Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of Cloud storage Security Mechanism using Digital Signature

Ashwini Bansode
PG Scholar CIIT, Indore
Madhya Pradesh, India

Megha Singh
Asst. Professor, CIIT Indore
Madhya Pradesh, India

***Abstract*— Data and computation integrity and security are major concerns for users of cloud computing facilities. Today's clouds typically place centralized, universal trust in all the cloud's nodes. This simplistic, full-trust model has the negative consequence of amplifying potential damage from node compromises, leaving such clouds vulnerable to myriad attacks. Unfortunately, adopting cloud computing has required users to cede control of their data to cloud providers, and a malicious provider could compromise the data's confidentiality and integrity. In this paper presents implementation of the cloud storage security mechanism that helps to secure data and provide better security form unwanted attack.**

***Keywords*— Chunks, TPA, MD5, Cloud Storage, Security**

I. INTRODUCTION

The past decade has seen the rise of cloud computing [1], an arrangement in which businesses and individual users utilize the hardware, storage, and software of third party companies called cloud providers instead of running their own computing infrastructure. Cloud computing offers users the illusion of having infinite computing resources, of which they can use as much or as little as they need, without having to concern themselves with precisely how those resources are provided or maintained [6]. Cloud computing encompasses a wide range of services that vary according to the degree to which they abstract away the details of the underlying hardware and software from users. More specifically, cloud computing offers users the following benefits:

1) *Scalability:* To operate their own computing infrastructure, users must make a fixed up-front investment in hardware and software. If the demands on their systems later increase, they must invest in additional resources and bear the burden of integrating them with their existing infrastructure.
2) *Availability, reliability, and global accessibility:* Because cloud providers are in the business of offering computing resources to many customers they typically have greater expertise in managing systems and benefit from greater economies of scale than their users.
3) *Maintainability and convenience:* By abstracting away the details of the underlying hardware, and in some cases, the software, cloud providers free users from having to maintain those resources.

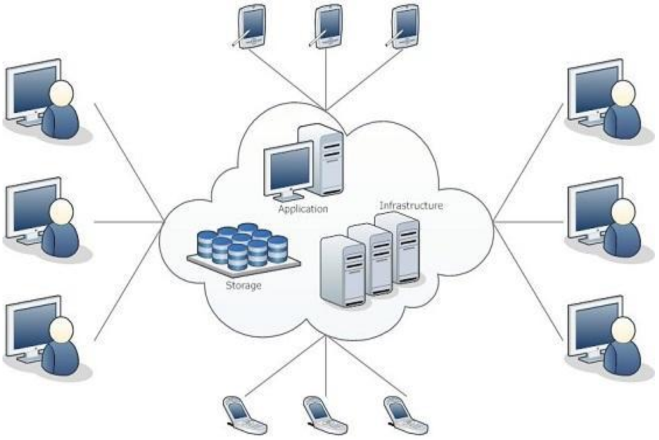


Fig 1 Cloud Computing Model

A. *Participants:*

In a cloud-model there are four main participants:[1][6][12]

1) *Cloud Provider:* A cloud provider (service provider) is an entity that is responsible for everything required for making a cloud service available.
2) *Cloud Consumer:* A cloud consumer is either a cloud service owner or a cloud service consumer. Cloud service owner is the individual or organization who subscribes for a cloud service. If there is any charge associated with the

service, the cloud service owner will be responsible for the bills. Cloud service consumer is an individual or application who accesses a cloud service.

3) *Cloud Broker:* A cloud broker is an entity that mediates between cloud providers and cloud consumers. The goal of a service broker is to provide the cloud consumer a service that is more suitable for its needs. This can be done by simplifying and improving the service and contract, aggregating multiple cloud services or providing value-added services. One can consider cloud brokers as a special cloud provider.
4) *Cloud Auditor:* A cloud auditor is an independent party who examines a cloud service stack to provide an assessment on security, privacy and availability level of the corresponding cloud services and ensures that the corresponding SLAs (Service Level Agreement) are fulfilled. The details and scope of auditing process is normally specified in the service contract.

B. Isolation Levels:

With respect to deployment model and isolation levels, clouds can be categorized into the following four categories:

1) Public Cloud: A public cloud is a cloud that its infrastructure is shared by many mutually untrusted cloud consumers.
2) Private Cloud: If the infrastructure of a cloud is dedicated to a specific organization, we refer to that cloud as a private cloud. A private cloud can be on or off premise.
3) Community Clouds: Community clouds are clouds that their services are accessible to a particular set of organizations which form a community. Community clouds can all be on or off premises.
4) Hybrid Clouds: A cloud that is a composition of two or more types of clouds is called hybrid cloud. These types of clouds are becoming increasingly more popular. Integration of these clouds poses some security challenges which we discuss in this chapter.[6][12]

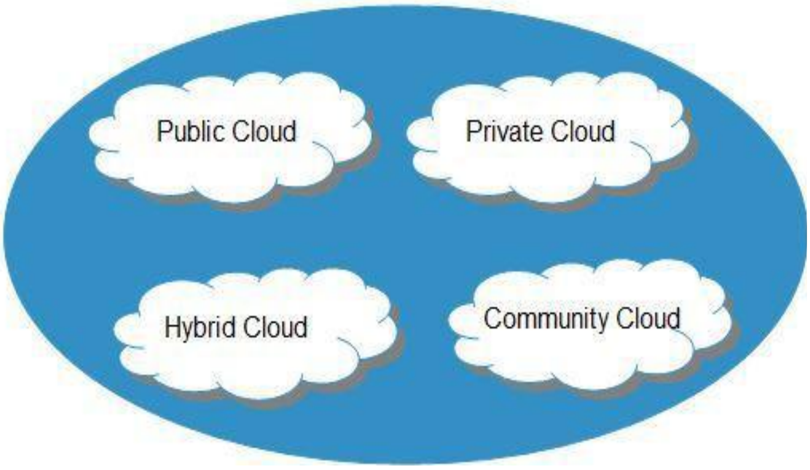


Fig 2 Categories of Cloud

II. LITERATURE REIVIEW

Shobha Rajak et. al. [2012] proposed a model for the integrity check over the cloud computing and we utilize the TPA and digital signature to achieve the integrity concept, in such a way to help the user to verify and examine the data from unauthorized people that manipulate with the cloud or extract from the data. Moreover, we are able to evaluate our work using a windows azure project that involves digital signature coding. As results, we found that our model worked well according to our claims. The approach used for the encryption in the verification process was the digital signature. In the implementation we used as an example of the client data in the cloud a text entered by the client, this research is not covering other various kinds of client data.

Faraz Fatemi Moghaddam et. al. [2013] presents hybrid asymmetric-key encryption algorithm has been suggested based on RSA Small-e and Efficient RSA according to the security issues in cloud computing environments [12]. In the proposed algorithm, the number of exponents has been increased to three and a dual encryption process has been applied to raise the security level of the algorithm in comparison of original RSA. According the simulation results, the total execution time in HE-RSA was increased up to approximately 50 percent less than the original RSA and this increase may be reasonable and acceptable according to the security level and the efficiency of HE-RSA.

Padmapriya et al.[2013] presents In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability among others. This paper analyses the importance of security to cloud. We compared three algorithms namely Data Encryption Standard (DES), RSA, Homomorphic encryption for data security in cloud. They are compared based on four characters; key used scalability, security applied to, and authentication type.

III. SYSTEM ARCHITECHTURE

Our security analysis focuses on the adversary model as defined. We also evaluate the efficiency of our Scheme via implementation of both file distribution preparation and verification token precomputation. In our scheme, servers are required to operate on specified rows in each correctness, verification for the calculation of requested token.

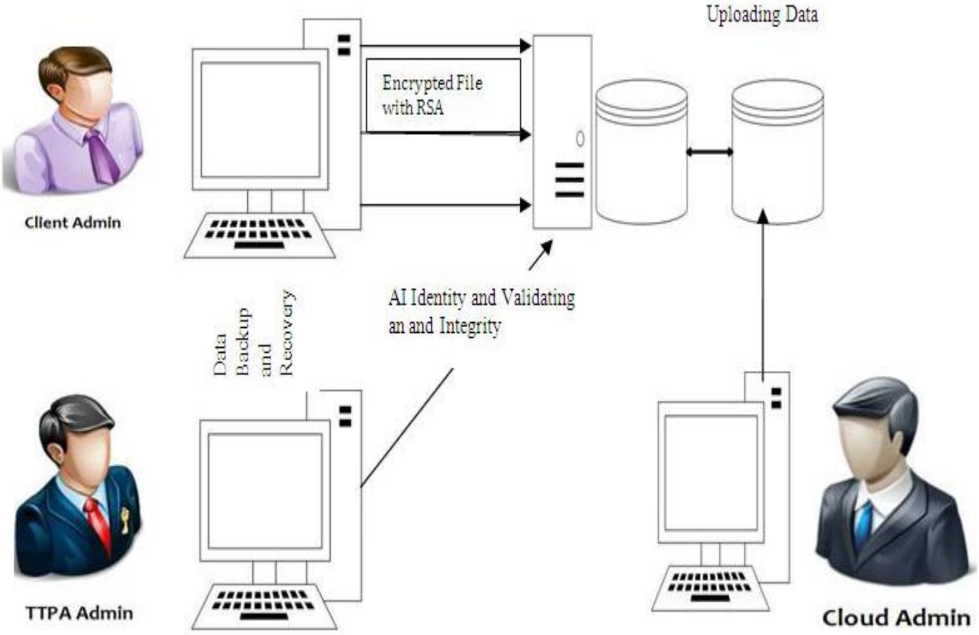


Fig. 3 System Architecture

For maintaining data confidentiality and integrity, the responsibilities of client admin are as follows:

A. Uploading Steps:-

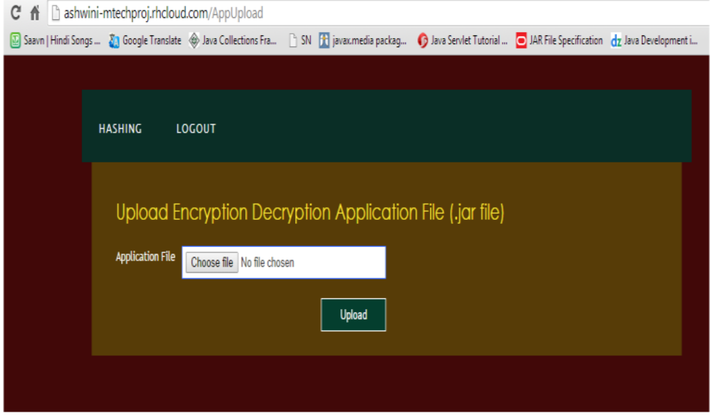
1) Each user logs on to the workstation using an own ID and Password.
2) No of user connected to a storage array via network.
3) The client computer sends a request to the storage array for storing a file.
4) This file is encrypted by two times.
   - At the time of transferring RSA works which will be encrypt our data.
   - And the second one is MD5 that will be work in data storage array.
5) MD5 need because, threats at storage level include tampering with data, which violates data integrity, and media theft, which compromises data availability and confidentiality.

B. Downloading Steps:-

1) When the client sends a request form a server, it sends a request, consist of valid ID and Password.
2) The storage array checks the permission and ensures that the user is authorized to use that service.
3) If user is authorized then reply the client machine and give respond.
4) The client computer sends the desired file name that want to access.
5) The storage array decrypts the file and the server automatically allows the client to access the appropriate resources.

IV. IMPLIMANTATION

The process is initiated from client admin with the generation of private and public keys by requesting the cloud server. Let us examine a simple scenario.[12] For instance client admin wants to store a file named as Backup.*txt* containing organization's employees' confidential records at the cloud storage. Cloud server requires the file and the public key for encryption process as represented in Fig. 4.

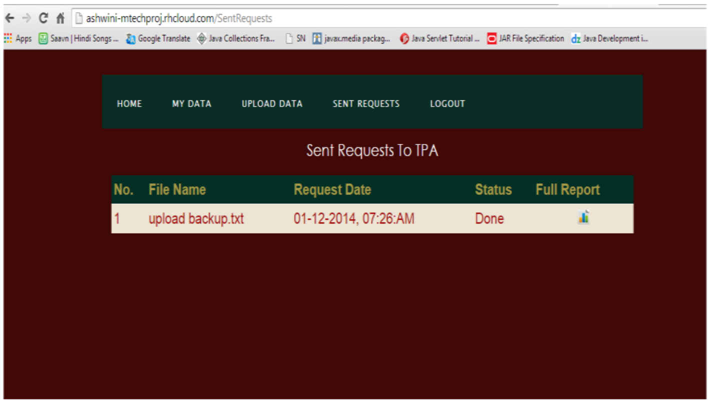


ashwini-mtechproj.rhcloud.com/AppUpload

Upload Encryption Decryption Application File (.jar file)

Application File: No file chosen

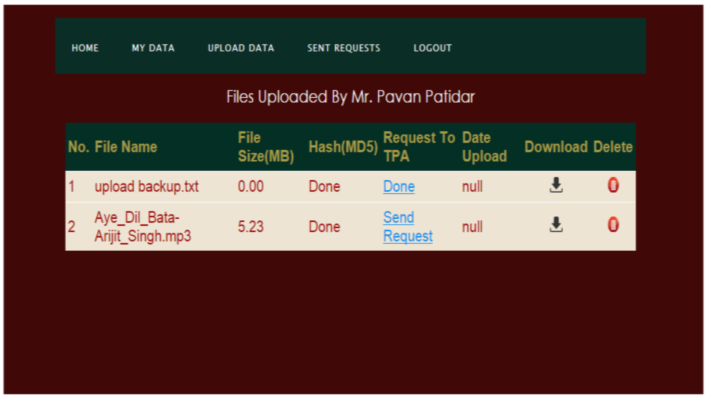
Fig. 4. Upload Encryption & Decryption File



Sent Requests To TPA

No.	File Name	Request Date	Status	Full Report
1	upload backup.txt	01-12-2014, 07:26:AM	Done	

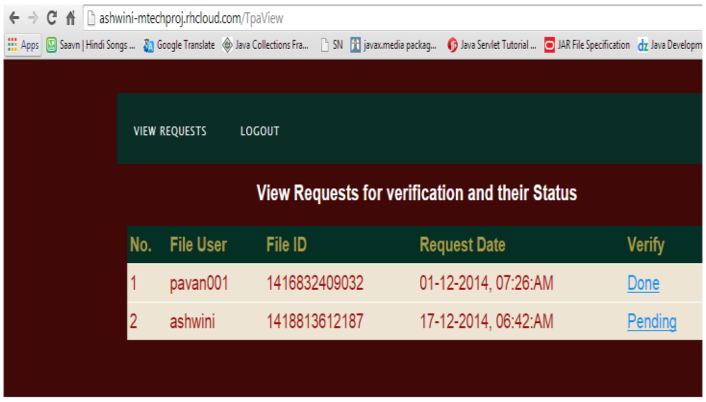
Fig. 5. Sent Request to TPA



Files Uploaded By Mr. Pavan Patidar

No.	File Name	File Size(MB)	Hash(MD5)	Request To TPA	Date Upload	Download	Delete
1	upload backup.txt	0.00	Done	Done	null	⬇	0
2	Aye_Dil_Bata-Arijit_Singh.mp3	5.23	Done	Send Request	null	⬇	0

Fig. 8. User Uploaded Data view



View Requests for verification and their Status

No.	File User	File ID	Request Date	Verify
1	pavan001	1416832409032	01-12-2014, 07:26:AM	Done
2	ashwini	1418813612187	17-12-2014, 06:42:AM	Pending

Fig. 9. View Incoming Request for Data Audit

For the verification of the data user or cloud sent request to the TPA shows in fig 5. After that Hash code generated with the help of the user reference data in the fig 6. Then if the hash code is valid then it generates the verification report that shows the valid user shows in fig 7. At the end user view their uploaded data list in fig 8.

V. RESULTS

During the experiments, we identified that client's privacy always remains intact despite the attacks launched by several malicious users. For-example if an expert hacker is able to attack the data during the transfer (downloading, uploading) or at the storage it doesn't affects the privacy because before data departs from the client it gets and remains encrypted throughout the entire process even when it is stored or processed at cloud storage. When attackers get access, they are not able to get any meaningful information just beside the cipher text and if an attacker violates the integrity at physical cloud storage, it is immediately identified during the auditing process and data is recovered back to its original state from the backup storage. Similarly when, TTPA admin wants to extract the private key of client, attacker will not be able to decrypt it because it is encrypted as sound.[12] Also if attacker gets the private key, attacker cannot decipher the client's data, since for decryption, system must perform the decrypt process and this task can only be initiated by the client when successfully logs in with required credentials. Un-authorized users cannot perform any operation, even if they break-in security of login menu they need to request for random security code and the code can be only sent to privileged users under the implemented RBAC. We concluded that using the proposed technique, besides the threatening attacks, client's privacy i.e., data confidentiality and integrity is preserved at off-premises cloud computing storage.

VI. CONCLUSION

The process such as the data owner can check the integrity of their data stored in cloud server using TPA which can be done in efficient manner. If any modifications find out by the TPA, TPA will immediately intimate to the owner of the file and so security and data integrity is secured properly.TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Cloud data security is an important aspect for the client while using cloud services. Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client.

REFERENCES

[1] Peter Mell and Timothy Grance. NIST special publication 800-145: The NIST de_nition of cloud computing.http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, September 2011.

[2] Adrian, D., S. Creese and M. Goldsmith, 2012. Insider attacks in cloud computing. Proceedings of 11th International Conference on Trust, Security and Privacy in Computing and Communications, Jun. 25-27, IEEE Xplore Press, England, pp: 857-862. DOI: 10.1109/TrustCom.2012.188

[3] Ateniese, G., R. Burns, R. Curtmola, J. Herring and L. Kissner et al., 2007. Provable data possession at untrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security, Oct. 29-Nov. 02, ACM Press, USA., pp: 598-609. DOI: 10.1145/1315245.1315318

[4] D. and G. Hogben, 2009. Benefits, Risks and Recommendations for Information Security. CSA, 2011. Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. USA.Francisco, R., S. Abreu and M. Correia, 2011. The final frontier: Confidentiality and privacy in the cloud. Computer, 44: 44-50. DOI: 10.1109/MC.2011.223

[5] Cong Wang, Sherman S.M.Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage", IEEE , Vol.62 , No. 2,February 2013.

[6] C.Wang, Q.Wang, K.Ren, and W.Lou, "Privacy Preserving Public Auditing for Storage Security in Cloud Computing", IEEE INFOCOM'10, March 2010.

[7] A.Juels and J.Burton, S.Kaliski, "PORs: Proof Of Retrieviability for Large Files", Proc. ACM Conf. Computer and Comm. Security(CCS'07), pp.584-597, October 2007.

[8] Dr.Sunitha Abburu, Saranya Eswaran, "Identifying Data Integrity in the Cloud Storage", IJCSI, Vol.9, Issue 2,No. 1, March 2012.

[9] Prof.R.Dheenadayalu, M.Sowparnika, "Improving Data Integrity on Cloud Storage Services", IJESI, Vol.2,Issue 2, February 2013.

[10] 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.

[11] Shobha Rajak, Ashok Verma " Secure Data Storage in cloud using Digital Signature Mechanism" International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012.

[12] Faraz Fatemi Moghaddam, Maen T. Alrashdan, and Omidreza Karimi "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments" Journal of Advances in Computer Network, Vol. 1, No. 3, September 2013.

[13] A. Rajathi, N. Saravanan ... Balakrishnan S, Saranya G, et al. (2011) Deshmukh P M, Gughane A S et al. (2012). Maintaining File Storage Security in Cloud.