Data Security Using Multi Prime RSA in Cloud

Sunanda Nalajala, Pratyusha Ch, Meghana A, Phani Meghana B

Abstract— Cloud computing plays a major role in providing the quality service and best model for obtaining the computer resources. Only authorized client have the right to access the data a that is available in the cloud computing structure. This paper mainly focuses on the security of data that is stored in cloud and issues regarding data security. For data storage and data security, we use an algorithm i.e Multi-prime RSA algorithm. In multi-prime RSA algorithm, the security services include the terms such as Key generation, Encryption and Decryption.

Keywords: Multi-prime RSA algorithm, cloud computing, Encryption, Decryption and Security.

1. INTRODUCTION

The different services that are provided in the internet in these modern time are known as the traditional hosting system where the usage and the storage of the data are secured. Mostly in the business area, the current trend needs the power for data evolution and data storage. These data storage, evolution, data security helps in the progressing the cloud model. In order to avoid the issues, the cloud computing presents a model which helps to solve the issues like compute, storage and provides allocation and reallocation whenever the data requires, network possibility is provided and also the sufficient storage is given.

The cloud computing model is able to clear the requirements of the user and it makes the service model process easier. Cloud computing became the popular model and in order to use it everywhere we want, the cloud management provides the data centers where it is used to move their data anywhere in the universe.

Cloud computing supports data movement universally and is able to modify the data on the web by eliminating the responsibility of the local data centers. Cloud computing service model keeps the entire information about the facts put away in the cloud automatically through the software. Cloud computing plays a key role in many small, medium and large companies where the services provided are used to secure their information set aside in the cloud platform.

Providing the security for the information is a critical and important issue in the cloud computing because a lot of complex information is also stored in it. Data security and data privacy are happening to be a blockade for the cloud computing services. To provide quality service, the data security is one of the important aspect and the security should be forced on the data by using different encryption techniques in order to achieve the data security and data accessibility.

Due to non-transparent nature of the cloud service model, there are still some security issues need to be solved. The most useful point in the cloud computing is that the cloud structure is designed in a way that is very valid and strong. But the disadvantage of cloud computing is that is facing a wide range of issues about the stored data.

For solving the major issue of cloud computing i.e. data security, we cannot take actions on the security directly because we cannot have access to implement it as data was not stored in the client area. So, the one way for solving the data security issue is that we apply multi-prime RSA algorithm before supplying the information in cloud mainly sensitive data.

Let us consider an authorized user had sent request to use the facts that is saved in the cloud computing platform then, the cloud will send the facts which is unscrambled to the user. In this way, the method suggested for the cloud service model provides data security and data storage using multi-prime RSA algorithm. In multi prime RSA algorithm, we provide the data safe facilities using key generation, encryption and decryption that are supplied in the cloud computing structure.

2. LITERATURE SURVEY

In cloud computing, the security major role and when the data stored in the cloud was changed or the data stored as the unknown owner in cloud will leads to the major issue of security and in order to overcome that issue, we use a technique known as adaptive information technique [1]. The cloud computing made a great advantage of eliminating the infrastructure issues in hardware and the software. But the cloud computing also involves some critical issues in the data security from the server side and can be eliminated using security techniques [2].

As the information network technology has been increasing, the usage of cloud computing services are also gradually increasing. To provide more applications and efficiency for the cloud security, this paper introduces the concept of reference model which includes security application, content matrix, cloud framework and many other [3].

Revised Version Manuscript Received on March 08, 2019.

Sunanda Nalajala, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India (e-mail : sunanda@kluniversity.in)

Pratyusha Ch, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India

Meghana A, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India

Phani Meghana B, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India

The technical terms like security and privacy has been a challenge for the virtual centralization. Many cloud applications are introduced on the networked side but here we introduced applications for the security on web service side [4]. A model which provides security and integrity malware detection and real time monitoring[5].

.In cloud computing, due to the security issues, we include a third party authentication which is trustful party used for the data movement in cloud. The issue involves in third party authentication can be reduced by a novel third party auditor scheme [6].

To provide the security in cloud computing, we use hybrid encryption algorithms i.e. RSA and AES. For security, we should be careful while uploading data as even the administrator should not be known about the content of data [7].

The private data that is stored in the cloud computing has the risk of confidentiality, integrity and availability. Before selecting the service provider, the security arrangements should be made in a proper way for cloud computing environment [8].

For ensuring the data storage and data security, we include public key crypto system RSA [9]. For achieving the security issues, we need to provide some security services like Symmetric and Asymmetric cryptographic algorithms [10].

3. CLOUD COMPUTING ARCHITECTURE

The cloud computing architecture involves three steps i.e. cloud architecture, storage architecture and cloud computing components. Cloud architecture includes the cloud computing components such as cloud service, cloud platform using web, cloud infrastructure and cloud storage using database communicate with each other all the time with programming interfaces using web services. This cloud architecture provides an extension to the clients so that the applications of the cloud can be accessible to the web browsers and software.

The cloud storage architecture includes 4 blocks such as data owner, server, user and third party auditor. When the request is sent to access the data, the third party auditor has an important role in accessing the information storage and the reliability on account of the client.

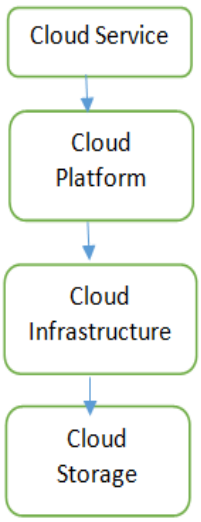

Fig1: Architecture of Cloud

In cloud model, maintaining the data at local storage infrastructure will be unstressed when the data owner represents as the individual or customer for the services on the cloud. The services provided by the data storage system has many advantages like data availability, service to low cost and it also makes multiple users to one group and allow the group to access the data.

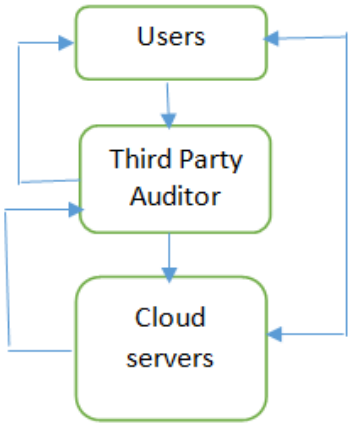

Fig2: Data storage system

The cloud computing copy is composed of 3 layers. They are characteristics, delivery representations and deployment representations. The featured layer composed of the locale unconventional resource pooling, on demand self-facilities, expeditious flexibility, wide network ingress and measured facility.

The second surface of cloud computing is delivery models and that composed of infrastructure as a facility (IaaS), Platform as a service (PaaS) and Software as a service (SaaS). IaaS is the service ofdistributing computer infrastructures and so it has the huge benefits of infrastructure facilities. The sample of IaaS is mesh services. In PaaS, the requisitions can be run by the users by cloud service with the service provider's materials and applications of the google is one of the example of PaaS. SaaS is used to operate software and provides the license to the applications that we use and one of such application is sales force application.

The third layer of the cloud computing structure is deployment copy and it is composed of public, private, group and cross clouds. Public cloud is used for the many occupants and convenient to the public users. The private cloud is used for only category of people and the community cloud is reform of group. Hybrid cloud is the emergence of the many clouds such as public, private or community clouds.

4. DATA SECURITY

Data availability is one the major security issue in cloud computing. The attendant's data is generally reserved in the blocks on dissimilar servers repeatedly occupying in the uncommon clouds. The availability of the data becomes the difficult in this caseas we cannot provide unbroken data. Supplying the complete data is difficult as data was stored in blocks.

Privacy and confidentiality is another issue in data security where the data supplied in the cloud structure has accessibility to the limited authorized users. An improper accessibility to the data in the cloud will lead to the major warning for cloud system. We should provide guarantee to the users that the data supplied in the cloud will be provided with the proper implementation, strategy and approaches for the safety of data. The cloud should be confident that the data is stored personally.

Data location and relocation is another data security issue in cloud. Cloud computing provides the high strength to the data. Users may or may not know where their data is stored. When the sensitive data that had stored in the cloud has to perform some operation, then they want to know the location of data.

For that reason, they should made an agreement that the data stored in cloud and user should live in a particular location. The users also should take responsibility in producing the reliability to the data that is supplied in the cloud structure provide strong and valid process to protect the data stored in the cloud model. Moving the data from one location to another location also been an issue. Users decide to store their data at one location and afterwards, the data will move from one place to another place and the cloud users also have an agreement to use each other's data.

Data integrity is another issue of security. By providing the security of the data, the users should apply different technique to tell about the operations or methods performed to the data at every point which leads to data integrity. Initially the cloud service should give the total information to the user about what data will be provided on thecloud platform.

Storage, Backup and Recovery is another issue in data security. If we want to move or add data to the cloud platform then, we should provide the enough data and that data should be flexible. Redundant array of independent disks should be provided because most of the users will store their data in the independent blocks. Many business based applications are also used in the cloud platform and in such cases, the backup option is most required. Even if the hardware was failed in any case, the backup will be used to get back to the normal state.

5. RELATED WORK

RSA is a public key algorithm. RSA was described in 1977 by Ron Rivest, Adi Shamir and Len Adleman. In this paper, we solve the data reliability issues in the cloud structure by operating the multi prime RSA algorithm. The data security has the major importance in the cloud as we store data in cloud, our data should be secure and only authorized users should use it in order to be secure.

So, by using the multi prime RSA algorithm, only authorized users have the accessibility to use data in cloud. Initially the customer data will be encrypted which is deposited in the cloud structure and when any client want to ingress the information, they search for the data in cloud platform and then when they found the data they verify the user and after validation they provides the data. In the entire process, the multi prime RSA is block cipher where it draws the given information to the integer format.

Advantages	Disadvantages
It takes less time and the computational time period is less than RSA.	With more no of primes, the less security.
Uses more than two prime numbers.	If prime number is not safe, the less security.
Efficient. And secured.	With increase in prime in modulus, the less security.

Table1: Classification of MPRSA

6. PROPOSED WORK

Like in RSA algorithm, multi prime RSA algorithm also composed of public key and private key. Public key is open to all and everyone can see it where as private key is only familiar to the client using data.In the process, we use encryption and decryption where encryption was done by the service and decryption is done by the client. We utilize the public and private key in encode and decode methods. If we use public key for encryption then, we should use respective private key for decryption process. Multi prime RSA also involves three steps. They are:

- Key generation
- Encryption
- Decryption

Key generation: Let N be the product of non specifically chosen distinct prime's p1…..pr. The Euler's Totient function is defined as

$N{:}f\,(N) = Q(N)i{=}1(pi - 1)$

Choose an integer e, such that, $1 < e < f(N)$, such that

Gcd (e, f (N)) = 1.

Public key – (n, e).

Compute the unique d, such that

$d = e^{-1} \bmod Q(N)$

Private Key – (d, e).

Encryption: For any message m, the ciphertext is

$C = M^e \bmod N$.

Decryption: For any ciphertext c, the plaintext is

$m = c\ d \bmod N$.

We call on the multi-prime RSA modulus, the RSA modulus (when r = 2). The integer e is public exponent and d is called the private exponent.

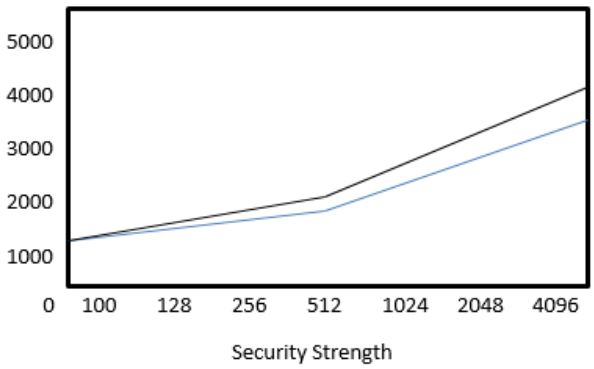

Fig3: Difference between RSA and MPRSA

Example of multi prime RSA:

Key generation: Let us choose an integer r as 15

Such that 15 > = 3

Let N be product of randomly chosen prime numbers where prime numbers are as follows

2,3,5,7,11,13,17

N = 2 * 3 * 5 * 7 * 11 * 13 * 17

N = 510510

The Euler's totient function is as follows:

Q (N) = (2-1)*(3-1)*(5-1)*(7-1)*(11-1)*(13-1)

= 92160

Choose e, such that e is not a factor of 92160 and the result is 45361.

Compute d, such that

$d = e^{-1} \bmod Q(N)$

= 104401

Public key – (45361, 510510)

Private Key – (104401, 510510)

Encryption: let us choose M = 7

$C = m^e \bmod N$

$= 7^{45361} \bmod 510510$

= 55

Decryption: $M = c^d \bmod N$

$= 55^{104401} \bmod 510510$

= 7

Therefore, the decrypted message result 7 matches to the plaintext we used m as 7 and hence the multi-prime RSA worked.

7. RESULTS

As we can see from the above chapter the results of the code which shows different output on the inputs with different prime values and the message values. When we take into consideration of the fig 3 we can see that there are 6 prime numbers that are given to as an input from which the public and private keys are generated. In the background as we have in the code it will check the numbers and calculate the phi (n), e, d values and generates the public and private keys. Later it accepts the message value to complete the encryption and decryption. We have obtained positive results and the outputs were correct considering the outputs of fig 3 and fig 4.

As the code has the function to find that if the number is prime or not it immediately gives a response saying the number is not a prime whenever it spots such value in the input the fig 5 shows that it has detected some value which is given as input instead of a prime value so it stops the execution and throws an error saying the values must be prime.

The prime values that are given as inputs should be unique from one another as the attacker cannot guess the number and the message should be safe. The code detects and throws an error when it finds that the 2 given prime values are same as in fig 6. it detected that the last 2 prime values are same and shows an error mentioning that both values should not be equal.

When we give the prime values as 2 we are almost doing the rsa algorithm as rsa has only 2 prime value capability. In fig 7 we tried to give the 2 prime values and the output was incorrect as it does not accept and do the mechanism of rsa through this code. So, we need to give more than 2 prime values for this multi prime RSA.

Until now we have found that the message we have given and prime values as input are taken and we got the correct outputs. But according to fig 8 we can give letters as the message inputs and we get the same message at the decryption as plain text. So message need not be a number it can also be letters also and they are acceptable and no error is detected if we give message as a letter.

8. EXPERIMENTAL RESULTS

Fig.3. Correct output

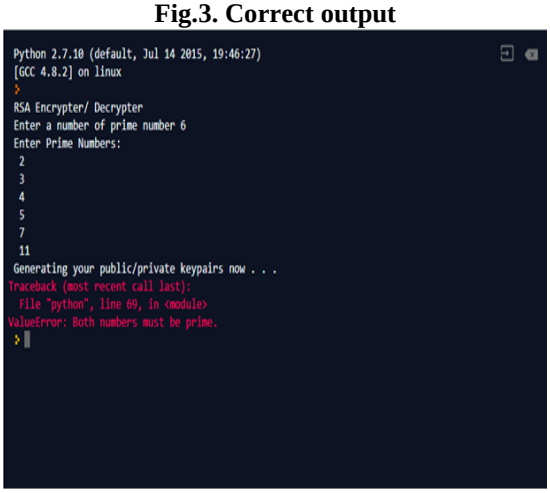

Fig.4. Numbers must be prime

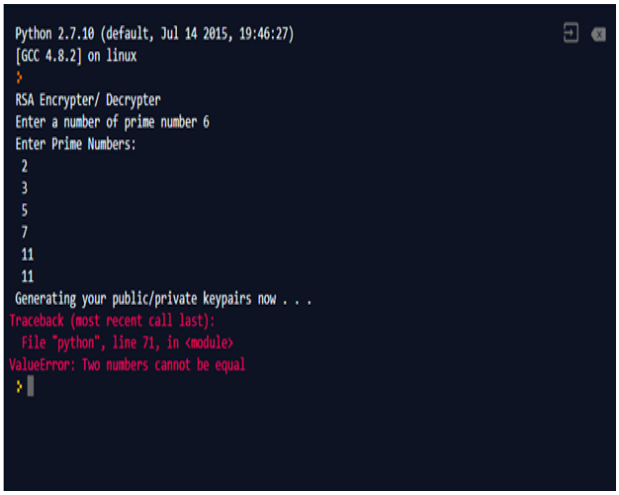

Fig .5. Number must not be equal

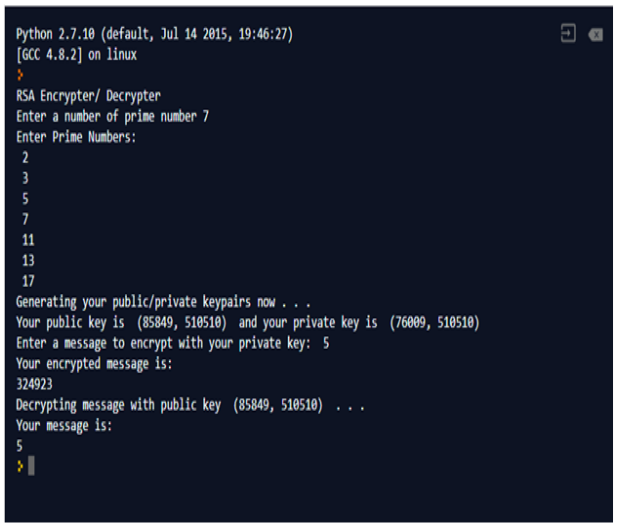

Fig .6. Correct output

Fig .7. Should give more than 2 primes

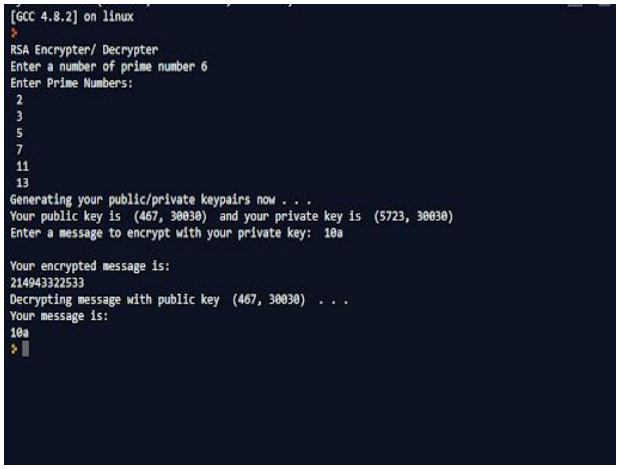

Fig .8. Correct output with letters

9. CONCLUSION

The intention for the proposed work is to enhance the reliability for the information that was stored in the cloud platform. This can be reached by utilizing the high potential encode method in the multi prime RSA algorithm. In encryption method, the encryption for the data was done before id stores in the cloud. Encryption plays a key role and it performs operations in two parts. The encryption was done with both the user data and the user identity in the first part. The encryption was done with both the identity of the user data and the keyword used in encryption process in the second part. We combine both phases and sends to the server. As a result, we get back the message which matches to the data identity and the key. This shows that this multi prime RSA achieves the data security.

REFERENCES

1. RSA Algorithm Evgeny Milanov3 June 2009
2. Vairagade, Rupali Sachin, and Nitin Ashokrao Vairagade. "Cloud computing data storage and security enhancement." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1, no. 6 (2012): pp-145.
3. Saravanan, N., 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, no. 19 (2012): 3574-3579.
4. Kalpana, Parsi, and Sudha Singaraju. "Data security in cloud computing using RSA algorithm." IJRCCT 1, no. 4 (2012): 143-146.
5. Sudha, M., and M. Monica. "Enhanced security framework to ensure data security in cloud computing using cryptography." Advances in Computer Science and its Applications 1, no. 1 (2012): 32-37.
6. Kumbhar, Nilesh N., Virend rasingh V. Chaudhari, and A. Badhe Mohit. "The comprehensive approach for data security in cloud computing: A survey." International Journal of Computer Applications (0975–8887) Volume (2012
7. The RSA Solution for Cloud Security and Compliance" A GRC foundation for VMware infrastructure security and compliance.
8. Hojabri, Mehdi, and Mona Heidari. "Union of RSA algorithm, Digital signature And KERBEROS in cloud security." In International Conference on Software Technology and Computer Engineering (STACE-2012), ISBN, pp. 978-93.
9. Jose, G.J.A., Sajeev, C. and Suyambulingom, D.C., 2011. Implementation of data security in cloud computing. International Journal of P2P Network Trends and Technology, 1(1), pp.18-22.

10. Wang, Hongbing, and Zhenfu Cao. "A fully secure unidirectional and multi-use proxy re-encryption scheme." ACM CCS, Poster Session 2009 (2009
11. Smys, S., and A. Dinesh Kumar. "Secured WBANs for pervasive m-healthcare social networks." In Intelligent Systems and Control (ISCO), 2016 10th International Conference on, pp. 1-4. IEEE, 2016
12. Sunanda Morampudi, Dr.Ch.G.V.N.Prasad, "An Efficient way to preserve privacy on Cloud"-2018
13. Koblitz, Neal. "Elliptic curve cryptosystems." Mathematics of computation 48, no. 177 (1987): 203-209.
14. Canetti, Ran, and Susan Hohenberger. "Chosen-ciphertext secure proxy re-encryption." In Proceedings of the 14th ACM conference on Computer and communications security, pp. 185-194. ACM, 2007.