INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

# DATA SECURITY OF PRIVATE CLOUD USING ENCRYPTION SCHEME WITH RSA

**ASST. PROF. RAJESH T. NAKHATE, MR. AAKASH D. WANI, MISS. PAYAL N. TOMPEY, MISS. NEHA S. CHAMATKAR, MISS. VAISHALI G. GOHANE**

Dept. of Information Technology, DMIETR, Wardha-442001

**Accepted Date: 15/03/2016; Published Date: 01/05/2016**

**Abstract:** A phrase used to describe a variety of computing concepts is Cloud computing that involve a huge number of computers systems connected through a real-time communication network such as the internet. Cloud Computing is a standard paradigm which has become today's hottest research area because of its capability to reduce the costs associated with computing. Due to the fast development of the Cloud Computing technologies, the rapid increase of cloud services are became very incredible. Securing data is a challenging issue in today's date. Most of the data travel over the internet and it becomes difficult to make data secure. The prevalent problem associated with Cloud Computing is the Cloud security and the proper Implementation of Cloud over the Network. In this Research Paper we are using RSA Algorithm for improving the Security.

**Keywords:** Cloud Computing, RSA Algorithm and Internet.

**Corresponding Author: MR. AAKASH D. WANI**

**Access Online On:**

www.ijpret.com

**How to Cite This Article:**

Aakash D. Wani, IJPRET, 2016; Volume 4 (9): 97-106

***PAPER-QR CODE***

## INTRODUCTION

Cloud computing is the extensive dreamed idea of computing as a service, where data vendors can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. Cloud is a new business model enfolded around new technologies such as server virtualization that take advantage of economies of scale and multi-tenancy to reduce the cost of using information technology resources. It also carries new and challenging security threats to the outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing actually resigns the owner's ultimate control over the providence of their data. The term cloud computing probably comes from (at least partially) the use of a cloud image to represent the Internet or some huge networked environment. Cloud computing really is accessing resources and services needed to perform functions with dynamically changing needs. An application or service developer requests access from the cloud rather than a specific end point or named resource. What goes on in the cloud manages multiple infrastructures across multiple organizations and consists of one or more frameworks overlapped on top of the infrastructures tying them together. Cloud computing platforms are rising very rapidly. Organizations can provide hardware for clouds internally, or a third party can provide it externally. A cloud might be restricted to a single organization or group, available to the general public over the Internet, or shared by multiple groups or organizations [1].

## SECURITY ISSUES OF DATA IN CLOUD

A few years ago, the big issue with the Cloud was security. Security issues of cloud such as storage security, data security, access security and application security. In Cloud Computing the user must ensure that their infrastructure is more secure [2]. In cloud systems, data is stored in a remote location on servers maintained by a cloud service provider. The cloud service provider should have facility to ensure that there is no direct interfering into client data. With the cloud model, you lose control over physical security. Storage services provided by one cloud vendor may be incompatible with another vendor's services should you decide to move from one to the other. Data integrity is guarantee that the data is consistent and correct. Guaranteeing the integrity of the data really means that it changes only in response to authorized transaction. These issues are generally attributed to slow down the deployment of cloud services. For example, by storing the information internal to the organization, but allowing it to be used in the cloud. If the provided cloud storage can be accessed or destroyed by attackers, it causes the breaking of personal data that could effect great harm to each individual user. In Cloud Computing the provider must ensure that their infrastructure is secure and that their clients'

data and applications are protected while the customer must ensure that the provider has taken the proper security processes to protect their information.

**PROPOSED WORK**

In this proposed work we want to secure our data in cloud. Because Security is the major concern which is faced by every user. Consider an organization where their are number of Users are working. Each User has its own USER ID and PASSWORD where they can store their data and all the organization is managed and operated by ADMIN. Admin restrict the system from unauthorized access because their are number of restriction to download the files of cloud with every user. RSA works on the encrypted data and generate the public key and private key. It provides a better storage and security technique over Cloud architecture. With the RSA Algorithm, it would be more secure to gets hacked. These Algorithm helps to provides security. Here we illustrate the Figure 1 which represents the basic design of our proposed work.

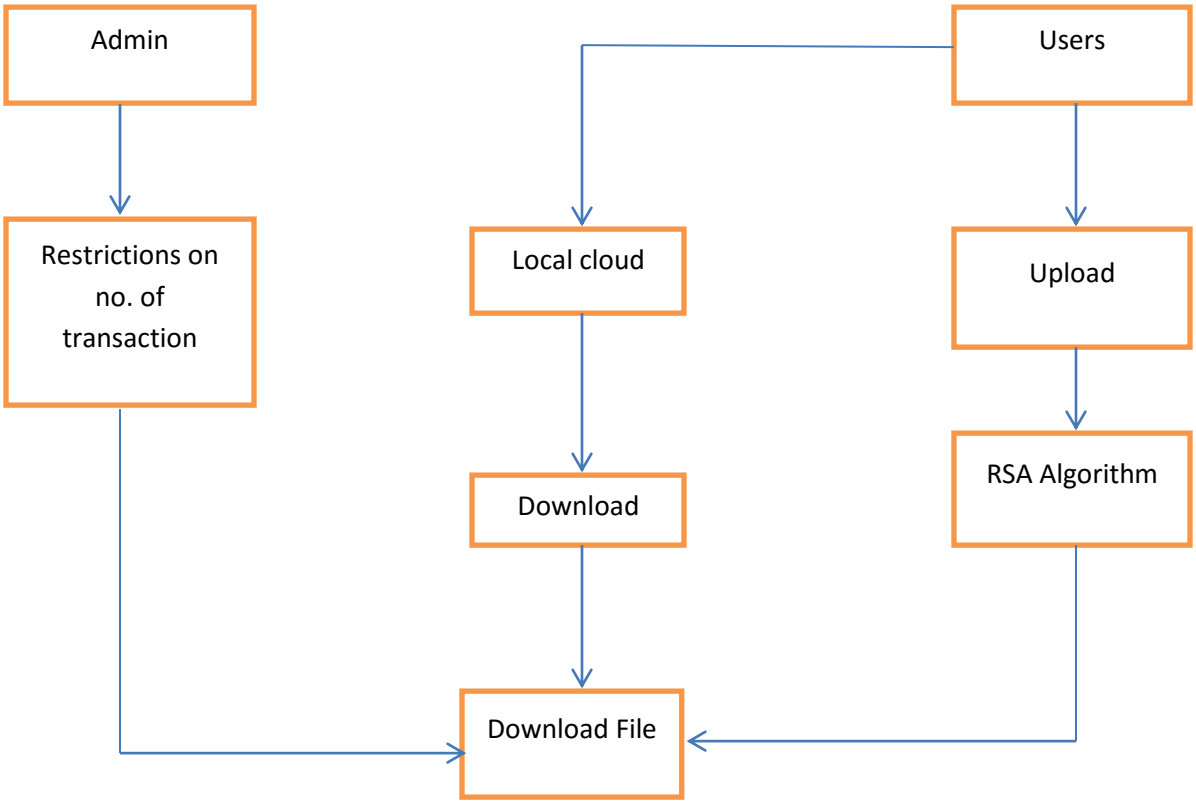


**Figure 1:- Basic design of proposed work**

Admin: In an organization, admin create roles for users & also specify the number of transactions per user as per their role.

User: A user can upload/download file. When uploading file RSA scheme are used to encrypt data when downloading the files inversely RSA are used to decrypt data.

Local Cloud: Local Cloud is used to store data in the encrypted form.

Below we will explain RSA Algorithm.

RSA

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it[5]. Here we explain RSA algorithm. RSA algorithm involves three steps:

1. Key Generation

2. Encryption

3. Decryption

An RSA algorithm is the genetic algorithms in the security system in the cryptography [6]. In RSA algorithms first we choose the two integer values.

Let P and Q are the integer values. Then we find the value of N.

$N = P \times Q$ … (1.1)

$\emptyset(N) = (P - 1) \times (Q - 1)$ … (1.2)

Then we choose the value of e, which is not factor of $\emptyset(N)$

And also we find the value of d, which is related the expectation value (e).

$ed = 1 \bmod \emptyset(N)$ … (1.3)

Or $d = ½ \bmod \emptyset(N)$ … (1.4)

Or $d = e^{-1} \bmod \emptyset(N)$ … (1.5)

By Euclidian theorem the value of d depends upon $|\emptyset(N)|$.

The value of d has the modulus values 1, 2…n.

$d = 1 + |\emptyset(N)|$ … (1.6)

RSA algorithms are also used in the encryption and decryption.

Encryption key = (e, N).

Decryption key = (d, N).

If the message M so the value of M <N.

Encrypt = E = $Me$ mod N ... (1.7)

Decrypt => M = $Ed$mod N … (1.8)

In equations (1.1), (1.2) and (1.6) are using

for the key generation but the equation (1.7), (1.8) are using encryption and decryption.

IMPLEMENTATION AND RESULT

1. The described work is implemented in

Advanced Java. Firstly we show the snapshot where admin restricts all the users to assign the size for one user. Figure 2. Represents assigning data size.

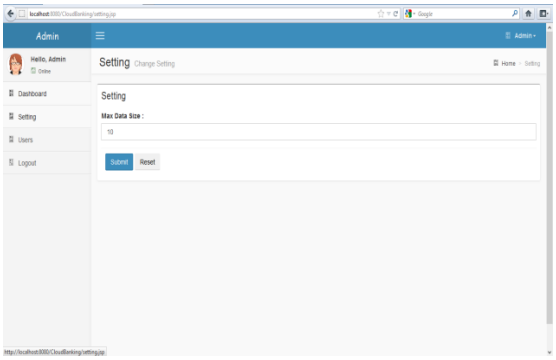


**Figure 2. Assigning Data Size**

2. The next snapshot represents the list of employees who are working in an organization and restriction in no. of download which is permitted by Admin. This restriction provides the security with the help of RSA Algorithm. Because an unauthorized user cannot download the files without admin permission.

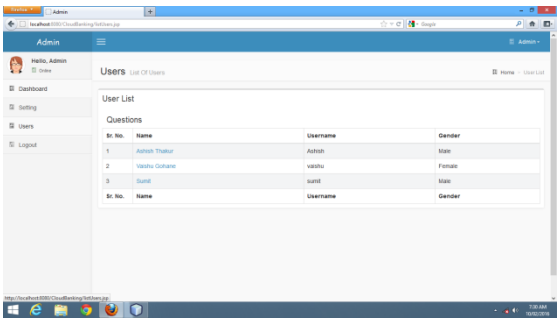


**Figure 3. Represents list of users**

3. Figure 4. Represents the uploading page where Employee upload the file and the processing can take place. When Employee upload a file Firstly RSA Algorithm applied on the file which encrypt the file and make not visible to the admin.

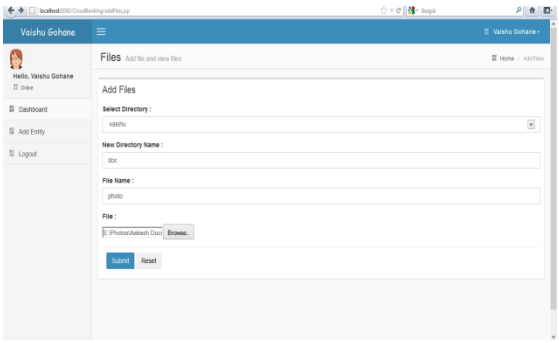


**Figure 4. Represents the uploading procedure**

4. Figure 5. Represents the downloading procedure where Employee wants to download the file. But during downloading a file RSA Algorithm decryption is required.

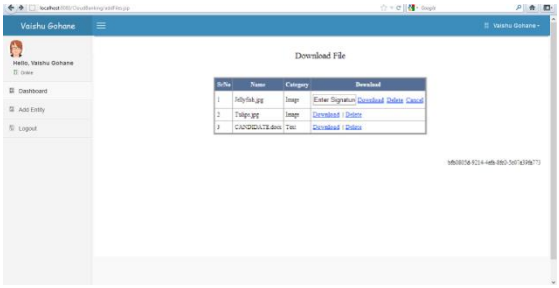


**Figure 5. Represents the downloading procedure**

5. Figure 6. Represents the downloading a page within No Permission to download the file. Because an Employee have restricted only two files have downloaded. Because Employee is restricted by an admin. After accessing two files when Employee wants to download a third file a message is generated that Contact to admin.

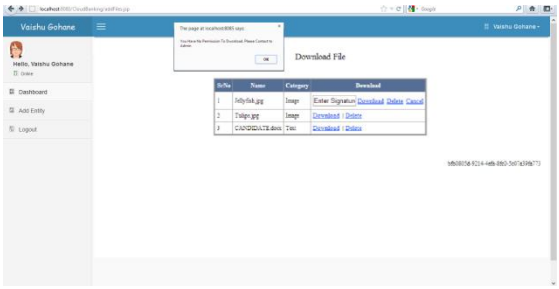


**Figure 6. Represents the downloading files with in Restriction**

6. RSA helps to encrypted the data which converts an image into an Encrypted form of data. Below Fig.7. Represents the encryption by using RSA Algorithm.

a. Image before encryption

b. image after encryption

**Fig.7. Encryption by using RSA Algorithm**

## CONCLUSION AND FUTURE SCOPE

Cloud Computing is still a new and evolving paradigm where computing is viewed as on demand service. Once the organization takes the decision to move to the cloud, it drops control over the data. Security of the Cloud relies on reliable computing and cryptography. Thus, in our proposed work, only the authorized user can access the data. Even if some unauthorized user gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and accessed it due to encryption techniques. With the kind of A RSA Algorithm it would be more secure to get hacked. It also provides a better storage and security over Cloud design.

In future our proposed work is very help full to increase the security on cloud in cloud computing As the Security need increases access and helps for safeguarding of data.

## ACKNOWLEDGMENT

Author would like to give his sincere gratitude to guide Mr. Rajesh T. Nakhate who encouraged and guided us throughout this paper.

## REFERENCES

1. Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010). Volume 64, pp.211-216.
2. Leena Khanna "Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3 March - 2013, pp. 279-283.
3. Wei-Tek Tsai "Role-Based Access-Control Using Reference Ontology in Clouds"978-0-7695-4349-9/11 $26.00 © 2011 IEEE DOI 10.1109/ISADS.2011.21
4. Ajit Singh, "Securing Data by Using Cryptography with Steganography ""International Journal of Advanced Research in Computer Science and Software Engineering" Volume 3, Issue 5, May 2013 ,pp.404-402.
5. Rashmi Nigoti "A Survey of Cryptographic Algorithms for Cloud Computing" IJETCAS 13-123; March-May 2013, pp.141-146.
6. Parsi Kalpana "Data Security in Cloud Computing using RSA Algorithm" International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

7. Esh Narayan" To Enhance the data security of cloud in cloud computing using RSA Algorthim", Bookman International Journal of Software Engineering, Vol. 1 No. 1 Sep. 2012, ISSN No. 2319-4278.
8. Farzad Sabahi, "Cloud Computing Security Threats and Responses," IEEE Trans. on Cloud Computing., vol. 11, no. 6, pp. 670 { 684, 2002.}
9. Mohammed Achemlal, Sa¨ıd Gharout and Chrystel Gaber "Trusted Platform Module as an Enabler for Security in Cloud Computing" Vol 978-1-4577-0737-7/11/$26.00 ©2011 IEEE.
10. Jianfeng Yang, Zhibin Chen "Cloud Computing Research and Security Issues" Vol 978-1-4244-5392-4/10/$26.00 ©2010 IEEE.
11. Victor Echeverr´ıa, Lorie M. Liebrock, and Dongwan Shin "Permission Management System: Permission as a Service in Cloud Computing" 2010 34th Annual IEEE Computer Software and Applications Conference Workshops.