PRIVACY-PRESERVING EXTERNAL AUDITING FOR DATA STORAGE SECURITY IN CLOUD

Bincy Joseph[1], Akhila Thejaswi R[2]

[1]*MTech Student, Computer Science and Engineering, SCEM, Karnataka, India*
[2]*Assistant Prof, Information Science and Engineering, SCEM, Karnataka, India*

Abstract

Cloud Computing is an emerging technology which has been envisioned as the next generation information technology enterprise architecture. It manages application software and databases to centralised large data centres where the services may neglect to keep the files which are rarely accessed. This work studies the problem of ensuring the integrity of user data stored in the cloud server. Here I consider the task of allowing a Third Party Auditor (TPA), to check the integrity of data stored in the cloud on behalf of the cloud user. Without gaining knowledge on the data content stored in the cloud server.

Keywords: *Cloud Computing, Cloud Server, Integrity, TPA, Privacy-Preserving*

----------***----------

1. INTRODUCTION

Using cloud storage users can remotely store their data on to the cloud. By data outsourcing users can be relieved from the burden of local data storage. And cloud storage provides more space for the user files on demand. However, since users no longer have physical possession on the data stored makes the data integrity a difficult task. Moreover cloud server must be reliable and users must be able to use their data without worrying about its integrity.

In order to fully ensure the data integrity and make wise use of cloud resources, it is required to enable public auditing service for cloud data storage. So that users can resort to a third party auditor (TPA) to audit the outsourced user data on demand when it is needed without retrieving the local copy of the same. The TPA must periodically check the integrity of the files on behalf of the users, which provides much easier way to ensure user data storage correctness in the cloud. Moreover, it will help users to evaluate the risk of their availed cloud data services; the auditing results from TPA would also be beneficial for the cloud service providers to improve their cloud based service platform. And even serve truthfully. This scheme is privacy-preserving because the TPA will not learn any knowledge on the data stored in server.

2. DESIGN METHODOLOGY

A representative architecture for cloud data storage is shown in the above figure. There are three different entities and they are:

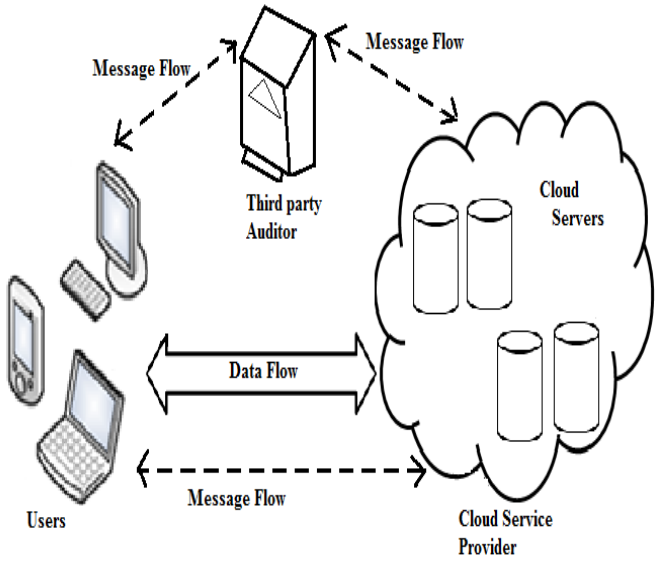

Fig 1: Cloud Data Storage Security Architecture

2.1 Client

An entity or a cloud user, who has large files to be stored in the cloud and relies on cloud for data maintenance and security, client, might be either individual customers or an organisation.

2.2 Third Party Auditor (TPA)

An entity or service, which periodically checks the integrity of data files stored in cloud server on behalf of the user.

2.3 Cloud Storage Server

An entity, which is managed by cloud service provider (CSP), has significant storage space and computation resource to maintain the client's data.

The working can be explained as: first the client needs to register onto the cloud server using TPA to avail the service. After registering the TPA will keep the user ID and the full details will be stored in the cloud server. If client wants to upload a file then a request is sent to TPA. The TPA will generate a public and a private key, sends the public key to the client and private key to the server. Now the client will encrypt the data files using the public key and send it to cloud server, at the same time it will generate the hash code of the data file and send that to TPA. When user wants to check the integrity of the data stored in the cloud server, the user will send a request to TPA, now the TPA will ask for the signature from server. The server will generate the signature of user data files upon request and send it to TPA. If the signature from the server matches that of the hash code saved in TPA then the data files are secure and integrity is verified. Here the important advantage is that, even the third party will not learn any knowledge on the data stored in cloud server. Hence it is privacy-preserving data integrity verification method.

3. CONCLUSIONS

One of the important concerns that need to be addressed is to assure the customer of the data integrity that is correctness of their data stored in cloud server. As the data is physically not accessible to the user the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. Here I have done initial requirements for verification of data integrity like client authentication, generating the keys and uploading client data to the cloud server database. TPA will check the integrity or correctness of the data which is stored by the client. Where, the TPA will not learn any knowledge on the data stored in the cloud server. And the client will have the option to increase or decrease the memory space required.

ACKNOWLEDGEMENTS

Here, I would like to take this opportunity to express my heartfelt gratitude to the supervisor for this project, Ms. Akhila Thejaswi R for her patience with me and down to earth personality which have given many pointers to guide me during my work in this paper. I hope that this paper can be as informational as possible to you.

REFERENCES

[1]. C. Wang, Q. S.M. Chow, Kui Ren and Qian Wang, "Ensuring data storage security in cloud computing," in December 2011.

[2]. Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2011.

[3]. Wang, K. Ren, W. Lou, and J. Li, "Towards publicly auditable secure cloud data storage services," IEEE Network Magazine, vol. 24, no. 4, pp. 19–24, 2010.

[4]. M. A. Shah, R. Swaminathan, and M. Baker, "Privacypreserving audit and extraction of digital contents" Cryptology ePrint Archive, Report 2008/186, 2008.

[5]. J. Kincaid, "MediaMax/TheLinkup Closes Its Doors,"at http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/, July 2008.

[6]. M. Naor and G. N. Rothblum, "The complexity of online memory checking," in Proc. of FOCS'05, Pittsburgh, PA, USA, 2005, pp. 573–584.

[7]. E.-C. Chang and J. Xu, "Remote integrity check with dishonest storage server," in Proc. of ESORICS'08 Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.

[8]. M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[9]. A. Oprea, M. K. Reiter, and K. Yang, "Space-efficient block storage integrity," in Proc. of NDSS'05, San Diego, CA, USA, 2005.

[10]. T. Schwarz and E. L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage," in Proc. of ICDCS'06, Lisboa, Portugal, 2006, pp. 12–12.

BIOGRAPHIE

M Tech Student in Sahyadri College of Engineering and Management