MODIFIED RSA ENCRYPTION ALGORITHM IS USED IN CLOUD COMPUTING FOR DATA SECURITY

Yogita Gangboir[1], Praveen Shende[2]

[1.,2]CSE Dept, CSIT Durg, (India)

ABSTRACT

Cloud computing is rising day by day around the world. It has potential to fulfill the requirements of users. Cloud computing share distributed resources and services which belong to the different sites. However the security threat to the data is the most critical problem faced by the organizations. Since data or information is not secure in cloud computing, so there is need to provide some security method. When data is upload or download in cloud, that time data can be hacked or crashed. Hence the cryptographic approach is a major solution to the problem. Modified RSA Encryption Algorithm will secure the data in cloud. This algorithm will ensures security to service model for upload and download data in cloud environment. Data can be in the form of pdf file, images, text file etc.

Keywords: ***Cloud Computing, Modified RSA Encryption Algorithm, Security, Software as A Service..***

I. INTRODUCTION

At presently, the cloud computing becomes most serviceable technology. In the conventional model of cloud computing, the user's computer is fully responsible for both computing, data storage and data analysis and manipulation. The user's computer is integrated with data and all the software. As the data size and computational complexity increases exponentially, user's system losses its computing efficiency. Moreover, expansion of industries over the globe, make organizations to share database around the world. Indeed, organizations require a system which can solve above problem efficiently. And hence cloud computing comes into the picture. Cloud computing offers a cost-effective answer to manage the IT infrastructure in a flexible and scalable way. Cloud computing enables software applications, deployment platforms, even the computing resources to be made available on-demand using a pay-as-you-work model. This has got a great deal of attention towards the domain in late years. Any user can share the resources in cloud. There are many security challenges and issues. So we need to provide security in cloud system. Cryptography is one of the best solutions to provide security in cloud computing. In cryptography, encryption and decryption are process are done. Encryption is the process of converted plain text into cipher text and Decryption is reverse process of encryption that means to convert cipher text into plain text at other end, this process is called decryption. Cryptography is an essential part of secure communication. There are two types of cryptographic algorithm symmetric cryptography and asymmetric cryptography. Initially unencrypted data is treated as normal text.

A Symmetric cryptography is used only 1 secret key which is knowing by both the user sender and receiver. For eg. Data encryption standards (DES) and advanced encryption standards(AES). In asymmetric cryptography, used different keys for encryption and decryption of the data. It is also called public key cryptography. It has a

pair of keys : public key and private key. [yogi 6] Rivest Shamir Adleman(RSA) is best known pubic key cryptosystem. ure. There are two ways in which we can achieve security 1.encrypted file transfer 2.Strong secure protocol for transmission of files. RSA (Rivest, Shamir & Adleman) is an asymmetric cryptographic algorithm developed in 1977. It generates two keys: public key for encryption and private key to decrypt message [2].RSA algorithm consist of three parts: one is key generation which is to be used as key to encrypt and decrypt data, second is encryption part, where process of conversion of plaintext to cipher text is being carried out and third is decryption, where encrypted text is converted in to plain text at other side. As a public key is used for encryption and is well known to everyone and with the help of public key, hacker can use brute force method to find private key which is used to decrypt message. MREA prevents files and data from hackers and help safe uploading and downloading data from one end to other [2]. In this paper we approach MREA algorithm that is a modified RSA encryption algorithm to the existing RSA algorithm. Cloud computing works in an open environment, when we upload or store data in cloud there are number of users in cloud who want to access that file or data so need security concern. So that only authorized user can access file. When any user share a file to client or other user that time brute force attacker can hack the file or unauthorized user can try to access file. Hence need any security algorithm or cryptography technique which will security when we uploading downloading and sharing a file.

II. DATA SECURITY ISSUES IN CLOUD

2.1 Data Integrity

To providing the security in cloud in data, cloud service providers should implement mechanisms to ensure data integrity. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

2.2 Data Availability

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

2.3 Data Segregation

Because of the multi-tenancy feature of the cloud infrastructure, knowledge of many users share same physical storage location, so giving rise to the chance of information intrusion. This could be achieved by hacking through some vulnerability or by injecting shopper code. It will permit intrusion into others knowledge. A SaaS model ought to so maintain correct isolation between the information of from totally different users.

2.4 Data Access

The issue of information access is said to the protection policies followed by the cloud supplier for accessing the information. Security policies ought to be designed with a read to manage the access to the information by the class of the user.

2.5 Privacy and Confidentiality[10]

Once the client host data to the cloud panel so there should be some guarantee that only authorized user can access the data. It should provide Assurances to the clients and privacy policies and procedures should be in

place to assure the cloud users of the data safety. It should be assured to the cloud seeker that data hosted on the cloud panel will be confidential.

III. RELATED WORKS

Cryptography means to store the data and transform that data in a particular form so that only authenticate user can access that data and process with in it[8]. It associate with converting the plain text into cipher text(encryption), then reverse process(decryption).

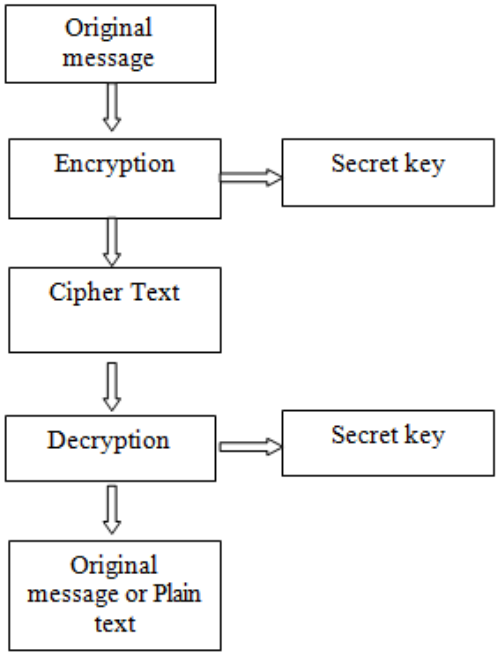

Fig. 1-Symmetric key Cryptography

In fig. 1, Symmetric key Cryptography is shown. Here for encryption, plain text is converted into cipher text, with use of secret key. And at decryption time it using again same secret key to convert cipher text into plain text

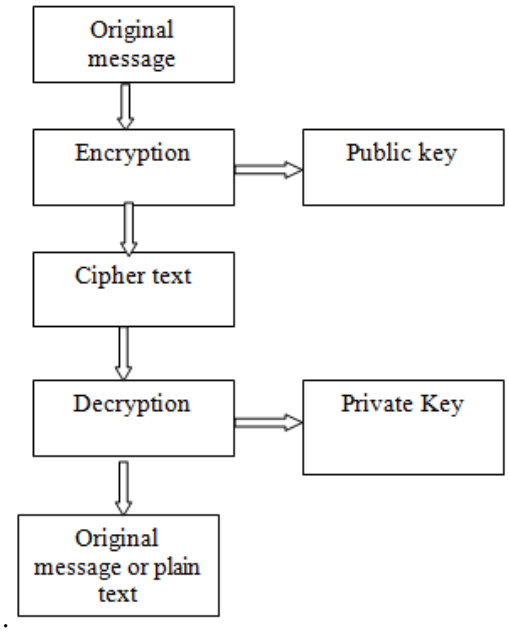

Fig. 2- Asymmetric key Cryptography

In fig. 2, Asymmetric key Cryptography is shown. Here for encryption process, plain text is converted into cipher text, with use of public key. And at decryption time it using private key to convert cipher text into plain text.

Asymmetric key cryptography is used two different keys: a public key and a private key for encryption and decryption respectively. Private key is cannot be derived from public key. This scheme, provide much strength of security.

IV. MODIFIED RSA ENCRYPTION ALGORITHM

RSA Algorithm can be summarized as follows:[3]

1. first generate keys with required digits.
2. Save and load the key, the key is saved as plain text.
3. Use specified key to encrypt any file with RSA algorithm.
4. Encrypted data can be loaded and decrypted with the specified key to restore the original data.

4.1 MREA Method

MREA is an asymmetric-key cryptosystem algorithm[5], for communication, two keys are required: a public key and a private key. The public key is used only for encryption [6], and the private key is used only for decryption [4]. key generation algorithm :[3]

This MREA method have removed the drawback of RSA [19] MREA Algorithm can be summarized as follows:

1. Choose four large prime numbers p, q, r and s randomly and independently of each other. All primes should be of equivalent length.
2. Compute $n = p \times q$, $m = r \times s$, $\varphi = (p-1) \times (q-1)$ and $\lambda = (r-1) \times (s-1)$.
3. Choose an integer e, $1 < e < \varphi$ such that $\text{Gcd}(e, \varphi) = 1$
4. Compute the secret exponent d, $1 < d < \varphi$, such that $e \times d \bmod \varphi = 1$.
5. Select an integer $g = m+1$.
6. Compute the modular multiplicative inverse: $\mu = \lambda^{-1} \bmod m$.

The public (encryption) key is (n, m, g, e). The private (decryption) key is (d, λ , μ)

Encryption: Let F be a data to be encrypted where the contents of data are taken into string S. Select random number r, where $r < m$. Compute cipher text as $C = g_{s\wedge e \bmod n} * r_m \bmod m_2$

Decryption: Compute original message: $S = (((c_\lambda \bmod m_2 - 1) / m) * \mu \bmod m)_d \bmod n$.

V. SECURITY ANALYSISI OF ALGORITHM

For security analysis of this algorithm there are three attack approaches: Brute Force, Mathematical, and Timing attacks

5.1 Brute Force Attack [6][7]

In this attack, attacker tries to guess the private key by all possible combinations [6]. In MREA method its complex to find out the keys. It uses four large prime numbers.

5.2 Mathematical Attack [6]

In this attack d, λ , μ were determined by the attacker to find the private key. This attack could be prevented by using keys with 2048 bits size. MREA 1024 bits key size is quite enough for preventing this attack.

5.3 Timing Attack[7]

In timing attack, the private exponent was determined by the attacker by calculating the time with exploiting the timing variation of the modular exponentiation.

Table1: Comparison between RSA and MREA method

S. No.	RSA method	MREA method
1.	Less Security	More Security
2.	More process speed	Less process speed
3.	brute force attack is more permeable	brute force attack is little permeable
4.	Use two prime numbers	Use 4 large prime nos.

VI. CONCLUSIONS

Modified RSA Encryption algorithm (MREA) is used, when data is uploaded in cloud panel and data is downloaded from cloud to user's system. Only authenticate user can access the file or data. This algorithm is more secure rather than other method. This algorithm is using large prime numbers, so it will be difficult for hackers to guess the prime numbers to find out the keys. Brute force attacker will not be crack or miss use the data. This method will ensure security for data in cloud when data will be uploaded and downloaded.

REFERENCES

[1] Agentless Recovery. http://www.ibm.com/deceloperworks/cloud/liberary/cl-agentlessrecovery/[Accessed`; january 2013]

[2] Amazon EC2 Service http://aws.amazon.com/ec2

[3] Rajan S Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption using Secure RSA", International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013.

[4] Gaurav R. Patel, Prof. Krunal Panchal, Sarthak R. Patel, "A Comprehensive Study on Various Modifications in RSA Algorithm", International Journal of Engineering Development and Research. ISSN: 2321-9939.

[5] Amare Anagaw Ayele, Dr. Vuda Sreenivasara, "A Modified RSA Encryption Technique Based on Multiple Public keys", International Journal of Innovative Research in Computer and Communication Engineering. Vol.1, Issue 4, June 2013.

[6] Faraz Fatemi Moghaddam, Omidreza Karimi, Maen T. Alrashdan, "A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments", IEEE 2nd International Conference on Cloud Networking (CloudNet) 2013.

[7] Dhananjay Puglai, Harsh Chitrala, Salpesh Lunawat, P. M. Durai Raj Vincent, "An Efficient Encryption Algorithm on Public key Cryptography", International Journal of Engineering and Technology, Vol 5 No 3 Jun-Jul 2013.

[8] Alok Kumar Shukla, V. Kapoor "Comparison among RSA, modified RSA using Two public key and MRSA using n prime number with n prime number", International Journal of Engineering Sciences & Research Technology[713-720].

[9] Sonal Sharma, Jitendra Singh Yadav, Prashant Sharma, "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering.

[10] Parsi kalpana, Sudha Singaraju. "Data Security in Cloud Computing Using RSA Method ", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[11] Bhupesh Kumar Dewangan and Sanjay Kumar Baghel, "Survey on Ensuring Security Model of Cloud Computing", IJAIR, ISSN, 2278-7844.

[12] Bhupesh Kumar Dewangan and Praveen Shende, "Survey on User Behavior Trust Evaluation in Cloud Computing", International Journal of Science, Engineering and Technology Research (IJSETR), ISSN, 2278 – 7798 Volume 1, Issue 1, July 2012

[13] http://2012ieeetitles.blogpost.in/2012/07/a-secure-erasure-code-based-cloud.html.

[14] Jeong-Min et al, "Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments", IEEE ACIS/JNU Int. Conference on Computers, Networks, Systems, and Industrial Engineering (CNSI 2011),Korea.

[15] "NIST Cloud Computing Standards Roadmap " NIST Special Publication 500-291, Version 2 (Supersedes Version 1.0, July 2011) .

[16] Pratap Murukutla, K.C. Shet, "Single Sign On for Cloud .In", International Conference on Computing Sciences,2012 IEEE DOI 10.1109/ICCS.2012.66.

[17] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing",

[18] Rashmi,Dr.G.Sahoo and Dr. S. Mehfuz, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", International Journal on Cloud Computing: Services and Architecture (IJCCSA) , Vol.3, No.4, August 2013 .

About Authors

Yogita Gangboir, received B.E. (Info. Tech.) in year 2013 and pursuing M.Tech.from (Computer Sc.) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India. Her interests are Programming Languages(Java, PHP) and Cloud Computing.

Mr. Praveen Shende, received B.E. (Computer Sc.) in year 2009 and in pursuit for M.Tech. (Computer Sc.) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh,India, His interests are Programming Languages(Java, PHP,Zoomla), Cloud Computing and DBMS, Computer Networks, Computer System Architecture.