ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (283-287), Month: April - June 2015, Available at: www.researchpublish.com

Ensuring Data Storage Security in Cloud Computing

Khushboo Chauhan

Department Of Computer Science & Engineering, Mahatama Gandhi Mission's Engineering College, Noida, India.

Abstract: **Now a day's Cloud computing is emerging field because of its performance and high availability at low cost. Cloud is kind of centralized database where many organizations store, retrieve and possibly modify their data. Many services are provided to the client by cloud. Data storage is main feature that cloud service provides to the big organizations for storing their huge amount of data. But still many organizations are not ready to implement cloud computing technology due to some reasons i.e. 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 homomorphic 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. In this paper, we focus on Ensuring data storage security in cloud computing, which is an important aspect of Quality of Service.**

Keywords: **Homomorphic token, Distributed scheme, Data redundancy, cloud.**

1. INTRODUCTION

Cloud computing has already been adopted worldwide. A clear rise in increased use of cloud services can be seen now a days. The Cloud technology is a growing trend and is still undergoing lots of experiments. Thus it raises the need for better security as well. There is a critical need to securely store, share, and manage the data. Analyzing the massive amounts of complex data needs best suitable approaches. The National Institution of Standard and Technology (NIST) has defined the cloud computing as a program for enabling useful, on-demand network access to a shared pool of configurable computing resources. Cloud computing is an internet based technology and provide services over internet. 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 thankful of their cloud service providers for the availability and integrity of their data. The security of data is important in the aspects of quality of service. Cloud computing every time invites the new challenges of security thread for number of reasons. Firstly, traditional cryptography cannot be used directly for 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 continuous demanding of long term storage of data with correctness, security become more challenging. Cloud Computing is not just a third party data warehouse. The data in cloud may be updated frequently by the user using actions like insertion, deletion, appending, recording, etc. So to ensure the data storage correctness under dynamic data update is hence important.

Figure 1: Cloud computing

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (283-287), Month: April - June 2015, Available at: www.researchpublish.com

2. CLOUD ARCHITECTURE

The Cloud Computing architecture comprises of many cloud components, each of them are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front End
- Back End

Each of the ends are connected through a network, usually via Internet.

Front End: 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.

Back End: Refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

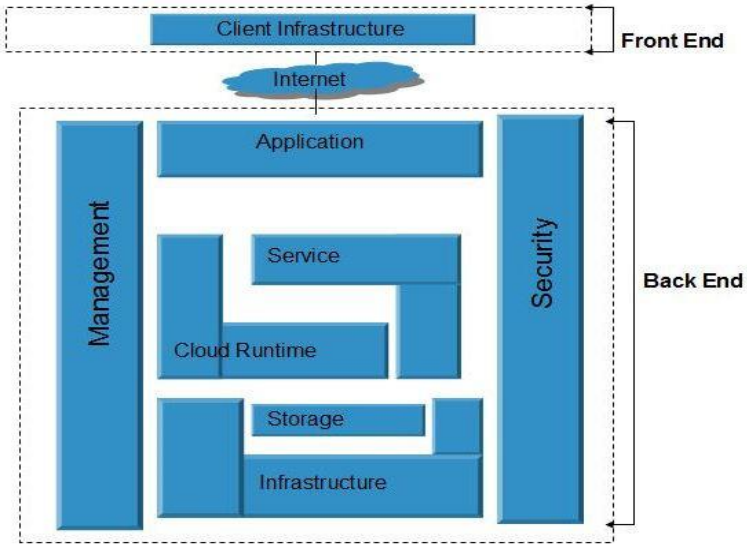

Figure 2: Cloud architecture

3. SERVICE MODELS

Cloud computing providers offer their services according to following fundamental models:

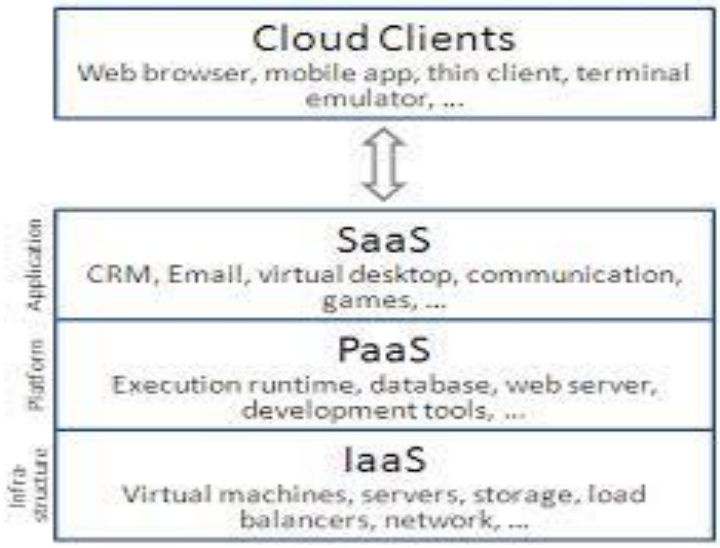

Figure 3: Service models level

Software as a Service (SaaS): Capability for clients to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client surface, such as web browser, or a program.

Platform as a Service (PaaS): Capability for clients to deploy their applications onto the cloud infrastructure, using programming languages, libraries, services, and tools supported by the provider.

Infrastructure as a service (IaaS): Capability for clients to utilize the provider's processing, storage, networks and other fundamental computing resources to deploy and run operating systems, applications and other software on cloud infrastructure.

The main difference between service levels relates to how control is shared between client and CSP, which in turn impacts the level of responsibility for both parties.

4. MODULES

The different modules are illustrated as follows:

1. Client Module: In this module, the client sends the query to the server. Based on the query the server sends the corresponding file to the client. Before this process, the client authorization step is involved. In the server side, it checks the client name and its password for security process. If it is satisfied and then received the queries form the client and search the corresponding files in the database. Finally, find that file and send to the client. If the server finds the intruder means, it set the alternative Path to those intruder.

2. System Module: Representative network architecture for cloud data storage is illustrated in Figure 4. Three different network entities can be identified as follows:

Cloud User: Stores data on cloud and depends upon cloud for all computation. User could be both individual consumer and organization.

Cloud Service Provide (CSP): It is the person who manages the whole service, data storage and lot more things of cloud computing like operating live cloud computing system.

Third Party Auditor (TPA): It is a person who has the capabilities and authority which users may not have. TPA is a trusted person to take a risk of cloud storage services on behalf of the users upon requests.

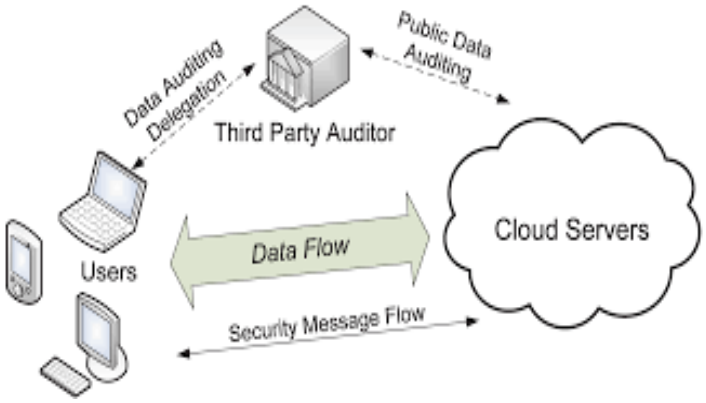

Figure 4: Network architecture

3. Cloud data storage Module: Cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. In case that users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead.

4. Cloud Authentication Server: The Authentication Server (AS) functions as any AS would with a few additional behaviors added to the typical client-authentication protocol. The first addition is the sending of the client authentication information to the masquerading router. The AS in this model also functions as a ticketing authority, controlling permissions on the application network. The other optional function that should be supported by the AS is the updating of client lists, causing a reduction in authentication time or even the removal of the client as a valid client depending upon the request

5. Unauthorized data modification and corruption module: One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance

6. Adversary Module: Security threats faced by cloud data storage can come from two different sources. On the one hand, a CSP can be self-interested, untrusted and possibly malicious. Not only does it desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data loss incident due to management errors, Byzantine failures and so on.

On the other hand, there may also exist an economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users' data while remaining undetected by CSPs for a certain period. Specifically, we consider two types of adversary with different levels of capability in this paper:

Weak Adversary: The adversary is interested in corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user.

Strong Adversary: This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident.

5. SECURITY THREATS

Security can be compromised both internally and externally. Attacks committed could be defined in two categories as follows:

Internal Attacks: These are initiated by malicious Cloud Service Provider (CSP) or malicious users. Those are intentionally corrupting the user's data inside the cloud by modifying or deleting. They are also able to obtain all the information and may leak it to outsiders.

External Attacks: These are initiated by unauthorized parties from outside the cloud. The external attacker, who is capable of comprising cloud servers and can access the user's data as long as they are internally consistent i.e. he may delete or modify the customer's data and may leaked the user private information.

6. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.

2. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.

3. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

REFERENCES

[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, Kui Ren, 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: Using Algebraic 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 Erasure coded Data," Proc. 26th ACM Symposium on Principles of Distributed Computing, pp. 139–146, 2007