Public Auditing: Security in Cloud Storage

Mr. Navanath P. Jadhav
M. Tech Student
Department of Computer Science Engineering
MLRIT, Hyderabad

Mrs. L. Laxmi
Assistant Professor
Department of Computer Science Engineering
MLRIT, Hyderabad

Abstract

Cloud computing has been envisioned as the next- generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history like on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. The Cloud server allows user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage. User can upload their data on cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on a cloud. The major problem of cloud data storage is security. 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.

Keywords: Cloud Computing, Public Auditing, Security, Data Integrity, Cloud Server.

I. INTRODUCTION

The cloud computing has rapidly grown in recent years due to the advantages of greater flexibility and availability of computing resources at lower cost. Security and privacy, however, are a concern for agencies and organizations considering migrating applications to public cloud computing environments. 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 resource. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud. The Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data.

Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for the cloud users [2]. Moreover, the overhead of using cloud storage should be minimized as much as possible, such that a user does not need to perform too many operations to use the data. In particular, users may not want to go through the complexity in verifying the data integrity. Besides, there may be more than one user accesses the same cloud storage, say in an enterprise setting. For easier management, it is desirable that cloud only entertains verification request from a single designated party. To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third-party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Moreover, in addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud-based service platform, and even serve for independent arbitration purposes [3]. In a word, enabling public auditing services will play an important role for this nascent cloud economy to become fully established, where users will need ways to assess risk and gain trust in the cloud.

II. SYSTEM AND THREAT MODEL

The cloud data storage service contains 3 different entities as cloud user, Third party auditor & cloud server . Cloud user is a person who stores large amount of data or files on a cloud server. Cloud server is a place where we are storing cloud data and that data will

be managed by the cloud service provider. Third party auditors will do the auditing on users request for storage correctness and integrity of data.

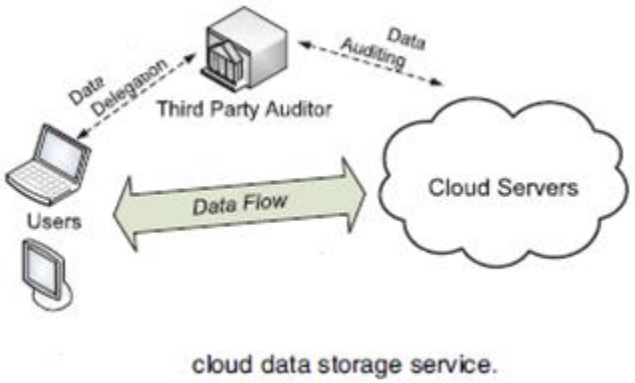

Fig. 1: Architecture of Cloud Data Storage

The major benefits of storing data on a cloud is the relief of burden for storage management, universal data access with location independent & avoidance of capital expenditure on hardware, software & personal maintenance. We assume the data integrity threats toward users' data can come from both internal and external attacks at CS. These may include: software bugs, hardware failures, bugs in the network path, economically motivated hackers, malicious or accidental management errors, etc. Besides, CS can be self-interested. For their own benefits, such as to maintain reputation, CS might even decide to hide these data corruption incidents to users. Using third-party auditing service provides a cost-effective method for users to gain trust in cloud. We assume the TPA, who is in the business of auditing, is reliable and independent. However, it may harm the user if the TPA could learn the outsourced data after the audit.

III. LITERATURE SURVEY

A. MAC Based Solution:

It is used to authenticate the data. In this, user upload data blocks and MAC to CS provide its secret key SK to TPA. The TPA will randomly retrieve data blocks & MAC uses secret key to check correctness of stored data on the cloud.

B. HLA Based Solution:

HLAs, like MACs, are also some unforgeable verification metadata that authenticate the integrity of a data block. The difference is that HLAs can be aggregated. It is possible to compute an aggregated HLA which authenticates a linear combination of the individual data blocks.

C. Using Automatic Protocol Blocker:

Balkrishna proposed efficient reed Solomon technique for error correction which check data storage correctness[4] Kiran Kumar proposed automatic protocol blocker to avoid unauthorized access [5]. When an unauthorized user access user data, a small application runs which monitors user inputs, It matches the user inpu t, if it is matched then it allow user to access the data otherwise it will block protocol automatically.

D. Using EAP :

S. Marium proposed use of Extensible authentication protocol (EAP) through three ways hand shake with RSA. They proposed identity based signature for hierarchical architecture. They provide an authentication protocol for cloud computing (APCC) [6]. APCC is more lightweight and efficient as compared to SSL authentication protocol. In this, Challenge –handshake authentication protocol (CHAP) is used for authentication. When make request for any data or any service on the cloud. The Service provider authenticator (SPA) sends the first request for client identity.

IV. PROPOSED SCHEME

The proposed system specifies that user can access the data on a cloud as if the local one without worrying about the integrity of the data. Hence, TPA is used to check the integrity of data. It supports privacy preserving public auditing. It checks the integrity of the data, storage correctness. It also supports data dynamics & batch auditing.

A. Design Goals :

1) Public auditability: Allows third party auditor to check data correctness without accessing local data.
2) Storage Correctness: The data stored on a cloud is as it. No data modification is done.
3) Privacy preserving: TPA can't read the users' data during the auditing phase.
4) Batch Auditing: Multiple users auditing request is handled simultaneously.
5) Light Weight: Less communication and computation overhead during the auditing phase.

B. Framework :

A public auditing scheme consists of four algorithms which are as follows.
1) KeyGen: a key generation algorithm that is run by the user to setup the scheme.
2) SigGen: used by the user to generate verification metadata, which may consist of digital signatures.
3) GenProof: run by the cloud server to generate a proof of data storage correctness,.
4)VerifyProof : run by the TPA to audit the proof.
Running a public auditing system consists of two phases,

1)Setup: The user initializes the public and secret parameters of the system by executing KeyGen, and pre-processes the data file F by using SigGen to generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server, and deletes its local copy. As part of preprocessing, the user may alter the data file F by expanding it or including additional metadata to be stored at server.

2) Audit: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive a response message by executing GenProof using F and its verification metadata as inputs. The TPA then verifies the response via VerifyProof

C. Privacy-preserving Public Auditing Schema:

Our design makes use of a public key-based HLA, to equip the auditing protocol with public auditability.

Setup Phase: The cloud user runs KeyGen to generate the public and secret parameters. Specifically, the user chooses a random signing key pair (spk,ssk). The secret parameter is sk and the public parameters are pk. The last part of SigGen is for ensuring the integrity of the unique file identifier name. One simple way to do this is to compute t = name||SSigssk(name) as the file tag for F, where SSigssk(name) is the signature on name under the private key ssk. For simplicity, we assume the TPA knows the number of blocks n. The user then sends F along with the verification metadata to the server and deletes them from local storage.

Audit Phase: The TPA first retrieves the file tag t. With respect to the mechanism we describe in the Setup phase, the TPA verifies the signature SSigssk(name) via spk, and quits by emitting FALSE if the verification fails. Otherwise, the TPA recovers name.
It is easy to see that our protocol achieves public auditability. There is no secret keying material or states for the TPA to keep or maintain between audits, and the auditing protocol does not pose any potential online burden on users. This approach ensures the privacy of user data content during the auditing process by employing a random masking.

D. Support for Batch Auditing & Data dynamics:

It also supports batch auditing through which efficiency is improved. It allows TPA to perform multiple auditing task simultaneously and it reduces communication and computation cost. Through this scheme, we can identify invalid response. It uses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve batch auditing. System performance will be faster. The individual auditing of these tasks for the TPA can be tedious and very inefficient. Given K auditing delegations on K distinct data files from K different users, it is more advantageous for the TPA to batch these multiple tasks together and audit at one time. Keeping this natural demand in mind, we slightly modify the protocol in a single user case, and achieves the aggregation of K verification equations (for K auditing tasks) into a single one. As a result, a secure batch auditing protocol for simultaneous auditing of multiple tasks is obtained.
Setup phase: Basically, the users just perform Setup independently. Suppose there are K users in the system, and each user k has a data file Fk (mk;1;...;mk) to be outsourced to the cloud server, where k ={1...k}. For simplicity, we assume each file Fk has the same number of n blocks. For a particular user k, denote his/her secret key as (xk,sskk).

Audit phase: TPA first retrieves and verifies file tag tk for each user k for later auditing. If the verification fails, TPA quits by emitting FALSE. Otherwise, TPA recovers name k and sends the audit challenge to the server for auditing data files of all K users.
It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation of insertion, deletion and modification. It uses Merkle Hash Tree (MHT) which works only on encrypted data. It [8] uses MHT for block tag authentication. In data dynamics support is achieved by replacing the index information i with mi in the computation of block authenticators and using the classic data structure— Merkle hash tree (MHT) [9] for the underlying block sequence enforcement.

V. PROPOSED WORK

A. Privacy-preserving Public Auditing :

1) *Cloud Server:*

As per above privacy preserving public auditing schema, we will create cloud server,TPA & cloud clients.In our proposed system first server runs & it waits for client requsts.It also having information of user & files name lists.CS gives response to TPA challenge message by executing GenProof module.

2) *Cloud TPConnector(TPA):*

It is second component in our proposed system.TPA allows to clients to upload file on to the cloud server,after allowing, verification metadata(Key,Sign) is generated by using RSA & SHA .So this verfication metadata along with file is stored on to the CS.It also give response to CS vai VerfiyProof module.

3) *Cloud Requestor(Client):*

Clients take permission from TPA for upload the file on to the CS.For performing operation like updation,deletion data on file which is present on CS firstly verfiy from the TPA.

B. Batch Auditing & Data dynamics:

For batch auditing in our system first CS & TPA ready. Clients must be logged in, then different operations of different clients are executed simultaneously.

Clients also update their data dynamicaly.for data updation we first verify from the TPA,then it send to server. If verification data matches the only give the permission for data update. Same for deletion process. Also we delete blocks of data by using Merkle hash tree.

VI. CONCLUSION

We propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphic non-linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data security. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloud- computing/index.html, June 2009.
[2] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance. org, 2009.
[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Comput- ing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.
[4] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan. S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012
[5] 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
[6] 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
[7] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," http:// www.techcrunch.com/2008/07/10/mediamaxthelinkup-closes- its-doors/, July 2008
[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.
[9] R.C. Merkle, "Protocols for Public Key Cryptosystems," Proc. IEEE Symp. Security and Privacy, 1980.