International Journal of Information Technology & Management Information System (IJITMIS)
Volume 6, Issue 2, July-December-2015, pp. 44-48, Article ID: IJITMIS_06_02_007
Available online at
http://http://www.iaeme.com/issue.asp?JType=IJITMIS&VType=6&IType=2
ISSN Print: 0976 – 6405 and ISSN Online: 0976 – 6413

SECURED DATA STORAGE IN CLOUD

Abhishek Pandey
Dr. C. V. Raman University, Kota, Bilaspur, India

Dr. R. M. Tugnayat
SSA College of Engineering, Wardha, Maharastra, India

Dr. A. K. Tiwari
Disha College, Raipur, India

ABSTRACT

Cloud Computing has attracted people from all arenas whether it be academics or industry for last decade. The basic objective is to provide users more supple services in a transparent manner, all services are allocated in a "cloud" is a combination of devices and resources connected across the Internet. The primary services provided by cloud computing is data storage. The challenge here is to secure the data stored in cloud and examine the facilities provided the end users.

The idea of this work is that cloud data storage should protect the data from an unauthorized access giving rise to various threats. Due to the nature of the cloud the data stored here is exposed to various threats resulting in data loss, incorrect data and possibility that it may be disclosed. The proposed work emphasizes on security issues evaluates how the use of different cryptographic methods will secure the data in cloud networks. The security can be achieved by securing the data in the cloud during transmission and storage with the use of various encryption algorithms whether it be symmetric or asymmetric.

Key words: Cloud, Cryptography, Message Digest, SSL, Security.

Cite this Article: Abhishek Pandey, Dr. R. M. Tignayat and Dr. A. K. Tiwari. Secured Data Storage In Cloud. *International Journal of Information Technology & Management Information System (IJITMIS)*, **6**(2), 2015, pp. 44-48.
http://www.iaeme.com/issue.asp?JType=IJITMIS&VType=6&IType=2

1. INTRODUCTION

The use of network based applications have transformed from server oriented storage architecture to a distributed one. Also we are aware of the fact that the information security is the primary concern in cloud network. However, this research in cloud computing security is still in its initial stages. The only consideration is that the unique issues linked with cloud security have not been recognized. Many still have an opinion that cloud security can be answered with the existing cryptographic techniques.

The other security issues are yet to be identified related to cloud, making cloud security an important area of research. The cloud service providers and the agencies have raised various threats on the security in the cloud computing model. There are two primary concerns when using the cloud. First is that the users do not want to expose their data to the cloud service provider. Another issue lies in the fact that users are not very certain about the integrity of the data they receive from the cloud. Hence we need to provide a security mechanism within the cloud for the security of the data.

2. SECURED DATA STORAGE USING CRYPTOGRAPHIC TECHNIQUES

The data storage is primary concern in this type of architecture as they are always open to threats and also the fact that the basic property of cloud also adds to this. We are aware that the cloud is often termed as boundary less network as it is extended over the internet for offering different services to its user. We will try to reconstruct the entire service model to have a broader idea of operations related to cloud, mainly the data storage. Here each transaction can be viewed as single session , wherein the user creates a file for the desired service to be obtained and adds the signature to it before transmission , on the other hand the service provider verify the request and the signature associated with it . Once this is done it adds up encryption method to the associated file and transfers it with the Message Digest MD5 in this case. For better understanding of the approach we have modelled the entire scenario as depicted below:

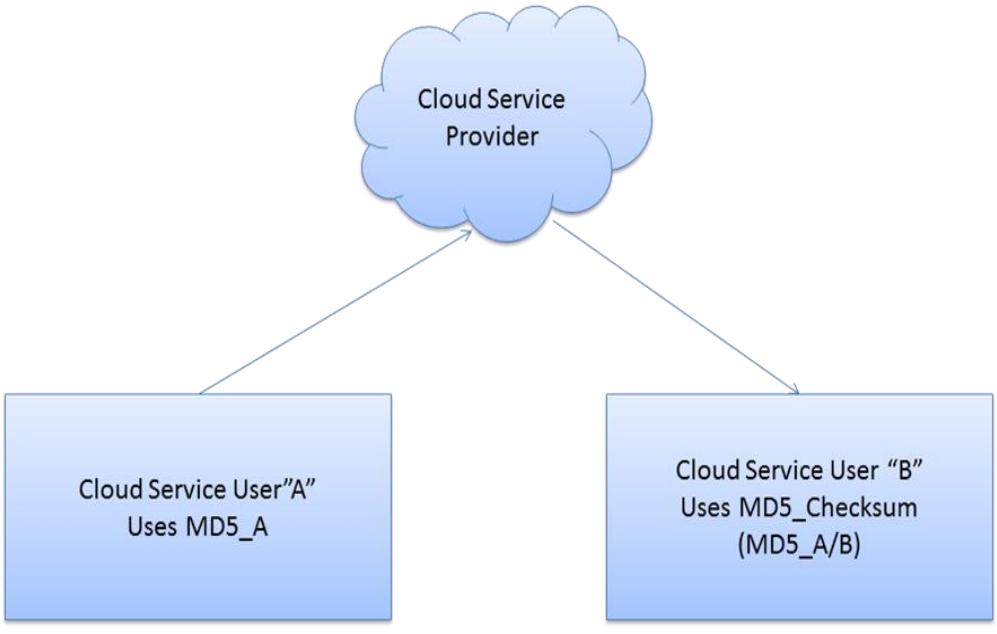

Figure 2.1 Capturing Cloud Integrity Issue

As shown in Figure 2.1, here USER A stores the data in the cloud along with the Message Digest MD5_A. The data is transferred and stored using the checksum MD5_A which ensure all the security attributes like confidentiality, Integrity and Authenticity of the data. On the receiving end the USER B gets the data along with the MD5_Cheksumnwhich is stored along with it and embedded with the message. On receiving the request for retrieval of the data stored by "A", the cloud service provider transfers the data along with the checksum MD5_A and a recomputed checksum MD5_A/B. The attribute related to integrity is achieved using the Secured Socket Layer (SSL) during the transmission of data over the cloud. In the cloud environment however it is maintained even when the data is stored at the providers end and while transmission of data be it uploading or downloading [1, 2].

An Enhanced Data Possession Checking Protocol [4, 5, 6, 7, 8] does not guarantee the storage as required with highest probability. In figure 2.2 (a) and (b) protocol for provable data possession [3,5] depicts the flow of protocol for the valid data. Here the data owner executes the protocol for verification of the data stored at the providers end and prior to uploading of the data into the providers end which is a remote storage in this case , the user pre-processes the data set and a new data set is generated. This new set of data is stored at the users end and the same will be transmitted to the server. The Cloud provider stores the data and transmits it to the user in response to its queries. Other operations related to this data set whether it be operation on the data to be performed, hence gives us a fair chance of data integrity. This is based on the fact that during the time data are stored in the cloud the user can generate a "Challenge" and send it to the provider to ensure the integrity of the data.

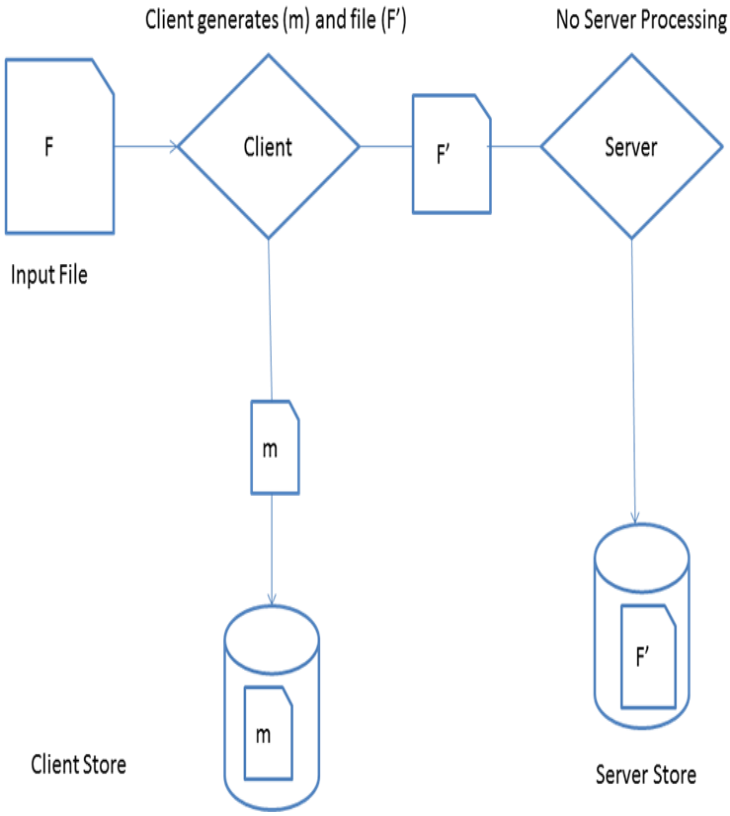

Figure 2.2 (a) Pre-Process and Store

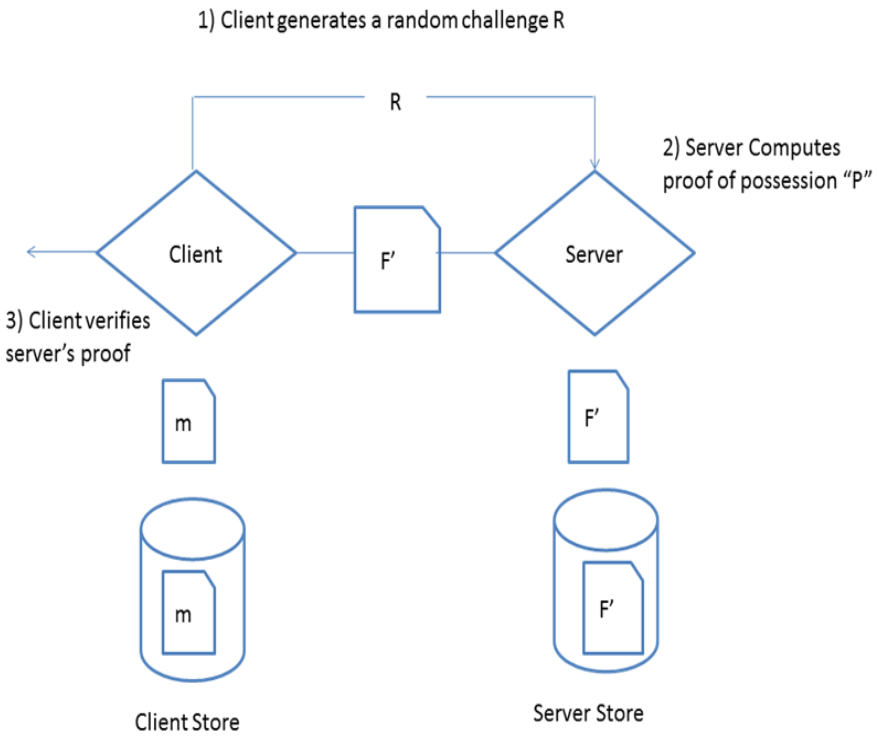

Figure 2.2 (b) Verify Server Possession

3. EVALUATION

The problem in cloud environment is the fact that it does not guarantee the integrity of the data stored. This can be illustrated as if USER B wants to retrieve the data stored by USER A which is through service provider , let it be "C", then to issue of confidentiality arises where "A" and "B" does not wants the information to be shared or revealed to "C". The integrity also is compromised as "B" is not sure that the information retrieved from "A" is as it was stored and "C" has not played with it. This issue can be handled and confidentiality can also be achieved by robust encryption techniques. The SSL here only guarantees one way integrity. The major issue lies while storing and retrieving the data from and to the cloud environment. There is no mechanism to check that the data is not being modified in cloud storage. To eliminate this problem we propose a Third Party Authentication (TPA) mechanism to which the service provider and the user agrees upon to make it more effective. This scheme can be elaborated as:

Storing Session

1. USER A sends the data to the cloud provider using MD5 along with the signature attached to it.
2. At the cloud storage the provider verifies the data with the checksum and verifies about the correctness of the same.
3. It then returns the MD5 signature by the providing the same to USER A
4. The user and the provider then send the checksum to TPA, in turn it checks and verifies MD5 values on finding it correct it distributes MD5 to the user along with Private Key Sharing (PKS) which is nothing but the private key for that session.

Retrieving Session

1. USER A send the request to the provider with the desired authentication code.
2. The provider then verifies the signature associated using the Checksum and returns the desired data.
3. User verifies the data through the MD5 checksum.

When the service provider is trustworthy, only the user needs the MD5 checksum; when the user is trustworthy, only the service provider needs MD5 checksum; if both of them can be trusted, the TPA is not required. This proving a secured approach for cloud computing networks.

4. CONCLUSION

This paper provides an insight to the security measures in storing data in the cloud. We have compared a scenario of cloud storage with the help of third party authenticator to the data stored at the providers end. Here we have used a cryptographic technique such as Message Digest 5 and appending the checksum while storing and retrieving the d ata from the cloud for each session.

REFERENCES

[1] T. S. J. Schwarz and E. L. Miller, “Store, forget, and check: Using algebraic signatures to check remotely administered storage”, In Proceedings of ICDCS ’06. IEEE Computer Society, (2006).

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson and D. Song, “Remote data checking using provable data possession”, In Proceedings of ACM Trans. Inf. Syst. Secur., (2011), pp. 12-12.

[3] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson and D. X. Song, "Provable data possession at untrusted stores", in Proc. ACM Conference on Computer and Communications Security, (2007), pp. 598-609.

[4] C. Hanser and D. Slamanig, “Efficient Simultaneous Privately and Publicly Verifiable Robust Provable Data Possession from Elliptic Curves", presented at IACR Cryptology ePrint Archive, (2013), pp. 392-392.

[5] F. Sebe, A. Martinez-Balleste, Y. Deswarte, J. Domingo-Ferrer and J.-J. Quisquater, “Time-bounded remote file integrity checking, Technical Report 04429, LAAS, (2004) July.

[6] Y. Deswarte, J.-J. Quisquater and A. Saidane, “Remote integrity checking”, In Proc. of Conference on Integrity and Internal Control in Information Systems (IICIS’03), (2003) November

[7] Y. Zhu, H. Wang, Z. Hu, G. Ahn, H. Hu and S. S. Yau, “Efficient provable data possession for hybrid clouds”, In Proceedings of ACM Conference on Computer and Communications Security, (2010), pp. 756-758.

[8] P. Golle, S. Jarecki and I. Mironov, “Cryptographic primitives enforcing communication and storage complexity”, In Financial Cryptography, (2002), pp. 120–135.

[9] D. Pratiba and Dr. G. Shobha. Privacy-Preserving Public Auditing For Data Storage Security In Cloud Computing. *International Journal of Computer Engineering and Technology*, **4**(3), 2013, pp. 441 - 448.