2015

Electronic International Interdisciplinary Research Journal

(EIIRJ)

REVIEWED INTERNATIONAL JOURNAL

VOL IV Issues I

Chief-Editor

Mr.Ubale Amol Baban

www.aarhat.com

25/2/2015

ISSN 2277-8721

Electronic International Interdisciplinary Research Journal (EIIRJ)
Bi-monthly Reviewed Journal Jan-Feb 2015

THIRD PARTY AUDITING (TPA) FOR DATA STORAGE SECURITY OF OUTSOURCED DATA IN CLOUD WITH DYNAMIC AUDITING

Research paper in Computer Engineering

V. V. Jog[1], Deepali Pande[2]

[1]Profeessor, Computer Engineering Department, SKNCOE, Pune, India

[2]M. E. Computer Engineering Department, SKNCOE, Pune, India

Abstract

Cloud Computing is current trend which is considered as the next generation information technology enterprise architecture. It manages all form of software starting from databases to the application software. Cloud Storage, can remotely store data and provide 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. This work helps us to have a third party auditor with integrity algorithm to protect the cloud. This enables public audit ability for cloud storage, a third party auditor (TPA) to check the integrity of outsourced data and relaxed that data is secure. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend this to enable the TPA to perform audits for no of users simultaneously with efficiency. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Key terms: *Integrity, TPA, metadata, public audit ability*

Introduction

Cloud storage allows user to store there data remotely on to the cloud. It relives the burden of data storage. It works like a on demand storage for user files. [1] But as users do not

have physical possession on the data stored makes the data integrity a difficult task. But the 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[2]. 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.

Problem Statement

The System and its Threat Model

We consider a cloud data storage service involving three different entities, as illustrated in Fig. 1: Data Owner(DO) module , who has large amount of data files to be stored in the cloud; Cloud Storage Server(CSS), which is managed by the cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP thereafter); the third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request. Authorized Application (AA) AA is the interface between application user and cloud storage. DO will assign permission rights to application user to AA; AA will in turn handle customers. AA can update/delete/insert the file. AA will compute verification information (tag & IHT) of modified file. Application user/Customer(AU) AU can be thin Client.(Laptop/mobile device/PDA).AU cannot upload the file. AU can view/delete/update file; if permission is given to that customer by DO.

The Existing Method

Cloud allows storing large amount of data in a single location in centralized format. The main problem is of security of sensitive data and data integrity. While introducing an effective

third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

Drawbacks

1. The management of the data and services may not be fully trustworthy.
2. Total security of data is a problem.
3. The main is security of data users might not be comfortable handling over their data to a third party.

The Proposed System

In this System , Client will have commercial tie-up with Third Party Auditor (TPA). And Client may have commercial tie- up with Cloud storage. Client will register on Cloud server as well as TPA. Cloud service provider will perform AAA .The client can upload read and modify file from the cloud server. TPA will store metadata of a file stored by client on cloud storage and communicated with the cloud storage on behalf of client. It perform the task of verification and have a logic of proof of retrievability (POR). TPA will inform client regarding data integrity of his file.(Security Message). TPA will periodically send verification messages to cloud storage for POR. (Security Message). This paper also suggests the security techniques for outsourced data through dynamic audit source and using third party auditor.

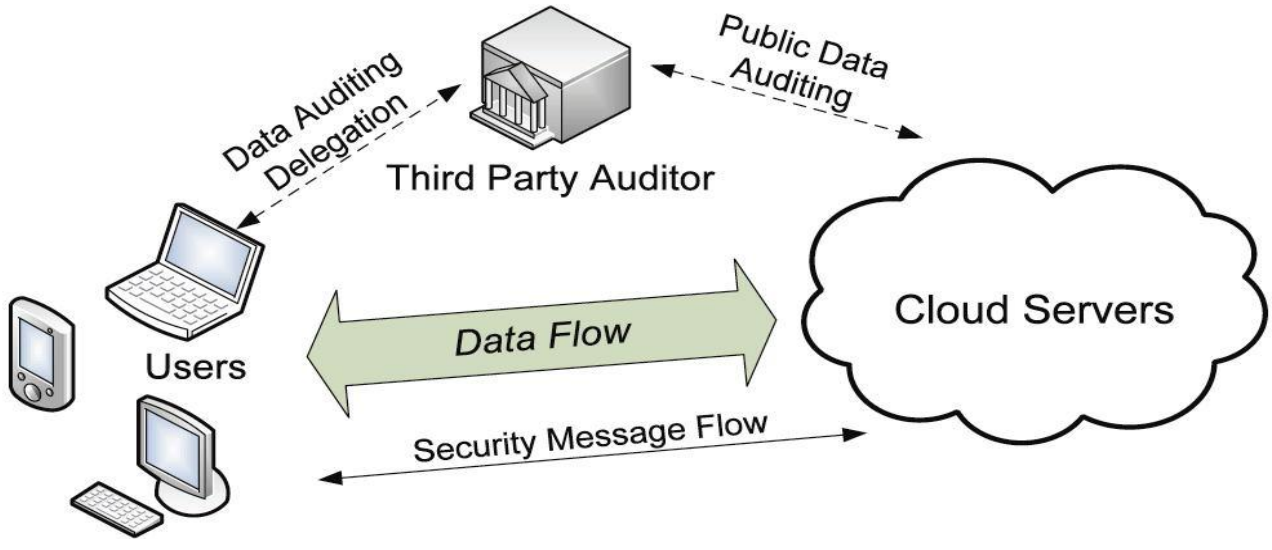

Fig 1: The architecture of cloud data storage service.

In proposed system TPA encrypts the file using AES algorithm and stores secret key in its database. TPA generates metadata of the file in order to achieve data integrity. To generate metadata following steps are carried out:

1) Split encrypted file into N blocks each of size M.
2) Select random L bytes as metadata from each block.
3) Apply encoding on each L bytes by using proposed chaotic based low overhead encoding.
4) Generate metadata of size N*L bytes and append to file.
5) TPA stores start and end position of L bytes of each block.
6) TPA also stores encoding key.

After this TPA transfers encrypted file along with encoded metadata to CSS and deletes encrypted file and metadata.

Data Verification Algorithm

TPA does periodic sampling audit of CSS.

1) TPA queries random block's random L bytes(start and end position is stored at TPA database) and corresponding metadata to CSS.
2) CSS will give corresponding response to TPA.
3) TPA decodes metadata by using decoding key and compares random L bytes with corresponding metadata.
4) If math found data is not tampered by adversary.
5) If match is not found it means that data is modified by adversary and TPA will inform corrosponding user by sending e mail.
6) If data and metadata is equal then file is correct .Otherwise file is modified.
7) Encoding is applied on metadata by proposed Low order hybrid chaotic sequence.

Advantages:

- Reduce the computational and storage overhead of the client as well as to minimize the computational overhead of the cloud storage server
- Minimized the size of the proof of data integrity so as to reduce the network bandwidth consumption
- Storage at the client is very much minimal compared to all other schemes

Ensuring Data Security With Encryption

Encryption is one of the best way to ensure confidentiality and security of data in cloud. Almost all cloud service providers support encryption for data storage, but few offer support for data at rest. In addition to this we are also using Low order hybrid chaotic sequence for encoding metadata. To protect a users confidential data in the cloud, encryption is a powerful tool that can be used effectively. Only user can confidently utilize cloud providers knowing that their confidential data is protected by encryption.

Conclusion and Future Work

- Computation complexity of proposed algorithm is less than existing hash based algorithms.
- Communication bandwidth required for auditing by TPA is less as compare to existing method.
- Metadata size of the proposed method is larger. But it is more secure. Because proposed Low order hybrid chaotic sequence tag generation method is applied. Mathematical analysis proves that proposed method is very difficult to crack.
- Proposed tag generation algorithm is having low overhead than existing hash based algorithms.

Future Work:

This work can be extended to reduce the size of metadata stored at CSS.

Bibligraphy

P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2009. http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

G.Ateniese et al., ―Provable Data Possession at Untrusted Stores, Proc. ACM CCS _07, Oct. 2007, pp. 598–609.

M. Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law," Technical Report HPL-2009-99, HP Lab., 2009.

M. Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law," Technical Report HPL-2009-99, HP Lab., 2009.

A.A. Yavuz and P. Ning, "BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems," Proc. Ann.Computer Security Applications Conf. (ACSAC), pp. 219-228, 2009.

H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.- H.Wang,H.Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang, "A Study of User-Friendly Hash Comparison Schemes," Proc. Ann. Computer Security pplications Conf. (ACSAC), pp. 105-114,2009.

A.R. Yumerefendi and J.S. Chase, "Strong Accountability for Network Storage," Proc. Sixth USENIX Conf. File and Storage Technologies (FAST), pp. 77-92, 2007.

Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 756-758, 2010.

Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Communications Security (CCS '07), pp. 584-597, 2007.

G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

M. Xie, H. Wang, J. Yin, and X. Meng, "Integrity Auditing of Outsourced Data," Proc. 33rd Int'l Conf. Very Large Databases(VLDB), pp. 782-793, 2007.

Yan Zhu, Gail-Joon Ahn, Hongxin Hu, S. S. Yau, H. G. An, Chang-Jun Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227-238, April-June 2013, doi:10.1109/TSC.2011.51