|| Volume 2||Issue 7||JAN 2017||ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Using Third Party Auditor for Secure Cloud Storage with Privacy Preserving Public Auditing and Data

Syed Hafeez, Balkrishna Patil
Master of Engineering, *Department of Computer Science and Engineering, Everest Education Society's College of Engineering and technology, Aurangabad, India*

***Abstract*— In this paper, we introducing a third party auditor (TPA), which will keep track of all the files along with their integrity. The task of TPA is to verify the data, so that the user will be worry-free. Verification of data is done on the aggregate authenticators sent by the user and Cloud Service Provider (CSP). For this, we propose a secure cloud storage system which supports privacy-preserving public auditing and block less data verification over the cloud.**

Keywords:- *Third party auditor (TPA), data integrity, public auditing, privacy preserving, cloud storage, block less data verification.*

NOMENCLATURE

F -	Data file is divided into blocks m_i; $i \in \{1,2,\ldots n\}$
F_i -	Set of files
m_i -	i^{th} block of data file
h_i -	Hash on block
σ	Signature

I INTRODUCTION

Cloud computing is the next generation information technology (IT) architecture for enterprises. Cloud service providers manage a high level infrastructure that offers a scalable, secure and reliable environment for users at a much lower marginal cost. Most of the cloud storage likes Google Drive and Drop box offering space to the users which has become a routine for users to share the data over the cloud. From users' perspective, storing data remotely to the cloud is beneficial, because it can be accessed on-demand and in a flexible way. It brings relief of the burden for storage management; it also brings new and challenging security threats toward users' outsourced data. As the cloud service providers (CSP) are separate entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. However, the integrity of data in cloud storage is subject to skepticism and scrutiny. As the data is stored in a non trusted cloud, it can be easily be lost or it can be corrupted due to hardware failures and human errors [1].

To verify the integrity of the data over the cloud, we introduce a third party auditor (TPA) for public auditing. TPA offers its auditing service with more powerful computation and communication abilities than regular users.

Specifically, the contribution can be summarized as the following three aspects.

- Our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA.
- Our scheme provides a privacy-preserving auditing protocol.
- Our scheme provides the better security and justifies the performance of our proposed schemes through concrete experiments.

II LITERATURE SURVEY

There are many techniques that are used to provide security to the user's data over cloud. These techniques are also used for data correctness, data integrity and its security over the cloud. But there earlier techniques are not efficient to work on dynamic cloud and there are some disadvantages with these existing systems. To do this, we suggested certain requirements for public auditing services-

A. Accountability

Auditing should be done is proper manner. That is it should identify the problems as well as the particular entity responsible for that problem if any unreliability occurs. Therefore there is need of system's accountability.

B. Performance

The major aspect of any system is performance. In cloud computing also security of data storage and its integrity is important task.

C. Dynamic Support

Various Clouds provides dynamic support for runtime system to access and share the data. The challenge is the legacy users. User has access to data and user can modify the data in the cloud. So, dynamic support in runtime system is the major challenge for public auditing system.

In this paper, we proposed a secure and efficient system for public auditing which covers all the requirements mentioned above. In this system we use external auditor which is used for checking the integrity of the user's data. At the same time external auditor should be unaware of the data so that the privacy will be preserved and the communication

overhead will be less. Also we use the block less data verification scheme, which verifies the correctness of the data without having its knowledge.

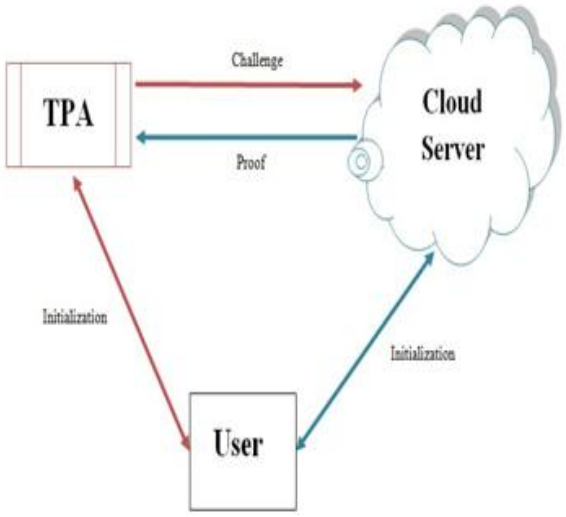

Figure 1 System model of the data auditing.

III PROPOSED SYSTEM

To save the user's computation time, storage resources and online burden, it is very important to introduce public auditing service for cloud data. This ensures the integrity of the data over the cloud and helps to reduce the online burden. Users may use the TPA to audit the data whenever they needed. Normally users don't have such expertise as TPA has. TPA has the capability and expertise to check the integrity of the data stored on the cloud on behalf of that user. This way it makes the integrity verification of the data easier and affordable for the user.

In the proposed scheme there are three algorithms for integrity verification -

- Key generation: It is a process of generating keys (Secret and public keys).
- Signing: Signing means generation of proof for verification.
- Verification: The proof generated by the cloud service provider will be verified by the TPA.

In this paper, we use Boneh–Lynn–Shacham (BLS) signature for the integrity verification purpose. The main purpose of using this scheme is it creates less overhead over the network which automatically decreases the communication cost. The BLS signature is only of 160 bits. As it is very short the size of authenticators is also reduced that means it requires less storage space over the cloud. Using this scheme aggregate authenticator is calculated on every block, and later all the individual authenticators are aggregated and calculated which is also of 160 bits. BLS signature scheme not only reduces the communication cost and required storage space.

Cloud architecture has three modules as shown in fig.1, User, Cloud Service Provider (CSP) and Third Party Auditor (TPA). User is responsible for storing the data over the cloud. CSP has the large space to store the user's data and has the resources to manage the user's data, whereas TPA which is an external auditor is responsible for auditing.

A. User

a. User first divides the file into blocks, i.e. $F = (m_1, m_2, m_3 \ldots m_n)$.
b. Once the file is divided into blocks hash value is calculated on each block, i.e. Hash $(m_i) \longrightarrow h_i$
c. After that digital signature is calculated, i.e. SignGen $(m_i) \longrightarrow \sigma_i$, here 'i' denotes the i^{th} block.
d. Finally the aggregate authenticator is calculated, i.e. Aggregate_auth $(\sigma_i) \longrightarrow \sigma$

This aggregate authenticator is sent to the third party auditor (TPA) for checking the correctness of the data.

B. Cloud Service Provider(CSP)

a. Calculate digital signature, i.e. SignGen (mi) $\sigma' \longrightarrow$
b. Claculate aggregate authenticator, i.e. Aggregate_auth $(\sigma') \longrightarrow \sigma'$

CSP sends the calculated aggregate authenticator to the TPA for verification of data.

C. Third Party Auditor(TPA)

a. Send file to check its integrity (Fi) Where Fi is a set of files and

$i \in \{1, 2, \ldots n\}$

b. Signature verification $\sigma = \sigma'$

Finally TPA is responsible for verifying the integrity of the data.

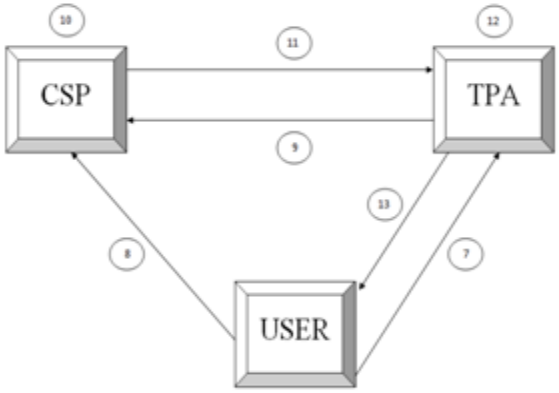

Figure 2 Architecture of cloud for integrity verification.

As shown in fig.2, following steps are performed for integrity verification on the user's data (single auditing).

1. First is the key generation process. User is responsible for generating public and private keys
2. User divides the file into individual blocks
3. User encrypts those blocks using 64 bit DES algorithm with the help of private key. This phase is called as signing.
4. Calculate hash for each block using MD5 and public key. MD5 is applied on 512 bit blocks and it produces hash of 128 bit.
5. Calculate digital signature which encrypts hash by

using private key

6. User calculates aggregate authenticator
7. User sends calculated aggregate authenticator to the TPA
8. User sends encrypted data blocks to the cloud server and delete its local copy
9. TPA requests for the authenticator to the CSP
10. CSP calculates the aggregate authenticator which is calculated on the encrypted blocks. So this system provides more security as compared to earlier systems.
11. CSP sends aggregate authenticator to the TPA in response to the request.
12. TPA compares both the authenticators, the one which is sent by the user and another which is sent by the CSP. Based on that verification is done.
13. Depending on the result calculated by the TPA, the security message is sent to the user. This message is used to indicate the integrity of the file. If both the authenticators are same then this means the integrity of the file is maintained. If both the authenticators are not same then this means the file is altered by the intruder.

In this scheme, for integrity verification of the data user and CSP do not send the original data to the TPA. So in this case TPA has no knowledge about the data which improves the security of the user's data. Depending on the aggregate authenticators sent by the user and CSP, TPA compares both the authenticators and gives the result accordingly. Hence, the proposed scheme achieves both i.e. privacy preserving and block less verification.

IV MODULES

A. Public Auditing

In this paper, we proposed a unique privacy preserving public auditing technique which achieves the block less data verification. At the CSP, the aggregate authenticator is calculated on the already encrypted data blocks. CSP doesn't decrypt the data blocks to calculate aggregate authenticator. This way the security of user's data over the cloud is achieved. Based on the authenticators calculated by both user and CSP on individual blocks are aggregated and compared at the TPA for its correctness. TPA has no knowledge of the data; it has only the authenticators obtained from user and CSP. This way the block less data verification is achieved.

B. Batch Auditing

Users may request for auditing service concurrently to the TPA. Auditing each task for individual user can be very inefficient and this can create the burden on the TPA. Using the batch auditing, TPA can simultaneously perform the multiple auditing tasks for different users. In this phase, multiple users send the aggregate authenticators to the TPA. Later TPA batch together all those requests and send it as a single request to the CSP. CSP then calculate the aggregate authenticator and sends it to the TPA. Finally TPA verifies the data. As compared to single auditing, batch auditing is better as multiple auditing requests are handled at a time. This improves the performance of the whole system.

C. Data Dynamics

Dynamic support for public auditing is very important. User may need to update, delete or add the data. Allowing dynamic support over the cloud improves the efficiency of the public auditor. External auditor has to manage the integrity of the data file where user may wish to do some block-level operations on data like update, delete and modify the file in the running system. The proposed system provides the dynamic support.

V CONCLUSION AND FUTURE SCOPE

Cloud storage is increasing day by day. Public auditing over the cloud is of critical importance. As the user doesn't have such capabilities and expertise as third party auditor has, user resorts to the TPA for the integrity verification of the data. This work studies the importance of integrity verification over the cloud with dynamic support. Also proposed system achieves the privacy preserving public auditing and block-less data verification. Batch auditing improves the efficiency of the TPA as multiple requests are handled at the same time, which reduces the burden of TPA. Since this system is effective and efficient for precise public auditing for integrity verification of user's data. Using different schemes the performance and security of this system can be improved.

REFERENCES

[1] 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, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. pp. 50–58, Apirl 2010.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[3] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.

[4] 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 Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[5] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107

[6] Cong Wang, qian wang, kui ren, wenjing lou , "Privacy – Preserving Public Auditability for Secure Cloud Storage", IEEE transaction on Cloud Computing Year 2013.