Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/3144
DOI URL: http://dx.doi.org/10.21474/IJAR01/3144
ISSN NO. 2320-5407

RESEARCH ARTICLE

PERFORMANCE ANALYSIS OF MODIFIED RSA AND RSA HOMOMORPHIC ENCRYPTION SCHEME FOR CLOUD DATA SECURITY.

D. Chandravathi and Dr. P. V. Lakshmi.
1. GVP College for Degree and PG courses, Rushikonda, Visakhapatnam-45.
2. GITAM University, Rushikonda, Visakhapatnam-45.

Manuscript Info

Manuscript History

Received: 15 December 2016
Final Accepted: 19 January 2017
Published: February 2017

Key words:-
Cloud Security, RSA Algorithm, Homomorphic Encryption, cipher text,decryption, Clustering, mRSA .

Abstract

Cloud computing plays an important role for storing large data. It is a large pool of easily and accessible virtualized resources. The major recourses are hardware, development platforms and services. Since the data is open, security of data is a major issue which has to be focused. To ensure the security of data in cloud environment, we propose a method called modified RSA (MRSA) algorithm along with homomorphic encryption. .Homomorphic Encryption enhances the security measures of un-trusted systems or applications. It converts the data into cipher text which is analyzed and worked with it as if it were still in its original form. It allows complex mathematical operations to be performed on encrypted data which does not compromise the process of encryption. This paper presents an effective analysis of RSA and a new modified RSA with Homomorphic operations. In the modified RSA (MRSA) encryption scheme clustering of prime numbers for the generation of keys for encryption and decryption is done which fastens the process of encryption. The weakness of RSA lies in the generation of Prime numbers. This is achieved by a new classification technique in modified RSA (MRSA). Hence, elimination of redundant messages is done on the same values of the product of two prime numbers by classifying the keys. Hence, Security is enhanced.

Introduction:-

Cloud Computing is the most innovative driving force in many small, medium and large sized companies. It has three delivery models named as Saas, Iaas, Paas. It has four deployment models such as private cloud, public cloud, hybrid cloud and community cloud [17][5]. As the services of cloud computing are used by many of the cloud users , the major concern is the security of their data in the cloud .Data security is always of major concern .It plays an important role in trust worthiness of computing .Cryptography is the art of protecting secret information. There are two types of cryptography: secret-key cryptosystem and public-key cryptosystem [4][5]. The first type is the secret-key cryptosystem which uses the same key to encrypt and decrypt the ciphertext .For this reason, this types is also called as symmetric cryptosystem. Since it takes less computational time, it has several drawbacks. There are too many keys along with the key distribution problem, authentication and nonrepudiation problem are of concern. Hence ,to solve the problems of symmetric cryptosystem,RSA cryptosystem is the one of the most popular approach for such problems. The RSA cryptosystem was developed in 1977 by Ronald L. Rivest, Adi Shamir, and Leonard Adleman at MIT and first published in 1978 [7].During the year in 1978 R.L. Rivest, A. Shamir, and L. Adleman

Corresponding Author:- D. Chandravathi.
Address:- GVP College for Degree and PG courses, Rushikonda, Visakhapatnam-45.

developed the RSA public-key cryptosystem[4]. The RSA cryptosystem is simply uses the concept of modular exponentiation which says that the modulus 'n' is the product of two large prime's p and q and the Public key and private key are obtained by:

$$e = d^{-1} \bmod Ø(n)$$

The encryption process is performed using the public key 'n ' and 'e 'as follows:

$$C = M^e \pmod n$$

Where M is the plaintext such that 0<M<n and C is the ciphertext which can be decrypted using the private key 'n ' and 'd' as follows:

$$M = C^d \pmod n$$

At present security should be provided to encrypt data that is stored both in Public Cloud and Private Cloud.Security also provides secure transmission from a local machine to a cloud data store. The stored data is encrypted and the channel of data transmission is well secured with the help of key exchanges. But actually performing computations on the data stored in the cloud, it requires decrypting it first, which makes critical data available to the cloud provider. The proposal here is to encrypt data before sending to the cloud providers. Thereby performing computations on clients' data at their request.To achieve this it is also necessary to hold the cryptosystems based on Homomorphic Encryption.

Homomorphic Encryption:-

Homomorphic Encryption can either be a Fully Homomorphic Encryption (FHE) or Somewhat Homomorphic Encryption (SHE)[3][4]. It has the property of mellability. Malleability is a property of some cryptographic algorithms. It states that an encryption algorithm is malleable if it is possible for an adversary to transform a ciphertext into another ciphertext which decrypts to a related plaintext. Homomorphic encryption is the process of performing encryption on encrypted data .The encrypted data which is stored in the cloud is encrypted using homomorphic operations and decrypted with operations .The operations are Additive and Multiplicative operations[3][4][5].

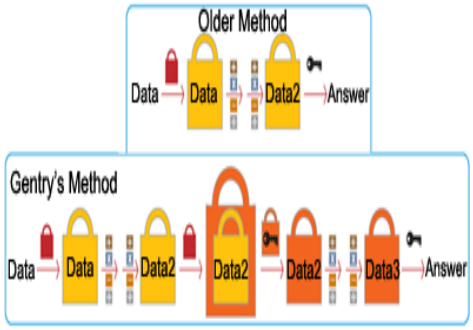

Fig 1.1:-

If the process has both additive and multiplicative operations performed on the encrypted data, then it is Fully Homomorphic Encryption (FHE).The partially Homomorphic encryption allows either additive or multiplicative operations on encrypted data.RSA encryption allows multiplicative operations on encrypted data.
Homomorphic encryption plays an important role in cloud computing. It allows companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services.

For example, a user sends a request to add the numbers 1 and 2, which are encrypted to become the numbers 33 and 54, respectively. The server in the cloud processes the sum as 87, which is downloaded from the cloud and decrypted to the final answer, 3.A normal symmetric cipher -- DES, AES is not homomorphic[2]. The RSA algorithm is homomorphic but only with respect to multiplication.

Related work:-

Craig Gentry of IBM, in 2009, has proposed the first encryption system "Fully Homomorphic". The system computes and evaluates an arbitrary number of additions and multiplications and also calculates any type of function on encrypted data[1][3]. The internal working of this adds another layer of encryption and for every few steps it uses an encrypted key to unlock the inner layer of scrambling. Hence, this decryption "refreshes" the data without exposing it and allowing an infinite number of computations on the same.

The application of fully Homomorphic encryption is an important brick in Cloud Computing Security. The outsourcing of the calculations on confidential data to the Cloud server is possible, keeping the secret key that can decrypt the result of calculation [3].

Proposed Method of MRSA:-

The new method mRSA is the encryption process which is carried out with two prime numbers p,q. In RSA algorithm, we take two prime numbers and the generate the keys for encryption. In this new approach generation of keys is done by taking prime numbers which are clustered using Euclidian Distance which solves the problem of redundant messages. The clustering simplifies the selection of prime numbers which are nearest to each other. So a situation in which the cipher text is the same as the plaintext in some values of n which is the product of two prime numbers p and q are resolved and messages which are redundant is eliminated.

The MRSA aims at classification of prime numbers for key generation. An agreement is done for communication with the parties with a secure set of alternative prime numbers (PR). This helps in alternative values of prime number for p or q or both. In addition, this set of prime numbers is divided into different classes. Each class contains a specified numbers of primes. We generate the prime numbers by taking odd numbers within the range N. This is a process of filtration. We eliminate all even numbers except 2 , since they are not prime. This clustering is done by taking into the account of the number of cluster or classes. Then each of the prime numbers starting from the beginning are taken one at a time and grouped one by one, cluster by cluster ie., 2 in c1, 3 in c2, 5 in c3, 7 in c4 and so on .

The number of clusters must be less than the half of the range of N and prime numbers within the range and can be limited. To select a certain neighbor of one of the classes in that set it is dependent on a secure distance (d1). This distance will be used to choose one prime number or both. By assigning another secure distance (d2) inside the selected class we generate the keys for encryption [16]. The purpose of the distance (d1) is to use an agreement secure parameter to choose one of the classes inside the set of all classes and this distance must be changed periodically to remove the redundant messages and to enhance more security for the RSA algorithm. Ciphers are generated for the corresponding keys due to a specific value of n and we can generate a new secure value of n to overcome these redundant values of messages.

Selection of the prime number 'p' is done from the clusters say p'. Then we compute 'n' ie n'. An agreement secure parameters is generated. In order to acknowledge the receiver by changing 'n', the sent ciphertex must be appended by a secure agreement parameter, denoted by f, inside the ciphetext[9][10] . This suggested parameter is used to prevent sending the value of alternative value as a public key, so we get a more secure procedure for RSA algorithm by reducing the public key into one parameter that is the public key of the user only because in the traditional method of RSA, the public key consists of two parameter; the value of n and the public of the user (e)[11].

Algorithm:-

The Algorithm has three phases:

Clustering Algorithm:-

1. Let C be the cluster where c1,c2,c3…cn be subsets of C.
2. Enter C value. Ex C=5.
3. Let N be the number of prime numbers starting from 2.
4. Input N. Say N=50.
5. Eliminate all even numbers with in N value.
6. Let it be N1.
7. Then select all the prime numbers from N1.
8. Depending on C, Place the numbers one by one in each cluster as shown in fig 1.3.

9. Now choose the one prime number from one of the cluster.
10. Select the next prime number and find the nearest from the first by Euclidean distance.

Key Generation:-
Choose two prime numbers from PR
n= p*q
Ø (n)=(p-1)*(q-1)
Let e be the public key
Let d be the private key
c= m^e mod n.
if c=m then

Sender operation:-
1: Choose d1 of the one of subsets Ci in S for the secure class
2: Choose d2 inside Ci to pick one alternative prime p'
3: Compute n'=p'*q
4: Compute Ø (n')=(p'-1)*(q-1)
5: Choose alternative public key , lets e'
6: Generate the corresponding private key d'
7: Compute the ciphertext C'=$m^{e'}$ mod n'
8: Combine the agreement factor f with the new ciphetext and send C'' as:
C''=[C',f]

Multiplicative Homomorphic encryption:-
Generate two ciphers and suppose we have two ciphers C1 and C2 such that:
C1 = $m1^e$ mod n
C2 = $m2^e$ mod n
C1.C2 = $m1^e m2^e$ mod n = $(m1m2)^e$ mod n

RSA with Homomorphic Encryption:-
The RSA cryptosystem is the most widely used public-key cryptosystem. It was developed in the year 1978 by Rivest, Shamir, and Adleman. It is one of the first homomorphic encryption schemes

Key Generation: KeyGen(p, q)
Input:- Two large primes – p, q
Compute n = p . q
φ (n) = (p - 1)(q - 1)
Choose e such that gcd(e, φ (n)) = 1
Determine d such that e . d ≡ 1 mod φ (n)

Key:-
public key = (e, n)
secret key= (d, n)

Encryption:-
c = me mod n
where c is the cipher text and m is the plain text.

RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product. Given ci = E(mi) = mie mod n, then **(c1 . c2) mod n = (m1 . m2)e mod n**

Example:-
- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20

- Choose e such that $1 < e < \varphi(n)$ and e and n are co-prime. Let e = 7
- Compute a value for d such that $e \cdot d \equiv 1 \bmod \varphi(n)$. One solution is d = 3
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)

Example of homomorphic property:-
Now, let m1=2 and m2=3 c1 = m1e mod n=27 mod 33=29 c2 = m2e mod n=37 mod 33=9 c1.c2 = 29 * 9 = 261 By decrypting (c1.c2) we get: 2613 mod 33 = 6 = 2 * 3.

Results:-

The Analysis of the two algorithms is below. With different file sizes in kilo bytes (KB) is taken and the estimation of time with respect to encryption and Decryption time (msec) is shown in the graph.

It is clear that the mRSA takes less time and secure and efficient than RSA with homomorphic operations.

Encryption Time Analysis:-
Table 1:-

File Size (KB)	RSA (msec)	MRSA(msec)
26	27	24
85	53	45
100	87	64
143	112	109
187	157	126
258	179	168
544	453	423
800	1098	976
1024	1478	1478

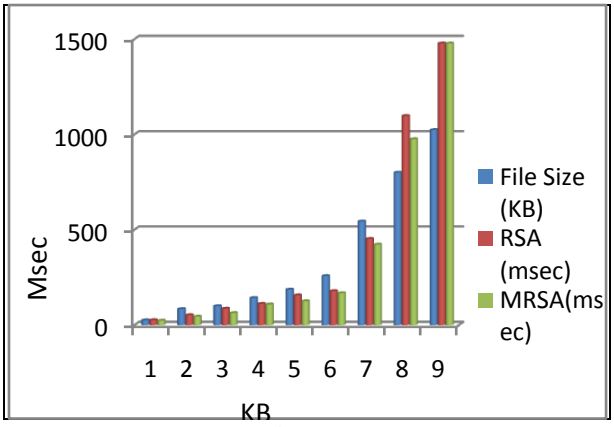

Fig 1.2:-

Decryption Time Analysis:
Table 2:-

File Size (KB)	RSA (msec)	MRSA(msec)
26	167	164
85	278	272
100	324	324
143	379	389
187	478	467
258	567	559
544	772	776
800	995	976
1024	1114	1101

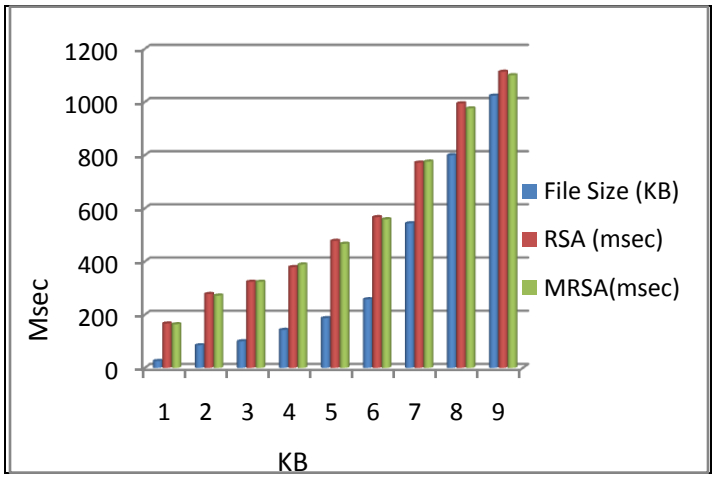

Fig 1.3:-

Conclusion:-

The cloud security is based on Homomorphic encryption, is a new concept of security which enables us to provide results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, with respect of the data confidentiality. Our work is based on the application of partially Homomorphic encryption to the Cloud Computing security. It also analyzes and the improvement of the existing cryptosystems to allow servers to perform various operations requested by the client. The improvement of the complexity of the Homomorphic encryption algorithms and compare the response time of the requests to the length of the public key is to be considered. Also this method reduces the redundant messages occurred in RSA method. We see that for some values of n, there is a major problem in which the message and its corresponding ciphetext are the same. At the presence of recent active attacks, this problem can be exploited by many attackers. For this reason, this method mRSA presents an active solution by changing the value of n. Hence,MRSA is more secure and efficient than RSA with homomorphic operations.

References:-

1. Craig Gentry, A Fully Homomorphic Encryption Scheme, 2009.http://crypto.stanford.edu/craig/craig-thesis.pdf.
2. Understanding Homomorphic Encryption http://en.wikipedia.org/wiki/Homomorphic_encryption.
3. Computing Blindfolded: New Developments in Fully Homomorphic Encryption Vinod Vaikuntanathan.
4. A Fully Homomorphic Encryption Implementation on Cloud Computing Shashank Bajpai and Padmaja Srivastava Cloud Computing Research Team, Center for Development of Advanced Computing [C-DAC], Hyderabad.
5. Homomorphic Encryption Applied to the Cloud Computing Security Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI.
6. Vic (J.R.) Winkler, "Securing the Cloud, Cloud Computer Security, Techniques and Tactics", Elsevier.
7. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2):120-126, 1978.
8. R. L. Rivest, A. Shamir and L. Adleman "A method for obtaining digital signatures and public – key cryptosystems" Communications of the ACM, vol. 21,pp. 120 - 126, 1978.
9. W. Stallings "Network and internetwork security: principles and practice" Prentice - Hall, Inc., 1995.
10. W.Stallings "Network security Essentials: Applications and Standards" Pearson Education India, 2000.
11. J. Joshi, et al. "Network Security" Morgan Kaufmann, 2008.
12. W. Stallings "Cryptography and network security vol. 2" prentice hall, 2003. K. Ming Leung , k-Nearest Neighbor Algorithm for Classification , POLYTECHNIC UNIVERSITY Department of Computer Science / Finance and Risk Engineering , 2007.
13. C .Aayush ,and M . Srushti ," Modified RSA Algorithm: A Secure Approach ", CSDL HomeCCICN2011Computational Intelligence and Communication Networks, International Conference on 2011.
14. V.Kuldeep, Kr.Rajesh,and C .Ritika , "Modified Prime Number Factorization Algorithm (MPFA) For RSA Public Key Encryption", International Journal of Soft Computing & Engineering 2012 .
15. R.S. Dhakar, and P. Sharma, "Modified RSA Encryption Algorithm (MREA)" , Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on , Page(s): 426 – 429, 7-8 Jan. 2012 .
16. A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm , Dr. Abdulameer K. Hussain ,Computer Science Department, Jerash University,Jerash, 00962-02, Jordan, IJISET , Vol. 2 Issue 1, January 2015.
17. Performance Evaluation of RSA Algorithm in Cloud Computing Security, *Asma Khatoon and Dr. Ataul Aziz Ikram,* International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 12 No. 1 Nov. 2014, pp. 336-345 © 2014 Innovative Space of Scientific Research Journals http://www.ijisr.issr-journals.org/