International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 12 December 2015

Cloud storage Security Mechanism with Authentication in Public Cloud

Apurva Patidar[1], Mohsin Sheikh[2]
Department of Computer Science & Engg.
Medicaps Institute Of technology and Management, Indore,(M.P.),India
patidarapurva@gmail.com[1]

Abstract*: In cloud computing, data is moved to a remotely located cloud server. Cloud server faithfully stores the data and return back to the owner whenever needed. 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. Many users place their data in the cloud and so data integrity is very important issue in cloud storage. After moving the data to the cloud, owner hopes that their data and applications are in secured manner. The Main Aim of this research is to provide security in the cloud with the help of the Third Party Auditor. This is done to enhance the hardness in security by the RSA encryption algorithms by adding some more security codes. Encryption is the vital part of information sharing so we will put our efforts into encryption area for RSA algorithm with digital abstract algorithm MD5 so that we can make security harder by giving a hybrid algorithm.*

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

1. Introduction

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. At the lowest level of abstraction, often referred to as infrastructure as a service, the provider only visualizes the hardware and storage while leaving users responsible for maintaining the entire software stack from operating system to applications. Examples of such services include Amazon EC2 and competing offerings from IBM, Microsoft .At the opposite end of the spectrum, called software as a service, the provider offers specific applications such as word processing, email, and calendaring directly to end users, usually via the Web, and manages all of the necessary hardware and software. Although this category typically refers to services intended to replace desktop applications such as Google Apps and Microsoft Office Live, it can also cover applications with no desktop analogs such as social networking services like Face book and Twitter.

1.1 Participants of cloud: A Cloud has four Participants.

- **Cloud Provider**: A cloud provider (service provider) is an entity that is responsible for everything required for making a cloud service available.
- **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.
- **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.

- **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.

1.2 Categories of Cloud:

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 that its infrastructure is shared by many mutually untrusted 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 that their 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. .

2. Literature Review

In this Paper [6] Authors Proposed and implement the digital signature for authentication and AES as encryption algorithms for data security in cloud computing. So this system more secures than the existing system which uses symmetric encryption algorithms RC4, Blowfish, 3DES, DES etc. In future we can optimize efficiency of system by reducing size of key for encryption and check the performance with the proposed algorithms.

This paper [7], Authors explores various security methods such as Access Control, Telecommunications and Network Security, Information security governance and risk management, Application Security, Security Architecture and Design. The performance characteristics of RSA are observed by implementing the algorithms for computation. In this paper, RSA was implemented through an encryption and decryption procedures over different key sizes.

In this Paper [8], Authors 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. 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.

In this Paper [9] authors 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. In future we are going to propose a backup plan to solve security issues in both cloud providers and cloud consumers.

In this Paper [10], authors Presents An Implementation of RSA Algorithm in Google Cloud using Cloud SQL. Cloud storage concern the user does not have control over data until he has been gain access. They have implemented RSA algorithm in google App engine using cloud SQL. From the results we obtained it is proved that RSA gives protection for the data, which is stored in Cloud.

3. Proposed System

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 precipitation. In our scheme, servers are required to operate on specified rows in each correctness, verification for the calculation of requested token. We will show that this “sampling” strategy on selected rows instead of all can greatly reduce the computational overhead on the server, while maintaining the detection of

the data corruption with high probability. Suppose nc servers are misbehaving due to the possible compromise or Byzantine failure.

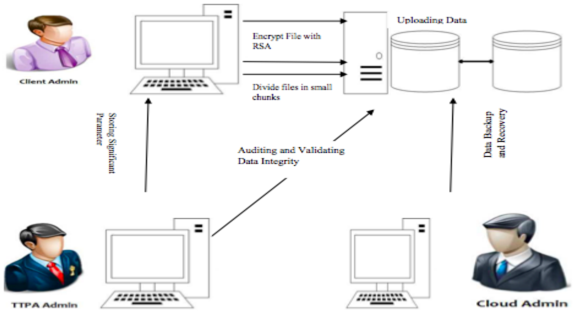

Client Admin
Uploading Data
Encrypt File with RSA
Divide files in small chunks
Storing Significant Parameter
Auditing and Validating Data Integrity
Data Backup and Recovery
TTPA Admin
Cloud Admin

Figure 1: System Architecture

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

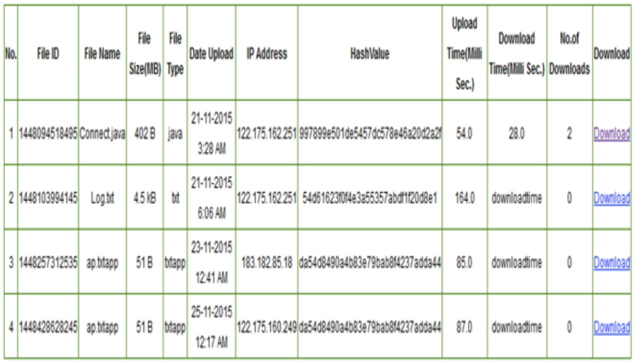
Downloading Steps:-

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 Cloud Server generates the hash value of user uploaded files. and also view all the user data. that want to access.
5. The storage array decrypts the file and the server Automatically allows the client to access the appropriate resources.

4. Implementation and Results:

Proposed system implemented in openshift (Red-Hat) cloud. With the help of openshift cloud we create public cloud which includes Jboss application server for web application and mysql for data storage. We created three user cloud admin, cloud Auditor (TPA) and cloud consumer. We calculate uploading time, downloading time, hash value, file status and number of downloads and maintain log file of cloud consumer .all these details shown in Table1. Cloud server view the all the details of file which are uploaded by different user and log file which contain activities of all cloud consumers.

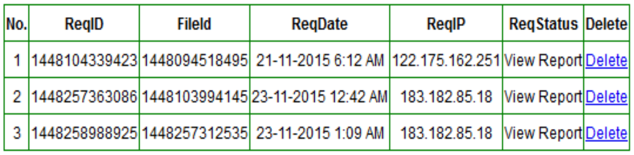
Table3.1: Calculate uploading time, downloading time, hash value, file detail and number of downloads of cloud consumers



No.	File ID	File Name	File Size(MB)	File Type	Date Upload	IP Address	HashValue	Upload Time(Milli Sec.)	Download Time(Milli Sec.)	No.of Downloads	Download
1	1448094518495	Connect.java	402 B	java	21-11-2015 3:28 AM	122.175.162.251	997899e501de5457dc578e46a20d2a2f	54.0	28.0	2	Download
2	1448103994145	Log.txt	4.5 kB	txt	21-11-2015 6:06 AM	122.175.162.251	54d61623f0f4e3a55357abdf1f20d8e1	164.0	downloadtime	0	Download
3	1448257312535	ap.txtapp	51 B	txtapp	23-11-2015 12:41 AM	183.182.85.18	da54d8490a4b83e79bab8f4237adda44	85.0	downloadtime	0	Download
4	1448428628245	ap.txtapp	51 B	txtapp	25-11-2015 12:17 AM	122.175.160.249	da54d8490a4b83e79bab8f4237adda44	87.0	downloadtime	0	Download

Cloud Consumer send request to cloud auditor for audit their uploaded files. And the cloud auditor audits their files under the server permission.

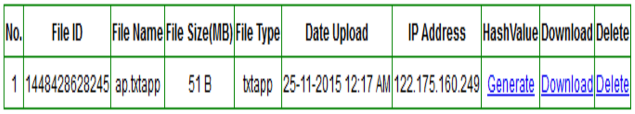
Table3.2: File audit request to cloud Auditor (TPA).



No.	ReqID	FileId	ReqDate	ReqIP	ReqStatus	Delete
1	1448104339423	1448094518495	21-11-2015 6:12 AM	122.175.162.251	View Report	Delete
2	1448257363086	1448103994145	23-11-2015 12:42 AM	183.182.85.18	View Report	Delete
3	1448258988925	1448257312535	23-11-2015 1:09 AM	183.182.85.18	View Report	Delete

Cloud Server generates the hash value of user uploaded files. And also view all the user data.

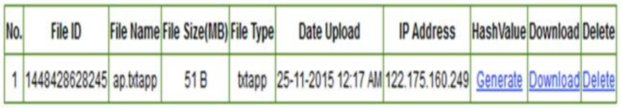
Table3.3: Show Server generates the hash value of users file.



No.	File ID	File Name	File Size(MB)	File Type	Date Upload	IP Address	HashValue	Download	Delete
1	1448428628245	ap.txtapp	51 B	txtapp	25-11-2015 12:17 AM	122.175.160.249	Generate	Download	Delete

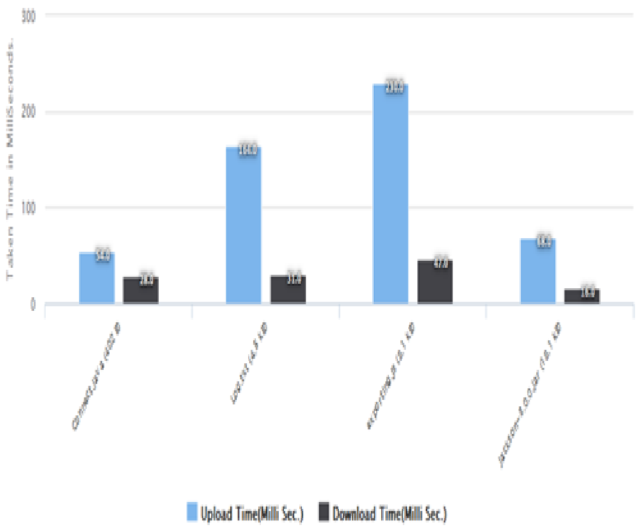
Cloud Auditor (TPA) is audit the file which uploaded by different cloud consumers and the cloud consumers send request to the cloud auditor for audit their respective file.

Table3.4: File audit request to cloud Auditor (TPA).



No.	File ID	File Name	File Size(MB)	File Type	Date Upload	IP Address	HashValue	Download	Delete
1	1448428628245	ap.btapp	51 B	btapp	25-11-2015 12:17 AM	122.175.160.249	Generate	Download	Delete

The graph shows the result of the uploading time and downloading time. With the help of the graph we have to calculate performance of the system finally we got that thing. The blue bar shows the upload time and the black bar shows the downloading time.



Graph3.5: Calculate uploading and download of files.

Overall Outcome: The proposed algorithm were suggested for using in Cloud computing environments and increasing the Reliability of this new technology, but the most challenging issue in using RSA encryption algorithm in cloud servers is time and memory limitations during the encryption and decryption process in servers according to the sharing performances. It is suggested to encrypt the stored data with a symmetric-key algorithm such as RSA in cloud servers and after that encrypt the secret key with HYBRID for sharing actions. This means, only the secret key would be encrypted with this algorithm and the encryption and decryption process will be more efficient and needless to say it would be less time consuming and memory deficient.

A hybrid asymmetric-key encryption algorithm has been suggested based on RSA and MD5 according to the security issues in cloud computing environments. 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 HYBRID 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 HYBRID.

5. Conclusion

This research is provide security in the cloud with the help of the Third Party Auditor. This is done to enhance the hardness in security by the RSA encryption algorithms by adding some more security codes. Encryption is the vital part of information sharing so we will put our efforts into encryption area for RSA algorithm with digital abstract algorithm MD5 so that we can make security harder by giving a hybrid algorithm. Cloud data security is an important work for the cloud client because they only believe on the cloud and they want their data is in safe hand. Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to give confidence to the cloud user and cloud service provider that their data is safe. The above-mentioned model is fruitful in data as a service, which can be extended in their service models of cloud. Also it is tested in cloud environment like Open Shift, in future this can be deployed in other cloud environments and the best among of all can be chosen.

References

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

[2] Michael Armbrust, Armando Fox, David A. Patterson and Matei Zaharia. Above the clouds: “A berkeley view of cloud computing”,Technical Report UCB/EECS-2009-28, Dept. of Electrical Engineering and Computer Sciences, University of California at Berkeley, February 2009.

[3] Kevin Hamlen, Marut Kantarcioglu, latifur Khan and Bhavani Thuraisingham, “Security issues for

Cloud Computing”, Technical Report UTDCS-02-10 February 2010.

[4] Andrzej M. Goscinski Rajkumar Buyya, James Broberg, “Cloud Computing: Prin- ciples and Paradigms”, Wiley, 2011.

[5] Jose M. Alcaraz Calero, Nigel Edwards, Johannes Kirschnick, Lawrence Wilcock, and Mike Wray, “a multi-tenancy authorization system for cloud services”,IEEE Security and privacy,8:48{55, 2010.

[6] Dhaval Patel, M.B.Chaudhari,“Data security in cloud computing using digital signature”, International Journal for Technological Research In Engineering, Volume 1, Issue 10, June-2014.

[7] Amandeep Kaur et. al “An Efficient data storage security algorithm using RSA Algorithm”, International Journal of Application or Innovation in Engineering & Management, (IJAIEM) Volume 2, Issue 3, March 2013.

[8] 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.

[9] Padmapriya et al., International Journal of Advanced Research in Computer Science and Software Engg 3 (4), March - 2013, pp. 255-259.

[10] N.Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam,“An Implementation of RSA Algorithm in Google Cloud using Cloud SQL”,Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574-3579, 2012.

[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] Deyan Chen, Hong Zhao “Data Security and Privacy Protection Issues in Cloud Computing”,InternationaL Conference on Computer Science and Electronics Engineering..

[13] V.Sreenivas and C.Narasimham, “Performance Evalution of Encyption Techniques and Uploading of Encrypted Data in Cloud”,IEEE,July 2013.