International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Implementation of Cloud storage Security Mechanism using Digital Signature

Kamlesh Kumar Rao† and Sanjay Kumar Yadav†

†Department of Computer Science & Information Technology, SHIATS, Naini, Allahabad, Uttar Pradesh, India

Accepted 10 March 2016, Available online 12 March 2016, **Vol.6, No.2 (April 2016)**

Abstract

Data and computation integrity as well as security are major considerations for end 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 with data's confidentiality and integrity. This paper presents implementation of the cloud storage security mechanism that helps to secure data and provide better Security from unwanted attack.

Keywords: *TPA, MD5, Cloud Storage, Security.*

1. Introduction

The past decade has seen the rise of cloud computing (Mell Peter and Timothy Grance *et al,* 2011) 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 customers the illusion of experiencing infinite processing resources, which they can use as often or as low as their requirement is, without having to concern about how exactly such resources are offered or preserved.(Michael Armbrust, *et al*, 2009).

Cloud computing encompasses numerous services that will vary according to the degree to which the details of the actual underlying equipment and software package are abstracted from customers. More specifically, cloud computing offers users the following benefits:

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. 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.

Maintainability and convenience: By abstracting away the details of the underlying hardware, and in some cases, the software, cloud providers absolve users from maintaining those resources.

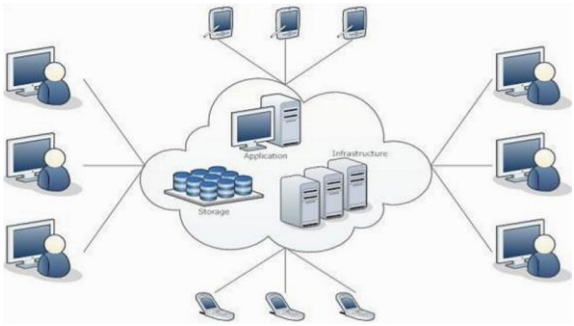

Fig.1 Cloud Computing Model

A. Participants

In a cloud-model there are four main participants: (Mell Peter, and Timothy Grance, 2011), (Michael Armbrust, *et al*, 2009), (Brohi, Sarfraz Nawaz, Mervat Adib Bamiah, and Suriayati Chuprat, 2014).

Cloud Provider: The cloud service (service provider) is surely an entity that is answerable to everything necessary for making a cloud program available.

Cloud Consumer: A new cloud buyer is either a cloud program owner or maybe a cloud program consumer. Cloud program owner may be the individual

*Corresponding author: **Kamlesh Kumar Rao**

or perhaps organization which subscribes for any cloud program.

If there is certainly any charge associated with the service, the cloud service seller will lead to the expenses. Cloud program consumer is surely an individual or perhaps application which accesses any cloud program.

Cloud Broker: Some sort of cloud broker is surely an entity that will mediate concerning cloud suppliers and Cloud consumers. The goal of a program broker is to always provide the actual cloud consumer a site that is a lot better for the needs. This is often done by simplifying or improving the actual service as well as through contract, aggregating multiple cloud services or offering value-added services. One can consider Cloud brokers like a special Cloud provider.

Cloud Auditor: Any cloud auditor is usually an independent party who investigates a Cloud service stack to offer an assessment on protection, privacy and availability amount of the equivalent cloud services and means that the equivalent SLAs (Service Stage Agreement) are fulfilled. The main points and setting of auditing process is usually specified inside service contract.

B. Isolation Levels

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

Public Cloud: A public cloud is a cloud whose infrastructure is shared by many mutually entrusted cloud consumers.

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.

Community Clouds: Community clouds are clouds whose services are accessible to a particular set of organizations which form a community. Community clouds can all be on or off premises.

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. (Armbrust, Michael, *et al.,* 2009), (Brohi, Sarfraz Nawaz, Mervat Adib Bamiah, and Suriayati Chuprat, 2014).

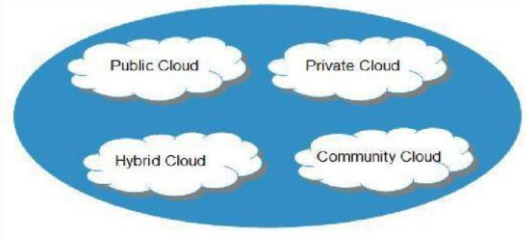

Fig.2 Categories of Cloud

Shobha Rajak *et al* 2012, proposed a model for the integrity check over the cloud computing. They operated the TPA in addition to digital signature to own integrity notion, in such a way to help anyone to verify and examine the information from unauthorized people who manipulate while using cloud or even extract on the data. Furthermore, they were able to evaluate their work using a windows purple project that requires digital unique coding. As results, they found their model well-labored based on their states. The approach for the digital encryption inside verification course of action was actually unique. In the actual implementation they used, for instance, the customer data inside cloud a text entered through the client. However, this research seriously isn't covering other types of client info.

Faraz Fatemi Moghaddam *et al* 2013, presents hybrid asymmetric-key encryption algorithm, HE-RSA based on RSA Small-e and an Efficient RSA, which offers good security in foreign computing conditions. In the actual proposed algorithm, the number of exponents have been increased to three and also a dual encryption process have been applied to improve the security a higher level the algorithm in contrast of original RSA. In respect the simulation outcomes, the full execution time in HE-RSA seemed to be increased as much as approximately 50 percent lower than the original RSA and also this increase could possibly be reasonable and also acceptable good security level plus the efficiency associated with HE-RSA.

Padmapriya *et al* 2013, presents a comparative study of Cloud computing security mechanisms based on a set of important policy issues such as issues of privacy, safety, anonymity, malicious applications, trust issues, reliability and a few more. This document analyses the importance of safety. They compared three algorithms namely Data Encryption Regular (DES), RSA, Homomorphic encryption regarding data safety. The algorithms are compared on four metrics of cloud security key employed, scalability, security put on, and authentication type.

2. System Architecture

Each of our security analysis targets the foe model as defined. We also evaluate the efficiency of our own scheme via implementation of both document distribution getting ready and proof token correctness, verification for the calculation of requested token.

Precomputation . Inside our scheme, servers have to operate with specified rows in each correctness, verification for the calculation of requested Token .media thievery, which compromises facts availability as well as confidentiality. For maintaining data confidentiality and integrity, the responsibilities of client admin are as follows:

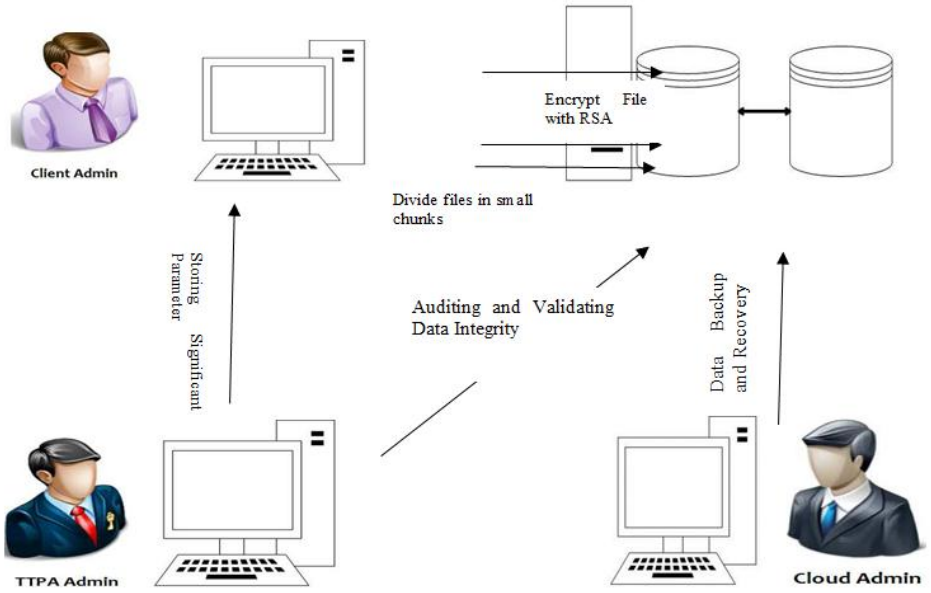

Fig.3 System Architecture

2.1. 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.

a) At the time of transferring RSA works which will be encrypt our data.
b) And the second one is MD5 that will be work in data storage array.

MD5 need because, threats at storage level include tampering with data, which violates data integrity, and media theft, which compromises data availability and confidentiality

2.2. 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.

3. System Workflow

The process is initiated from client admin with the generation of private and public keys by requesting the cloud server.

Digital Signature

Digital Signatures are based on the concept of public - private key pair. Digital signature is created by the generating a message digest first from the source message using hash function. Then file is encrypted with senders private key. this encrypted message digest of the original message is called the Digital signature.

When the file is uploaded the digital signature create public key, when file is download from the cloud key verification

Verify the key if keys are equal then it is accepted and if not then rejected.

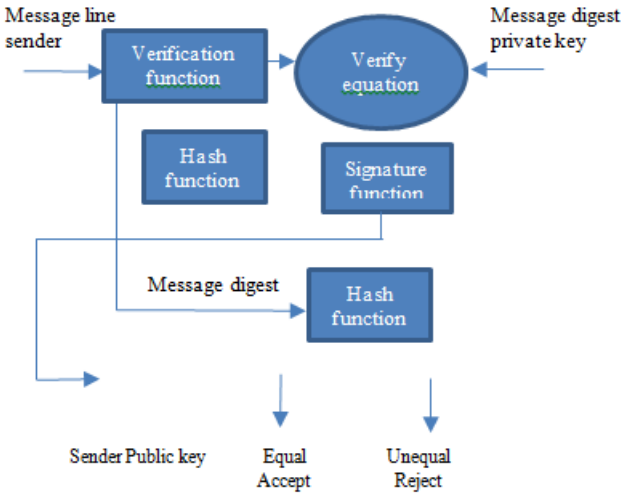

Fig.4 Digital Signature

Let us examine a simple scenario. 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. 5.

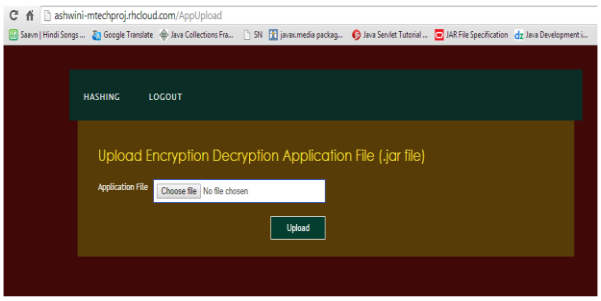

Fig.5 Upload Encryption & Decryption File

Fig.6 Sent Request to TPA

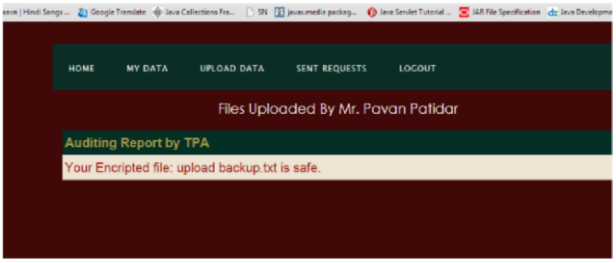

Fig.7 Generate Hash Value for Uploaded File

Fig.8 User Uploaded Data view

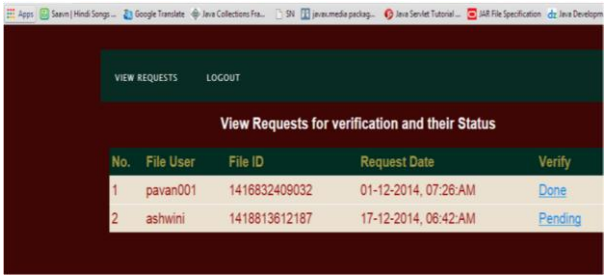

Fig.9 View Incoming Request for Data Authentication

For the verification of the data, user or cloud send request to the TPA as shown in fig 5. After that hash code is generated with the help of the user reference to the data in the fig 6. Then if the hash code is valid, 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.

4. Experiment & Evaluation

We created a public cloud with the help of Open shift (Redhat) by using Eclipse kepler editor and Jboss for WebServer. We performed coding in Java.

In next step, we created three services, namely- User service, Admin service, TPA service. User service can perform operations like active login, file encryption (using RSA/Hybrid Algorithm), encrypted file upload on cloud server, sending request to TPA for audit, encrypted file download and file decryption (using DES/Hybrid Algorithm) and analysis of the hash value sent by cloud server and viewing all files. Similarly, TPA is designed to perform the following services like login and verification/audition of user files. Admin service, in addition to enable login, it is also designed to generate hash value for uploaded user file and monitor various files of user. The result we obtained from the experiment is shown in the following table:

Table 1 Comparative Study of Performance of RSA and Hybrid algorithms on certain parameters

Parameter	RSA Algo	HASH Algo	Hybrid Algo
Size	12MB	10MB	0.8MB
Speed	Slow	Slow	High
Key used	Symmetric Key	Public & Private Both	Public & Private Both
Security	Client Side	Both Provider	Cloud Provider only
Authentication type	-	MD5	Message Digest
Key generation time	92ms	91ms	90ms
Encryption time	97ms	98ms	92ms
Decryption Time	97ms	99ms	91ms
Uploading Time	-	-	108ms
Downloading Time	-	-	107ms

5. 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. 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.

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 particular TPA, TPA may immediately belongs to who owns the file so security along with data ethics is collateralized 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

Peter Mell and Timothy Grance (2011), the NIST Definition of cloud computing, NIST Special publication, pp 800-145

Adrian, D., S. Creese and M. Goldsmith (2012), Security and Privacy in Computing and Communications, Insider attacks in cloud Computing. Proceedings of 11th International Conference on Trust, Jun. 25-27, IEEE Xplore Press, pp 857-862

Ateniese, G., R. Burns, R. Curtmola, J. Herring and L.Kissner (2007), Provable data possession atuntrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security, pp 598-609.

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.

Cong Wang, Sherman S.M.Chow, Qian Wang, KuiRen, and Wenjing Lou (2013), Privacy PreservingPublic Auditing for Secure Cloud Storage, IEEE, Vol.62, No. 2

Michael Armbrust, Armando Fox, Rean Grith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia (2009),above the clouds: A Berkeleyview of cloud computing.

Technical Report UCB/EECS-2009-28, Dept. of Electrical Engineering and Computer Sciences, University of California at Berkeley, February 2009.

C.Wang, Q.Wang, K.Ren, and W.Lou(2007),Privacy Preserving Public Auditing for Storage Security in Cloud Computing, IEEE INFOCOM'10, March 2010.

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.

Sunitha Abburu, Saranya Eswaran(2012),Identifying Data Integrity in the Cloud Storage, IJCSI, Vol.9, Issue 2, No. R.Dheenadayalu, M.Sowparnika (2013 Improving Data Integrity on Cloud Storage Services, IJESI, Vol.2,Issue 2.

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

Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Suriayati Chuprat a Jamalul-lail Ab Manan (2014), Design and Implementation of a Privacy Preserved off Premises Cloud Storage, Journal of Computer Science,10(2) pp 210-223.

A.Padmapriya, P.Subhasri (2013), Cloud computing : Security Challenges and Encryption Practices, International Journal of Advance Research in Computer Science and Software Engineering, Vol.3,issue3 .