Volume 1 , Issue 06, PP: 190 - 193 , DEC ' 2014.

INFLUENTIAL TOKENIZED APPROACH FOR GUARDED DATA STORAGE AND COMMUNICATION IN CLOUD COMPUTING

P VENKATESWARLU 1*

1 . Professor , Dept of CSE, Nagole Institute of Technology & Science, Hyderabad.

ABSTRACT:

Cloud computing is a tremendous and most demanding technology which reduces the overhead of creating and maintaining the infrastructure to deploy the applications by small and large scale industries. Storing data on the cloud storage and transferring data to and from client and cloud server are two basic problems in the context of Infrastructure as a service. We are proposing new distributed storage architecture for secured data storage. We are also proposing a tokenized approach to transfer data between client and server. This method has mainly two advantages that data correctness and transmission speed. Data correctness can be improved by using error localization at each client.

KEYWORDS: cloud computing, data security, public clouds, distributed storage, dynamic tokenization.

I.INTRODUCTION

Cloud computing is a tremendous and most demanding technology which reduces the overhead of creating and maintaining the infrastructure to deploy the applications by small and large scale industries. Cloud computing provides a common platform to develop, deploy and host new range of applications by using the help of internet. Cloud computing can be defined in terms cloud and computing. Cloud is a collection of heterogeneous resources connected together to achieve the common goal. It provides an infrastructure for providing services to the end users. Computing specifies set rules and regulations to provide services to the end user by using these resources.

Moving data to clouds makes more convenient and reduce to manage hardware complexities. Data stored at clouds are maintained by Cloud service providers (CSP) with various incentives for different levels of services. However it eliminates the responsibility of local machines to maintain data, there is a chance to lose data or it effects from external or internal attacks. To maintain the data integrity and data availability many people proposed several algorithms and methods that enable on demand data correctness and verification. So Cloud servers are not only used to store data like a ware- house , it also provides frequent updates on data by the users with different operations like insert, delete , update and append. Lastly the deployment of cloud computing is powered by the data centers

running in cooperated and distributed manner.

II.RELATED WORK

According to Cong Wang, Qian WangKui Ren, Ning Cao et all [1] & [2] the basic cloud storage architecture can be defined as set of three entities as shown in figure.

User: The preliminary entity who stores and access data on the cloud storage.
Cloud Server (CS): The cloud server entity is managed and maintained by cloud service provider to provide storage service and provides large storage space and computational resources.
Third-Party Auditor: an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

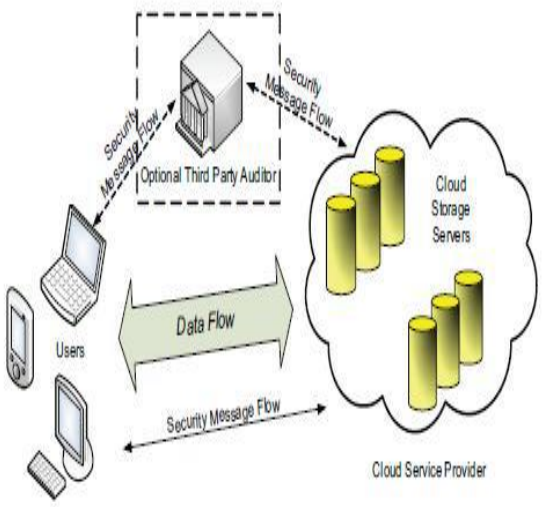

Figure 1: Cloud Storage architecture

The working principle of the behind the existed system is a client can store data on the cloud storage. The data can be stored on different servers in a distributed manner. Data redundant techniques can be employed using erasure correcting code to protect from faults or server crashes. The client can also perform modification on the data by using the operations like insert, delete, and update. These operations can be performed on the block level on the data by generating tokens to ensure security on the data. These tokens can be generated at client or Third party auditor.

In this paper we are proposing a new method to generate tokens dynamically to ensure the storage security. The tokens are prepared at Third party auditor so that we can reduce the processing complexity at the client machine. It also ensures the data integrity of the cloud servers.

III.PROPOSED SYSTEM

Clients are going to store data on the cloud servers without prior knowledge of the cloud architecture. Correctness and availability of the data is very important goals in cloud storage architecture. In order to achieve correctness of the data we are proposing a dynamic tokenized approach by generating homo-morphic tokens at TPA. These tokens are pre-computed in order to identify the corrected blocks during data transmission. Erasure coded technique is used to collect the data from different servers. The proposed system has following modules.

3.1 *Challenge Token Pre-Computation*

3.2 File Retrieval and Misleading block checking using Token Computation

3.1 CHALLENGE TOKEN PRE-COMPUTATION

Generating and maintaining tokens is one of the key responsibilities of TPA. The tokens are generated before the actual file stored on the cloud servers. This process includes dividing the file in to equal size blocks and then generating the token to each block. These blocks are stored on the servers along with the corresponding tokens. Hash based technique is used to generate the tokens. The corresponding tokens for each block are also stored on to the client machine for verification purpose. The following algorithm explains how the tokens are generated.

Algorithm: Pre token Generation

Input: File F, Fl length of the file, V secret matrix

Output: set of tokens

Algorithm:

Find no of blocks with fixed block size as

X = F + Fl + V

Compute key

For i=1 to n

File Token = file Token $+(\sum_{i=1}^{n} Split(Xi))$

Compute short signature by using the tokens and file blocks and store the results in client machine for future verification of data.

3.2 **File Retrieval and Misleading block checking using Token Computation:**

We are going to explain how the data is being validated and retrieved back from the cloud servers in this phase. Before going to retrieve the exact data the client validation will be verified at TPA. An authorized client can request for the data from the cloud servers. The process of getting exact data can be done by using the tokens generated by using homo-morphic methods at servers. The following algorithm clearly explains the correctness and relevance data to the client.

Algorithm: File retrieval and misleading block checking

Input: Client requested data blocks

Output: Valid blocks

Algorithm:

Process the client request blocks.

Compute the short signature at server side.

Send the signature to TPA.

Compare the pre computed signature and new signature.

If two are equal the send the data blocks.

If not equal don't send the data.

IV. CONCLUSION

In this paper we are discussed and proposed a new approach to enhance the data correctness and integrity. Our proposed system drastically improves the performance of client machine because of the introduction of the TPA. We can reduce the burden of authorizing the client on servers. The data transmission rate also improves because of the less computational overhead at both client and server machine. We can extend our future work to correct error blocks in order to minimize the data loss.

V. REFERENCES

[1] Cong Wang, Qian WangKui Ren, Ning Cao, and Wenjing Lou "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE transactions on services computing, vol. 5, no. 2, april-june 2012 .

[2] Qian Wang,Cong Wang, Kui Ren, Wenjing Lou Jin Li "Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing" IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011 .

[3] K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. ACM Conf. Computer
and Comm. Security (CCS '09), pp. 187-198, 2009.

[4] T. Schwarz and E.L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS '06),pp. 12-12, 2006.

[5] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard,"A Cooperative Internet Backup Scheme," Proc. USENIX Ann. Technical Conf. (General Track), pp. 29-41, 2003.

[6] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 398-461, 2002.

[7] L. Carter and M. Wegman, "Universal Hash Functions," J.Computer and System Sciences, vol. 18, no. 2, pp. 143-154, 1979.

[8] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasure-Coded Data," Proc. 26th ACM Symp. Principles of Distributed Computing, pp. 139-146, 2007.

[9] J.S. Plank and Y. Ding, "Note: Correction to the 1997 Tutorial on Reed-Solomon Coding," Technical Report CS-03-504, Univ. of Tennessee, Apr. 2003.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.

[11] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan,"Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

[12] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy- Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186,http://eprint.iacr.org, 2008.