ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Secure Communication using RSA Algorithm for Cloud Environment

Kriti Singhal

B.Tech Student, Dept. of Computer Science, Shyama Prasad Mukherji College, University of Delhi, New Delhi, India.

ABSTRACT: The term "Cloud Computing" is a recent buzzword in the IT world. It is a newly developing paradigm of distributed computing. In today's era, it is the most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud Computing stores the data and disseminated resources in the open environment, security has become an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud. In this paper, we will discuss RSA algorithm used to provide security in the field of cloud computing.

KEYWORDS: Encryption; Decryption; Cloud Computing; Algorithm; Security; Plain Text; Cipher Text; Authentication; Repudiation

I. INTRODUCTION

Cloud computing is nothing but a next generation internet based computing system which provides easy and customizable services to the users for accessing or to work with various cloud applications. It provides a way to store and access cloud data from anywhere by connecting the cloud application using internet. By choosing the cloud services the users are able to store their local data in the remote data server. The data stored in remote data centre can be accessed or managed through the cloud services provided by the cloud service providers

These group of servers and datacentres are placed at different places and these servers and datacentres are responsible for providing on demand service to its users with the help of internet. The service provided by cloud is not present on user's computer.

Fig. 1. Shared Resources in Cloud Computing

Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. It is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Because of these benefits each and every organizations are moving

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

their data to the cloud. So there is a need to protect that data against unauthorized access, modification or denial of services etc.

Comparisons of cloud services are made by their nature and utilize services such as gas or electricity. It is there whenever you need it, as much as you need, and you pay as you go and only for what you use.

Examples of cloud services include online file storage, social networking sites, webmail, and online business applications.

II. RELATED WORK

Cloud computing has been defined by US National Institute of Standards and Technology (NIST) [12] as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction ".The NIST definition is one of the clearest and most comprehensive definitions of cloud computing and is widely referenced in US government documents and projects.

Brian Hay et. al [3] have focused on data authentication, data integrity, querying and outsourcing the encrypted data.Their research says that, the risks can arise at operational trust modes, resource sharing, new attack strategies. In operational trust modes, the encrypted communication channels are used for cloud storage and do the computation on encrypted data which is called as homomorphic encryption. New attack strategies like Virtual Machine Introspection (VMI) can be used at virtualization layer to process and alter the data.

Kevin Curran et.al [4] mentions that Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud computing has become a variable platform for companies to build their infrastructures upon. If companies are to consider taking advantage of cloud based systems by storing their data in Cloud Storage they will be faced with the task of seriously reassessing their current security strategy.

Randeep Kaur et.al [5] mentions some of the notable challenges associated with cloud Storage. The challenges are Security, Privacy and Lack of Standards which slow down services in the cloud. Rashmi Nigoti et.al [11] defines some privacy and security-related issues that are believed to have long-term significance for cloud storage.

III. DATA SECURITY CHALLENGES IN CLOUD COMPUTING

Cloud Computing security is the major concern to be addressed nowadays. If security measures are not provided properly for data operations and transmissions then data is at high risk. Since cloud computing provides a facility for a group of users to access the stored data there is a possibility of having high data risk. Strongest security measures are to be implemented by identifying security challenge and solutions to handle these challenges.

Following are the major security challenges that need to be addressed immediately.

- **Privacy:**Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or intentionally alter or even delete information. This becomes a major concern.

- **Data Integrity:** With getting the security of data, cloud service providers should apply mechanisms to ensure data truthfulness. Security should be maintained such that data can be only modified by the authorized person. In cloud based environment, data integrity must be maintained correctly to avoid the data lost.

- **Confidentiality:** To maintain confidentiality data understanding and its classification, users should be aware of which data is stored in cloud and its accessibility. Top vulnerabilities are to be checked to ensure that data is protected from any attacks. So security test has to be done to protect data from malicious user such as Cross-site Scripting, Access Control mechanisms etc..,.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

- **Access:** To secure the data from the unauthorized users the data security policies must be strictly followed. Since access is given through the internet for all cloud users, it is necessary to provide privileged user access. User can use data encryption and protection mechanisms to avoid security risk.

- **Breaches:** Data Breaches is another important security issue to be concentrated in cloud. Since large data from various users are stored in the cloud, there is a possibility of malicious user entering the cloud such that the entire cloud environment is prone to a high value attack. A breach can occur due to various accidental transmission issues or due to insider attack.

- **Storage:** The data stored in virtual machines have many issues one such issue is reliability of data storage. Virtual machines needs to be stored in a physical infrastructure which may cause security risk.

IV. PROPOSED ALGORITHM

A. *DESCRIPTION OF THE PROPOSED ALGORITHM:*

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Sharmir, and Leonard Adleman, who first publicly prescribed the algorithm 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. By securing the data, we are not allowing unauthorized access to it.
RSA algorithm uses two different but mathematically linked keys, one public and one private. In our cloud environment, public key can be shared with everyone, whereas the private key must be kept secret. Both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it.
Functioning of RSA is based on multiplication of two large numbers. Two large prime numbers are generated and multiplied. After multiplying two numbers, modulus is calculated the number that is generated is used as the public and private key. The two numbers that are used for multiplication-one of them is public other is private.

RSA algorithm involves three steps:

- Key Generation
- Encryption
- Decryption

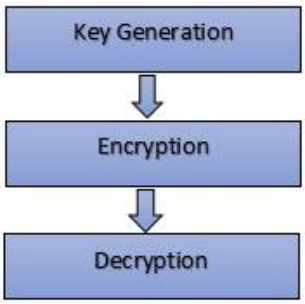

Fig.2. Steps involved in RSA Algorithm

B. *Steps involved in the Algorithm:*

Step 1: Key Generation:

The keys for the RSA algorithm are generated using the following way:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

- Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
- Calculate n=p*q.
    - n is the modulus for the public key and the private keys.
- Calculate the Euler's Totient function: $\phi(n) = (a-1) * (b-1)$.
- Choose an integer e such that $1<e<\phi(n)$, and e is coprime to $\phi(n)$ i.e. e and $\phi(n)$ share no factors other than 1; gcd $(e, \phi(n)) = 1$.
    - E is released as the public key exponent.
- Determine d as $d \equiv e^{-1} (\text{mod } \phi(n))$; i.e. d is modular multiplicative inverse of e (modulo $\phi(n)$).
    - This is done so that $d*e \equiv 1 (\text{mod } \phi(n))$.
    - d is kept as the private key exponent.

Now, the public key consists of the modulus n and the public exponent e. The private key consists of the modulus n and the private exponent d, which must be kept secret.

Step 2: Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data).
Following are the steps involved in the encryption process:

- Cloud service provider transmits the Public Key (n, e) to the user.
- The user maps the plaintext message as a positive integer m, $1<m<n$.
- Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user and the computed cipher text (data) C is $C = m^e (\text{mod } n)$.
- This cipher text or encrypted data is now stored with the Cloud service provider.

Step 3: Decryption:
Decryption is the process of converting the cipher text (data) to the original plain text (data).
Following are the steps involved in the de-encryption process:

- The cloud user requests the Cloud service provider for the data.
- Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e., C.
- The Cloud user then decrypts the data by computing, $m = C^d (\text{mod } n)$.
- Once m is obtained, the user extracts the original data from the message representative m.

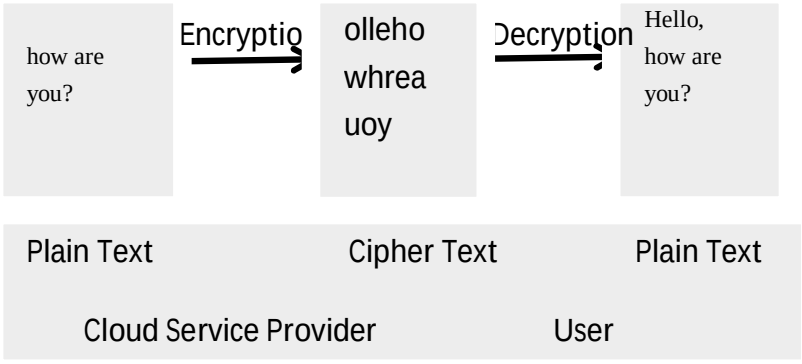

Fig 3: Encryption- Decryption Process

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

C. ***WHY TO USE RSA ALGORITHM?***

We should RSA algorithm because of its following features:

- **Secrecy and privacy**: The content of the information and communication must be ONLY accessible to the sender and the recipient of the information.
- **Integrity and Reliability**: The content must not be altered during the exchange phase, therefor it must stay in its original form.
- **Authentication**: This aspect is very important because RSA guarantees the origin of the sent information, only the sender with his own private key is able to encrypt the message therefor transform the message into an unreadable form consequently the receiver will have confirmation of the origin because he will be able to decrypt the message only through the corresponding public key.
- **Non repudiation**: The sender cannot state that the message has not been encrypted with his private key because the private key used for the encryption is unique and it's the owner's responsibility to make sure that it is not used by non-authorized third parties.

V. EXPERIMENTAL RESULTS

In this section, we are taking sample data and implementing RSA algorithm over it.

Step 1: Key Generation:

Table 1. Key Generation

Key Generation	
Choose two distinct prime numbers	Let p=61 and q=53.
Compute n=p*q	n=61*53 = 3233.
Compute Euler's totient function: • **Ø(n)=(p-1)*(q-1)**	Ø (n) = (61-1)*(53-1) = 60*52 = 3120.
Chose any integer e, such that 1 < e < 3120 that is coprime to 3120	Let e=17.
Compute d: • **$d = e^{-1} \pmod{Ø(n)}$**	$d=17^{-1} \pmod{3120} = 2753$
• **Public Key** • **Private Key**	(e, n) = (17, 3233) (d, n)= (2753,3233)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Step 2: Encryption:

Table 2. Encryption

Encryption	
Plaintext	Let the positive integer, m=65.
Cipher text • **$C = m^e \pmod n$**	$C = 65^{17} \pmod{3233} = 2790$

Step 3: Decryption:

Table 3. Decryption

Decryption	
Cipher text	C
Plain text • **$C = m^e \pmod n$**	$m = C^d \pmod n = 2790^{2753} \pmod{3233} = 65.$

VI. CONCLUSION AND FUTURE WORK

Cloud computing appears very useful service for many people; every third person is using cloud in different ways. Due to its flexibility, many persons are transferring their data to cloud. Cloud computing proves a very successful application for organisations because organisations have large amount of data to store and cloud provides that space to its user and also allows its user to access their data from anywhere anytime easily.

Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.

Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing RSA algorithm.

REFERENCES

1. Kalpanaand P. and Singaraju Sudha, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, Vol.1, Issue 4, 2012.
2. Arora Priyanka, Singh Arun and Tyagi Himanshu, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World ofComputer Science and Information Technology Journal, pp.179-183, 2012.
3. Hay Brian, Nance Kara and Bishop Matt, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th HawaiiInternational Conference on System Sciences, pp.1-7, 2011.
4. Curran Kelvin, Carlin Sean and Adams Mervyn, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August2011.
5. Kaur Randeep and KingerSupriya, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation inEngineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014.
6. Rao Velumadhava R. and Selvamani K., "Data Security Challenges and Its Solutions in Cloud Computing", Procedia Computer Science 48, pp.204 – 209, 2015.
7. Patwal MayankandMittal Tanushri, "A Survey of Cryptographic based Security Algorithms for Cloud Computing", International Journal of Technology Innovations and Research, Vol.8, 2014.
8. Khan S. Shakeeba and Tuteja R.R., "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Issue 1, 2015.
9. Pansotra Ashima and Singh Preet Simar, "Cloud Security Algorithms", International Journal of Security and Its Applications, Vol.9, No.10, pp.353-360, 2015.
10. Kaur Jai Puneet and KaushalSakshi, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume169, pp.103-112, 2011.
11. AroraRachna and ParasharAnshu, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of EngineeringResearch and Applications (IJERA), Vol. 3, pp.1922-1926, Jul-Aug 2013.
12. Jansen Wayne and Grance Timothy, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication, NIST SP - 800-144, 80 pp., 2011.

BIOGRAPHY

Kriti Singhalis a final-year student pursuing B.Tech in Computer Science from Shyama Prasad Mukherji College, University of Delhi.She has knowledge of Java, C++ and ASP.NET. Being a keen interest towards research, her interest area includes Cloud Computing, Data Mining and Prediction Methods.