iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: III Month of publication: March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3243

Performance Analysis of Homomorphic Encryption algorithms for Cloud Data Security

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

Abstract: Data security is one of the crucial tasks for any information that is stored in the cloud server. Many cryptographic algorithms have been in existence but still are prone to various types of attacks. The major functionality for a cryptosystem is to prevent from various attacks from learning messages which are confidential. Cryptography plays an important role in data transmission and protecting the network. It also prevents reading private messages from third party. The cloud security involving homomorphic encryption is a new concept of providing security to confidential information. It enables us to provide results of calculations on encrypted data without knowing the raw data on which the calculation was carried out. It maintains data privacy and confidentiality. This paper focuses on the performance analysis of different homomorphic encryption algorithms. The algorithms include Modified RSA (MRSA), RSA, Hybrid

homomorphic encryption and hill cipher with respect to homomorphic encryption. A comparative study is carried with the above algorithms and it is clear that MRSA is more efficient and secure than others.

Keywords: Data security, cryptography, attacks, homomorphic encryption, MRSA.

I. INTRODUCTION

Cryptography is the art of protecting secret information. There are two types of cryptography namely, secret-key cryptography and public-key cryptography. The first type, secret-key cryptography, which uses the same key to encrypt and decrypt the cipher text [1][2].Hence, this type is also called as symmetric key cryptography. Since it requires less investment for processing, it has a few disadvantages [2]. There are many keys along with the key distribution problem, authentication and non-repudiation problems which are of great concern [3]. Hence, to solve the problems of symmetric cryptography, RSA cryptography is the one popular approach [3][4]. RSA algorithm is one of the most efficient algorithms which provide security as one key is used for encryption and another key is used for decryption. But still it has its limitations. The shortcoming of RSA scheme is in the generation of prime numbers which is achieved by a new classification technique in modified RSA (MRSA)[2][3].

Cloud computing is the most innovative driving force in many small, medium and large sized companies. It has three delivery models namely Iaas , Saas, Paas and four deployment models such as private, public, hybrid and community cloud. As the services of cloud computing which are used by many of the cloud users, the security of their data in the cloud is of major concern. Data security is always a major concern .It plays a prominent role in trust worthiness of computing.

Homomorphic Encryption scheme enhances security factors of untrusted applications or systems. It changes over the information into cipher text which is dissected and worked with it as though it were still in its unique[4]. It permits to perform complex mathematical operations to be performed on encrypted data. Hence, the process of encryption is a secured mechanism where the security is not compromised [5].

Homomorphic encryption permits computing on encrypted data. That is, the client can encrypt his data x and send the encryption Enc(x) to the server. The server can then take the cipher text Enc(x) and evaluate a function f on the underlying x obtaining the encrypted result Enc(f(x))[2][5]. The client can decrypt this result achieving the wanted functionality, but the server learns nothing about the data that he computed on. Homomorphic encryption is functional encryption, where our goal is to reveal the result of the computation to the server, but protect all other information about our encrypted input [3].

A. MRSA homomorphic Encryption

The new MRSA method is a new technique in which the prime numbers are classified into clusters basing on the sieve method and then by using Euclidian distance the nearest prime numbers are selected[1][2]. By doing so, the efficiency is increased and also reduces the redundant messages. Hence, elimination of redundant messages is done on the same values with multiplication of two prime numbers by classifying keys. Hence, security is improved.

B. Algorithm

The Algorithm has three phases:

1) Clustering Algorithm

a) Let C be the cluster where c1,c2 ,c3…cn be subsets of C.
b) Enter C value. Ex C=5.
c) Let N be the number of prime numbers starting from 2.
d) Input N. Say N=50.
e) Eliminate all even numbers with in N value.
f) Let it be N1.
g) Then select all the prime numbers from N1.
h) Depending on C, Place the numbers one by one in each cluster as shown in fig 3.1
i) Now choose the one prime number from one of the cluster by calculating the distance of the neighbor.
j) Select the next prime number and find the nearest from the first by Euclidean distance.

2) Key Generation

a) Choose two prime numbers from PR
b) n= p*q
c) Ø (n)=(p-1)*(q-1)
d) Let ‘e’ be the public key
e) Let’ d’ be the private key
f) c= m^e mod n.

If c=m then performs sender operation as below:

3) Sender Operation

a) Choose d1 of the one of subsets Ci in S for the secure clas
b) Choose d2 inside Ci to pick one alternative prime p'
c) Compute n'=p'*q
d) Compute Ø (n')=(p'-1)*(q-1)
e) Choose alternative public key , lets e
f) Generate the corresponding private key d'
g) Compute the ciphertext C'=$m^{e'}$ mod n
h) Combine the agreement factor f with the new ciphetext and send C" as:

C"=[C',f]

C. Multiplicative Homomorphic encryption:

Generate two ciphers and suppose we have two ciphers C1 and C2 such that:

$$C1 = m1^e \bmod n$$

$$C2 = m2^e \bmod n$$

$C1.C2 = m1^e m2^e \bmod n = (m1m2)^e \bmod n$

II. ANALYSIS AND RESULTS

The analysis was carried with different file sizes starting with a small size of file taken in MB to a bigger one. The encryption time and decryption times were observed in milliseconds. An average time was taken for each of the execution of the files .It is observed that the encryption time of MRSA homomorphic encryption is less when compared to RSA, Hill cipher and hybrid encryption algorithms.For a file size of 26 KB the encryption time of MRSA is 24 msecs, RSA is 27msecs and Hybrid and Hill cipher are 37 msecs. And as the file size is increased to 1023KB both MRSA and RSA are near to each other but still there were no redundant messages in MRSA when compared to RSA homomorphic encryption.

A. Encryption Time

Table 1

File size(KB)	Hill cipher(msecs)	Hybrid ELGAMAL(msecs)	RSA(msecs)	MRSA(msecs)
26	57	35	27	24
85	116	87	53	45
100	145	103	87	64
143	223	217	112	109
187	299	298	157	126
258	367	317	179	168
544	789	607	453	453
800	1223	1185	1098	976
1023	3045	2070	1477	1478

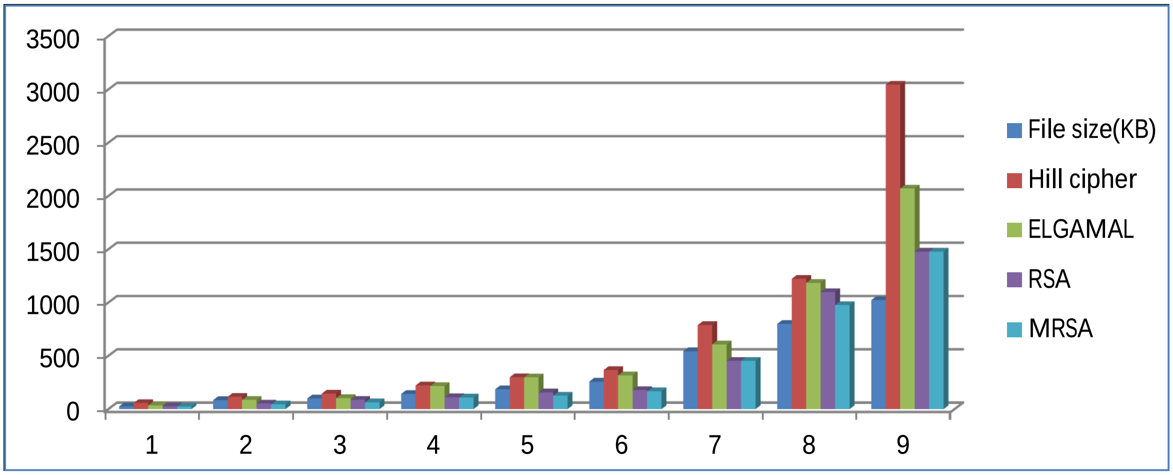

Fig 1

B. *Decryption Time*

The average decryption time of MRSA, RSA, Hybrid encryption and Hill cipher with homomorphic encryption scheme is analysed. From the analysis it is clear that MRSA homomorphic encryption is fast when compared to the rest of the algorithms. The decryption time of MRSA is 165 msecs for a file size 26 KB and is gradually increased for 1023 KB file size. It is observed that RSA homomorphic takes more time for decryption than MRSA.

Table 2

File Size (KB)	Hill cipher(msecs)	Hybrid-Elgamal(msecs)	RSA(msecs)	MRSA(msecs)
26	265	230	167	165
85	389	318	278	272
100	415	385	324	324
143	512	460	380	389
187	598	521	477	470
258	710	639	570	559
544	903	870	772	776
800	1130	1080	995	980
1023	2123	2070	1120	1101

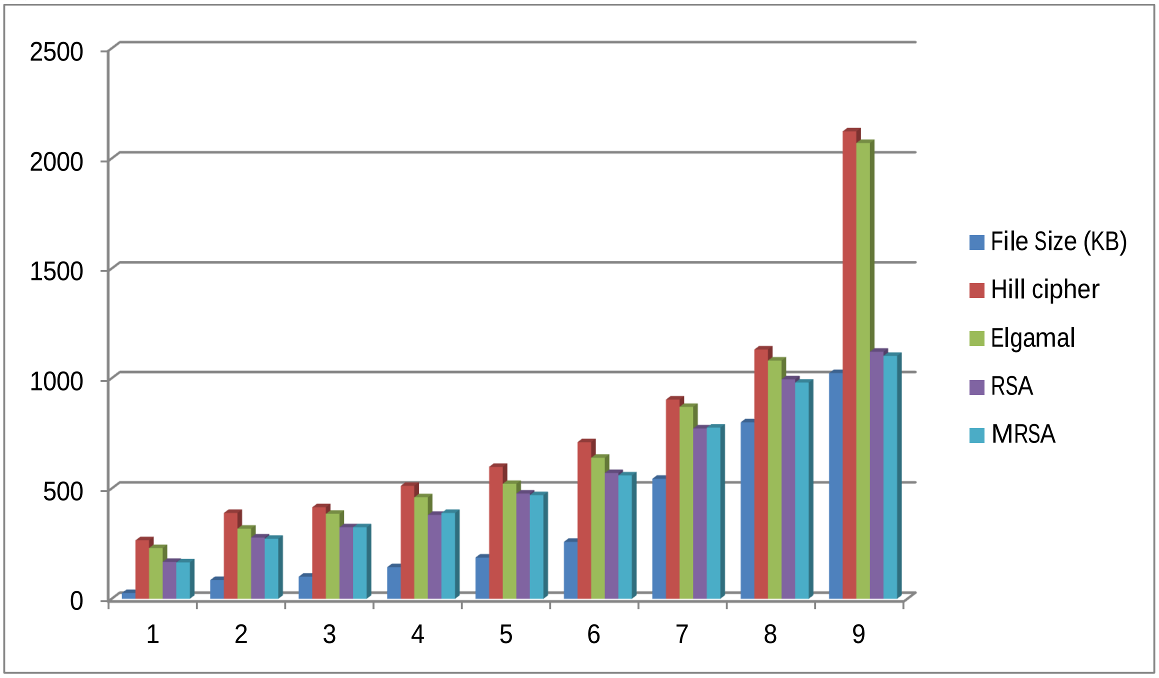

Fig 2

III. CONCLUSION

The application of Homomorphic encryption is an important milestone in Cloud Computing security which allows performing calculations on confidential data in the Cloud server. It is a new concept which generates the results of calculations on encrypted data without knowing the raw data by performing operations on encrypted data. The new algorithm MRSA homomorphic encryption plays a very important role in generation of prime numbers which are classified into clusters. This helps in reducing the redundancy messages and also takes less time for encryption than that of Hill cipher, Elgamal, RSA and MRSA homomorphic algorithms. The proposed Scheme preserves the data from invisibly leaking of the sensitive information which enhances security.

REFERENCES

[1] ‘Performance Analysis of Homomorphic encryption schemes for cloud data security’ , IJAR vol5(2) ISSN 2320-5407, Feb 2017.
[2] ‘A Novel Homomorphic encryption Technique for generation of keys using cluster classification for cloud security’, IJSER, vol 7, ISSN 2229-5518, Jun 2016.
[3] ‘Homomrphic encryption using Hill cipher for cloud data security’, IJAIST vol 7 ISSN 2229-5518,sept 2016.
[4] ‘A New Hybrid Homomorphic encryption scheme for cloud data security’,ACST vol 10, ISSN 0973-6107,April 2017.
[5] Craig Gentry, A Fully Homomorphic Encryption Scheme,2009.http://crypto. stanford.edu/craig/craig-thesis.pdf.
[6] Understanding Homomorphic Encryption http://en.wikipedia.org/wiki/ Homomorphic_encryption.
[7] Computing Blindfolded: New Developments in Fully Homomorphic Encryption Vinod Vaikuntanathan.
[8] A Fully Homomorphic Encryption Implementation on Cloud Computing Shashank Bajpai and Padmija Srivastava Cloud Computing Research Team, Center for Development of Advanced Computing [C-DAC], Hyderabad.
[9] Homomorphic Encryption Applied to the Cloud Computing Security Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI.
[10] 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.
[11] HOMOMORPHIC ENCRYPTION BASED DATA SECURITY ON FEDERATED CLOUD COMPUTING, Anitha R.,and Vijayakumar V, ARPN Journal of Engineering and Applied Sciences,VOL. 10, NO. 5, MARCH 2015 ISSN 1819-6608.
[12] Faster RSA Algorithm for Decryption Using Chinese ,Remainder Theorem , G.N. Shinde1 and H.S. Fadewar2, 2008 ICCES ICCES, vol.5, no.4, pp.255-261.
[13] W. Stallings “Network and internetwork security: principles and practice” Prentice - Hall, Inc., 1995.
[14] W.Stallings “Network security Essentials: Applications and Standards” Pearson Education India, 2000.
[15] 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.