International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4
ISSN: 2454-4248
585 – 590

Review paper On Modifed RSA for Cloud Computing MRSA -ENCRYPTION

Tanya Pandey,
Department of Computer Science & Engineering,
DPGITM, Maharishi Dayanand University,
Haryana, India
tanya1618@gmail.com

Sonal Arora,
Assistant professor,
DPGITM, Maharishi Dayanand University,
Haryana, India

Abstract— Cloud computing is advance practical application for healthy communication over the internet. The internet supplies some layer of network facilities via which they pass on the above remote network. The cloud is virtual network hub where we store our confidential data and make it secure. The cloud gives some facilities one authenticate users can access our data. The cloud authentication service is an approach and authentication integrity with a hybrid cloud framework. The cloud authentication service enables your association to control how user's access resources with centralized access along with authentication policies also can raise user productivity with single sign-on sso.

Keywords- *RSAAlgorithm, Encryption, Decryption, Cryptosystem, Security, Public Key, Private Key*.

*****

I. INTRODUCTION

Cloud computing architecture is basically divide into section one front end and the back end. The connection is established through the network over the internet. Front ends include client machine and the application required to access cloud computing system. All cloud computing service not provide user interface some services like Amazon cloud service, mail, Firefox.

Back end system is connected with the different server, and data are the stored different servers over the network and internally connected make a cloud of computing service.

Cloud computing is centralized administer the system, monitoring traffic and client demand to access and the run service are run smoothly. It follows as set of rule called as protocol and uses specific kind of software called middle layer.

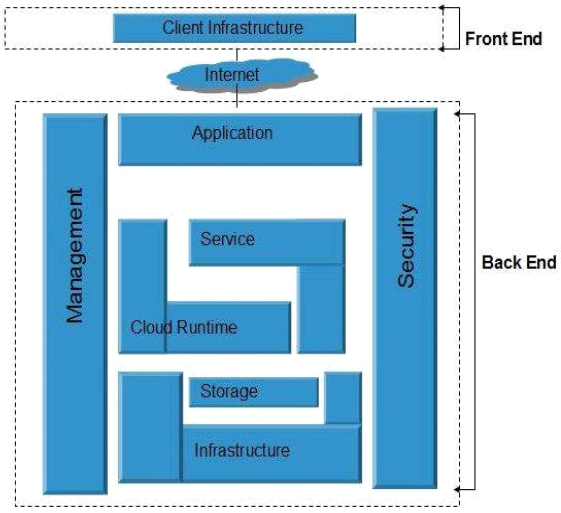

Figure.1. cloud computing architecture

A. TYPE OF SERVICES

Cloud are provides 3 type of services:

a) Infrastructure as a Service, or IaaS, contributes business passageway to vital web framework, such as deposit space, computing machine, and communications, destitute of the business need of purchasing as well as managing this internet infrastructure themselves. Because of the economies of calibration and specialization involved, this can be to the benefit of both the business providing the infrastructure and the one using it. In particular, IaaS allows an internet organization a way to develop and grow on demand. Both PaaS and SaaS clouds are grounded in IaaS clouds, as the company adding the software as service is also providing the infrastructure to run the software. Choosing to use an IaaS cloud demands a willingness to put up with complexity, but with that complexity comes flexibility. Amazon EC2 and Rackspace Cloud are examples of IaaS.

b) The platforms as a Service (PaaS) cloud are created, many intervals inside IaaS Clouds by authorities to render the scalability and deployment of any application trivial and to help make your costs scalable and predictable. Some examples of a PaaS system include: Mosso, Google App Engine, and Force.com. The chief benefit of a facility like this is that for a bit as no funds you can initiate your application with no pressure more than fundamental development and maybe a little porting if you are dealing with an existing app. Furthermore, PaaS allows a lot of scalability by design because it is based on cloud computing as defined earlier in the article. If you want a lean processes staff, a PaaS can be highly useful if your app will come to terms. The most

 ISSN: 2454-4248
585 – 590

important denial of using a PaaS Cloud provider is that these facilities may implement some conditions or trade-offs that will not work with your product under any scenarios.

c) Software as a Service (SaaS) is relatively mature, and the expression's use predates that of cloud computing. Cloud applications allow the cloud to be leveraged for application architecture, cutting down the burdens of allowance, support, and processes by having the application run on information processing system being connected with to the vendor. Gmail and Salesforce are in the midst of examples of SaaS run being clouds, but not all SaaS has to be supported in cloud computing.

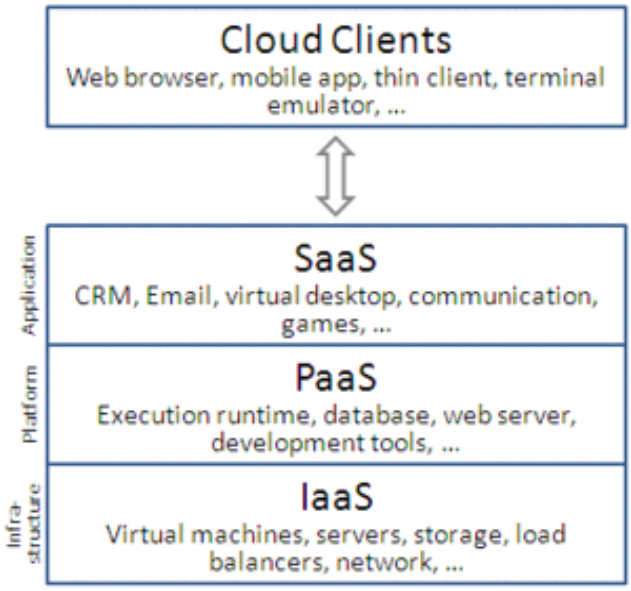

Figure .1.2. Cloud computing service

B. CLOUD AUTHENTICATION SERVICES

The Cloud Authentication Service executes run-time authentication for the secure resources. The Cloud Authentication Service as well allows RSA to transform and enhance authentication abilities. The Cloud Authentication Service proceed Microsoft Azure, a cloud computing programmer that is hosted from one side to the other of a worldwide network of Microsoft data centers. RSA Secure-ID Access uses a multi-tenant database in an environment that shares structure while segregating.

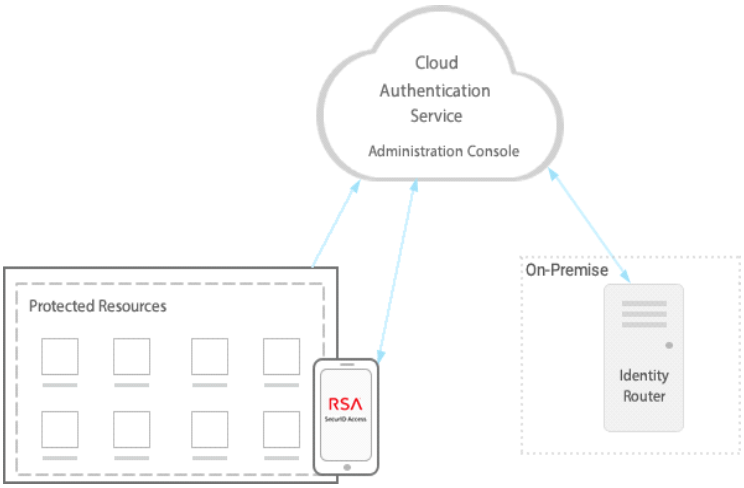

Figure.1.3. Authentication service

Client data to secure confidentiality. Service levels along with functional performances are standardized for all clients due to the distributed nature of the platform.

C. CLOUD STORAGE SERVICES

Nowadays, the most famous cloud storage services are possibly Dropbox, OneDrive and Google Drive. Each offers alike, but a little different facilities, which makes it hard to evaluate which is the best cloud service. Dropbox offers 2GB free cloud depository, while OneDrive offers 5GB cloud depository for free in their Basic Plan. Google Drive's cloud storage free plan offers 15GB. We reconsidered the best cloud storage providers, so you can take a look at our judgments below:

Dropbox Cloud
OneDrive Cloud
Google Drive Cloud
Amazon Cloud

There are several other facilities which are very similar to cloud computing models: x

1) Client-server computing model – This model differentiates between the facility supplier and the customer, or the object who requests access to a specific service.

2) Grid computing – This was the basic model for virtual mainframe computer. It's like a grid or a web that involves numerous physical workstations. These workstations pool their sources in order to perform larger and more complicated assignments.

3) Fog Computing – Requested data is processed at a network level using smart devices. This computing model eliminates the use of remote location for sending data.

 ISSN: 2454-4248
585 – 590

4) Peer-to-peer model – A variant of the client-server model. The main difference is that the client is concomitantly supplier and client.

D. DATA SECURITY

Cloud is possessed of the security trouble in Data partitioning, Data fraud, unauthorized entry, unlearned Owner and role of Data Protection, Data Loss conditions Data security schema Security is the major concern to obtain the data in cloud. Security includes protecting information's from being lost, destroyed or modified.

1) **Preservation of Data**: Data can be secure by the external user by causing the protection keys such as private key.

2) **Building Blocks**: Mathematical and cryptographic principles server as the building blocks of the security.

3) **Integrity of data**: While uploading the data the user can verify the correctness of the integrity principles.

4) **Accessing the Data**: Due to the Encryption and Decryption techniques data can be accessed securely.

5) **Authentication:** Authentication allows only authorized user to access Data in cloud.

II. LITERATURE REVIEW

This review paper I have been worked with the following security algorithms:
1) RSA algorithm for secure communication for cipher text.
2) Modified RSA Encryption algorithm develop to cover come the RSA drawback and give the speed and time utilization.

A. DEFINATION RSA ALGORITH

RSA is an asymmetric method, which means that a key pair will be generated, a public key and a private key, certainly, you remain your private key secure and circulate the public one.
The algorithm was promulgated in the 70's by Ron Rivest, Adi Shamir, and Leonard Adleman, hence RSA and it rather implement's a trapdoor function such as Diffie's one.
The RSA algorithm is commonly used for key encryption and decryption for authentication algorithm and is include key generation, encryption and decryption
The large number is easily factorized or decomposes and the limited prime numbers are easily decomposed which will not be provided security throw the networks. That's why we used 'n' prime numbers to provide more security throw the networks and it is also not easily factorized.
Although in D-H I'm going to be applying rather limited numbers, but confine understanding that the real value of most of mod (p) placed algorithmic rule occurs when enormous primary numbers are used. The first part I will show how the trapdoor function works, and then I will describe why it works. RSA is preferably slow so it's not used to encrypt data, more commonly it is used to encrypt and circulate symmetric keys which can really deal with encryption at a more rapid speed.

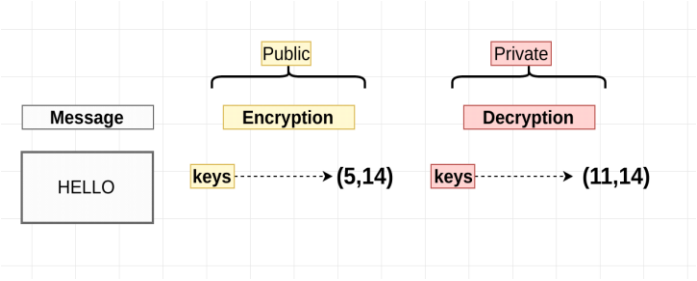

Figure 2.1 Encryption of RSA

We have received a message ("HELLO"), including we have selected two tuples escorted by two numbers one and all. Assuredly there is no arithmetic operation we can represent with strings , so the message has to go to convert it to something , then let's indicate "HELLO" converts using some conversion algo to "2"
Commonly, in development, a lot of various techniques are extant used to encode the message and padding is also used.

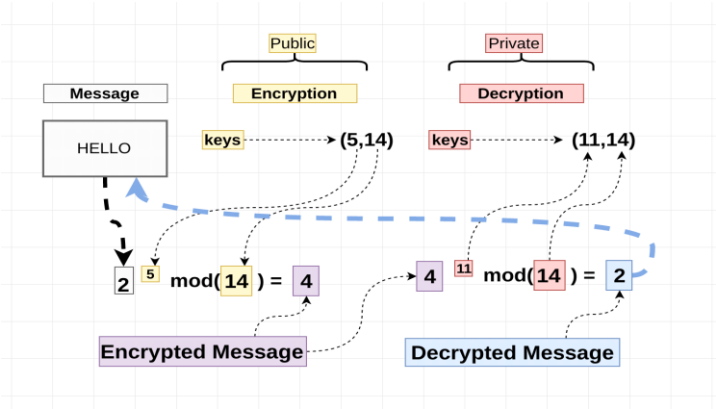

Figure 2.2 Encryption and decryption of RSA

So there we have the fundamentals about the RSA and how the trapped function is laid out.
The attractive bit is how we come about those, and how (5, 14) is related to (11, 14), and this is the interesting part let's start:
The details of the Decryption/Encryption pair:

1. Select two prime I will select 2 and call them p and q.

For example: P = 2 and **Q** = 7

2. Multiply **P** and **Q**, and that becomes the modulus

N = P * Q = **14**

 ISSN: 2454-4248
585 – 590

3. Make a list between 1 and 14 and remove the common factors:

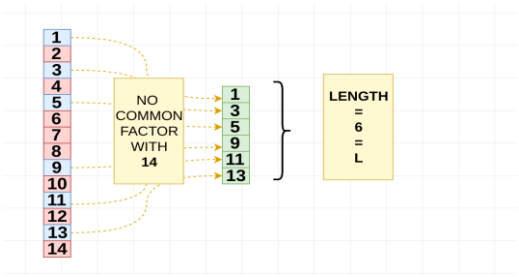

Figure 2.3 RSA common factor

Now there's an easy way to get this and that is:
(Q - 1) * (P - 1) = **L**

(7 - 1) * (2 -1) = **6**

Let's save this number, let's call it "L"

4. Now we achieved to select the encryption in the example was (5, 14 we know 14 is the modulus. So for the encryption a few rules: it's got between 1 and L [2, 3, 4, and 5]

Coprime accompanied by L (6) including the Modulus. Therefore there we came to a conclusion of why we chosen (5, 14)

5. The Decryption In the example we have chosen (11, 14 again 14 is the modulus but where does 11 come from?? , from now on let's call it let's find out why D is 11:D has to follow one rule and this is it:

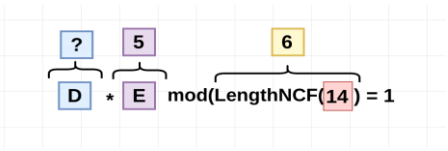

Figure 2.4 Decryption of RSA algorithm

So the Decrypt or (11) multiplied by the Encrypt or (5) modulus the length of the non-common factor with the modulus (14) has to be equals to 1.

D * **E** % **LNCF** (N) = **1**
11 * 5 % 6 = 1

So we know if we multiply D * E and E is 5, D will need to be a common factor of 5, so:

So I have made a list of integers from 1 to 50 and filtered the ones that when multiplied by E and modules by LNCF (N) are equals 1, therefore let's see if those can decrypt the message :)

Remember the encrypted message is present "4", and the decrypted message is "2" so the function should be something like:

4 ** D % 14 = 2 <---Decrypted message
It you see how applying the function to all the Decryption keys that follow the rule (D * E % LNCF (N) = 1 decrypted the message successfully.

B. DRAWBACKS

1. RSA is a public key cryptosystem (asymmetric cryptography) which is slow compared to symmetric cryptography.
2. It requires a more computer domination supply compared to single key encryption.
3. In this cryptosystem, if the private key is lost then all received message cannot be decrypted but security wise, it's great.
4. Complexity of algorithm i.e. key is too large and calculation time is long.

Very slow key generation.

III. METHODLOGY

A modify RSA algorithms is proposed using "n" distinct prime numbers. A pair of an arbitrary number and their standard multiplicative inverse is used to increase the protection of the RSA algorithm. Key formation, encryption and decryption period of Modified RSA (MRSA) algorithmic program to separate the system is enormously higher. A survey has been performed using JAVA programming language. Modified RSA (MRSA) is implemented applying JAVA Big Integer program library roles for simulation reason. It is likely for the individual to register a prime number or set, the
Bit length of prime integers to make automatically using the reliable random function. Big Integer Library provides various functions such as modular arithmetic .GCD estimation, primality testing, prime formation, and bit manipulation
And some other operations. Different bit length prime integers are generated by applying the prime generator function of Java Big Integer program library to determine keys formation, encryption and decryption time frame. The Modified RSA (MRSA) model. Perform a comparison for key formation, encryption and decryption time frame between RSA and Modified RSA (MRSA) based on these calculated times for particulars bit length.

IV. MODIFIED RSA ENCRYPTION ALGORITHM

To improve the security, a new cryptography algorithm based on additive homomorphic properties called Modified RSA Encryption Algorithm (MREA) is being used. MREA is secure as compared to that of RSA, as it is based on the factoring problem as well as decisional composite residuosity assumptions which is the intractability hypothesis. M-RSA is

 ISSN: 2454-4248
585 – 590

an additive homomorphic cryptosystem; this means that, if given only the public-key and the encryption of m1 and m2, one can compute the encryption of m1 +m2. It` also presents comparison between RSA and M-RSA cryptosystems in terms of security and performance.

A new technique was proposed to provide maximum security for data over the network by using a modified RSA cryptosystem based on 'n' prime. This method involves encryption, decryption, and key generation. This technique used 'n' prime number which is not easily breakable. 'n' prime numbers are not easily decompose. So this modified RSA algorithm handled 'n' prime numbers and provides security

V. PRAPOSED SYSTEM

During RSA implementation, there might be a condition where Cipher text and Plaintext have same values of n where n is Cartesian of two prime numbers p and q. Such situations are vulnerable for attacks and are required to be handled.

A possible solution is to construct a secure set of prime numbers and user can select alternate values of p or q or both to change the value of n.

This set of prime numbers are further divided into different classes with each class containing specified numbers of prime. Choices depend on:

a) Secure distance (d1) – to select a neighbor of one of the classes in the set. d1 is used to choose one or both prime number. Purpose of d1 is to use as agreement secure parameter to choose one of the classes inside set of all classes. This distance is changed periodically to remove redundant messages and enhance security for RSA algorithm.

b) Another secure distance (d2) is assigned under the selected class. Purpose of this to select k – nearest neighbor of primes inside the selected class by distance d1.

c) Based on specific value of n, we can get equality of both message and its corresponding cipher text. A new secure value of n can be generated to overcome redundant values in messages. For this, system uses parameter k which is nearest neighbor of p or q in one of the neighbor class in the set of alternative prime number.

VI. COMPLEXITY ANALYSIS

Comparison between complexity analysis of RSA algorithm and Modified RSA
(MRSA) algorithm is discussing in below.

A. Complexity OF RSA Algorithm

Complexity for Random selected two prime numbers:

- The complexity of MILLER-RABIN demonstrates the preceding complexities for finding a prime integer is O (s ∗ (log 2 p) ∗ln p).
- Uniformly, the complexity of the second integer is O (s ∗ (log 2q)*ln q).Complexity for calculation of N:
- The complexity of calculation of N is O (log 2 p *log 2q).

Complexity of Computing Euler phi values of N

- By MODULAR-EXPONENTIATION, the complexity intended the second bit is
- (N) -1. The complexity of computing Euler phi value of N is:
- ((log 2 (p −1) ∗ (q −1)) ∗ ((p −1) ∗ (q −1) −1)).
- Complexity intended random variables e:
- The complexity about retrieving the random variable e is
- (log 2(p -1)*(q -1) + gcd (e,(p -1).(q -1))) , as it is well-known that e as well as (N)
- Are coprime to each other so gcd (e,(p -1)*(q -1)) =1 , and so complexity is O((log 2 log 2 p −1) ∗ (log 2q −1)) +1).

B. Complexity OF MODIFIED (*MRSA*) RSA Algorithm

The complexity will increase based on the number of the prime numbers conceded

For the proposed algorithm.

- Complexities for obtaining first prime number is O(s ∗ (log 2w) 4 ∗ ln w).
- Similarly, the complexity of the second integer is O(s ∗ (log 2x) 4 ∗ ln x).
- The complexity of the third integer is O(s ∗ (log 2y) 4 ∗ ln y).
- Similarly, the complexity of the fourth integer is O(s ∗ (log 2z) 4 ∗ ln z).

Complexity for calculation of N:

- The complexity of computing of n is O (log 2w* log 2x *log 2y *log 2z).
- Complexity of Computing Euler phi value of N
- Complexity of compute Euler phi value of N is:
- O((log 2(w-1)*(x-1)*(y-1)*(z-1)4)) *((w -1)*(x -1)*(y -1)*(z -1)-1).

Complexity for random variables e and f:

- The complexity of retrieving the random variable e is
- O((log 2(w-1)*(x-1)*(y-1)*(z-1)) +gcd(e(w -1)*(x -1)*(y -1)*(z -1)-1).,as
- It is acknowledged that e and (N) are coprime to each other so
- gcd (e,(w-1)*(x -1)*(y -1)*(z -1)) =1, and so complexity is

 ISSN: 2454-4248
585 – 590

- ((log 2 (log 2w-1)* (log 2x -1)*(log 2y -1) *(log 2z -1)) 4+1).
- Similarly, Complexity of finding the random variable f is
- ((log 2 (log 2w-1)* (log 2x -1)*(log 2y -1) *(log 2z -1)) 4+1).
- Comparing the above complexity it depicts that Modified RSA (MRSA) is
- More complex than RSA algorithm. The complexity will increase be influenced binding on
- The number of primes remembered for the algorithm.

VII. CONCLUSION

Above method reduces the redundant messages that occur in RSA method. Situations where the messages and cipher text are the same, this method presents an active solution by changing the value of n by applying k-nearest neighbor values of p or q or both. This process enhances security of RSA algorithms and the value of n is known only to the authorized users who know the agreement factor. This is essential owing to presence of recent active attacks.

REFERENCES

[1]. SU Mang, LI Fenghua, SHI Guozhen, GENG Kui, XIONG Jinbo (July 2016), “A user- centric data Secure creation scheme in cloud computing”, University of science and Tech., Nanjing, China, Vol 25, N0.4.

[2]. Lifeng Li, Xiaowan Chen, Hai Jiang (June 2016), “Parallelizing cipher text policy attribute based encryption for clouds”, College of Info. Science and Tech., Chin,. [

[3]. HUANG Qinlong, MA Zhaofeng, YANG Yixian (October 2015), “Attribute based secure data sharing with efficient revocation in cloud computing”, Information security center, Beijing, China, vol 24, No.

[4]. Xianping Mao, Junzuo Lai, Qixiang Mei, Kefei Chen, Jian Weng (November 2015), Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption”, Volume: 13, pgs 533-546.

[5]. Mahavir Jain, Arpit Agrawal, "Implementation of Hybrid Cryptography Algorithm", International journal of Core Engineering & Management, vol. 1, no. 3, pp. 1-8, June 2014.

[6]. Rupali Sachin Vairagade1, Nitin Ashokrao Vairagade” Cloud Computing Data Storage and Security Enhancement”International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 6, August 2012

[7]. M.Sudha1, M.Monica “Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography” Advances in Computer Science and its ApplicationsVol. 1, No. 1, March 2012

[8]. N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam"An Implementation of RSA Algorithm in Google Cloud using Cloud SQL" Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574-3579, 2012.

[9]. Parsi Kalpana, Sudha Singaraju," Data Security in Cloud Computing using RSA Algorithm"IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[10]. McKinsey & Co. Report presented at Uptime Institute Symposium, “Clearing the Air on Cloud Computing”,April 18, 2009