Ensuring File Security In Private Cloud

Aishwarya Sundar[1], Adithi Narayanaswamy[2] and Kavitha Priyadarshini[3]

**[1,2,3] Department of Information Technology,
Jerusalem College of Engineering,
Chennai, Tamil Nadu, India**

Abstract

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management, thereby reducing the computational cost. This paper presents a modified approach for enhancing security for files in private cloud using distributed storage integrity auditing mechanism.Firstly,it involves the usage of a third party auditor which uses a token computation mechanism to ensure file integrity.Secondly,the cloud service provider computes a signature for each file that is being uploaded.Hence,homomorphic token verification is easily done to ensure that no modification has been made to the uploaded file.This paper specifically focuses in retrieving the original files in the case of distributed denial of service attack.It is also ensured that sufficient back up servers are employed in order to retrieve the original files in case of corruption without giving way to redundancy.Token verification mechanism is employed each time a user requests for a file download. In case the file is corrupted, it is retrieved from the back up servers and the original file is returned to the cloud users by the cloud service provider.

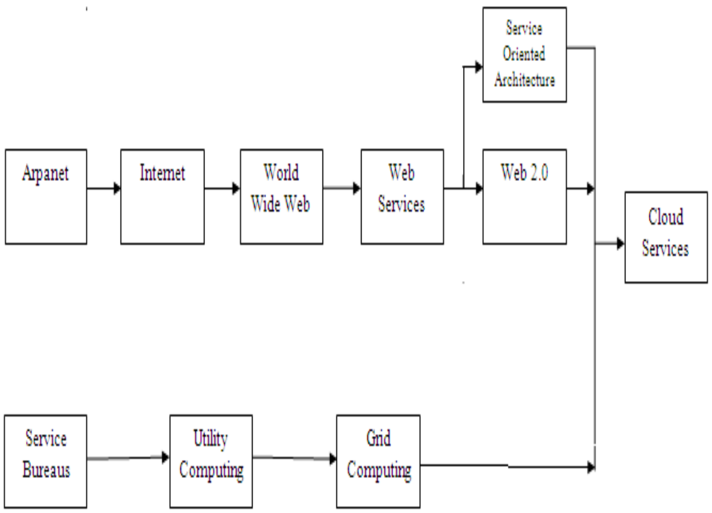
Keywords: *distributed storage, integrity auditing mechanism, signature, homomorphic token, token verification.*

1. Introduction

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. A simple example of cloud computing is Yahoo email or Gmail etc. You do not need software or a server to use them. All a consumer would need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc. The consumer gets to use the software as service and enjoy the benefits. Cloud computing is broken down into three segments: "applications," "platforms," and "infrastructure."

2. Origin of Cloud

The origin of cloud is given below as a flowchart.



Fig,1 Origin of cloud

2. Related Work

2.1 System Model

Network architecture for cloud storage service is illustrated in Fig. 2

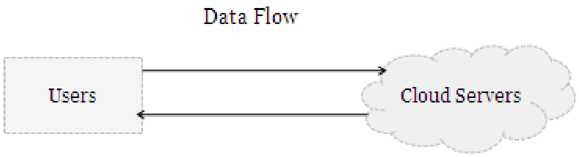


Fig.2. Cloud storage architecture

Two different network entities can be identified as follows:

User: An entity, who has data to be stored in the cloud and relies on the cloud for data storage & computation, can be either an enterprise or individual customers.
Cloud Server (CS): An entity, which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computational resources.

2.2 Related Issues

In the past, software had to be installed in an infrastructure close to end users.With the scheme employed in [1],there are no solutions provided for the following issues.
1. In the existing system, the correctness of cloud storage is not measured. When corruption occurs, only binary results will be provided regarding the security status of the file and the original information cannot be retrieved.
2. There are no recover methods present in the existing system. It is more advantageous for individual users to store their data across multiple physical servers so as to reduce the data integrity and availability threats.Thus, distributed protocols for storage correctness assurance will be of great importance in achieving robust and secure cloud storage systems.
3. There is no user data privacy provided.

3. Ensuring Cloud Data Storage

3.1 Cloud Architecture Design

The architecture that is used to overcome the problem of cloud data storage is represented below.

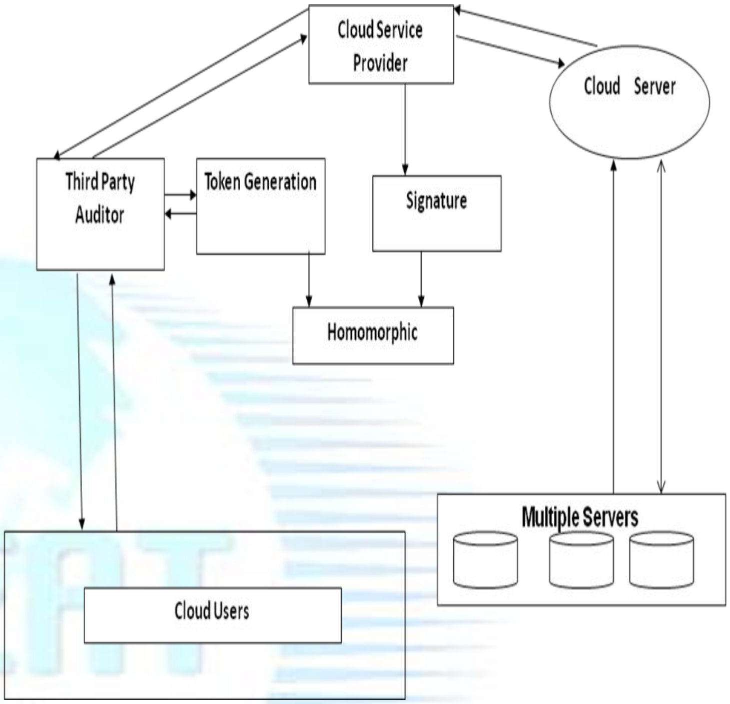


Fig.3 Ensuring cloud data storage

An additional entity named Third Party Auditor is made use of in our proposed work.
Third-Party Auditor (TPA): An entity, which 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. [5]

3.2 Proposed Work

Step 1: The user uploads his/her file to the cloud.
Step 2: A random file id number is generated and is made known to the user.
Step 3: The file is first forwarded to the TPA, which is managed by the Cloud Service Provider.
Step 4: The TPA will now compute a token for the particular file using the token generation algorithm[1].
Step 5: The TPA stores the generated token in its database and the file is sent to the CSP.
Step 6: The CSP now generates a signature using the same algorithm as employed for token generation.
Step 7: As the CSP manages more than one server, the CSP now stores the file and its corresponding signature in one main server and randomly in any of the alternate servers.

Step 8: The CSP uses only the main server for all purposes and the alternate servers that are restricted to the access of CSP alone is made use only in the case of file corruption.
Step 9: The user now sends a download request for a particular file using the file id.
Step 10: The CSP now searches for the file in its main server and sends it with the corresponding signature to the TPA.
Step 11: The TPA generates a token for the file and a comparison is made with the corresponding signature.
Step 12: If there is no mismatch, the file is directly sent to the user.
Step 13: Unauthorized users may try accessing the file of other users by making use of the file id of that particular file.
Step 14: Requesting the server over and over again for the same file leads to distributed denial of service(DDoS) attack.
Step 15: As a result of DDoS attack, the particular file gets corrupted leading to loss of data.
Step 13: Hence if a mismatch is found while comparing the token with signature, the TPA notifies the CSP regarding this and the CSP now retrieves the file from the alternate servers in which the file is stored.
Step 14: The file is then sent to the user after ensuring that there is no modification.

3.3 Algorithm Used

Token Generation Algorithm:

Step 1: Read the file from the first character till the end of the file is reached.
Step 2: Parse each string in the file as a token.White spaces are also parsed as tokens.
Step 3: The total number of tokens parsed till the end of the file is reached is generated as the token for that particular file.

4. Conclusion

The problem of data security in cloud data storage has been investigated and it poses a challenge for this internet based technology. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for the cloud users, we propose an effective and flexible distributed scheme which aids the emerging technology to overcome its challenging problem of security.

Acknowledgment

We thank with respect and gratitude Mrs.Marykutty Cyriac,Head Of Department of Information Technology,Jerusalem College of Engineering for extending her support and encouragement throughout this work.

References

[1]Cong Wang,Qian Wang,Kui Ren,Ning Cao and Wenjing Lou,"Towards Secure And Dependable Storage Services in Cloud Computing",IEEE Transactions on Service Computing,vol 5,no. 2,April-June 2012.
[2]Cong Wang,Qian Wang and Kui Ren,"Ensuring Data Storage Security in Cloud Computing",pp 1-9,July 2009.
[3]Zhiguo Wan Jun'e Liu and Robert H.Deng,"HASBE:A hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in cloud Computing",IEEE Transactions on Information Forensics and Security",vol 7,no. 2,April 2012.
[4]Amazon Web Services:Overview of Security Processes,September 2008.
[5]M.A.Shah,M.Baker,J.C.Mogul,and R.Swaminathan,"Auditing to keep Online Storage Services Honest",pp 1-6,2007.
[6] http://en.wikipedia.org/wiki/Cloud_computing.
[7]http://www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues
[8]http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf
[9]http://www.nist.gov/itl/csd/cloud-102511.cfm.