Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 9, September : 2024

Stub Signature-Based Efficient Public Data Auditing System using Dynamic Procedures in Cloud Computing

Dr. Mahabubul Haq Atif, Professor, Department of CSE, Deccan College of Engineering and Technology, Osmania University, Hyderabad, Telangana, atif@deccancollege.ac.in

Husna Sultana, PG Scholar, Department of CSE, Deccan College of Engineering and Technology Osmania University , Hyderabad, Telangana, husnasultana250498@gmail.com

***Abstract*— Online cloud data storage is a rapidly growing pillar of the IT industry that offers data owners an array of attractive developments in highly sought-after online scalable storage services. Cloud users can easily access these services and have the flexibility to manage their process data effectively without worrying about the deployment or maintenance of personal storage devices. As a result, the number of cloud users has increased to purchase these convenient and cost-effective services, while Cloud Service Providers (CSP) are also rising to meet this demand for appealing cloud solutions. However, there is one major security issue related to outsourced data on shared cloud storage: its privacy and accuracy cannot be guaranteed as it may be vulnerable to unauthorized access by malicious insiders or hackers from outside sources. To address these issues, we suggest proposing a partial signature-based data auditing system so that both privacy and accuracy can be fortified while reducing the computational cost associated with auditing processes significantly. This system would involve using cryptographic techniques such as homomorphic encryption and hash functions, which would enable secure sharing between multiple parties while ensuring integrity checks on stored files at regular intervals for any potential tampering attempts made by external attackers or malicious insiders who may try to gain unauthorized access into confidential user information stored within cloud sites. Another benefit of the plan is that it supports dynamic operation on outsourced data. This research work may achieve the desired security qualities, according to the security analysis, and it is effective for real-world applications, as demonstrated by simulation outcomes of dynamic operations on various numbers of data blocks and sub-blocks.**

***Index Terms*— Edge computing, distributed storage, cloud-native orchestration, blockchain.**

I. INTRODUCTION

Cloud computing has been visualized as the next-generation information technology (IT) for businesses due to a lengthy list of unmatched benefits in IT's historical past, including on-demand self-service, widespread network services, location-independent dynamic resources, quick resource stretch ability, utilization pricing, and threat transmission . Since using the services of cloud allows users to outsource their data without having to pay high hardware and software servicing fees, users benefit greatly from using it. However, if users move their data to the cloud and stop keeping it locally, they will no longer have physical control over it. It is challenging to guarantee the integrity of cloud data because hardware/software faults and human mistakes are unavoidable in the cloud. To examine whether the data saved in the cloud is unbroken or not and to evaluate whether the information is properly stored in the cloud, a variety of data auditing approaches have been presented . In global file integrity auditing methods, data blocks must first be signed by the cloud user before being delivered to the cloud. The evidence for that reason is provided by such signatures. At this stage of the integrity inspection, these data blocks are genuinely present in the cloud. After that, the data owner uploads these data blocks and their matching signatures to the

cloud. Many users of various cloud storage services, such as Google iCloud, Drive, and Dropbox, often share the infor motion stored in the cloud. Sharing of data is one of the most numbers of individuals who can access it thanks to common cloud storage characteristics to allow others to see their information. Many research works discussed pairing schemes because of their time-consuming nature during com potation. In research paper , public verification scheme has been proposed to check cloud users' data integrity and also to resist external adversaries using Boneh_Lynn_Shacham (BLS) signature. A unique hash function called Map-To Point, which is also employed by the majority of traditional cryptographic systems from pairs, is required for BLS short signatures. This hash function involves more pairing operations, which makes it probabilistic and inefficient in general. Zhang_Safavi_Susilo (ZSS) short signature is more efficient than BLS method because it performs less pairing operations. ZSS signature is utilized in the study article for batch auditing and to protect data privacy in cloud servers .

When creating third-party cloud data auditing techniques, the bilinear paring is frequently used. However, these auditing schemes' verification processes will result in a significant cost for that calculation. As a result, a better auditing system must be created with cloud computing in mind. An algebraic signature-based cloud data integrity auditing technique that can satisfy the security features of data secrecy, privacy preservation, and free-riding attack resistance has been proposed in a research study .

The majority of the auditing techniques currently in use are focused on the challenging issues of discrete logarithms and large integer decomposition. These systems will confront a security risk when quantum computers get more advanced since they can handle these challenging issues with ease. Designing a data audit system that is impervious to quantum attacks is crucial. Therefore, a novel data audit system is used in this research work to ensure post-quantum security, based on the ring signature problem of learning with errors. Most often in research works a cloud user divides his or her data into data blocks, creates a signature for each data block, and uploads the original data blocks together with the signatures of each data block to shared cloud storage. Signature generation can occasionally take longer for all data blocks, and this highlights problems with data secrecy.

Later, cloud users pay a Third-Party Auditor (TPA) to verify the authenticity of the data using signatures that are kept in a CSP's shared cloud storage. Because cloud user stores the original file block along with its identification information at cloud storage, despite the existence of all features does not guarantee data secrecy there. As a result, security risks still exist for cloud storage of outsourced data. Therefore, considering the current situation and in order to address the aforementioned issues, this research work pro poses an efficient public data auditing scheme using stub signatures that upholds data confidentiality, data privacy, auditing correctness, unambiguity, anonymity, resists collision and forgery attacks and supports dynamic operations at the sub-block level. In this study, we present a partial signature 2 based outsourced data auditing scheme that can safeguard data security and privacy while conducting data integrity audits.

II. LITERATURE REVIEW

"A Survey on Cloud Computing Security Issues and Challenges"

This paper provides a comprehensive overview of the various security challenges faced in cloud computing. It discusses issues related to data integrity, confidentiality, and privacy, which are critical for efficient public data auditing systems. The survey also explores different security models and solutions, including signature-based methods, to address these concerns.

"Efficient Public Data Auditing in Cloud Computing with Improved Privacy Protection"

This paper focuses on privacy-preserving techniques for public data auditing in cloud computing. It introduces enhanced privacy models and cryptographic techniques that improve the efficiency of

auditing processes while protecting user data from unauthorized access and exposure.

"Dynamic Data Auditing with Secure and Efficient Methods in Cloud Storage"
The study presents methods for dynamic data auditing in cloud storage environments. It emphasizes the need for efficient auditing mechanisms that can handle data modifications and updates securely. The paper evaluates various auditing techniques and their impact on system performance.

"Signature-Based Approaches for Data Integrity in Cloud Computing"
This paper investigates signature-based approaches for ensuring data integrity in cloud environments. It explores different types of signatures, such as digital and cryptographic signatures, and their effectiveness in verifying data accuracy and integrity during auditing processes.

"Dynamic Auditing Protocols for Cloud Storage Systems"
The paper proposes dynamic auditing protocols designed to handle changes in cloud storage data efficiently. It evaluates the performance and security aspects of these protocols and their ability to support continuous auditing despite frequent data modifications.

"Cloud Data Integrity Checking Using Dynamic Auditing Procedures" This research focuses on dynamic auditing procedures for cloud data integrity checking. It discusses how these procedures can adapt to changes in the data and maintain accuracy in auditing results, while also minimizing the computational overhead involved.

"Efficient Algorithms for Public Data Auditing in Cloud Systems" The paper presents various algorithms designed to improve the efficiency of public data auditing in cloud computing. It compares these algorithms in terms of their performance, accuracy, and scalability, and provides recommendations for implementing them in real-world scenarios.

"Advanced Cryptographic Techniques for Secure Data Auditing in Cloud Computing" This study explores advanced cryptographic techniques for enhancing the security of data auditing processes in cloud computing. It covers methods such as homomorphic encryption and zero-knowledge proofs, which contribute to both security and efficiency in public data auditing.

"A Review of Efficient Public Data Auditing Systems in Cloud Computing" The paper reviews various public data auditing systems and their efficiency in cloud computing environments. It highlights key challenges, current solutions, and emerging trends in auditing systems, providing a detailed analysis of their performance and practicality.

III.EXISTING METHODS:

Many research works discussed pairing schemes because of their time-consuming nature during computation.
In research work, public verification scheme has been proposed to check cloud users' data integrity and to resist external adversaries using Boneh_Lynn_Shacham (BLS) signature.

A unique hash function called Map-To Point, which is also employed by the majority of traditional cryptographic systems from pairs, is required for BLS short signatures. Zhang's Avi Susilo (ZSS) short signature is more efficient than BLS method because it performs fewer pairing operations. ZSS signature is utilized in the study article for batch auditing and to protect data privacy in cloud servers

IV. PROPOSED SYSTEM

The proposed research offers a partial signature-based data auditing method that, while maintaining data security, is more effective and computationally time-consuming for signature creation and verification than related schemes.

The following is a summary of our contributions: - To validate the data integrity in shared cloud storage, we provide a public auditing mechanism through a TPA.

The security requirements for maintaining the privacy of outsourced data stores in cloud storage are met by this auditing system, which also upholds data confidentiality, data correctness, auditing correctness, unambiguity, anonymity, etc. while the audit is being conducted. –

We present a privacy method to protect the original block elements from malicious insider and outsider assaults in cloud storage. This technique stops forgery, substitutes attacks on cloud storage, and resists block collusion issues.

METHODOLOGY:

- **Cloud User (CU):** CUs are the consumers of cloud computing who offload their personal data or private files to the cloud resource's servers and take advantage of the cloud's functionalities. They employ fixed or portable tools and wired or wireless networks to access the cloud. The fact that their storage and computing capacities are constrained in comparison to the cloud, despite the fact that their terminals differ, is a shared feature

- **Cloud Service Provider (CSP):** A remote cloud server can be thought of as a storage and computational pool, giving CU access to an endless number of resources. Numerous redundant and distributed servers are leased by CSP, and these servers deliver various services to CU in accordance with their needs. CSP is honest but not entirely dependable; it is interested in a user's data, particularly sensitive data. CSP will carry out all actions in line with the security assurance protocol while it is active on introducing the system.

.

- **Public Third-Party Checker (PTPC):** PTPC is an independent third party, apart from users and the cloud. The PTPC is qualified and equipped to examine cloud data. After CU submits an audit checking request to the PTPC, the PTPC will create a challenge for the data auditing process. The challenge will then be sent to CSP by the PTPC. In accordance with the challenge information, the CSP will produce proof. After examining the proof, the PTPC can produce an audit result. The PTPC can be used to audit user data in a cloud system, saving CU's computing and storage resources while guaranteeing the integrity of the verification process.

- **Remote Cloud Server (RCS):** An amalgam of both public and private cloud storage servers makes up a Remote Cloud Server. A brand-new remote storage server technology provides both the efficiency of a traditional dedicated server and the adaptability of both private and public cloud computing.

ARCHITECTURE:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 9, September : 2024

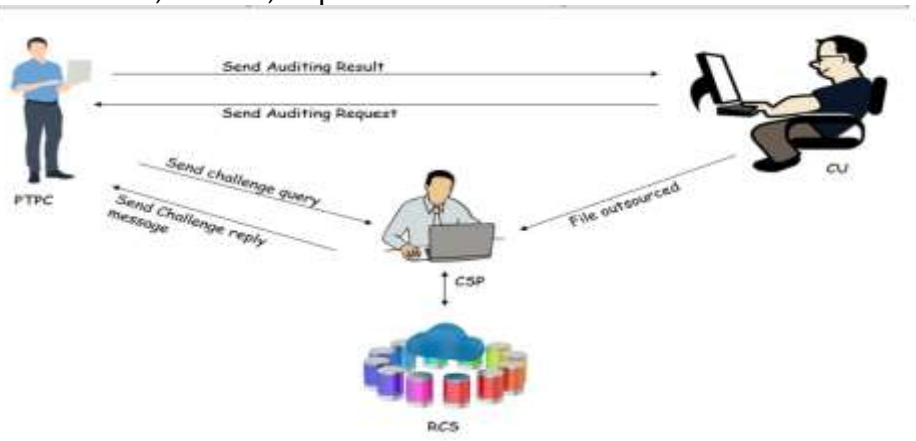


Figure 1. System Architecture

The suggested system model represented in Figure 1, has been provided in this section. The auditing of the suggested scheme with an overview of the proposed system model, a basic description, an example of cloud storage security model, design objectives, and dynamic operations on data blocks is covered in more detail in this part. The four elements that make up the unabridged suggested system are as follows: Cloud User (CU), Cloud Service Provider (CSP), Public Third Party Checker(PTPC), and Remote Cloud Server(RCS).

ALGORITHM:

Attention KeyGen() → Para(sk,vk): DO generates a group generator g1 from G1 using a bilinear map and two random numbers r1, r2 to produce a pair of public and private keys (DOpub,DOpri) where g1 ∈ G1 and r1, r2 ∈ Z∗ q.DO also prepares a file tag ω for file identification.CU selects a random parameter x from p at the start of the scheme. CU and CSP randomly select private parameters an as sk1 and b as sk2 respectively where a,b ∈ Zp.CUprepares a public parameter vk1 as ga andCSPpreparesapublic parameter vk2 as gb. Here, p denotes Z's prime order. Here, g is a G's generator and G is a p's group of prime order. CU also prepares ϕ from the combination of A, B, and Zas file identifiers. MsgEncrypt(x,Bi[Mj]) → Cipher Message(B′ = {B1[M′ j],B2[M′ j],...,Bn[M′ j]}): CU executes this phase because it generates an encrypted version for each data block. The random parameter and the data blocks are the phase's inputs, and its output is an encrypted set containing all of the data blocks' cipher versions.CU sends the information message

Algorithm 1 Algorithm for Stub Signature Generation Method

Input: $vk_1, vk_2, \tau, \phi, B', H(B[M'_{ij}]$

Output:Stub Signature $= \sigma, \kappa, t$ out

Initialisation :

1: After verifying the $chal\_pro$ message, the CSP generates $chal\_reply$ message to the CU.
2: **for** $i = 1$ to t **do**
3: **for** $j = 1$ to w **do**
4: Calculates $\sigma = H[\sum_{i=1}^{t} \sum_{j=1}^{w} B_i[M'_j]||vk_1||vk_2)].a^t$ and κ=$(b.H(\sum_{i=1}^{t} \sum_{j=1}^{w} B_i(M'_j) + \sigma.a) + t$.
5: **end for**
6: **end for**

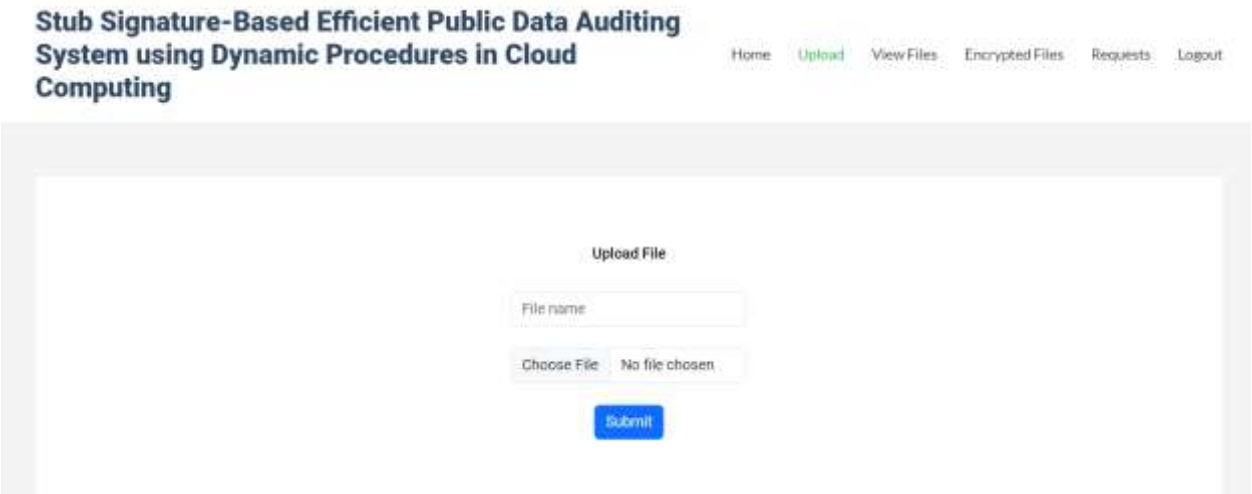
Figure 2. Model Flow Diagram

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 9, September : 2024

V. RESULTS

Home Page:

Upload Data:



View Data:

Send request:

Check attack:

View attack or Normal:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 9, September : 2024

View requested data:

Download Data:

VI. CONCLUSION

Dynamic operations are accomplished to protect the integrity of outsourced data on shared cloud storage by auditing correctness at the block level. Consistency of outsourced data for CU at RCS is ensured through the use of a partial signature and original data encryption technology using random number generation. It aids in thwarting replace and forgeability attacks. Additionally, PTPC is capable of detecting block corruption during auditing and notifying CU. Additionally, this user-friendly auditing architecture protects the privacy of CU's data from all entities, including CSP and PTPC, while conducting the audit.

.

VII. FUTURE SCOPE

Enhanced Scalability: Developing methods to further scale auditing systems to handle larger datasets and more frequent data modifications without compromising performance.

Adaptive Algorithms: Creating adaptive algorithms that can dynamically adjust their auditing strategies based on data usage patterns and system load.

Integration with Emerging Technologies: Investigating the integration of emerging technologies such as quantum cryptography and blockchain to enhance the security and efficiency of data auditing systems.

User Privacy Enhancements: Implementing advanced privacy-preserving techniques to better protect user data during the auditing process, potentially through more sophisticated encryption methods.

Cross-Cloud Compatibility: Ensuring compatibility and seamless auditing across different cloud service providers and heterogeneous cloud environments.

Automated Auditing Tools: Developing automated tools and frameworks that can simplify the deployment and management of auditing systems for diverse cloud applications.

Performance Metrics: Establishing comprehensive performance metrics and benchmarks to evaluate the effectiveness of different auditing approaches under various operational scenarios.

Regulatory Compliance: Addressing regulatory and compliance challenges related to data auditing and ensuring that auditing systems adhere to evolving standards and legal requirements

VIII. REFERENCES

[1] P. Mell and T. Grance, “Draft nist working definition of cloud computing, || referenced on june. 3rd, 2009 online at http://csrc. nist. gov/groups,” SNS/cloud-computing/index. html, 2009.
[2] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet computing, vol. 16, no. 1, pp. 69–73, 2012.
[3] B. Shao, G. Bian, Y. Wang, S. Su, and C. Guo, “Dynamic data integrity auditing method supporting privacy protection in vehicular cloud environment,” IEEE Access, vol. 6, pp. 43785–43797, 2018.
[4] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, “Enabling identity based integrity auditing and data sharing with sensitive information hiding for secure cloud storage,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 331–346, 2018.
[5] S. Debnath, B. Bhuyan, and A. K. Saha, “Privacy preserved se cured outsourced cloud data access control scheme with efficient multi-authority attribute based signcryption,” Multiagent and Grid Systems, vol. 16, no. 4, pp. 409–432, 2020.
[6] Y. Zhang, C. Xu, H. Li, and X. Liang, “Cryptographic public verification of data integrity for cloud storage systems,” IEEE Cloud Computing, vol. 3, no. 5, pp. 44–52, 2016.

[7] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in International workshoponpublickeycryptography, pp. 277–290, Springer, 2004.
[8] H. Zhu, Y. Yuan, Y. Chen, Y. Zha, W. Xi, B. Jia, and Y. Xin, "A secure and efficient data integrity verification scheme for cloud-iot based on short signature," IEEE Access, vol. 7, pp. 90036–90044, 2019.
[9] P. Goswami, N. Faujdar, S. Debnath, A. K. Khan, and G. Singh, "Zss signature-based audit message verification process for cloud data integrity," IEEE Access, 2023.
[10] J. Shen, D. Liu, D. He, X. Huang, and Y. Xiang, "Algebraic signatures-based data integrity auditing for efficient data dynamics in cloud computing," IEEE Transactions on Sustainable Computing, vol. 5, no. 2, pp. 161–173, 2017.
[11] B. Dan, L. Ben, and S. Hovav, "Short signatures from the weil pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004.
[12] M. Tian, Y. Zhang, Y. Zhu, L. Wang, and Y. Xiang, "Divrs: Data integrity verification based on ring signature in cloud storage," Computers & Security, p. 103002, 2022.
[13] C. Wang, S. S. 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, 2011.
[14] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu, and J. Ma, "Data integrity auditing without private key storage for secure cloud storage," IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1408–1421, 2019.
[15] M. Thangavel and P. Varalakshmi, "Enabling ternary hash tree based integrity verification for secure cloud data storage," IEEE Transactions on Knowledge and Data Engineering, vol. 32, no. 12, pp. 2351–2362, 2019.
[16] A. Bender, J. Katz, and R. Morselli, "Ring signatures: Stronger definitions, and constructions without random oracles," in Theory of Cryptography Conference, pp. 60–79, Springer, 2006.