time-consuming, resource-consuming, and lacking in the real-time monitoring capabilities necessary to detect and respond promptly to data manipulation or unauthorized access. Users of cloud storage services have difficulties in guaranteeing the consistent and trustworthy validation of their data due to the lack of a defined and automated mechanism. A degree of vulnerability that is incompatible with the developing threat environment is introduced when confidence is placed in a central authority for auditing. The need for a safer and more sophisticated method of auditing in cloud storage systems is becoming more apparent in light of the increasing data quantities and the critical nature of information integrity. This insight motivated the creation of a new system that uses blockchain technology to remedy the problems with current auditing methods, which are either too laborious or too centralized.

IV. PROPOSED SYSTEM

Users' data must be protected in a MultiCloud environment by implementing remote data integrity verification. Data uploading to the cloud is the responsibility of the users. The file is saved in a MultiCloud setting after being partitioned using the Dynamic Block creation Algorithm. Every single cloud storage unit has its own File Allocation Table (FAT) file system, which contains specific data and indexing.

Here, the auditor promises to check whether certification criteria are being satisfied by evaluating the logs usually generated by service providers while monitoring operations. If data is compromised in a multicloud environment, the verifier may remotely validate the integrity of the data at the block and file levels using the verified data integrity verification method. To prevent the verifier (an outside party) from gaining access to users' private information, the cloud uses random block creation for integrity checks. If data damage happens during checking, the Verifier will restore files right away. Users have the option to use cloud file recovery. Furthermore, blockchain technology is used by the proposed approach. We include all data pertaining to audit records to guarantee the blockchain's security.

V. SYSTEM ARCHITECTURE

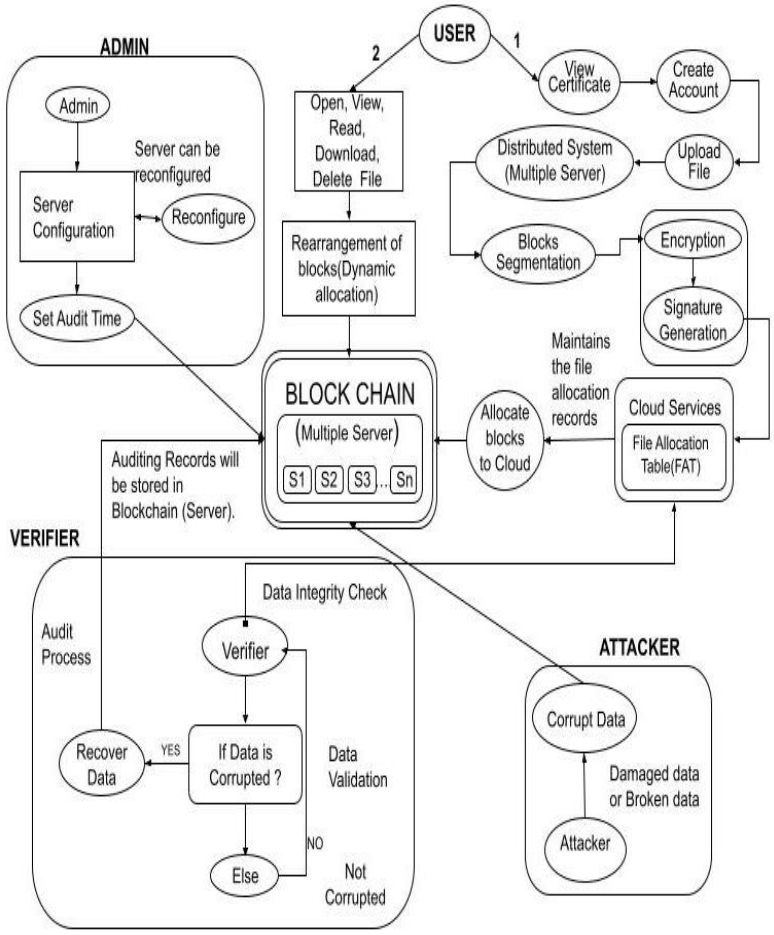

Figure 1. System Architecture

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 3, March 2024

VI. METHODOLOGY

1. Server Configuration:

The administrator sets up the MultiCloud server. Each cloud is assigned an IP address and port number by the administrator. A MultiCloud Storage Server Architecture is now being developed. The previous MultiCloud server configuration may be easily changed by the administrator. The FAT files may be changed or left unchanged for older server configurations. The scheduled time for auditing data integrity will be determined by the administrator.

2. Data Upload and Block Split

At the web end, there is an initial level of registration for users. Users are required to provide their own personal details in order to complete this procedure. The data is then saved in the server's database. Users are able to upload files to the server once they have registered. The files that are uploaded will be saved on a server. Before the data is stored in FATFS, it is first uploaded to several clouds, where it is then divided into blocks using a dynamic block creation algorithm. Signatures are then applied to each block. A digital signature created using the MD5 algorithm. Moreover, the Base64 Algorithm is used for data encoding.

3. Data Integrity Checking and Update details in Blockchain

Each chunk of data that the user uploads to FATFS is properly indexed and metadataed. Cloud data is subject to remote integrity checking by the verifier. During integrity verification, the cloud instead of retrieving the whole file assigns a random mix of blocks to the verifier. That way, a third party (the Verifier) won't be able to pry into user data. Block checking and file checking are the two stages that make up the Verifiable Data Integrity Checking Algorithm. Three signatures are created for Block level checking in the Block Checking process.

- A FATFS-retrieved block signature
- In order to verify a block, a new signature is created.
- It is possible to extract a signature from the cloud-stored block that has one added to it.

For Block level Integrity Checking, the three signatures mentioned above are cross-checked. Additionally, file-level integrity checking is used to validate the block contents. Ensure that all auditing information are updated in the blockchain.

4. File Recovery and Certificate Generation

Any one of those cloud servers might be compromised by an attacker. As part of its data integrity checking process, the verifier notifies the cloud of corrupted blocks. In the event that data corruption occurs, the verifier will immediately initiate the recovery process. If a user's file becomes corrupt, they may submit a complaint to the cloud service (the verifier does not verify this file).The FAT File System is updated and blocks are reallocated dynamically whenever a user accesses a file in the cloud, ensuring access confidentially. On the basis of the cloud's performance, auditors will issue certificates after constant monitoring.After a new user joins the cloud, they will be able to establish an account after reading the certificate.

VII. RESULT AND DISCUSSION

Blockchain, smart contracts, cryptography, and a decentralized consensus process have all been expertly integrated to solve the problems that have long plagued conventional auditing methods. Thanks to smart contracts, the system can automate a lot of formerly manual tasks, which greatly improves efficiency and accuracy. The auditing process is made more efficient and less prone to human mistake as a result, which sets the stage for a more trustworthy verification system. Significantly improving the security and integrity of stored data, the decentralized structure of the blockchain guarantees a distributed ledger that is tamper-resistant.

Continuous monitoring of data transactions is now possible thanks to real-time monitoring tools, which also provide a proactive way to identify and react to data tampering or illegal access quickly. A decentralized verification method has been established via the use of a consensus mechanism that incorporates numerous nodes. This has created a trustless environment that protects against hostile audits, collusion, and single points of failure.

Data verification has been strengthened with the addition of cryptographic methods, such as hashing and encryption, which guarantee the authenticity, integrity, and secrecy of stored information. The system's overall resilience is strengthened by this multi-layered security strategy, which adds to a powerful defense against unauthorized alterations. Users now have a verifiable and auditable record of data exchanges because to the blockchain's built-in features, which greatly improves openness and accountability. By making it possible to see every step of data restoration, this openness helps build confidence in cloud storage. In addition, the system is scalable and flexible, thanks to its modular architecture that lets users tailor it to different cloud storage settings. Because of its flexibility, the system can adjust to the demands of various users and businesses, handling data quantities and transaction frequency that vary widely.

VIII. CONCLUSION

To combat the tardy auditor, CPVPA, we provide a certificate-less public verification mechanism in this article. Each audit that an auditor does is turned into a transaction on the blockchain of on-chain currency via CPVPA. In addition, the certificate management issue does not affect CPVPA. When compared to other schemes, the security study shows that CPVPA offers the best security guarantee. We have also performed an extensive performance study that shows

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 3, March 2024

CPVPA is efficient with respect to calculation overhead and has constant communication overhead and also image or file restoration mechanism is included. So that if any data is corrupted it can be recovered easily.

IX. FUTURE WORK

There are a number of exciting potential future directions that might lead to even more improvements and extensions to the automatic auditing system built on blockchain for verifying and preserving data in the cloud. First, to keep up with the ever-increasing data quantities and transaction frequency, constant scalability optimization is essential. To do this, it may be necessary to investigate more sophisticated consensus techniques and make changes to the architecture to guarantee smooth scaling. It is important to focus on making the system work with multiple blockchain platforms so that cross-chain functionality may be enabled in the future. A more inclusive ecosystem might be created by increasing the system's flexibility to accommodate users on multiple blockchain networks. Anomaly detection skills might be improved by integrating developing technologies like AI and machine learning. In order to make the system more resilient to ever-changing threats, future research might look at integrating these technologies to make it better at detecting and responding to security issues in real-time. Another area that may need some improvement is the user interface and overall experience. Adding visualization tools and dashboards might be a priority for future versions, with the goal of improving user knowledge and involvement by giving them better insights into the auditing process. Implementing methods for smart contract upgradability would guarantee the system's flexibility. This would make sure the system adapts quickly to new needs by allowing for the addition of features and enhancements without interfering with its functioning. Immediate attention must be given to issues pertaining to sensitive data, and research in the future may investigate methods that protect individuals' privacy. To further improve data security measures, advanced cryptographic approaches or privacy-focused blockchain systems might be explored to secure user data during audits. The system's reliance on proof-of-work consensus makes energy efficiency all the more important. Alternate consensus methods or improvements to reduce the ecological footprint of blockchain-based audits might be the subject of future research. It is crucial to work together with industry stakeholders, regulatory agencies, and standards groups to promote worldwide acceptance and standardization. To help blockchain-based auditing solutions gain traction, we need to establish best practices and make sure they work with each other. Stakeholders might be included in decision-making processes for the system's creation, updates, and general governance if decentralized governance models were to be considered.

REFERENCES

[1] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "Privacy-preserving data aggregation computing in cyber-physical social systems," ACM Transactions on Cyber-Physical Systems, vol. 3, no. 1, p. 8, 2018.

[2] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, vol. 32, no. 6, pp. 144–151, 2018.

[3] J. Li, H. Ye,W.Wang,W. Lou, Y. T. Hou, J. Liu, and R. Lu, "Efficient and secure outsourcing of differentially private data publication," in Proc. ESORICS, 2018, pp. 187–206.

[4] L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on blockchain," Future Generation Computer Systems, vol. 93, pp. 327–337, 2019.

[5] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870–885, 2019.

[6] Bai, Y. et al. A cloud data integrity verification scheme based on blockchain, 357–363 (IEEE, 2021).

[6] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, "Privacypreserving attribute-keyword based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116– 131, 2017.

[7] W. Shen, B. Yin, X. Cao, Y. Cheng, and X. Shen, "A distributed secure outsourcing scheme for solving linear algebraic equations in ad hoc clouds," IEEE Trans. Cloud Computing, to appear, doi: 10.1109/TCC.2016.2647718.

[8] H. Yang, X. Wang, C. Yang, X. Cong, and Y. Zhang, "Securing -centric networks with content-based encryption," Journal of Network and Computer Applications, vol. 128, pp. 21–32, 2019.

[9] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS, 2009, pp. 355–370.

[10] X. Zhang, H. Wang, and C. Xu, "Identity-based key-exposure resilient cloud storage public auditing scheme from lattices," Information Sciences, vol. 472, pp. 223–234, 2018.33

[11] K.Wang, J. Yu, X. Liu, and S. Guo, "A pre-authentication approach to proxy re-encryption in big data context," IEEE Transactions on Big Data, 2017, to appear, doi.10.1109/TBDATA.2017.2702176.

[12] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Providing task allocation and secure deduplication for mobile crowdsensing via fog computing," IEEE Transactions on Dependable and Secure Computing, to appear, doi. 10.1109/TDSC.2018.2791432.

[13] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," IEEE Trans. Information Forensics and Security, vol. 12, no. 3, pp. 676–688, 2017.

[14] H. Shacham and B. Waters, "Compact proofs of retrievability," of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[15] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013.