ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Cloud Data Security Using Third Party Auditing and Encryption

Alpesh D.Patil[1], Abhijit T. Sapkale[2], Bhushan D.Shimpi[3] , Archana K. Bhavsar[4]

UG Student, Department of Information Technology, Shram Sadhna Bombay Trust COET, Jalgaon, India[1,2,3]

Associate Professor, Department of Information Technology, Shram Sadhna Bombay Trust COET, Jalgaon, India[4]

Abstract: Security for the data which is stored on the cloud by user is very important issue. User may expect some security for their data from the cloud service provider, there can be serious issues regarding data security between user and service provider. To solve this kind of issues, we can use third party as an auditor. Here we have analyzed different ways to ensure secure data storage in cloud. We are going to provide the security to the user's data by using encryption technique. For this we are using the Advanced Encryption Standard algorithm for encryption and decryption. But when Cloud Service Provider has both encryption and decryption keys, there is threat to security and privacy of data. CSP may pass the user data without user's knowledge. For auditing we are introducing Third Party Auditor. Here the data will be encrypted at user side and will be in encrypted form over network and to TPA. TPA will verify the data before storing it on the cloud. There are large numbers of users of cloud computing who are accessing and modifying the data and they need the reliable service provider who can provide complete security for their data. So the TPA will audit the data and check the data integrity of client's data. No one else rather than user is able to view data. But if someone tries to access the data, and then there will be a file alert generated to the user. Hence user will have more elaborated view over his data privacy. In this paper we are providing solution for the user who needs security and privacy for their data.

Keywords: Third Party Auditor (TPA), Cloud Service Provider (CSP), Data Integrity, Encryption.

I. INTRODUCTION

In last few years, the emerging cloud-computing technology is rapidly growing as an alternative for orthodox information technology. Basically cloud computing is a simple concept, here the cloud user will store his data on the server. The cloud service provider will give some space on server for the user to store his data. The concept of cloud-computing is very useful when user does not want to possess the data physically and want to have access to data wherever when required. For example if I want to store the data then I will sign up cloud account and store my data, and can access and modify data by using my cloud account. Here we are providing the solution to the problem of security and privacy of data by introducing Third Party Auditor. The TPA will check the data integrity weather the data uploaded by the user is correct or not. We just have to select a trusted TPA.

In some cases the attacker might alter the data over the network. Hence we are providing the encryption to user data so that there will be encrypted data on the network and cloud. No one else has viewing privileges of user file than user. If someone tries to do so, then a file alert will be generated to the user. Also we are providing Software as a Service to the user in which user can use the application that resides on the cloud.

The user will also have the record of all the files that he will upload and update. And the admin has authority to see which user id uploaded which kind of file along with file status and file type but has no authority to alter the user data. This introduced concept will provide a better service for user about his data security and integrity.

II. LITERATURE SURVEY

We know Literature survey is one of the most important stag and plays main role in software development process. In that cloud computing is very hot issue now days. Cloud computing is nothing but the combination of different entities like software, data which are accessible by using internet. We can say that cloud is nothing but internet [1]. Client data is mainly stored in banks of server. Before cloud computing people were storing there data in data centre with some important security techniques to protect their confidential data. Day by day people data is increasing for that data storing space is not enough. The client has less control over the stored data. We can use cloud computing for that to build the trust on cloud computing the cloud providers should protect the user data from illegal access. There are many techniques to provide security to user confidential data out of them security Services like computing hash, encryption/decryption service. The cloud service is totally browser base, therefore any browser enabled Device like desktop, smart phones and laptop etc. can use to access these services. There are different cloud layers and cloud computing architecture is partitioned into following layers

- Front end
- Back-end
- The network

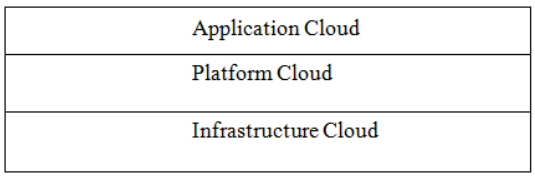

Fig. 1 Layer of Cloud

DOI 10.17148/IJARCCE.2015.4327

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

This client communicates with cloud data by using an application that is accessible via browser.
Following are different cloud service models

- Software as a Service (SaaS):

In Software as a Service clients use software service provided by cloud provider by using web browser. The Software as a Service is the application layer. The managements of different applications this is the responsibilities of cloud provider.

- Platform as a Service (PaaS):

The Platform as a Service is the platform layer. This PasS layer provides a platform for creating application.

- Infrastructure as a Service (IaaS):

The Infrastructure as a Service is the Infrastructure layer. No need to purchase or manage physical data centre equipment. The client can deploy and execute his application using this infrastructure.

A. Security issues in cloud

We know there are many security issues related cloud computing. There is big issue about privacy in cloud, because administrator can access data stored in cloud and he can modify this data or access this client data, also administrators can access our data intentionally or unintentionally[3]. Traditional Security or protection techniques need to consider again, with a view to changing a decision for cloud. Security issues in clouds which are of concern to the client and these are classified into, data keep separate from others, confidential data access, recovery, accountability, account control issues, bug exploitation. For different cloud security issues have different types of solutions are available. If you want to provide solution there are solution like you can use more than one cloud provider, treaty between client and cloud provider etc. Also the Cloud Service Provider may pass or delete user data without user's permission. When auditing is done by CSP then privacy of user's data may be compromised.
Now when we introduce the Third Party Auditor, it creates issue whether to trust them or not. Users have the query to resolve the data incontinency and how to trust the TPA. If TPA become intruder and delete or pass user data, then how user will come to know about it is a problem. TPA needs to be a trusted party from user side as they are responsible for data consistency. Encryption may help in this issue. An encrypted data file will be there to TPA. We can also give least permissions to the TPA for user data. Hence TPA may not cause any manipulation to user data.
TPA checks integrity of data on behalf of user[1].

III. PROBLEM DEFINITION

Cloud services increased drastically and with this growth they brought up the problem related to data security and data integrity. The clients are also concerned about the sharing of data with specific addressed group of people. These issues can be solved by encrypting data before storing it on cloud, and sharing the key to decrypt it. But this becomes more tedious for client to share data in this way by storing data and later keys for sharing. Also same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, can have use of both services for maintenance, hence the information might be compromised by the cloud service provider. This violates the privacy expectations of clients. Also if the cloud service provider has the work of encryption and decryption then it slows down the process and adds time to the completion of process.
Hence a third party can be involved which will be dedicated to the auditing process only, without having any kind off access to the data. This solves the issue of data integrity. And encryption service can be implemented through Advanced Encryption Standard algorithm. For the cloud service provider's perspective, we can add the alerts for file update so that user won't deny it. Also the data could be shared by to some addressable group of people.

IV. IMPLEMENTATION

Implementation involves turning the theoretical design into a practical system. Hence it is considered as an important stage for success of project. Concepts in the design phase are interpreted to produce a working model. The implementation stage constitutes proper planning, thorough investigation of the existing system and it's constraints on implementation, designing of methods to achieve the required output. As shown in figure 2, TPA will be an intermediate between user and CSP.

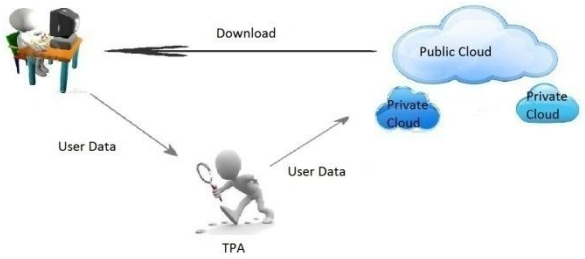

Fig. 2. TPA's role.

A. Data Storage Service System

In this module, we considered FOUR entities to store the data in secure manner:

- Data owner (DO)

Data owner has ample of data to be stored on the cloud and can access it when required.

- Cloud service provider (CSP)

CSP has enough memory storage space that he provides to store data owner's data,. CSP also have computation resources and applications that manipulate data.

- Third party auditor (TPA)

TPA has capabilities to manage or monitor – outsourced data under the delegation of data owner.

- Granted applications (GA)

GA is applications that may reside inside or outside cloud to perform data manipulation. These applications are also used to provide services to user.
User uploads the file where it is encrypted before going over the network. This reduces the risk of data theft on network breach. The file in encrypted format is not uploaded to the cloud directly; it is forwarded to the TPA system for verification. Until and unless TPA verifies the file, user does not see the upload status.

DOI 10.17148/IJARCCE.2015.4327

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

B. Third Party Audit Service System

In this module, Third Party Auditor is involved after the user uploads the file. The file uploaded to cloud comes to TPA first where it verifies the file and forward it to the cloud where it is uploaded on user storage space. TPA also generates the upload alerts and update alerts for user files. For preserving the data integrity and security, we provide the soundness property and zero-knowledge property of proof systems. Due to these properties we can ensure that our system not only prevents forgery of cloud service providers but also reduce chances of data leakage during verification.

C. Software as a Service

In this module, there will be one application that will reside and configured on cloud and will be used by users as per their requirement. Due to this, users do not have to have the software with them all time, they will use it when they require. Here we are using Mail Manager Application to demonstrate software as a service on cloud. In this application, users can access account from Gmail, Yahoo & Hotmail and send mail by specifying the time to send it.

D. User Log.

In this module, we will provide the alerts for user's file. When someone else rather than user tries to access of update the file, then alert for this will be send in form of Log to the user. This will keep surveillance on user files and keep the privacy of data.

V. CONCLUSION

We addressed the construction of an efficient audit service for data integrity in clouds. We proposed an interactive audit protocol to implement the audit service based on a third party auditor. In this module, the third party auditor acts as an agent of data owners. Third party auditor performs periodic verification to monitor the data transfer by providing an optimized schedule. As auditor doesn't demand local copy of data and it's in encrypted form, hence it does not bring any new vulnerability towards data privacy and integrity. We only need to maintain the security over the third party auditor to ensure the privacy and security issues.

Hence, our concept can be easily adopted in a cloud computing. This approach minimizes the workload of the cloud service providers, while it still tends to successfully detect misbehaviour of cloud service providers with a high probability.

REFERENCES

[1] Ashish Bhagat, Ravi Kant Sahu, "Using Third Party Auditor for Cloud Data Security: A Review" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013

[2] Elsenpeter Robert, Anthony T.Velte and Toby J.Velte, Cloud Computing a Practical Approach 2010. K. Elissa, "An Overview of Decision Theory," unpublished. (Unplublished manuscript)

[3] Qian Wang and Cong Wang and Kui Ren, Wenjing Lou, Jin Li "Enabling Public Auditability And Data Dynamics For Storage Security in Cloud Computing" in IEEE transactions on parallel and distributed systems, 2011, vol. 22, no. 5.

[4] Cong Wang and Kui Ren and Wenjing Lou and Jin Li,"Toward Publicly Auditable Secure Cloud Data Storage Services" in IEEE, 2010.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[6] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[7] N. Bonvin, T. G. Papaioannou, and K. Aberer, "Cost-efficient and differentiated data availability guarantees in data clouds," in Proc. of the ICDE, Long Beach, CA, USA, 2010.