Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure and Data Dynamics Storage Services on Cloud

Manasi Doshi
PG student of Department of
Computer Engineering,SCOE, Pune, India

Swapnaja Hiray
Associate Professor of Department of
Computer Engineering,SCOE, Pune, India

Abstract*— Cloud storage allows users to store their data and enjoy high quality of services. It enables highly scalable, on demand and only pay per use services to be easily consumed over the Internet on an as needed basis. Cloud stores data on remote machine, so necessary to need more security from unauthorized person. To achieve this, perform flexible distributed storage, utilizing the homomorphism token and distributed erasure-coded data. Also allows for strong cloud storage correctness and simultaneously achieves fast data error localization.

Keywords*— Cloud, homomorphism token, distributed erasure-coded data, error localization and security.

I. INTRODUCTION

Cloud computing is the use of computing of sources that are delivered as a service over a network. Cloud enables user to store data. But data is stored at remote machine, so it poses new security risks. A major characteristic of the cloud services is that user's data are usually processed remotely in unknown machines that users do not operate. So, basic need is to provide security to cloud server. One of the most challenging problem in Cloud computing is about the security of the outsourced data which is mainly handled by untrusted parties. Third unauthorized person can easily modify that data or misuse that data. Risks in terms of confidentiality, integrity of data. So it is necessary to provide security to data stored on cloud. Now new target it to achieve this.

II. RELATED WORK

In this section we first review related works addressing security in cloud. Security issue is very important in cloud there are many techniques available so here is review of all these. Data security is the major challenge in the cloud computing as user's data reside in the servers which are remotely situated and far away from the end-users. These data may include confidential data (financial data, health records), personal information which may be disclosed to competitors or publicly. So security emerges as the highest priority issue [2]. In [3] Third party auditor for verification, they describes three network entities i.e. client which is user, cloud storage server which is handled by cloud service provider and Third Party Auditor which is verifier.TPA having public key, it is act with only trusted server, they are not focuses on data privacy. In [4] it defines 2 basic schemes. Scheme 1 : User computes the MAC of every file block. Transfers the file blocks & codes to cloud and shares the key with TPA. During the Audit phase, the TPA requests from the cloud server a number of randomly selected blocks and their corresponding MACs to verify the correctness of the data file. Drawback of this scheme is TPA can see cloud data. Scheme 2: In Setup phase, User uses s keys and computes the MAC for blocks and user shares the keys and MACs with TPA. During Audit, TPA gives a key (one of the s keys) to CSP and requests MACs for the blocks. TPA compares with the MACs at the TPA. Improvement from Scheme 1: TPA doesn't see the data, preserves privacy. Drawback: a key can be used once, Schemes 1 & 2 are good for static data (data doesn't change at the cloud). In paper [5] they discuss main challenges for achieving cloud computing services, this problem focuses on accountability in cloud computing. Accountability means verification of access control policies.

III. PROPOSED WORK

3.1 System Modules:

1. Client:
   Client is that entity who is using of cloud services and who has to store data on cloud. Multiple clients can use cloud storage services.
2. TPA:
   TPA is an optional entity. It has expertise and capability to expose dummy client. E.g. authentication of client.
3. CSP:
   CSP is an entity which provides cloud services. E.g. client want to upload file then CSP give call to CS.
4. CS:
   CS is an entity which allow client to perform operation on data stored on itself.

5. Main Backup server:
   It is an entity which stores complete file.

3.2 System Architecture

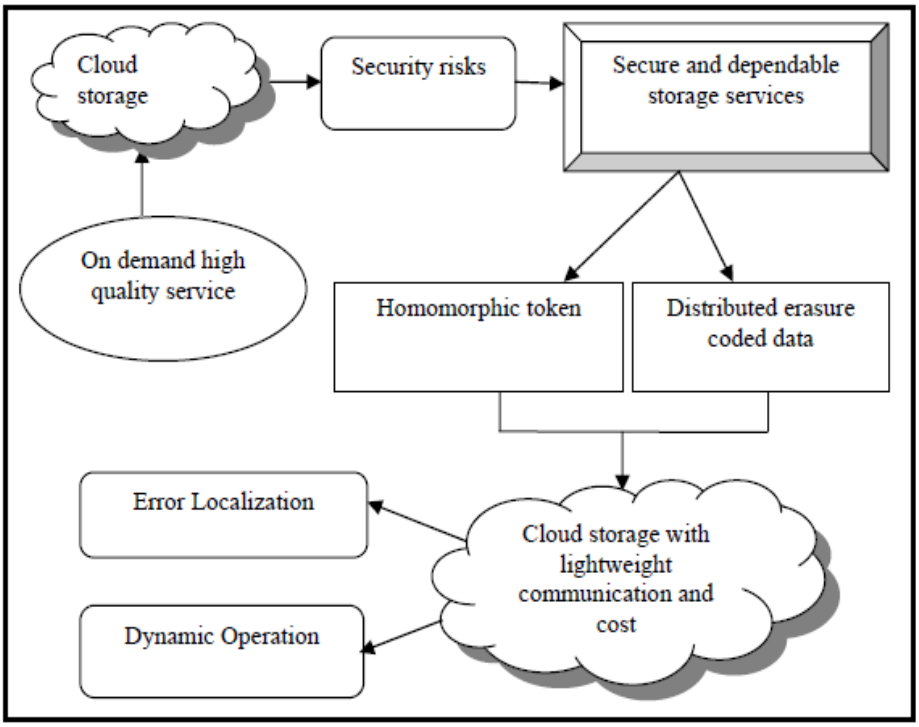

Fig 1. Functions of cloud storage service architecture

Above fig. is showing functional details of cloud storage service architecture. It tells that Cloud is serves as storage. It provides on demand, high quality of services. As data data stored at remote machine new security risks may come. To achieve security homomorphic tokens and distribution of data is necessary. Distributed data means user's data/file is divided into some fixed number of blocks and each block is stored on separate machine in cloud. Now for each block token are generated which helps in error detection. This architecture allows user to perform dynamic operations on data like modify, append, delete. It easily finds where error occurs i.e. modification of data by unauthorized person is done. This is called error localization. It is time to allow user to audit the cloud storage with very lightweight communication and computation cost.

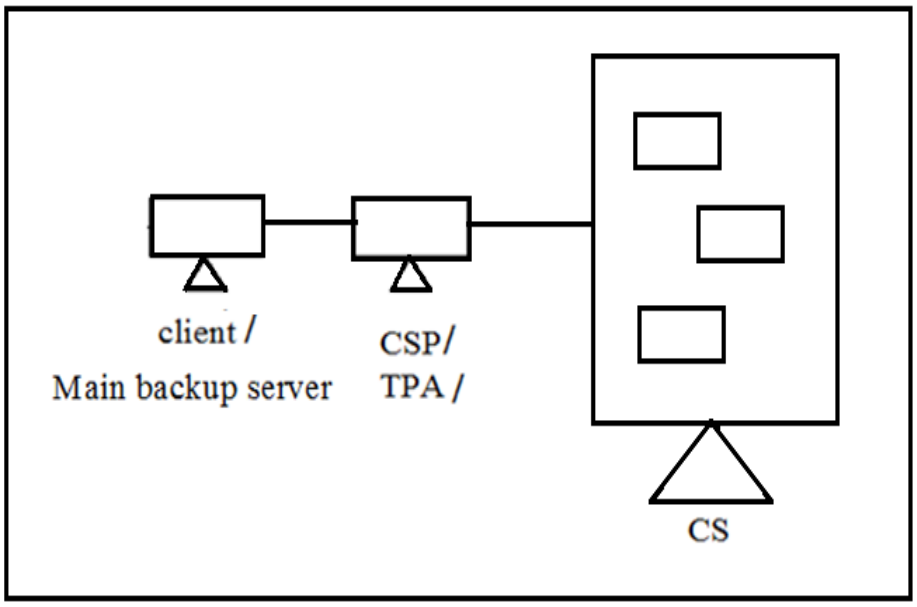

Fig 2. Proposed cloud storage service architecture (using 3 machines)

Here client, main backup server working on one machine. CSP, TPA on one machine. For storing client's data i.e. input file is divided into 3 blocks. Size of each block is same and is store on CS. CS machine is virtualized. There are 3 instances of OS and is it showing as cloud. Each block is stored on 1 instance of OS on CS. Complete file is stored on main backup server machine to recover if CS crashes. CSP gives services to clients by taking it from CS. TPA is responsible for audit log report.

3.3 Ensuring cloud data storage

1. Storage of data in a Cloud

In a cloud, the users are expected to store their data in a cloud and once stored, the data is not accessed locally. As a result it is important to maintain the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. Hence, it is challenging to find out the unauthorized or corruption of data on servers and also more importantly in a distributed case when such inconsistencies are successfully detected. It is also equally challenging to find the server on which the error occurs as it would help resolve the issue faster. We will look at the method to overcome this issue in various parts. To start with, the basic tools will be reviewed and then homomorphic tokens are introduced. Moving on, we will look at challenge response protocol for verifying the storage correctness as well as identifying misbehaving servers and will conclude with the procedure for file retrieval and error recovery based on erasure-correcting code.

2. File Distribution Preparation

File which client want to store is divides into 3 blocks depending upon size of original file. Each new block is of same size. To achieve availability each block is stored twice. E.g. 1st block is stored on CS 1 and CS 2, 2nd block is stored on CS 2 and CS 3, 3rd block is stored on CS 3 and CS 1.

3. Token Pre-computation

To ensure that the data present on the cloud is correct, the method we are looking at depends on the pre-computed verification tokens as the main idea is that the user pre-computes a certain number of short verification token before file distribution. Towards end when the users want to ensure data storage correctness, they confront the servers of the cloud with a lot block indices that are generated in an arbitrary manner and when these confrontations are received, each cloud server computes a short signature over the specified blocks and returns them to the user.

4. Verification and Error Localization

The main requirement for getting rid of errors in the storage system is error localization. Though many previous methods do not consider the data error localization as an issue and only provide binary results for the storage verification.

IV. CONCLUSIONS

From all above discussion, it shows that we can provide security to data stored on cloud i.e. providing security to remotely stored data is possible. First data is distributed on multiple machines. With the help of tokens generation and token matching we are providing security. By taking backup of data we can achieve availability even if CS crash. It allows user to perform block operation i.e. append, delete, modify as well as to give challenge to uploaded to check correctness of data. In future focus will be towards performance, CPU utilization etc.

.

ACKNOWLEDGMENT

I am very thankful to my guide for guiding me and heartly thankful to IJARCSSE to give me such a wonderful chance for publishing my paper. Also thankful to Microsoft to help me in writing this paper.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009.

[3] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, preprint, 2012, doi:10.1109/TC.2011.245.

[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 and Distributed Systems, vol. 22,no. 5, pp. 847-859, 2011.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[6] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine,vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[7] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012.

[8] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine,vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[9] Amazon.com, "Amazon Web Services (AWS)," http://aws.amazon.com, 2009.

[10] http://windows.microsoft.com/en-IN/windows-8/internet-information-services-iis-8-0

