International Journal of Computer Applications Technology and Research
Volume 5– Issue 5, 292 - 294, 2016, ISSN:- 2319–8656

# Approved TPA along with Integrity Verification in Cloud

Krathika A
Department of Computer Science and Engineering
Shree Devi Institute of Technology, Kenjar, Mangalore, Karnataka
India

**Abstract**

Cloud computing is new model that helps cloud user to access resources in pay-as-you-go fashion. This helped the firm to reduce high capital investments in their own IT organization. Data security is one of the major issues in cloud computing environment. The cloud user stores their data on cloud storage will have no longer direct control over their data. The existing systems already supported the data integrity check without possessions of actual data file. The Data Auditing is the method of verification of the user data which is stored on cloud and is done by the TTP called as TPA. There are many drawbacks of existing techniques. First, in spite some of the recent works which supports updates on fixed-sized data blocks which are called coarse-grained updates, do not support for variable-sized block operations. Second, an essential authorization is missing between CSP, the cloud user and the TPA. The newly proposed scheme will support for Fine-grained data updates on dynamic data using RMHT algorithm and also supports for authorization of TPA**.**

**Keywords:** Cloud Computing, Data Security, TPA, Fine-Grained Data Updates, RMHT Algorithm

## 1. INTRODUCTION

A. Cloud Computing:

It is being intensively mentioned as one of the most dominant innovation in information technology in recent period. By using resource virtualization cloud will deliver us computing components and services in a pay-as-you-go scheme, by which the cloud visualize to turn into as suitable to use similar to way of life needs such as electricity, irrigate, telephone and water in the upcoming future. The various cloud computing services that are categorized into IaaS, PaaS and final one is SaaS. Many multinational IT corporations now present a powerful public cloud services to the users on a level from individual to endeavor all over the world. As we know the present growth and propagation of cloud compute is fast increasing, debate and hesitation on the practice of cloud still going.

*B.* Fine-Grained Data Updates:

The data owner can utilize clouds SaaS concept to store data. The data files which are stored are in the format of fixed-sized data blocks that limits operations like modification, insertions and deletions on blocks. This results in storage and data processing overheads in cloud. To solve this problem of existing systems, in proposed system the RMHT algorithm is implemented.

## 2. LITERATURE SURVEY

Compared to conventional systems, scalability and elasticity were the major benefit of cloud. In this paper, we will concentrate on small and frequent data updates on variable-sized data blocks. Cloud users also need to break larger datasets into minor datasets and store them on different physical servers for privacy-preserving and reliability. The major pressing issue related to cloud is data security/privacy. It is one of the most regularly raised concerns and there is a lot of progress trying to increase cloud data security/privacy with technical approaches on CSP part.

The Integrity verification for expanded data storage has attracted huge research interest. The topic on POR was first model and discovered by Jules. But, this method can only be used to static data storage. In the same year, Ateniese discovered alike scheme which he named „provable data possession". This method provided a „blockless verification". Achievement by Shacham, gave a better POR model with stateless verification. They also founded a MAC-based private verification scheme and also the first public verification scheme which was based on BLS signature.

In second method, the generation and verification of integrity proofs are alike to signing and verification of BLS signatures. It also proved the security of both the above methods and also for the PDP method by Ateniese. Later he extended his method for increased scalability, but only partial data dynamics were supported along with predefined number of challenges.

In 2009, Erway, discovered the first PDP method based on skip list that can provide full dynamic data updates. But, defaultly it did not support for public auditability and variable-sized file blocks. Wang discovered a technique which was based on BLS signature that can provide public auditing and also full data dynamics that was his latest work on public data auditing which provided dynamics support. But, this technique lacks support for fine-grained update. Later Wang added a random masking technology to ensure that the TPA cannot conclude the raw data file from a series of integrity proofs. In this technique, they also included an approach that was first discovered in to segment file blocks into multiple sectors. But in this technique, the use of this approach was restricted to trading-off storage cost with communication cost.

The author of paper PDP discovered the technique that can be used to provide dynamic operations such as deletion, modification, updating on data blocks by avoiding use of large encryptions.

## 3. OBJECTIVE

Contribution in this paper is listed below as follows:

1. We encourage the authorized public auditing method for ensuring secure verification of file by TPA in cloud domain. TPA cannot retrieve important information about user data. TPA is made authorized by swapping a keying material with CSP and Data owner.
2. RMHT algorithm is used in this approach. This algorithm supports for block level operations by providing variable-sized data blocks. As a result, there will be reduction in storage and computational overheads compared to other previous schemes.

## 4. EXISTING METHODS

The major issues in cloud computing can persist in loss of control over certain important data of cloud user, and the lack of

security for stored file. To have authorization for TPA, swapping of credentials is required such as signatures between three participating parties in cloud. The coarse-grained data updates are available in existing methods that provides update which has fixed-sized blocks. This will result in, every small periodic updates will experience higher communicational costs.

## 4.1 Drawbacks of Existing System:

1. The existing methods like PDP and POR support only public data integrity checks by TPA. But, it does not ensure that if TPA is authorized or not. A malicious Third Party can set DoS attack and get important information of user data by sending multiple challenge requests to cloud. This will generate additional cost on CSP.
2. Even though Coarse-grained data updates use BLS signature technique to support for small integrity proofs, it does not support for variable-sized block updates. Data updating process is difficult in existing works. Deletion of data entire size is less than block size is not permitted. If user wants to add new data in the file, then new blocks will be produced for every small insertion of data. Update of user desired block is also not provided.

# 5. PROPOSED SYSTEM

In this system, it shows that the TPA is made authorized by using the signature technique in which data owner after storing data on cloud will send a signature to TPA that is encrypted with owner secrete key. Later TPA owns this key to prove that he is an authorized auditor. Using this technique privacy preserving public auditing is obtained. The proposed technique brings outstanding security and is greatly efficient. The RMHT algorithm in this technique has increased storage capability of cloud. The cost of data storage is greatly reduced.

To produce the key for the file which is stored on the cloud, key generation and file pre processing methods are used. File Pre processing is carried to separate the files into block structure. This will increase the storage structure of data files. RMHT is a data structure that will arrange the file in separate block levels such that each block can have different authenticators which are connected at the root node to form metadata. Later this metadata is used for file verification purpose. When file is updated by data owner the metadata also keeps on changing. The user sends challenge request for TPA to check integrity of file on the cloud.

## 5.1 Advantages of Proposed System:

1. To audit for a batch of files TPA is allowed, therefore it minimizes the time of auditing task for several files at a time.
2. To execute auditing task as asked by data owner using signature scheme then the TPA is made authorized.
3. To achieve better performance and reduce extra storage, a fine-grained technique is presented in this paper

# 6. SYSTEM ARCHITECTURE

Fig.1 represents the three parties participating in public auditing process. And it consists of the following:

i. Cloud Service Provider (CSP)

The duty of CSP is to issue data storage and services for users. And the CSP is the main part of the cloud because it has more storage space to store and maintain data. It gives all its services as per pay-as-you-go scheme.

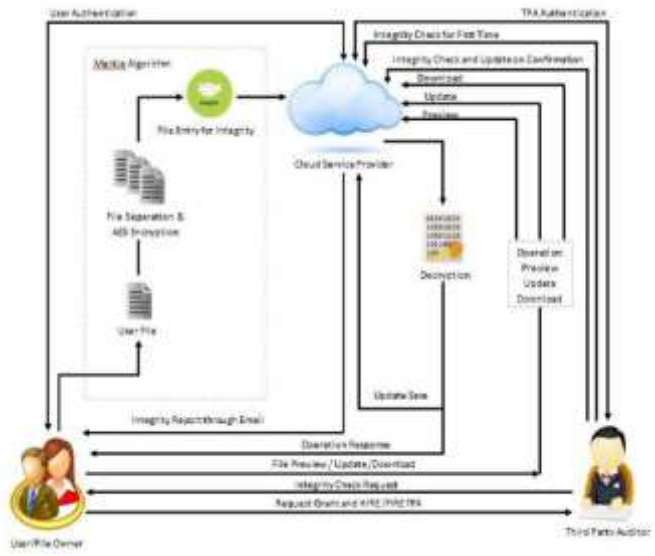

Fig. 1: System Architecture

ii. Cloud User:

A number of users can be created in which one of the users can be the group admin and can share data files with other users. And the other users can download and alter this shared file in group. If real owner of the file desires to check file for integrity then they can send challenge request to TPA. After receiving the request TPA will thus forward it to CSP and retrieves back the result of integrity proofs. Later TPA verifies proof for correctness and returns it to data owner the one who sent challenge request.

iii. Third Party Auditor (TPA):

TPA is the trusted person that store verification parameters and provide public query services for these parameters. In this paper the TTP is the one who view the user data blocks and uploads to the distributed cloud. If any alteration attempted by cloud owner a notification is sent to the TTP.

# 7. Scheme Used

1) Setup:

This part is based on the BLS signature technique. The client will generate keying material by using KeyGen and Fileproc. Later client will upload the data to CSS. The client will store RMHT as metadata and will authorize TPA by alloacting the value of sigAUTH.

2) Fine-grained Update Verification:

This method generates between client and CSS. The client will request for fine-grained update request to CSS via PerformUpdate and then client executes verifyUpdate algorithm to verify whether CSS has carried the update faithfully on the data block.

To update some portion of the data block, the client has to choose the PM (partial modification) process. It contains the following steps listed below:

1) In first step, the client produces an Update Request and sends to CSS. The CSS executes the PerformUpdate (UpdateRequest,F) algorithm .
2) In second step, the CSS sends the Pupdate to client then the

client executes the VerifyUpdate (Pk,; Pupdate) algorithm .

3) Challenge, Verification and show Proof generation:

In this step, TPA has to report that it is the actual one who is challenging the CSS for data integrity checking. TPA executes the GenChallenge() algorithm along with private key and signature as parameters. Later challenge message is produced with TPA‟s new ID chosen arbitrary from the set of total blocks. After this activity TPA sends challenges to CSS.

When CSS receives the challenges it will execute another algorithm to validate the signature, VID and client‟s public key. If it returns a true value, then CSS will forward a proof "p" to TPA and TPA will execute the algorithm to validate (pk, challenge, p) otherwise it returns false, and the request is rejected. For TPA permission, a signature method is chosen which cannot be faked by malicious TPAs.

The actors of three Parties Involved In Public Data Auditing Scheme is shown Using Sequence Diagram as Below:

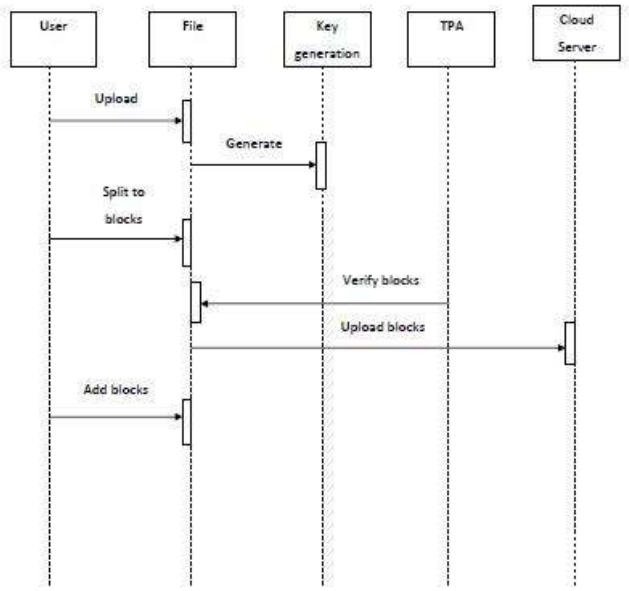


Fig. 2: Sequence Diagram

## 8. RESULTS AND DISCUSSIONS

Several projects progressed previously which can just store data and share data between huge numbers of user in a group. In our proposed work we have introduced a third party auditing technique to form a secure data organization process with great privacy protection technique along with working on audit ability

In this technique the main functionalities are data security, privacy protection, audit details to the data owner and finally Auditability aware data preparation

## 9. CONCLUSION

Cloud computing is a great computing model in which data security is the main feature for the cloud user. The newly developed technique gives support for fine-grained data updates and authorization of TPA for data security. Theoretical and experimental output for proposed system can provide higher scalability and flexibility in storing data on cloud by minimizing storage costs. This is very beneficial in big data application like social media and business transactions where minor periodic modification of data is of great importance. Security and privacy of user data is increased by using authorization scheme in public auditing. TPA cannot retrieve user data entirely during the activity of public auditing and also signature technique is used that cannot be copied so that it can avoid from malicious TPA.

## 10. ACKNOWLEDGEMENT

I would like to thank to my guide Prof. Rasheeda Z Khan and my parents for their highly appreciable support and encouragement .

## 11. REFERENCES

[1] J. Yao, S. Chen, S.Nepal,D. Levy, and J. Zic, „„TrustStore: Making Amazon S3 Trustworthy With Services Composition,"" in Proc. 10th IEEE/ACM Int"l Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2010, pp. 600-605.

[2] 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 Distrib. Syst., vol. 22, no. 5, pp. 847-859, May 2011.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, „„Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,"" in Proc. 30st IEEE Conf. on Comput. and Commun. (INFOCOM), 2010, pp. 1-9.

[4] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, „„Scalable and Efficient Provable Data Possession,"" in Proc. 4th Int"l Conf. Security and Privacy in Commun. Netw. (SecureComm), 2008, pp. 1-10.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, „„Remote Data Checking Using Provable Data Possession,"" ACM Trans. Inf. Syst. Security, vol. 14, no. 1, May 2011, Article 12.

[6] G.Ateniese, R.B. Johns,R. Curtmola, J.Herring, L. Kissner,Z. Peterson, and D. Song, „„Provable Data Possession at Untrusted Stores,"" in Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), 2007, pp. 598-609.