International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (online): 2347-5552, Volume-11, Issue-3, May 2023
https://doi.org/10.55524/ijircst.2023.11.3.21
Article ID IJIRD-1259, Pages 105-108
www.ijircst.org

Secure Cloud Storage Privacy-Preserving In Public Auditing

Suresh Dara[1], K. Pujitha[2], I. Santhi[3], V. Saikavya[4], and K.V.S. Rushitha[5]

[1,2,3,4,5] Department of Computer Science & Engineering, PACE Institute of Technology and Sciences,
Ongole, Andhra Pradesh, India

Correspondence should be addressed to Suresh Dara; darasuresh@live.in

ABSTRACT- Cloud computing is a technology that is both efficient and cost-effective, thanks to its low maintenance requirements. This paper implemented a approach is used to share group resources across cloud users. Regrettably, as a result of the frequent differences in participation, the issue of sharing information in a multi-owner manner while also preserving privacy and information from a trusted cloud continues to be a challenging one. During the course we put into place a safe method of data sharing among multiple owners using the Diffe- Hellman algorithm that are cloud-based and applicable to rotating groups. By leveraging techniques like as group signature and dynamic broadcast encryption, any user of the cloud has the ability to anonymously share data with other users. In the meanwhile, the number of users whose access has been revoked does not have any impact on the storage overhead or encryption computation costs associated with our system. In addition, employ rigorous proofs to investigate the scheme's level of safety, and conduct tests to verify the scheme's usefulness.

KEYWORDS- Cloud computing, Encryption methods, Dynamic Groups Privacy, Shared Data, Revocation Data

I. INTRODUCTION

Cloud computing manages data and applications over the internet and remote servers. Cloud computing allows customers to utilize non-installed apps to access their private files from any internet-connected device. This technology boosts computer efficiency by centralizing storage, memory, bandwidth, and computation. Cloud computing is a complete ITaaS solution. Cloud computing adapts to resource distribution. Before the cloud, servers ran websites and programs. Cloud computing includes application, storage, and networking. Cloud storage offers cost savings, scalability, and lots of storage capacity. Thus, organizations and individuals use qualified cloud specialist cooperatives (CSP) for monitored and maintained distributed storage [1].

Cloud storage removes client control over files. However, CSP must store client data in the cloud without altering it. Checking downloaded data accuracy is easiest by doing it. Since verifying massive amounts of data is time-consuming, there are several methods. Distributed computing typically involves fine-grained, self-administration of Web-based services. An off-site third-party supplier fees the customer for utility computing and shares resources via web apps and online services.

Cloud computing offers on-demand self-service, widespread network access, resource pooling regardless of location, rapid resource elasticity, usage-based pricing, and risk transference [2]. Cloud computing is revolutionizing company IT. This paradigm shift involves cloud data outsourcing. Flexible, on-demand cloud data storage offers individuals and IT firms weight assistance for board capacity, all-encompassing information access with autonomous geographical areas, and capital savings on maintenance-related equipment, software, and faculty systems [3]. Cloud Computing brings new clouds and security risks to consumers' outsourced data, making it more enticing than ever. Most cloud services require sharing, internet storage, and database processing. Cloud computing simplifies resource sharing. This technology is simpler to maintain. Distributed computing includes Framework, Stage, and Programming as an Assistance. These three simplify complicated ideas. Foundation as a Help offers basic business processing and capabilities.

Third-party auditors inspect. Public and private auditability exist. Public auditability allows anybody, not just the client, to challenge the cloud server for data storage accuracy while preserving no private information, whereas private auditability can increase scheme efficiency. TPA will analyze client data to lighten the information proprietor's board. Cloud Computing can achieve economies of scale by checking the client's cloud-stored data without client input. The public audit report will help owners assess the risk of their cloud data services and help cloud service providers enhance their platforms. TPA will help the data owner protect his cloud data and make data management easier and faster [4].

II. LITERATURE SURVEY

The long-held concept of computing as a utility, cloud computing, has the potential to revolutionize a significant portion of the IT sector by increasing the appeal of software as a service and influencing the creation and acquisition of IT hardware. Innovative Internet service providers no longer need to invest significant sums of money in expensive gear or hire a huge staff to run it. They do not have to worry about under-provisioning a service that becomes extremely popular and losing out on prospective consumers and money, or over-provisioning one whose popularity exceeds their expectations and wasting expensive resources.

A. The use of the cloud for computing safe, scalable, and fine-grained data access control

This paper addresses this difficult open problem by defining and enforcing access policies based on data attributes and by allowing the data owner to delegate the majority of the computation tasks required for fine-grained data access control to untrusted cloud servers without disclosing the contents of the data. In doing so, the paper avoids revealing any of the sensitive information contained within the data. We are successful in achieving this goal as a result of our utilization of and innovative approach to the technologies of attribute-based encryption, proxy re-encryption, and lazy re-encryption. The accountability of user secret keys and the confidentiality of user access privileges are also major characteristics of the strategy that we have developed. Our proposed plot has been subjected to extensive testing, and the results show that it is not only highly effective but can also be demonstrated to be completely safe [5].

B. Scalable, secure file sharing on unreliable storage with plutus

This study employs Plutus, a new secure file system designed for untrusted servers. Plutus stores data encrypted and distributes keys decentralized. Clients handle cryptography and key management, therefore the server has little cryptographic overhead. Plutus's core file system security capabilities distinguish between read and write access to files, detect and prevent unwanted data modifications, and adjust user access privileges. Plutus is an encryption-on-disk solution where the client manages and distributes keys. As opposed to encrypt-on-wire systems, we can (1) protect against data leakage attacks on the physical device, such as by an untrusted administrator, a stolen laptop, or a compromised server; (2) allow users to set arbitrary key distribution (and file sharing) policies; and (3) improve server scalability because most cryptographic operations that require a lot of computation are done on end systems rather than centralized servers [6].

C. New proxy re-encryption techniques and their uses for distributed storage security

Both theoretical and practical aspects of proxy re-encryption were investigated in this particular research project. provide a variety of improved ways for re-encrypting data over bilinear maps and evaluate these new approaches in light of the characteristics and guarantees of existing encryption schemes. In addition to protecting the master secret key of the delegator, these pairing-based techniques offer protection against a colluding proxy and delegate, making them one of the most important new features. Providing the key server of a confidential distributed file system with proxy capabilities is one of the applications that has the most potential to benefit from proxy re-encryption. By doing so, it is not necessary to entirely trust the key server with all of the keys of the framework, and the amount of mysterious storage required for each client can also be decreased [7].

III. RELATED WORK

The ownership plot provided two PDP plans that were found to be secure and utilized homomorphic authenticators based on RSA. This maintains public confirmation because correspondence and calculations are less expensive. A legitimate security model of check of retrievability (POR) and a sentinel-based POR scheme with specific properties were first proposed by Juels and colleagues simultaneously. After that, Ren, et al. [8] worked on the POR conspiracy and proposed a second public inspection strategy based on the BLS signature that is secure in the irregular prophet model. The algorithms used are:

A. Diffe Hellman Algorithm

Distributed storage reviewing have recently been conducted. The key exchange protocol that enables two parties to communicate over a public channel is the primary topic of discussion in this algorithm:

Step 1: P, G => available public keys. P, G => available public keys.
Step 2: a is selected by private key b is selected as private key
Step 3: Eq. to generate key: Eq. to generate key:
$y=G^b$ modP $x=G^a$ modP
Step 4: After Key exchanges, user1 receives key y
After key exchanges user 2 receives key x
Step 5: User1 generates a secret key by using the received key y:
$k_a=y^a$ modP
User2 generates a secret key by using the received key x:
$k_b=x^b$ modP
Step 6: Algebraically, 5th step can be shown as follows:$k_a=k_b$

B. Dynamic encryption for broadcastin

It disseminates keying information that enables authorized users to decipher the content encryption key. Methods for efficiently transmitting information to a dynamically shifting group of privileged users who are authorized to receive the data are the focus of the concept of broadcast encryption. It is frequently helpful to consider it a renouncement plot, which tends to the situation where some subset of the clients is rejected from getting the data.

IV. EXISTING SYSTEM

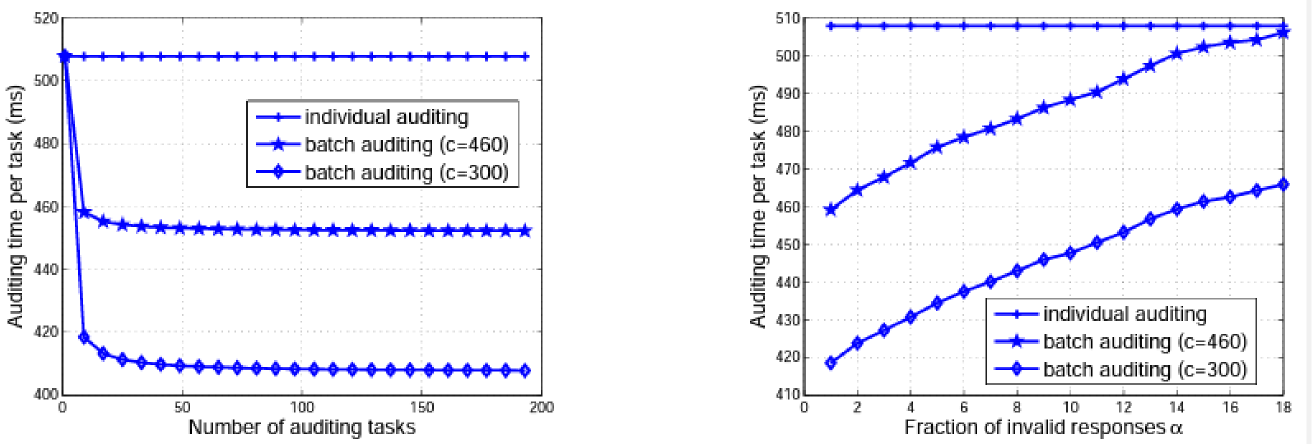
The cloud allows members of the group to completely avoid the troublesome local data storage and maintenance. Additionally, it entails a significant risk to the confidentiality of those stored files. First, one of the biggest obstacles to widespread cloud computing deployment is identity privacy. Traceability, which gives a group manager (like a company manager) access to a user's true identity, is also highly desired. Second, it is strongly suggested that each group member have full access to the cloud's services for multiple-owner data storage and sharing. The single-owner method, in which only the group manager can store and modify data in the cloud, is less adaptable in real-world applications. To put it all the more solidly, every client in the gathering approaches both read and adjust segments of the organization shared information document. The cloud servers managed by cloud providers may not be completely trusted by users, and the data files stored in the cloud may be private and sensitive, such as business plans. A fundamental safeguard for data privacy is to encrypt data files and then upload the encrypted data to the cloud. Tragically, making a cloud-based information sharing technique that is both compelling and secure is certainly not a simple errand.

V. PROPOSED SYSTEM

To solve the foregoing issues, dynamic groups need a secure way to share cloud-hosted data with various owners. This study made these main contributions. Multiple owners can securely share data with a proposal. The cloud, which cannot be trusted, allows group members to safely share data. The plan can help dynamic organizations. Recent accesses can decrypt data files posted before their involvement without contacting the data owners. An innovative revocation list lets users be revoked without changing their secret keys. The encryption and computational overhead are unaffected by revoked users. Secure and private access control and unique identifiers for each user allow group members to use the cloud resource anonymously. Investigate the plan's security and test it to prove its viability given the capacity and calculations. The suggested system's principal benefit is that Dynamic groups can receive information simultaneously and confidentially. Our proposed system includes a new revocation list policy. This list includes former members.

A. Results

In order to demonstrate that the implemented privacy-protecting public auditing techniques are not cumbersome, we will now evaluate the performance of these schemes. We will concentrate on both the efficiency and cost of the privacy-protecting protocol as well as the implemented methodology for database audits. The experiment is carried out using a Linux system equipped with an Intel Core 2 CPU operating at 1.86 GHz, 2048 megabytes of random access memory (RAM), and a 7200RPM Western Digital 250 gigabyte serial ATA drive equipped with an 8 megabyte buffer. The Pairing-Based Cryptography (PBC) library version 0.4.18 is utilized by our code.The MNT curve is the elliptic curve that was used in the experiment. It had a base field size of 159 bits and an embedding degree of 6.The security level has been set to chosentobe80bit, which indicates that vi = 80 and p = 160.The findings of every experiment are the mean of twenty separate tests.



(a)

(b)

Figure 1: (a) Comparison of the amount of time required for batch auditing versus individual auditing (b) Comparison of the amount of time required for auditing when performed individually versus in batches

The above Fig. 1 (a) describe a comparison of the amount of time required for batch auditing versus individual auditing. Particular auditing time is the overall amount of time spent auditing divided by the total number of tasks. When c equals 300, the straight curve for each auditing is not shown because doing so would make the discussion less clear. Fig. 1(b) shows, A comparison of the amount of time required for auditing when performed individually versus in batches, given that a fraction of 256 responses are invalid. The auditing time that is allocated each task is calculated by dividing the total auditing time by the number of tasks.

VI. CONCLUSION

Low maintenance makes cloud computing efficient and cost-effective. This article used to share group resources between cloud users. Unfortunately, due to frequent participation differences, sharing information in a multi-owner manner while preserving privacy and information from a trusted cloud remains difficult. Using Diffe Hellman algorithm, we created a cloud-based, rotating group-safe data sharing system. Cloud users can anonymously transfer data using group signature and dynamic broadcast encryption. Our system's storage overhead and encryption computation costs are unaffected by the number of revoked users. Test the scheme's utility and safety using rigorous proofs.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." arXiv preprint arXiv:1609.01107 (2016).

[2] Worku, Solomon Guadie, et al. "Secure and efficient privacy-preserving public auditing scheme for cloud storage." Computers & Electrical Engineering 40.5 (2014): 1703-1713.

[3] Tian, Hui, et al. "Privacy-preserving public auditing for secure data storage in fog-to-cloud computing." Journal of Network and Computer Applications 127 (2019): 59-69.

[4] Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." 2010 proceedings ieee infocom. Ieee, 2010.

[5] Yu, Shucheng, et al. "Achieving secure, scalable, and fine-grained data access control in cloud computing." 2010 Proceedings IEEE INFOCOM. Ieee, 2010.

[6] Kallahalla, Mahesh, et al. "Plutus: Scalable Secure File Sharing on Untrusted Storage." Fast. Vol. 3. 2003.

[7] Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage." ACM Transactions on Information and System Security (TISSEC) 9.1 (2006): 1-30.

[8] Ren, Yongjun, et al. "Attributed based provable data possession in public cloud storage." 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE, 2014.