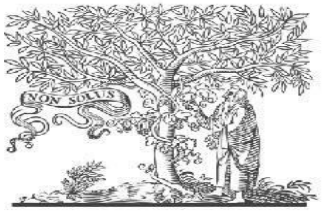
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 28 Aug 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 08

10.48047/IJIEMR/V12/ISSUE 08/45

Title **Zero-Knowledge Leakage Public Auditing Scheme in Secure Cloud Storage**

Volume 12, ISSUE 08, Pages: 316-320

Paper Authors **Anil P Jawalkar, Subba Reddy Borra**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Zero-Knowledge Leakage Public Auditing Scheme in Secure Cloud Storage

[1]Anil P Jawalkar, [2] Subba Reddy Borra,

[1]Assistant Professor, Department of IT, Malla Reddy Engineering College for Women, Maisammaguda, Dhulapally, Secunderabad, Kompally-500100 T.S, India.

[2]Professor& Hod, Department of IT,Malla Reddy Engineering College for Women, Maisammaguda, Dhulapally, Secunderabad, Kompally-500100 T.S, India.

Abstract— **By using cloud storage, users can remotely store their data and access high-class apps and services from a pool of configurable computing resources without having to worry about maintaining and managing local data storage. In order for consumers to engage a third party auditor (TPA) to guarantee the integrity of outsourced data and feel at ease, it is crucial to make public auditing of cloud storage possible. The auditing procedure should not create any new online burdens for users or vulnerabilities affecting user data privacy in order to launch a TPA properly and effectively. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.**

Index Terms—**Cloud Computing, Cloud Storage, Privacy, Privacy-Preserving**

I. INTRODUCTION

In all online computing settings, security is a crucial component for effective privacy measures, yet security by itself is insufficient. Customers and companies are prepared to

Only those who are confident that their data will be kept private and secure should use internet computers. Therefore, we must construct software, services, and processes with privacy in mind in order to provide clients with a trusted environment.

Cloud computing is the biggest buzz in the computer world these days. Cloud computing is everywhere. The locality of physical resources and devices being accessed are in general not known to the end user. It also provides services for users to build up, deploy and manage their applications „on the cloud", which involves virtualization of resources that maintains and manages by itself [1]. NIST definition of cloud computing:

Cloud storage was one of the earliest cloud services offered, and it is still a common solution. A networked online storage solution known as "cloud storage" places data in virtualized storage pools that are often hosted by outside parties. Data saved remotely can be momentarily cached on smartphones, desktop computers, and other Internet-connected devices thanks to cloud storage. Depending on the provider one chooses, security and pricing are the main concerns in this area. Despite the first success and recognition of the cloud computing model and the extensive availability of providers and tools, a number of challenges and risks are innate to this new model of computing.

Privacy issues in cloud storage

Numerous advantages come with cloud storage, including easy data access, scalability, and affordability. However, it

also brings up a number of privacy issues. Here are a few typical privacy concerns with cloud storage:It is crucial to take into account privacy hazards in the cloud context since they vary depending on the cloud situation. The following are some of the privacy-related topics that are presented in the publications [2][3]: data breaches, service provider access to data, location and jurisdiction of the data, third-party data sharing, cloud service provider, and lack of user control Lack of training and experience, restrictions on transborder data flow, complexity of regulatory compliance, litigation, uncertainty of the law, compelled disclosure to the government, lack of trustworthiness, data security and disclosure of breaches, data accessibility, location of data, and transfer

II. Related Work

In this plan, the data owner and the cloud storage provider work together to carry out the auditing process. Here is a high-level explanation of how such a plan functions:
Initial Phase:

A public key and a private key pair are created by the cloud storage service provider.
The data owner and the auditor are given access to the public key.
Phase of Key Generation:

For each data block that will be saved in the cloud, the data owner creates a secret key and calculates a tag. The tags are based on the secret key and the data content.
Using the secret key and a symmetric encryption technique, the data owner encrypts the data blocks.
Inspection Phase:

Using the cloud storage service provider's secret key, tags, and private key, the data owner creates an audit proof for each data block. Without disclosing any details about the encrypted data, the auditor can use the audit proof's information to confirm the data block's integrity.
The data owner delivers the cloud storage service provider the encrypted data, the audit proofs, and the tags.
Phase of Verification:

With the public key, the auditor can ask the cloud storage provider for a specific data block.
The cloud storage company gives the auditor the required data block, the associated audit evidence, and the tag.
The auditor verifies the integrity of the data block by using the received data block, the audit proof, the tag, and the public key. The verification process is designed in such a way that the auditor learns nothing about the actual content of the data block.

For the first time, Ateniese et al.'s "provable data possession" PDP) model for establishing ownership of data files on untrusted storages [9] takes public auditability into account. They advise randomly selecting a few blocks of the file while auditing outsourced data using the RSA-based homomorphic linear authenticators. The public auditability of their two suggested methods, however, makes the linear combination of sampled blocks visible to an outside auditor. Their protocol is not demonstrably privacy-preserving when used directly, which might cause user data to be disclosed to the external auditor.
A better PoR technique is created by Shacham and Waters [13] using BLS signatures [18] and proofs of security in the security model stated in [11]. They build publically verifiable homomorphic linear authenticators from provably secure BLS signatures, which is similar to the approach in [9]. A concise and publicly verifiable system is created using the elegant BLS design. Again, for the same reason as [9], their technique does not protect privacy.
In particular, due to the high I/O and network transmission costs, downloading all the data at once to verify its integrity is not a workable approach. Additionally, it is sometimes insufficient to just identify data corruption while viewing the data, as this does not guarantee users' access to proper data and may come too late to undo data loss or harm.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

III. System Design

It has been suggested in [7] to employ secret key recovery to enhance user privacy while enabling users to encrypt their information in cloud storage. To recover keys, a secret sharing algorithm is employed. User files are encrypted using AES-128 with a key length of 128 bits. Because only the user has complete knowledge of the encryption key, there is some confidence in the key recovery technique. Here, ZIP is the compression algorithm in use. The danger of losing the encryption key is reduced, and the user's privacy is safeguarded. But it makes users bear a heavy computational load. It worries about the speed of transformation. Users can't search for terms and there is dispersion, making it difficult to renew the user's key. Here, symmetric and asymmetric encryption in conjunction with the interaction protocol, Key derivation Algorithm, and Bloom Filter are employed. It has the ability to deal with encrypted data, lessen the effort placed on data owners in managing the data and storage area, and cut down on communication, compute, and storage overhead. It is effective, safe, and economical and can manage several keys. However, it does not provide cipher text-based computation and only enables owner-write-user-read. The work [9] discusses symmetric predicate encryption-based customizable privacy-preserving search features for cloud storage, such as revocable delegated search and un-decryptable delegated search. As a result, the Owner of the cloud may simply govern the data's lifetime and search capabilities, which is excellent for business applications that rely on delegation. However, elaborate access control and search rights cannot be supported. In a cloud computing architecture, a method employing the discretion algorithm [10] is explored that offers a security solution that calls for more than just user identification and a digital certificate. Here, the SP is more adaptable and secure to preserve people's privacy since it can use data without a key directly. However, using encryption has its limitations and calls for interoperability with diverse hosts as well as communication. The main problem in using encryption based technique is that it limits the data usage and puts into an additional burden. The access control mechanisms are available which will overcome the burden of the above overheads.

Access Control Mechanisms

The access control strategies that provide privacy were covered. A privacy-preserving access authenticated access control technique for safeguarding data in clouds has been presented in [11], which checks the user's authenticity without knowing the user's identity prior to storing information. The methods and procedures used to govern and manage access to resources, systems, or information inside a computer system or network are referred to as access control mechanisms.

Query Integrity/Keyword Searches

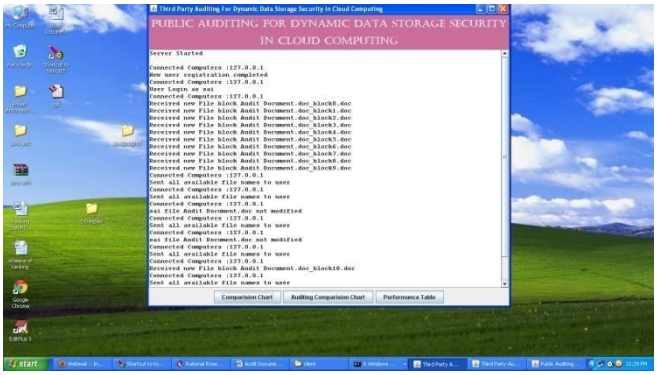
The idea of upholding the precision, dependability, and consistency of queries in a system or database is known as query integrity. Making certain that user or application-submitted queries are free of mistakes, manipulation, or illegal alterations is part of this process. There are methods for checking the privacy in clouds and documents that employ queries and keyword search schemes. These plans are discussed in [12]–[13]. In order to facilitate partial decryption and allow service providers to search the keywords on encrypted files, Qin Liuy et al. [12] suggested an effective privacy-preserving keyword search strategy for cloud computing. It employs an effective EPPKS (privacy-preserving keyword search system). It offers user data privacy protection, query privacy protection, and key word search capabilities for encrypted data. It is deemed effective, useful, provably secure, and semantically secure. However, computing with encrypted data proved difficult. Sayi et al. [13] employ a privacy-preserving method for outsourcing data in a cloud environment that makes use of fragmentation and a heuristic algorithm. Although it works well and efficiently, secrecy is not achieved.

Auditability Schemes

Auditing lowers client risk and encourages service providers to enhance their offerings [14]. When we look at

the various auditability schemes, we may divide auditability into two categories: private auditability and public auditability. Although private auditability schemes can achieve greater scheme efficiency, public auditability allows anyone—not just the client (data owner)—to interact with the cloud server to verify the accuracy of data storage without retaining any private information. Clients can then, without using their own computation resources, send along the evaluation of the service performance to an impartial third party auditor (TPA). As a result, Data Owner Auditing and Third Party Auditing are the two categories of auditing procedures. It is based on the development of an interactive PDP protocol to prevent both the disclosure of verified data and the dishonesty of the prover (both soundness and zero-knowledge properties). It defines the routine checks used to boost audit services' effectiveness. Here, a sampling-based technique to verification is used. The plan not only stops cloud storage providers from lying and forging documents, but it also stops the leaking of outsourced data throughout the verification process.

The TPA Contains the information about the users sessions as shown below :



IV. CONCLUSION

The customer should consider cloud data security while employing cloud services. To guarantee the security and integrity of data, a third party auditor might be engaged. An impartial third party, such as a third party auditor, can mediate disputes between the customer and the cloud service provider. Over the years, writers have put up a number of different strategies to offer a secure environment for cloud services. When hiring a third-party auditor, encryption and decryption methods are utilized to give users security. This study offers an abstract overview of various modern cloud data security techniques that include third party auditors. The majority of writers have put forth plans that entail utilizing an encryption method to encrypt the data and requiring a third party auditor to keep a message digest or encrypted duplicate of the same data that is kept with the service provider. Any disputes between the service provider and the client are handled by the third party. The cloud storage service provider cannot alter the data blocks or the audit proofs without the auditor seeing it, thanks to the zero-knowledge leaking public auditing system. The plan also ensures that the auditor will not learn anything about the information that has been kept, protecting the owner of the data's privacy.

REFERENCES

[1] D. Shrinivas, “Privacy-Preserving Public Auditing in Cloud Storage security”, International Journal of computer science nad Information Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011

[2] K Govinda, V. Gurunathprasad and H. sathishkumar, “Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA”, International Journal of Advanced science and Technical Research, vol 4,no. 2, ISSN: 2249-9954,4 August 2012

[3] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, “Implementation of EAP with RSA for Enhancing The Security of Cloud Computig”, International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012.

[4] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, “Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing”, International Journal of Computer science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229-4333(Print), March 2012

[5] Lingaraj Dhabale, Priti Pavale, “Providing Secured Data Storage by Privacy and Third Party Auditing In Cloud”, International Conference on Computing and Control Engineering, ISBN 978-1-2248-9, 12 & 13 April, 2012

[6] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J. ,“Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing”, Bioinfo Security Informatics, vol. 2, no. 2,pp. 49-52, ISSN. 2249-9423, 12 April 2012

[7] Dr. P. K. Deshmukh, Mrs. V. R. Desale, Prof. R. A. Deshmukh, "Investigation of TPA (Third Party Auditor Role) foe Cloud Data Security", International Journal of Scientific and Engineering Research, vo. 4,no. 2,ISSn 2229-5518, Feb 2013.

[8] Gayatri. R, "Privacy Preserving Third Party Auditing for Dynamic Data", International Journal of Communication and engineering, vol. 1, no. 1, issue: 03, March 2012

[9] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www. cloudsecurityalliance.org. [20] Juels, B. Kaliski. "Pors: proofs of retrievability for large files[C]", Proceedings of CCS 2007. Alexandria, VA, USA, 2007. 584-597.

[10] Honywei Li, Yuanshun Dai, Bo Yang. "Identity-Based Cryptography for Cloud Security".

[11] C. Hota, S. Sanka, M. Rajarajan, S. Nair, "Capabilitybased Cryptographic Data Access Control in Cloud Computing", in International Journal of Advanced Networking and Applications, Volume 01, Issue 01, 2011.

[12] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

[13] C. Wang, Q. Wang, K.Ren, and W.Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", in Proc. Of IEEE INFOCOM" 10,March 2010.

[14] Y. Zhu,Z. Hu,Gail-J Ahn, H. Hu,Stephen S. Yau, Fellow, IEEE, Ho G. An, and Shimin Chen,"Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds",in Proc.of IEEE SAC" 11 March 2011.

[15] Q. Wang, C. Wang, Kui Ren, W.Lou and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", in IEEE transaction on parallel and distributed system May 2011.

[16] Nandeesh.B.B, Ganesh Kumar R, Jitendranath Mungara"Secure and Dependable Cloud Services for TPA in Cloud Computing" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-3, August 2012.

[17] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage service honest", in Proc. Of HotOS"07, CA, USA: USENIX Association, 2007, pp.1-6.