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 with Authentication

Vaibhav Srivastav†*, Prajna Jha‡ and Tulika†

†Department of Computer Science & Information Technology, SHIATS, Naini, Allahabad, Uttar Pradesh, India
‡Department of Computer Science, AIM & ACT, Banasthali University, Tonk, Rajasthan, India

Accepted 25 June 2015, Available online 30 June 2015, **Vol.5, No.3 (June 2015)**

Abstract

Facts 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: *Chunks, 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 processing 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 processing 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.

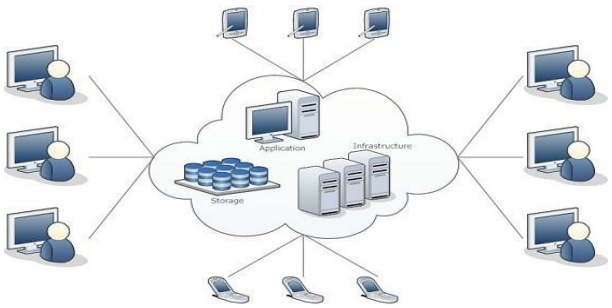

Fig.1 Cloud Computing Model

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: **Vaibhav Srivastav**

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.

2. 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).

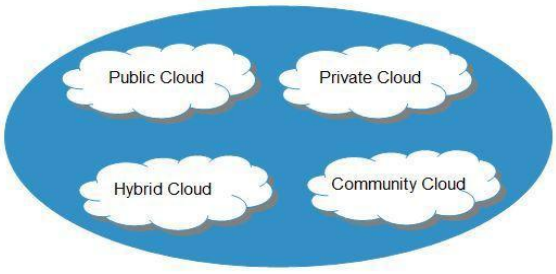

Fig.2 Categories of Cloud

3. Literature Survey

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.

4. 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 precomputation. Inside our scheme, servers have to operate with specified rows in each correctness, verification for the calculation of requestedToken.media thievery, which compromises facts availability as well as confidentiality.

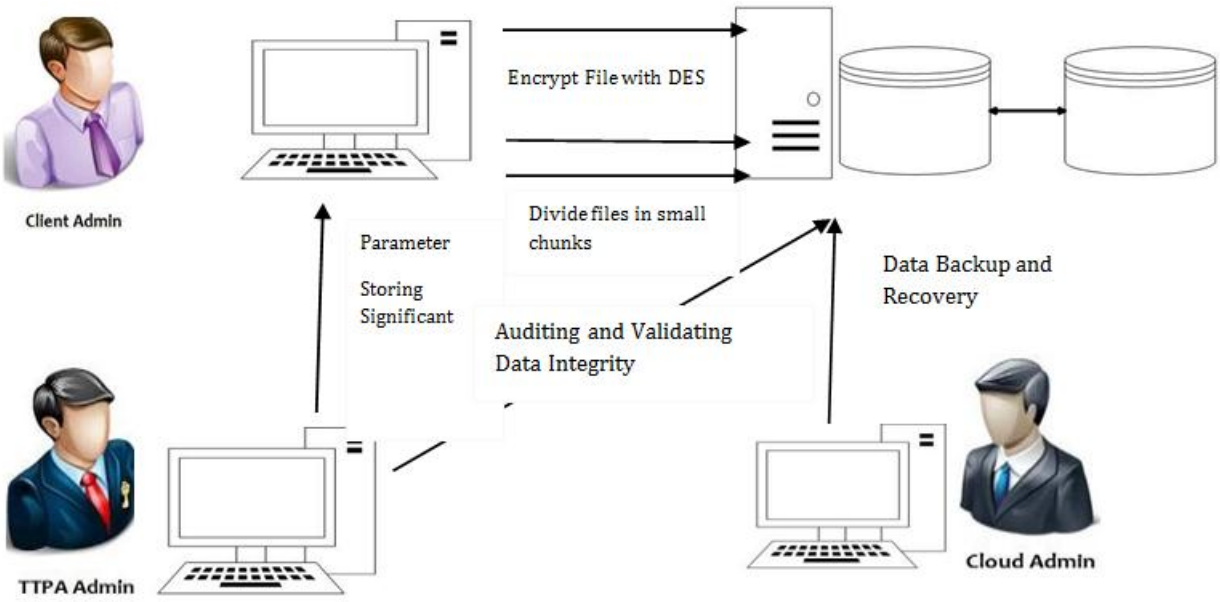

Fig.3 System Architecture

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

Uploading Steps

1. Each individual logs on to the workstation using its own Username and Password.
2. If not connected, user is linked to a safe-keeping array by means of network.
3. The client's computer directs a request towards the storage variety for holding a report.
4. This report is encrypted by two fold.
(a) At each step of shifting, DES encrypts each part of our data.
b) And the next one can be SHA that will work throughout data safe-keeping array.
5. SHA will be required because challenges at safe-keeping level include things like tampering with data, which in turn violates facts integrity, as well as media theft, which compromises facts availability as well as confidentiality.

Downloading Steps

1. When the client transmits a request from a new server, client admin generates a new request which include things like valid IDENTITY and Password.
2. The safe-keeping array verifies the security credentials and verifies that the end user is authorized to work with that program.
3. If end user is approved then admin send reply to the client machine and present response.
4. The consumer computer sends the specified file name looking to gain access to.
5. The safe-keeping array decrypts the actual file plus the server automatically allows the client to access the proper resources.

5. System Workflows

The procedure begins from client admin while using the generation of private and also public secret key by seeking the impair server. It allows us to examine an effective scenario. As an illustration client admin really wants to store a new file called as Back-up - text containing organization's employees' discrete records with the cloud safe-keeping. Cloud server needs the file as well as the public essentials for encryption method as displayed in Fig .3

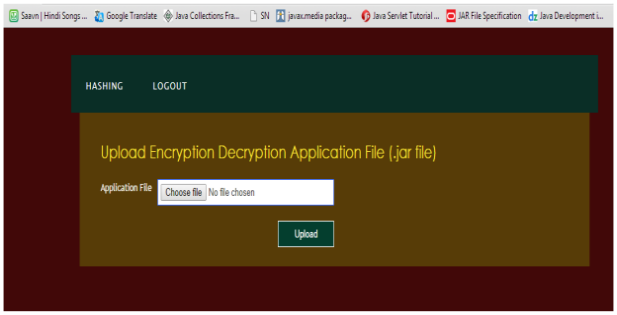

Fig.4 Upload Encryption & Decryption File

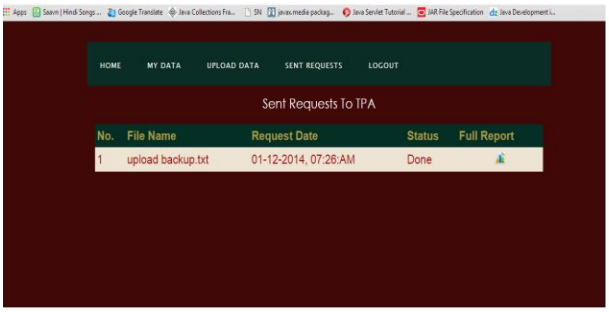

Fig.5 Sent Request to TPA

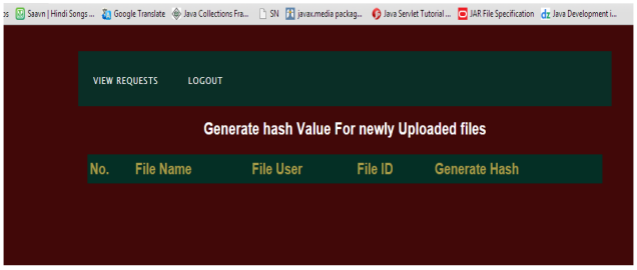

Fig.6 Generate Hash Value for Uploaded File

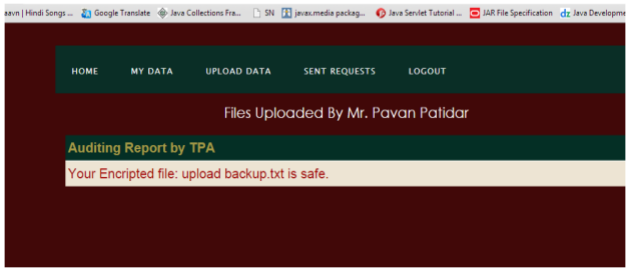

Fig.7 TPA Verification Report

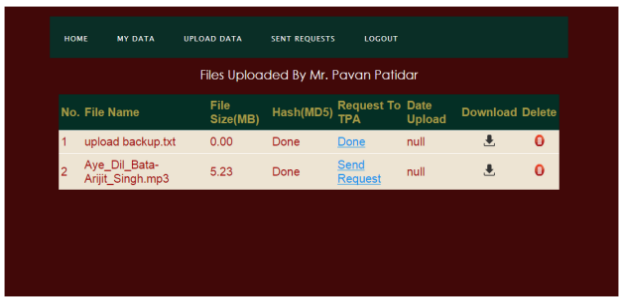

Fig.8 User Uploaded Data view

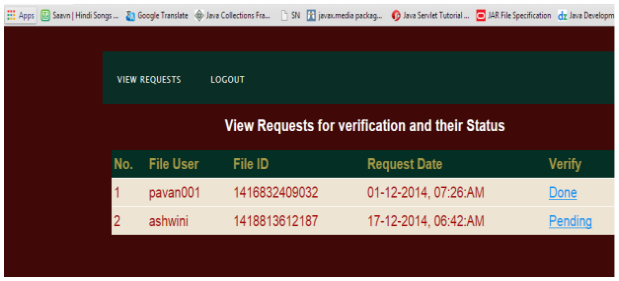

Fig.9 View Incoming Request for Data Authentication

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.

6. 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 DES/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 DES and Hybrid algorithms on certain parameters

Parameter	DES 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

7. Results

In the experiments, we identified that client's privacy always remains intact in spite of the attacks launched by a number of malicious consumers. For-example if a pro hacker can attack the results during the particular transfer(downloading, uploading) or with the storage it doesn't has an effect on the privacy because prior to data departs the client system, it gets encrypted over the entire procedure even when it is stored or maybe processed at cloud storage space. When attackers get access, they can't get almost any meaningful details except the cipher text. In case an opponent violates the particular integrity at physical foreign storage, it is immediately identified during the auditing procedure and files are recovered at its original state in the backup storage space. Similarly while, TTPA admin would like to extract the particulars of a private key purchaser, attackers aren't going to be able to decrypt it because it is encrypted as sound. (Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Suriayati Chuprat and Jamalul-lail Ab Manan, *et al,* 2009) Likewise if attacker gets the private key, attacker cannot decipher the particular client's files, since intended for decryption, system ought to perform the particular decrypt process and this task is always be initiated by the client only, while successfully recording required

recommendations. Un-authorized consumers cannot perform any operation, even as long as they break-in safety measures, to get access menu, they should intend for some random safety measures code and also the code can be only shipped to privileged users beneath the implemented RBAC. We concluded that using the particular proposed strategy, besides the particular threatening problems, client's privacy i.e. data secrecy is stored at off-premises foreign computing storage space.

Conclusion

The method, for example the data owner can look at the integrity in their data stashed in impair server applying TPA that is done within efficient method. If almost 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 may not learn any knowledge about the information content stored for the cloud server during the efficient auditing procedure, which not simply eliminates the duty of impair user from tedious and perchance, expensive auditing process, but also alleviates the particular users' concern with their outsourced information leakage. Cloud information security is definitely an important aspect for that client when using the cloud solutions. Third Party Auditor can be used to ensure the particular security along with integrity connected with data. Third Party Auditor could be a trusted mechanism to fix the conflicts between the Cloud Company and customer.

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 (2011),Benefits, Risks and Recommendations for Information Security, CSA Security Guidance for Critical Areas of Focusin Cloud Computing v3.0. USA.

Francisco, R, S. Abreu and M. Correia, (2011). The final frontier: Confidentiality andprivacy in the cloud Computer, pp 44-50.

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 waz 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.

Moghaddam, Faraz Fatemi, Maen T. Alrashdan, and Omidreza Karimi (2013) A Hybrid Encryption Algorithm based on RSA Small-e and Efficient-RSA for Cloud Computing Environments. Journal of Advances I Computer Networks1.3: 238-241.

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