ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Third Party Auditing with Time based Secret Key in Cloud Storage

Chandaka Asha
M.Tech,
Dept of CSE, (CN&IS Branch),
MVGR College of Engineering,
A.P, Vizianagaram, India.

B.Aruna Kumari
Associate Professor,
Dept of CSE,
MVGR College of Engineering,
A.P, Vizianagaram, India.

ABSTRACT:
Cloud Computing is one of the practice of using a network of remote servers hosted on internet to store, access, retrive data from remote machines not from local machines. As the cloud is used mainly for storing the data on remote servers it has various services like PaaS, IaaS, SaaS and so on. Here each and every service has its own advantages and limitations due to its hardware and software usage. In this cloud the users who are placing the data in the cloud are known as Data Owners and the user who is accessing that file is known as Data users. As the data is been placed on remote system not on our local machines data integrity plays a very important role for both data owners and data users, these two users need to have audit for the cloud data without retrieving the entire data. As the cloud is deployed both public and private use ,the two users need to have a secure audit in order to view the integrity of their stored data without retrieving the entire data to the un-authorized users.

Till now there are many audit mechanisms in the cloud servers which was not at all achieved total data integrity as they have failed in some instances. So in this paper we formalize the definition and the security model of auditing protocol with key-exposure resilience and propose such a protocol. In our design, we employ the binary tree structure and the preorder traversal technique to update the secret keys for the client. We also develop a novel authenticator construction to support the forward security and the property of block less verifiability.

Keywords:
Data storage, cloud storage auditing protocols, cloud computation, key exposure resistance.

1 INTRODUCTION:
Cloud computing can be thought of as anything that involves delivering hosted services over the Internet. cloud computing is a promising computing model that enables convenient and on-demand network access to a shared pool of configurable computing resources. The first offered cloud service is moving data into the cloud: data owner slet cloud service providers host their data on cloud servers and data consumers can access the data from the cloud servers. This new paradigm of data storage service also introduces new security challenges [1], because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to make sure that the data is correctly hosted in theCloud.

2 CLOUD DATA INTEGRITY:
Data integrity[2] means data should be correctly stored on the cloud server without any modification and if any violations i.e. if the data is get lost, altered or compromised can be detected. It must remain in the same state. But the integrity of data is at risk in cloud server. So to maintain the data integrity and to minimize the storage risk it is important to take assistance of a Third party auditor (TPA) who checks the data integrity for the cloud user and helps the user in minimizing his risk.

Third Party Auditor:
The Third party auditor is a kind of inspector. The Third Party Auditor who has resources and checking the integrity that is difficult for users. The auditors can understand the threats and they know best practices.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The released audit report helps the user to evaluate the risk of their services. It also helps the cloud service provider to improving their cloud platform.

Cloud Data Storage Model:

There are three different network entities in cloud system which is users, cloud service provider and third party auditor.The cloud data storage system model shown in fig.1.

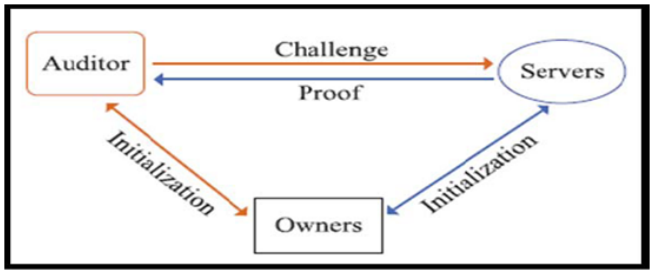

Fig.1 Cloud Data Storage System Model

1. Users:These are active participants. They have data to be stored in the cloud and rely on the cloud for data maintenance and computation.
2. Cloud service provider (CSP):It has significant storage space and computation resource to store and maintain the user data.it provides all his services in pay per use manner.
3. Third party auditor (TPA):It has more capabilities than the user and checks the integrity of data for the user and his audit reports helps the users to evaluating the risk.

Different Schemes used for TPA:

1. MAC (Message Authentication Code) Based solutions:

There are two types of MAC based solution the first solution does not ensure privacy preserving the second one suffers from auditor statefulness and other demerits. In first solution user first divides the files into blocks and calculate the MAC for each block. Users transfer the file blocks and the MACs to the cloud service provider and share the secret key to Third party auditor. TPA demands for a random no. of blocks and theirs MACs from cloud service provider. Then TPA uses the secret key to verify the correctness of stored data on the cloud server.

2. HLA (Homomorphic Linear Athentication) based solution:

To support public auditability without retrieving the data blocks the HLA based solution is used. Like the MACs, HLAs are also some enforceable verification metadata that is used to check the integrity of data. The only 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. It allows efficient auditing and consumes constant bandwidth. But this solution may reveal user data information to TPA and violates privacy preserving.

3. Privacy-Preserving Public Auditing Scheme:

To achieve privacy preserving public auditing, public key based homomorphic linear authentication with random masking is used. TPA checks the integrity without demanding the actual copy of data. The linear combination of sampled blocks in the server's response is masked with randomness generated by the server. With random masking, the TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the user's data content, no matter how many linear combinations of the same set of file blocks can be collected.

4. Digital signatures based solution:

An Authorproposed digital signature method to protect the privacy and integrity of data. It uses the RSA algorithm for encryption and decryption which follows the process of digital signatures for message authentication.

3. AUDITING PROTOCOL WITH KEY-EXPOSURE RESISTANCE

The system consists the four modules they are Client, TPA (Third Party Auditor)[3],Cloud, Key Exposure

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Resistance. And the system architecture is shown in fig.2.

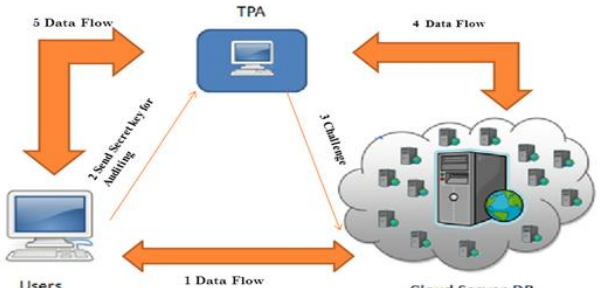

Fig 2. System Architecture

Client:

The client produces files and uploads these files along with corresponding authenticators to the cloud.The client can periodically audit whether his files in cloud are correct. The client will update his secret keys for cloud storage auditing in the end of each time period, but the public key is always unchanged.

TPA (Third Party Auditor):

In order to reduce the computational burden of the client, a third-party auditor (TPA) is introduced to help the client to periodically check the integrity of the data in cloud. However, it is possible for the TPA to get the client's data after it executes the auditing protocol multiple times. Auditing protocols[4] are designed to ensure the privacy of the client's data in cloud. Another aspect having been addressed in cloud storage auditing is how to support data dynamic[5] operations.

Cloud:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

Key Exposure Resistance:

The client needs to produce a new pair of public key and secret key and regenerate the authenticators for the client's data previously stored in cloud. There is a one-time public key sharing for each file and a Time Stamp based secret key Generation[6]. For each instance the timestamp based key exposure will be vary according to the current time stamp.

Algorithm:

An auditing protocol with key-exposure resilience is composed by five algorithms they are Sys Setup, Key Update, Auth Gen, Proof Gen, Proof Verify.

1 Sys Setup (1k, T) →(PK, SK0): This algorithm run by client. Algorithm which takes a input as security parameter *k* and the total number of time periods T and generates a public key PK and the initial client's secret key SK0.

2 Key Update (PK, j,SKj) → (SKj+1) : This algorithm is run by the client. Algorithm which takes a input as the public key PK, the current period jand aclient's secret key SKj and generates a new secret keySKj+1 for the next period j + 1.

3AuthGen(PK, j, SKj , F) → (Φ): Thisalgorithm is also run by the client. which takes a input as the public key PK, the current period j,a client's secret key SKjand a file F and generatesthe set of authenticators Φ for Fin time period j.

4 Proof Gen(PK, j,Chal, F,Φ) → (P) : This algorithm is run by the cloud. which takes a input as the public key PK, a time period j, a challenge Chal, a file F and the set of authenticators Φ and generates a proof P which means the cloud possesses F.Here(j,Chal)pair is issued by the auditor and thenused by the cloud.

5 Proof Verify (PK, j,Chal, P) →('True' or 'False'): This algorithm is run by the client. which takes a input

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

as the public key PK, a time period j, a challenge Chal and a proof P and returns ‘True’ or ‘False’.

4.CONCLUSION:

As this complete paper narrates the different methodologies on enabling cloud storage auditing with key exposure resilience, but none of the methodologies seems to be perfect. So, this paper as a bit proposes a method of an effective time based secret keyto provide data integrity in cloud storage. In this protocol, the integrity of the data previously stored in cloud can still be verified even if the client’s currentsecret key for cloud storage auditing is exposed. This protocol is secure and efficient for cloud data integrity.

5.BIBLIOGRAPHY:

[1]Grobauer, Walloschek, and Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE, pp. 1540-7993, APRIL 2011.

[2]Huaglory Tianfield, "Security issues in cloud computing," in IEEE International Conference, December 2012, pp. 1082 - 1089.

[3]Cong Wang, Kui Ren, and Wenjing Lou, "Toward publicly auditable secure cloud data storage services," IEEE, vol. 24, no. 4, pp. 847-859, august 2010.

[4]Q wang, C wang, ren, lou, and li, "Enabling public auditing and data dynamics for storage security in cloud computing," IEEE, vol. 22, no. 5, pp. 847-859, May 2011.

[5]Zhu, Ahn, H.Hu, Yau, and C.J.Hu, "Dyanamic Audit services for outsourced storage in clouds," IEEE, vol. 6, no. 2, pp. 409-428, 2013.

[6]Jia Yu and Kui Ren, "Enabling cloud storage auditing with key-exposure resistance," IEEE, vol. 10, no. 6, pp. 1167 - 1179, 2015.