ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

Secure Cloud storage Using TPA

[1] J.JeganAmarnath, [2]Aravinthsamy, [3]Ashwinkumar.T, [4]Balaprasanna.A.S, [5] Pranau.N
[1]Associate Professsor, [2][3][4] Student
[1][2][3][4] Department of Computer Science and Engineering, Sri Sairam Engineering College, Chennai,India.
[5] Associate Software Engineer, Torry Harris Solution

***Abstract* – Storing large amounts of data with cloud service providers (CSPs) raises concerns about data protection. Data integrity and privacy can be lost because of the physical movement of data from one place to another by the cloud administrator, malware, dishonest cloud providers, or other malicious users who might distort the data. Hence, user data must be verified at regular intervals. This verification of remote (cloud) data is performed by third-party auditors (TPAs). And we also focuses on cryptographic algorithms for ensuring no privacy constraints with the third party auditor who obtain and keep the copy of user original data in encrypted form.**

I. INTRODUCTION

Cloud storage is one of the service provided by Cloud computing in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). The user is concerned about the integrity of data stored in the cloud as the user's data can be attacked or modified by outside attacker. Therefore, a new concept called data auditing is introduced which check the integrity of data with the help of an entity called Third Party Auditor (TPA). The purpose of this work is to develop an auditing scheme which is secure, efficient to use and possess the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. Thus the new auditing scheme has been developed by considering all these requirements. It consist of three entities: data owner, TPA and cloud server. The data owner performs various operations such as splitting the file to blocks, encrypting them, generating a hash value for each, concatenating it and generating a signature on it. The TPA performs the main role of data integrity check. It performs activities like generating hash value for encrypted blocks received from cloud server, concatenating them and generates signature on it. It later compares both the signatures to verify whether the data stored on cloud is tampered or not. It verifies the integrity of data on demand of the users. The cloud server is used only to save the encrypted blocks of data.

II. PRESENTATION

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. 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.

For the registration of user with identityID the group manager randomly selects a number. Then the group Manager adds into the group user list which will be used in the traceability phase. After the registration, user obtains a private key which will be used for group signature generation and file decryption.

Homomorphic authenticatorsare unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we propose to uniquely integrate the Homomorphic authenticator with random mask technique. Supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. We can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics. The user download the particular file not download entire file.

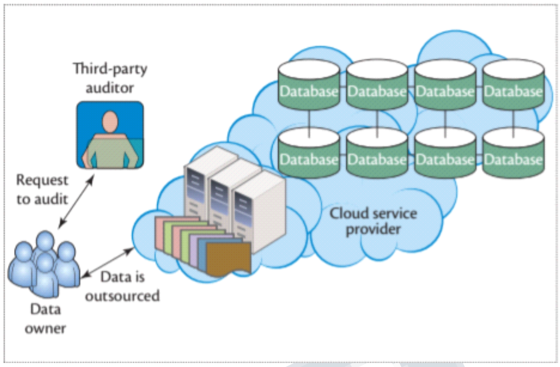
III. EXISTING SYSTEM

In the existing model, provides a secure third party auditor based storage utilising homomorphic token and distributed erasure coded data which allows users to audit the cloud storage with very light weight communication and computation cost .This existing system has the demerit of privacy preserving which is the major drawback in the cloud storage .So user cannot be satisfied with the integrity of the data stored and audited by the third party auditor . In order to curb this problem we proposed secure cloud storage third part auditing with privacy assurance.

IV. PROPOSED SYSTEM

It supports an external auditor to audit the user's outsourced data without learning knowledge on the data content .User supposed to give the request to third party auditor to start auditing of his data.AES algorithms is utilised to perform the encryption of user original data to create a copy of data in decrypted form to ensure the privacy. Third party auditor will check the user data on cloud , if any corruption occur TPA will regenerate the user data .The intimation relating the data corruption and regeneration will be sent to the user. The user can download his file anytime on his own with integrity.

DIAGRAM



CONCLUSION:

It supports an external auditor to audit the user's outsourced data without learning knowledge on the data content .User supposed to give the request to third party auditor to start auditing of his data.AES algorithms is utilised to perform the encryption of user original data to create a copy of data in decrypted form to ensure the privacy. Third party auditor will check the user data on cloud , if any corruption occur TPA will regenerate the user data .The intimation relating the data corruption and regeneration will be sent to the user. The user can download his file anytime on his own with integrity.

REFERANCE

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE 5th Int'l Conf. Cloud Computing (CLOUD 12), vol. 2, no.1, 2012, pp. 295–302.

[2] C. Wang et al., "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. 29th Conf. Information Communications (INFOCOM 10), 2010, pp. 525–533.

[3] C. Wang et al., "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, 2013, pp. 362–375.

[4] M. Bellare, R. Caneti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO 96), 1996, pp. 1–15.

[5] M. Zhou et al., "Security and Privacy in Cloud Computing: A Survey

[6] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.

A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 584–597.

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

[9] J. Li, J. Li, D. Xie, and Z. Cai, "Secure auditing and deduplicating data in cloud," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2386–2396, Aug 2016.

[10] J. Hur, D. Koo, Y. Shin, and K. Kang, "Secure data deduplication with dynamic ownership management in cloud storage," IEEE Trans.

[11] onKnowl. and Data Eng., vol. 28, no. 11, pp. 3113–3125, Nov. 2016.

[12] G. Ateniese, D. H. Chou, B. de Medeiros, and G. Tsudik, "Sanitizable signatures," in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 159–177.

[13] G. Ateniese and B. de Medeiros, "On the key exposure problem in chameleon hashes," in Security in Communication Networks. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 165–179.

[14] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K. K. R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," IEEE Transactions on Dependable and Secure Computing, 2017. [Online]. Available: DOI:10.1109/TDSC.2017.2662216