IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Modified RSA Cryptosystem in a cloud based environment

Harsh Sahay

Master of Technology, Institute of Engineering and Management, Kolkata, India

Corresponding Author: Sahayharsh53@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i6.963966 | Available online at: www.ijcseonline.org

Accepted: 11/Jun/2019, Published: 30/Jun/2019

Abstract **-**A traditional RSA Cryptosystem is based on only two prime numbers which is an efficient algorithm for preventing an unauthorized access over the internet. But there are some drawbacks of RSA cryptosystem, such as its high computational time. The primary motivation of our work is to reduce average computational time and provide better data security compared to traditional RSA. In this work we are modifying basic RSA cryptosystem algorithm by using three prime numbers which provides better data security as compared to standard RSA algorithm. Instead of applying RSA over each data unit, multiple data units are merged together to form one merged unit. The modified RSA is applied on the merged unit to form a cipher text which is sent by the sender. For merging multiple data units into single data unit, Cantor's pairing algorithm has been used. At the receiver's end the cipher text sent is received. The cipher text is deciphered using our modified RSA algorithm. Then this merged data unit is separated (unpaired) using Cantor's unpairing algorithm. The highlight of this work is that, it increases the efficacy of the asynchronous cryptography (as compared to traditional RSA). The proposed framework increases security and reduces the average time taken for sending the data from sender to receiver. We are showing all procedures in a cloud environment.

Keywords –Cloud Computing, Cryptography, RSA, public key, private key, pairing and unpairing algorithm.

I. INTRODUCTION

In recent trends internet provides communication between peoples, defense personals, gives facility to electronic payment and many others. This is reason behind much concern of privacy, identifying theft, security etc. Recently, due to the large losses from illegal data access, data security has become an important issue for public, private and defense organizations. In order to protect valuable data or information from unauthorized access, illegal modifications and reproduction, various types of cryptographic techniques are used. [1]There are two kinds of cryptography symmetric key cryptography and asymmetric key cryptography. In symmetric key cryptography same key is used between the sender and receiver. While in asymmetric key cryptography two different keys (public key and private key) are used between sender and receiver for encryption and decryption.RSA is most famous asymmetric cryptography algorithm.

RSA the most common public key algorithm. RSA named for his three inventors Rivest, Shamir and Adleman (RSA).In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers i.e. the factoring problem. In a secure communication using public key cryptography (RSA algorithm), the sender encrypts the message using receiver's public key, this key is known to everyone in the communication network. The encrypted message is sent to the receiving end that will decrypt the message with its private key. Only the intended receiver can decrypt the message because only receiver knows the private key. Thus using RSA algorithm we can communicate in a secure way. [1]

Cloud Computing indicates virtual servers available on the internet. That it is usage of computing resources (hardware, software or both) that is not owned by application owners, but is hosted in data centre owned by third party provider, in a consolidated manner. This frees the application owner of the computing resources from worrying about the underlying technology and implementation details. They can ask for more or less resources on demand. They can ask for more or less resources on demand, and it is the responsibility of the third party provider to dynamically adjust to these requirements. Thus application owner can just concentrate on the application logic, and do not have to keep scaling up or down in terms of hardware infrastructure, personnel, or software licensing, instead, they can pay per use to the third party provider. The subject of cloud security is still evolving, since cloud computing itself is still evolving. Collectively a set of policies, technologies and approaches that are needed to protect data, application and cloud infrastructure is the area of cloud security. Cloud security involves two parties cloud provider and cloud client. The cloud provider can provide the cloud platform as an infrastructure as a service or as an application .Security is needed in each case. Client's data and application must be secure in cloud computing, especially because the client relies on the cloud provider much more than the non cloud application consequently, cloud security must deal with all aspect of securing data access, storage, application hosting and storage, user information and authentication. [2]

II. RELATED WORK

R. Rivest, A. Shamir, and L. Adleman has proposed a method for implementing a public key cryptosystem whose security rest in a part on the difficulty of factoring the large numbers. It permits secure communication to be established without the use of couriers to carry key and it also permits one to 'sign' digitized documents [2].

Alaa Hussein, Al-Hamami and Ibrahem Abdallah Aldariseh proposed enhancing the RSA algorithm; in this RSA algorithm they used additional third prime number in the composition of the private and public key. Because of additional prime number the factoring complexity of variable (n) is also increase. [3]

Vivek Choudhary and Mr. N. Praveen have proposed a secure algorithm in their work, which includes the architectural design and enhanced form of RSA algorithm through the use of third prime number in order to make a modulus n which is not easily decomposable by intruders. Further, their approach eliminates the need to transfer n, the product of two random but essentially big prime numbers, in the public key due to which it becomes difficult for the intruder to guess the factors of n and hence the encrypted message remains safe from the hackers. [4]

III. METHODOLOGY

In this work we have modified RSA cryptosystem. There are two drawbacks of RSA cryptosystem

a) High time of computation to compute mathematical operation of RSA algorithm
b) Needs to increase security, security can be compromised in the network.

Here in this work we are reducing time of computation of mathematical operation of RSA algorithm by cantor's pairing and unpairing algorithm. Even security is modified by using three big prime numbers instead of two as used in the RSA algorithm.

RSA Algorithm

1. Choose two large prime numbers P and Q.
   Let it be P=7 and Q=17.

2. Calculate N=P*Q. We have N=7*17= 119
3. Select the public key i.e. encryption key) E such that it is not the factor of (P-1) and (Q-1).
Let us find (17-1)*(7-1) =96 Factor of 96 are 2, 2,2,2,2 and 3(96=2*2*2*2*2*3).Thus, we have to choose
E none of the factor of E is 2 and 3.As a few example we can't choose E as 4(because it has 2 as a factor), 15(because it has 3 as a factor),6(because it has 2 and 3 both as Factor).Let us choose E as 5 (it could have been any other number that does not its factors
as 2 and 3).

4. Select a private key (i.e. decryption key) D such that the following equation is true
    (D*E) mod (P-1)*(Q-1) =1

5. Let us substitute the value of E, P and Q in the equation.

We have: (D*5) mod (7-1)*(17-1) =1.

That is, (D*5) mod (6 * 16) =1.

That is, (D*5) mod (96) = 1.

After some calculation let us take D=77.Then
the following is true:

(77*5) mod (96) = 385 mod 96 = 1.Which is
what we wanted.

6. For encryption, calculate the cipher text CT
from plain text PT as follows:

CT= (PT^E) mod N

Let us assume that we want to encrypt plain text 10.Then we have, CT= (10^5) mod 119=100000 mod 119 = 40. Send CT as a cipher text to the receiver.

7. For decryption, calculate plain text PT from cipher text
CT as follows,
  PT= (CT^D) mod N.

 We perform the following
PT= (CT^D) mod N. That is, PT= (40^77)
mod 119=10 which is original plain text.[2]

Modified RSA Algorithm

1. Generate a single integer number of sent messages by cantor's pairing algorithm.
Pair@[x, y] =(x^2+3*x+2*x*y+y+y^2)
2. Choose three prime numbers those are large.
3. Calculate N=P1 *P2 *P3.

Here P1, P2 and P3 are big prime numbers.
4. Calculate Q= (P1-1)*(P2-1)*(P3-1)
5. Select the public key (i.e. encryption key) E such that it is not the factor of Q.
6. Select the private key (i.e. the decryption key) D such that the following equation is true:
(D * E) mod Q =1.
7. For, encryption calculate cipher text CT from the plain text PT as follows
CT= (PT^E) mod N
Send CT (Cipher Text) as a secret code to the receiver from sender.
8. For decryption, calculate the plain text from the cipher text CT as follows
PT= (CT^D) mod N.
9. Displaying each character by using unpairing algorithm (Reverse process of
Pairing) to the receiver side.
Let Z is a plaintext
i= -1+sqrt (1 + 8 * Z) / 2;
x= Z-i (1+i)/2
y=i (3+i)/2-Z [2]

Modified RSA Algorithm Example

1. Let we are sending ABC
Ascii value of ABC are 65, 66, and 67
After going through pairing algorithm
305917454 integer number generated.
2. Choose three large prime numbers P, Q and R
Let it be P=7 and Q=17. R=11.
3. Calculate N=P*Q*R. We have N=7*17*11= 1309
4. Select the public key i.e. encryption key) E such that it is not the factor of (P-1) and (Q-1) and (R-1).
Let us find (17-1)*(7-1)*(11-1) =960
Factor of 960 are 2, 2,2,2,2, 2and 3,
5(96=2*2*2*2*2*2*3*5).Thus, we have to choose
E none of the factor of E is 2 , 3 and 5.As a few example we can't choose E as 4(because it has 2 as a factor), 15(because it has 3 and 5 as a factor), 6(because it has 2 and 3 both as Factor).Let us choose E as 7 (it could have been any other number that does not its factors
as 2 , 3 and 5).

5. Select a private key (i.e. decryption key) D such that the following equation is true
(D*E) mod (P-1)*(Q-1)*(R-1) =1

6. Let us substitute the value of E, P and Q
in the equation.

We have: (D*7) mod (7-1)*(17-1) *(11-1) =1.

That is, (D*7) mod (6 * 16*10) =1.

That is, (D*7) mod (960) = 1.

After some calculation let us take D=137.2857
.Then
the following is true:

(137.2857*7) mod (960) = 960.99999 mod 960 =
1(Aprox.)This is
What we wanted.

7. For encryption, calculate the cipher text CT
from plain text PT(Integer number generated by cantor's pairing algorithm) as follows:

CT= (PT^E) mod N

We have, CT= (305917454^7) mod
=25074356332646265936499477183205218802346490920
7285556902784mod 1309= 864
. Send CT as a cipher text to the receiver. Send 864 as a cipher text to the receiver.

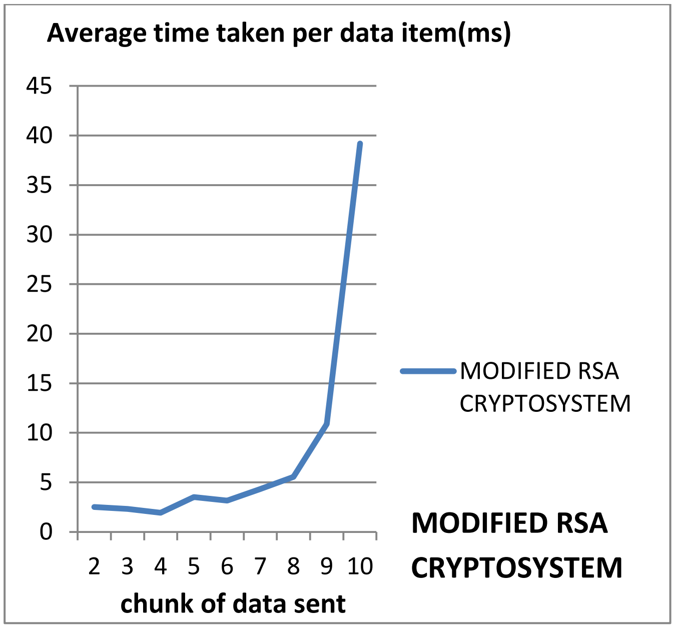
8. For decryption, calculate plain text PT from cipher text CT as follows,
PT= (CT^D) mod N.

We perform the following
PT= (CT^D) mod N. That is, PT= (864^137.2857)
mod 1309=305917454which is original plain text.

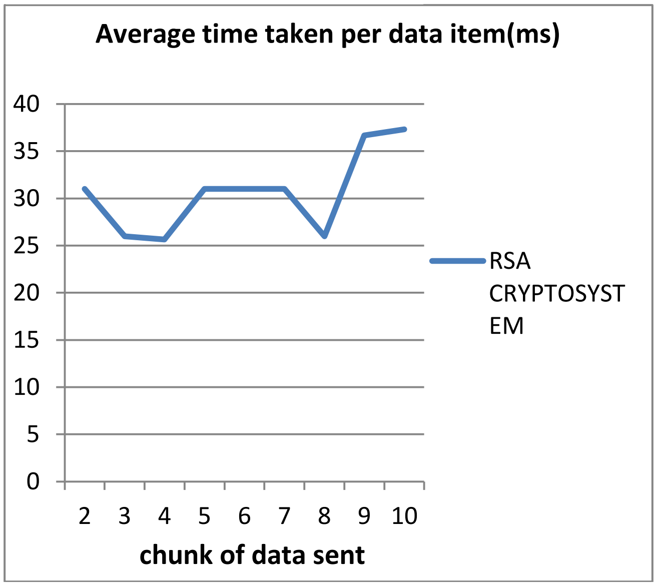
9. After going to cantor's unpairing algorithm ABC is received to the receiver side.

IV. RESULT AND DISCUSSION

According to graph which has been drawn experimentally it is clear that when we are using modified RSA cryptosystem in cloud based environment it performs very well as compared to RSA algorithm if number of characters up to nine are sent by modified RSA cryptosystem. Even security is better in modified RSA cryptosystem because here we are using three prime numbers instead of two as we used in RSA algorithm as shown in the diagram below



RSA CRYPTOSYSTEM



In above work cantor's pairing algorithm generates single integer number of number of characters those are going to be sent. After encryption it is converted into cipher text this integer number in the form of cipher text goes to the network and in the receiver side it is decrypted. Now we are getting plain text in the form of integer number. After going to unpairing algorithm original plain text is received to the receiver side..

V. CONCLUSION AND FUTURE WORK

Here we have found a conclusion that modified RSA algorithm performs very well as compared to standard RSA algorithm if chunk of data up to nine are sent by it. Even security is very high because in this work we are using three big prime numbers instead of two as used in standard RSA algorithm.

In future work we will increase chunk of data from nine, also we will be reducing time of computation of RSA algorithm.

REFERENCES

[1] IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 1, January 2017 written by HARSH SAHAY

[2] Atul Kahate, Cryptography and network Security

[3] Al-Hamami, A. H., & Aldariseh, I. A. (2012, November). Enhanced Method for RSA Cryptosystem Algorithm. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp. 402-408). IEEE.

[4] Vivek Choudhary1 and Mr. N. praveen2 "Enhanced RSA Cryptosystem Based On Three Prime Numbers" 1 Post Graduate Scholar, Department of Computer Science & Engineering, SRM University, Chennai, Tamilnadu, India 2 Assistant Professor, Department of Computer Science & Engineering, SRM University, Chennai, Tamilnadu, India.