International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: http://doi.org/10.31695/IJASRE.2018.32789

Volume 4, Issue 7
July - 2018

Remote Data Integrity Checking in Cloud Storage

Sunil B P[1] and Sadhana[2]

P.G. Scholar and Assistant Professor [2]

Department of Computer Science & Engineering

Sahyadri College of Engineering & Management

Mangaluru, Karnataka

India

ABSTRACT

As an important application in cloud computing, cloud storage provides data users flexible, scalable and high-quality data computation and storage services. A large number of data users opt to outsource their data files to the cloud storage. Because cloud storage services are not completely reliable, data users require trusty means to check the possession for their data files deployed to remote cloud servers. To overcome this critical issue, a few remote data integrity checking protocols have been presented. But many existing schemes have drawbacks in data dynamics or efficiency. So a new efficient remote data integrity checking protocol based on homomorphic hash function has been developed. The new scheme is certainly safe against replacing attack, replay attack and forgery attack based on a typical security model. To brace data dynamics like inertion, updation or deletion operations on file blocks, an operation record table is included to trace functions on data blocks, and also makes the cost of accessing operation record table almost less or firm. Prototype implementation shows that the scheme is beneficial for real-world applications.

Key Words: *Cloud Computing, Data integrity, Data dynamics, Homomorphic hash, Operation record table.*

1. INTRODUCTION

The most commonly used storage service now a day is cloud storage. Cloud computing has been growing rapidly and is the most commonly used business model. With Big Data and Analytics and Artificial Intelligence coming into picture, the importance of cloud has risen above. The cloud is not only being used by the IT industries, academic institutions, government agencies, small and medium organizations but also by common man. Be it to store documents on google drive or build android applications over the cloud or to share photos and media over social media applications, which rely on cloud.

The beauty of using cloud computing is that cloud users need to spend only for what they use. If enterprise is emergent, consumer can hire extra resources from cloud provider without having to pay for computing resources.

As cloud clienteles require not to worry on groundwork upkeep, so they only concentrate on consuming resources on 'pay as you go' model. Cloud computing exploit resources more competantly, means same infrastructure may be used by many customers ensuring in less number of required servers.

It makes cloud greener and cloud customers more eco-friendly. Additional benefits of cloud include multi-tenacy, flexibility, disaster recovery and many more. Cloud computing follows three models i.e. SaaS, IaaS and Paas. We also know that there are three types of clouds.

Since it is the most adapted technique of storage, the companies that use them choose to outsource this from another company or they use build their own cloud and use them. If outsourced, the entire responsibility of maintaining the cloud, taking care of the cloud, restoring the backup in case of a failure, rests upon that company. In either case, it is a huge responsibility and a lot of resources like, time, energy, money etc. are spend on cloud storage and maintenance.

With above mentioned characteristics, benefits and advantages, Cloud service offers scalable, reliable, minimum cost, outsourced data storage & computational services to users. And a flexible pay as you go model providing storage & computational resources on demand.

Cloud owners rely on cloud storage for storing varoius buisness sensitive data of their day to day applications. When the users stores their data files in cloud server, will be most worried on data integrity.

According to recent studies, there is a growing number of forgery attack and replay attacks of files are on the rise. For example, unfair cloud storage server might forge a valid information like tag, keys, etc., related to a file during verification to cheat the data user. This may result in huge loss and creates issues to the data user, if the data is very sensitive, important and critical to user's business applications.

Considering the fact that the integrity of files are important and avoid such loss of integrity issues, we have come with the unpretention solution of data integrity.

The users can verify the files stored on cloud server through sending tag challenges to the the cloud storage server, without downloading entire file. The cloud storage server inturn sends response with a proof, so that client can check and verify them for integrity of files. Hence, customers will be in good impression to use cloud storage services.

2. LITERATURE REVIEW

In Cloud computing, the problem of data integrity is still addressed out through many researchers. There are lot of research work taking place in this discipline in order to give secure and efficient data integrity in cloud computing. Researchers provided many solutions to address on resolving issues of data integrity. Some of them are as follows, Initial remote data integrity checking protocol was mainly implemented using RSA hash function [1]. Downside was that, entire file block has to be accessed in order to verify integrity. According to Ateniese et al. [3], "the provable data possession scheme uses probabilistic proof technique and checks remote data integrity without accessing entire file. Two protocols S-PDP, E-PDP [4], based on RSA was proposed and provided good performance, but lack dynamic file operations."

Further Sebé et al. [5] states that "remote data possession checking protocol on factoring large integers which supports dynamic operations." After that Erway et al. [6] provided "fully dynamic PDP scheme where user could insert, update or delete file blocks".

Merkle hash tree (MHT) was proposed by Wang et. al [7], "where every block will be hashed as leaf node of the tree. Here MHT recognizes position of the block by sorting entire leaf nodes starting from left till right for dynamic operations." Downside was that it had huge computation cost.

Index table was introduced for handling dynamic operations where version number, logical location of the block can be utilized to insert or delete a block, but position have to be computed by the verifier and shift remaining entries while deleting or inserting rows in index table, which was very cumbersoome and costs high on computation [8].

According to Curtmola et al. [9], "the remote integrity checking for multiple replicas in cloud storage aims to provide secure data integrity by verifying multiple replicas using provable data possession method."

Hao and Yu [10] presented "a protocol for the multiplereplicas with public verifiability and privacy preservation." Mukundan et al. [11] proposed "a dynamic multiple replicas provable data possession, which supported dynamic operations on replicas while holding the features of multiple replicas integrity checking."

3. IMPLEMENTATION

3.1 System Framework

As cloud computing has its own benefits and cloud storage has been utilized by many customers. The cloud storage server provides robust services like storage ability and computing resources for storing and accessing users' data files. The data owner keeps huge amount of business application data onto the cloud storage and rely on the cloud storage in real time, without keeping local backup. To check integrity of user data, customers indeed require a way to verify integrity of files kept on cloud storage. So in this scheme, which is based on homomorphic hash function been implemented, which gives security across forgery attack, replace and replay attack. And also supports functions to perform add, modify and delete file blocks.

3.2 Remote Data Integrity Checking

Remote data integrity checking is a useful way to make sure data placed on cloud server storage is safe and secured. It provides data user to effectively verify their files placed on cloud server storage without downloading entire file, by challenging the integrity of files kept. In reply, cloud server storage views all challenges from the various users and can develop proofs to confirm consent of the file to be uncorrupted and complete. Since the cloud service providers are not fully trustable, they may occasionally modify or delete partial files, which can be verified by the data users. This scheme includes following methods: KeyGen, TagGen, Challenge, ProofGen, Verify, PrepareUpdate, ExecUpdate.

3.3 Security Requirement

The following are the types of attacks might be involved with the dishonest cloud storage server, they are

Forge attack: In which tag of a challenged data file may be forged by the cloud storage server.

Replay Attack: Information related to valid proof from earlier proofs will be sent by cloud storage server without processing challenged data.

Replace Attack: Cloud storage server might provide some other correct data as proof for challenged data, which might be changed or discarded.

Hence our scheme need to prevent the issues mentioned above, which assures that anyone who can build a correct proof sending the verification should have whole file.

3.4 Homomorphic Hash Function and Operation Record Table

The basic scheme uses homomorphic hash function technique, where the hash value of the sum for two blocks is equal to the product for two hash values of the respective blocks. Also a linear table to track data operations like block insertion, updation and deletion. In order to enhance the efficiency for accessing operation record table, the table is stored on the data user side and used to record all the dynamic activities on data file blocks. Further, the record table make use of doubly linked list and array to provide an optimized implementation of operation record table which reduces the cost to nearly constant level.

4. CONCLUSION

Checking integrity of data present on remote server and an able secure way to protect from replay attacks and also works well with data dynamics on files. This project operates on a homomorphic hash method which justify the integrity of data uploaded on faraway remote server, also lowers the computation and storage expenditure of the files holder. Aim is to model a unique incompetant efficient data structure to allow various file activities which draws least possible data processing amount by lowering the number of node traversing. Using this method, the data user may implement insert, delete, edit activity over data easily. The presented scheme is proved secure in current security model.

REFERENCES

[1] Y. Deswarte, A. Saïdane, and J. J. Quisquater, “remote integrity checking,” in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst. (IICIS), 2003, pp. 1–8.

[2] Z. Hao, N. Yu, and S. Zhong, “A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability,” IEEE Trans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432–1435, Sep. 2011.

[3] G. Ateniese, D. Song, R. Curtmola, L. Kissner, Z. Peterson, J. Herring, and R. Burns, ‘‘Provable Data Possession at Untrusted Stores,’’ in Proc. 14th ACM Conference on Computer and Communication Security (CCS), 2007, pp. 600-605.

[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] F. Sebé, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, “Efficient Remote Data Possession Checking in Critical Information Infrastructures,” IEEE Trans. Knowledge and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[6] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, “Dynamic Provable Data Possession,’’ in Proc. 16th ACM Conf. on Comput. And Commun. Security (CCS), 2009, pp. 213-222.

[7] 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.

[8] X. Jia and K. Yang, ‘‘An efficient and secure dynamic auditing protocol for data storage in cloud computing,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1719-1722, 2013.

[9] O. Khan, R. Curtmola, R. Burns, and G. Ateniese, ‘‘MR-PDP: Multiple-replica provable data possession,’’ in Proc. 28th IEEE Conf. on Distrib. Comput. Syst. (ICDCS), 2008, pp. 412-418.

[10] Z. Hao and N. Yu, ‘‘A multiple replica remote data possession checking protocol with public verifiability,’’ in Proc. 2th International Symposium. Data, Privacy, E-Commerce (ISDPE), 2010, pp. 84-88.

[11] R. Mukundan, S. Madria and M. Linderman, ‘‘Efficient integrity verification of replicated data in cloud using homomorphic encryption,’’ Distributed Parallel Data, vol. 32, no. 4, pp. 507-528, 2014.