International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Ensuring Data Storage Security in Cloud Computing

Nikita pathrabe, Deepali khtawar
Computer Science And Engineering, M-tech
Email: nikitapathrabe@rediffmail.com

Abstract- Now a day's Cloud computing is emerging field because of its Performance, high availability, at low cost. Cloud is kind of Centralized database where many organizations store their data, retrieve data and possibly modify data. In the cloud many Services are provided to the client by cloud. Data store is main future that cloud service provides to the big organization to store huge amount of data. But still many organizations are not ready to implement cloud computing technology because of following reason. That is Lack of security, Data redundancy, Misbehavior of the server. So the main objective of this paper is to solve the above reasons that are To prevent unauthorized access, it can be done with the help of a distributed scheme by using homomorphism token to provide security of the data in cloud. The cloud is support for data redundancy means clients can insert, delete or can update data so there should be security mechanism which ensure integrity of data. This paper also secures the data while the misbehaving of the server arise.

In this paper, we focus on Ensuring data storage security in cloud computing, which is an important aspect of Quality of Service.

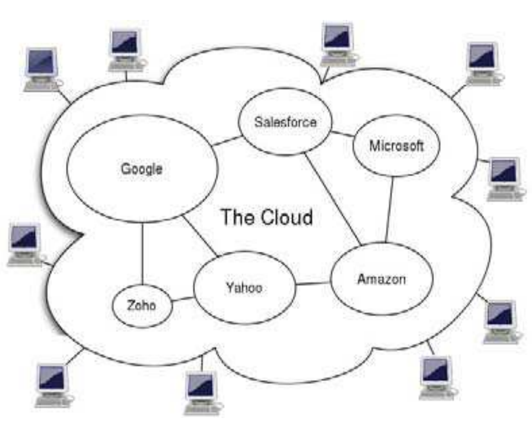
Index Terms- ***Homomorphism token, Distributed scheme, Data redundancy, cloud***.

Fig.1 (b) Overview of a cloud

1. Introduction

Now a day Cloud Computing become so strong, because it is an Internet-based development and use of computer technology and also cheaper as well as more powerful processors, together with the software as a service (SaaS) computing architecture. Due to increase in network bandwidth it becomes faster to provide quality of services as compare to previous. Also support to moving the data between cloud and client without any complexity because of releasing the hardware complexity. Because of online base computing it provide huge amount of data storage and resources to the local machine and eliminate the local machine to maintenance separate data. As a result, users are at the thankful of their cloud service providers for the availability and integrity of their data.

Data security is always been the important aspect of quality of services, Cloud computing every time invites the new challenges of security thread for number of reasons. Firstly, traditional cryptographic cannot be used directly data security purpose because users' loss control of data under Cloud Computing. Therefore, verification of correct data whether it store correctly or not in the cloud must be conducted without explicit knowledge of the whole data. Due to the continuously demanding of long term storage of data with correctness and security become more challenging. Secondly, Cloud Computing is not just a third party data warehouse.



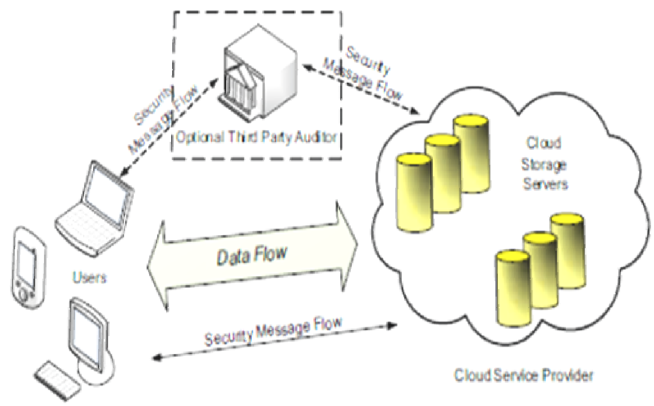


Fig.1 (a) Structure of a cloud

Whatever the data store in the cloud that may be update frequently by the user like insertion, deletion, appending, recording, etc. So to ensure the data storage correctness under dynamic data update is hence so much of important.

However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. The different user data is stored in different physical locations to further reduce the data integrity threats. Therefore, it is most importance to achieving a robust and secure cloud data storage system in the real world. Recently, the importance of ensuring the remote data integrity has been highlighted by the following research works. Since they are all focusing on single server scenario so these techniques can be useful to ensure the storage correctness without having individual users possessing data, also cannot address all the security threats in cloud data storage, and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers.

2. Cloud Architecture

Cloud architecture is nothing but the systems architecture of the software systems which involved in the delivery of cloud computing, generally it involves multiple cloud components communicating with each other over loose coupling mechanism like messaging queue. The most important components of the cloud computing architecture are front end and back end. Where the front end is the part seen by the client, i.e., the computer user, which includes the client's computer and the applications used to access the cloud via a user interface such as a web browser or any system application. The back end of the cloud computing architecture is the cloud itself i.e. admin of cloud, which comprising various computers, servers and data storage devices.

The network architecture for cloud data storage is shown in above Fig2.Three various network elements can be identified as follows:

Users: Who have data to be stored in the cloud and depend on the cloud for data computation, also consist of both individual consumers and organizations.

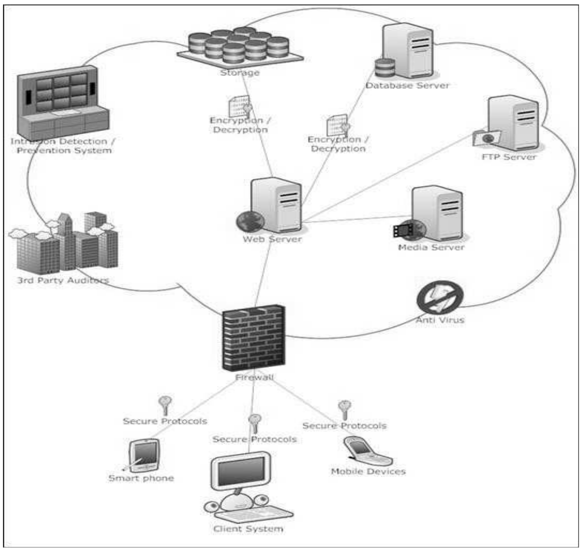


Fig. 2: Cloud data storage architecture

CSP (Cloud Service Provider): CSP is the person who can manage whole services as well as data storage and lot more thing of cloud computing like operate live Cloud computing system. And having optional TPA (Third Party Auditor), who has capabilities and authority that users may not have, TPA is trusted person to take a risk of cloud storage services on behalf of the users upon request.

3. Ensuring Cloud Data Storage

In cloud data storage system, users store their data and do not possess longer data locally. Due to which, the correctness and availability of the data files which being stored on the distributed cloud servers must be guaranteed. The most important issue is to effectively detect any unauthorized data modification and corruption, which occur due to server compromise and random Byzantine failures. Whereas, in the distributed case such inconsistencies are successfully detected, and also to find on which server the data error lies become great significance, hence it can be the first step to fast recover the storage errors. So to address and solve all these kind of problems, our main scheme for ensuring cloud data storage is presented in this section. The first part of the section is to develop and review of basic tools from coding theory that is needed in our scheme for file distribution in cloud servers. Then, our main tool homomorphic token is introduced. The token computation function we are considering belongs to a family of universal hash function, chosen to preserve the homomorphism properties, which can be perfectly integrated with the verification of erasure-coded data. Side by side, it is also shown verifying the storage correctness as well as identifying misbehaving server.

The last but not the least the most important point of this paper is that, here trying to implement the cloud computing with the mobile computing. So that the user are not restricted to access the data in the cloud via personal computer or laptop. But he or she can be access the cloud account via mobile phone also. It will be so handy for the user to take the cell phone with them. So that they can access their cloud account everywhere.

4. Security Analysis and Performance Evaluation

Our security analysis focuses on the model as defined. We also provide an efficiency of our scheme via implementation of both file distribution preparation and verification token pre-computation. In our scheme, servers are required to operate on specified rows to check correctness and verification for the calculation of requested token. We will show that this "sampling" strategy on selected rows instead of all document or data which can greatly reduce the computational overhead on the server, also maintaining the detection of the data corruption with high probability. Suppose any servers are misbehaving due to the possible compromise or Byzantine failure. In the following analysis, we do not limit the value of any server, i.e., servers $\leq$ n. Assume the adversary modifies the data blocks in z rows out of the l rows in the encoded file matrix. Let r be the number of different rows for which the user asks for check in a challenge. Let X be a discrete random variable that is defined to be the number of rows chosen by the user that matches the rows modified by the adversary.

5. Reference:

[1] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High- Availability and Integrity Layer for Cloud Storage," 2008.

[2] Cong Wang, Qian Wang, KuiRen, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2012.

[3] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: UsingAlgebraic Signatures to Check Remotely Administered Storage," Proc.

[4]M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," *Proc. of the 2003 USENIX Annual Technical Conference (General Track)*, pp. 29–41, 2003.

[5] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High- Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report 2008/489, 2008, http://eprint.iacr.org/.

[6] L. Carter and M. Wegman, "Universal Hash Functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[7] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasurecoded Data," *Proc. 26th ACM Symposium on Principles of Distributed Computing*, pp. 139–146, 2007.