ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ACHIEVING SECURITY IN CLOUD COMPUTING THROUGH ADVANCED RSA ALGORITHM AND PERFORMANCE ANALYSIS

Somnath Dey *1, **Somnath Basak** 2
* Department of Computer Science & Engineering, Brainware Group of Institutions, Kolkata, India

DOI: 10.5281/zenodo.1130846

ABSTRACT

Now a days security of data become a large concern to insure various attributes like confidentiality, integrity, authentication etc. Cryptography techniques are used for this purpose. It plays a major role in protecting the data in those applications which are running in a network environment. Cloud computing is a large amount of easily and accessible virtualized resources such as hardware, development platforms and services. Main goal of cloud computing is to provide easily scalable access to computing resources to improve organization performance. But one of the barriers for cloud adoption is security. To ensure the security, we propose a method by implementing Advanced RSA algorithm. After implementing Advanced RSA Algorithm, we have also analyzed the performance of our algorithm based on three parameters namely Time Complexity, Space Complexity and Throughput.

KEYWORDS: Cloud Computing, Advanced RSA Algorithm, Security, Complexity, Throughput

I. INTRODUCTION

In Modern days the computer and the communication technologies are very important part of strong economy. That's the reason we need a suitable security standards systems [9] and technologies to meet that security needs. Cloud computing is the concept of using remote services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way. In the cloud, the end user is just using a very light device which is capable of using a network that connects it to a server at some other location.

Organizations today are increasingly looking towards Cloud Computing as a new revolutionary technology promising to cut the cost of development and maintenance and still achieve highly reliable and elastic services. The Cloud technology is a growing trend and is still undergoing lots of experiments.

Cloud computing usually involves the transfer, storage and processing of information on the 'providers' infrastructure, which is not included in the 'customers' control policy. The concept Cloud Computing is linked closely with those of Information as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) all of which means a service oriented architecture. In the cloud, the end user is just using a very light device which is capable of using a network that connects it to a server at some other location. The users do not need to store the data at its end as all the data is stored on the remote server at some other place. So there is a need to protect the data against unauthorized access, modification or denial of services, data loss and data integrity problem.

Cloud computing is rapidly emerging as a viable means to create dynamic, rapidly provisioned resources for operating platforms, applications, development environments, storage and backup capabilities and many more IT functions. A significant number of security considerations exist that information security professionals need to consider when evaluating the risks of cloud computing.

For achieving the security in cloud computing we use the RSA algorithm which was publically described by Ron Revister, Adi shamir and Leonard Adleman [10] at MIT in 1977. For Public key Cryptography RSA is the well known algorithm. But traditional RSA algorithm is not sufficient for getting the desired security level. So in our proposed work, we are using Advanced RSA algorithm to provide security so that only the concerned user can access it [1]. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data.

II. RELATED WORK

In this section, we provide some related work in the area of cloud computing security and cryptographic algorithm used in cloud computing security. Malakooti, et al [2] proposed a model which is based on the scrambling algorithm and multilevel encryptions. They have designed, implemented, and tested their security model on the image type of information that is to be stored on the cloud environment.

Yang Xu, et al. [3] proposed an agent-aid model by combining decision-making theory and multi-agent system toward working load balancing problem in large clouds environment. In their work, they put forward a novel model to balance data distribution to improve cloud computing performance in data-intensive applications, such as distributed data mining.

Arockiam, et al. [4] proposed technique which emphasizes on improving classical encryption techniques by integrating transposition cipher and substitution cipher. Both substitution and transposition techniques have used alphabet for cipher text. In their proposed algorithm, initially the plain text is converted into corresponding ASCII code value of each alphabet.

Mohamed, et al. [5] makes evaluation for selected eight modem encryption techniques namely AES, DES, 3DES, RC4, RC6, Two-Fish and Blowfish through their software to select the most suitable and the highest security encryption algorithm for secure cloud computing environment.

Veerraju Gampala, et al. [6] explore data security of cloud in cloud computing by implementing encryption with elliptic curve cryptography and digital signature. In their work authentication and encryption for secure data transmission from one cloud to other cloud is presented which requires secure and authenticated data with elliptic curve cryptography. Their proposed work contains steps like key generation, signature generation, encryption algorithm, decryption algorithm and signature verification.

Tirthani, et al [7] have contemplated a design for cloud architecture which ensures secured movement of data at client and server end. They used the Elliptic curve cryptography for data encryption and Diffie Hellman Key Exchange algorithm for connection establishment. Their proposed encryption mechanism uses the combination of linear and elliptical cryptography methods. It has three security checkpoints named as authentication, key generation and encryption of data.

In 2012, A.H. Al-Hamami and I.A. Aldariseh [8] proposed a new concept in traditional RSA cryptosystem by enhancing the RSA algorithm by the use of additional third prime number in the composition of the public and private key with reduced size, instead of two large prime numbers. In this method they generate the variable n Large and the process of analysis of the factors is more complex than the original algorithm.

III. PROPOSED WORK

The proposed scheme is trying to provide an enhancement to the Hamami and Aldariseh [8] method by proposing a method that have speed improvement on the RSA decryption side and also provide the security by avoiding some attacks possible on RSA. Using the random number k if same message is encrypted more than one time it will look different every time. The general idea towards this scheme is to use the Key generation algorithm of Hamami and Aldariseh method and proposed a proposed scheme for encryption and decryption algorithm. The existence of three prime numbers, the difficulty of analysis of variable n must be increases and the key generation time must be reduces.

The algorithm for the proposed scheme is as follows:

Key Generation for Proposed Scheme:

To generate the key using three prime numbers user A should

do the following:

(a) Generate three large prime numbers p, q, s.

(b) Calculate n=p*q*s and $\varphi(n) = (p-1)(q-1)(s-1)$.

(c) Select e such that (e, $\varphi(n)$) are relatively co-prime.

(d) Get the value of d by using $e*d=1 \bmod \varphi(n)$.

(e) Find dp=d mod (p-1),dq=d mod(q-1), ds=d mod(s-1).

(f) Public Key Ku=<e, n>and Private key Kr=<d, p, q, s, dp, dq, ds>.

Encryption for Proposed Scheme:

To encrypt the massage M user B should do the following: User B should obtained the public key of user A <e, n>

(a) Represent the message M as an integer form in interval [0 to n-1].

(b) Select k as a random integer gcd(k, n)=1 and $1< k < n-1$.

(c) Compute $C1=k^e$ mod n.

(d) Compute $C2=M^e.k$ mod n.

(e) Send the cipher text values (C1, C2) to user A.

Decryption for Proposed Scheme:

On decryption process use concept of RSA with CRT. To recover the message from cipher text C2 user A should do the following:

(a) Calculate Cp=C1 mod p,Cq=C1 mod q, Cs=C1 mod s. and then calculate $kp=Cp^{dp}$ mod p, $kq=Cq^{dq}$ mod q and $ks=Cs^{ds}$ mod s.

(b) By using the formula calculate k

$k=[kp.(qs)^{(p-1)} \bmod n + kq.(ps)^{(q-1)} \bmod n + ks.(pq)^{(s-1)} \bmod n]$.

(c) By using the Euclidean algorithm, calculate the value of the unique integer t, t*k= 1 mod n and $1< t < n$.

(d) Compute M^e , $C2*t = (M^e .k)t = (M^e) k.t = M^e$ mod n.

(e) For getting the value of message M should do the following steps

First calculate $C'p=M^e$ mod p, $C'q=M^e$ mod q, $C's=M^e$ mod s and then calculate $Mp=C'p^{dp}$ mod p, $Mq=C'q^{dq}$ mod q, $Ms=C's^{ds}$ mod s.

(f) Finally recover the message M by using the following formula:

$M= [Mp.(qs)^{(p-1)} \bmod n + Mq.(ps)^{(q-1)} \bmod n + Ms.(pq)^{(s-1)} \bmod n]$.

IV. RESULT AND ANALYSIS

Each of the encryption techniques has its own strong and weak points. In order to apply a suitable cryptography algorithm to an application, we should have knowledge regarding performance, strength and weakness of the algorithms. Therefore, these algorithms must be analyzed based on several features. In this paper, analysis is done with following metrics under which the cryptosystems can be compared are described below:

Time Complexity

Time complexity is commonly calculated by counting the total operations performed by the system where each operation takes a fixed amount of time. An algorithm performance time may vary with different input size therefore it is a common practice to express the time complexity in worst case donated as T(n).For instance the algorithm with T(n)=O(n) has linear time complexity whereas T(n)=O(n^2) is nonlinear and T(n)=O(2^n) is exponential.

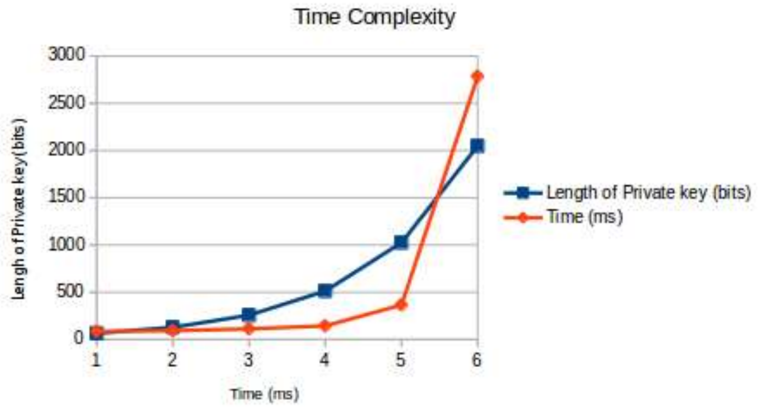
In our case we have computed the time complexity by varying the Private key length of the RSA algorithm and finding the required execution time for each Private key length.

The time complexity of RSA is analyzed by varying the private key length in bits and noting the execution time for each key length. A summary of the different key lengths in bits and their execution time is given in bits as shown in Table 1.

Table 1. Time Complexity

Length of Private key (bits)	Time (ms)
64	85.33
128	92.14
256	111.33
512	143.17
1024	364.33
2048	2785.25

Graph is shown below:



Since we can see that the estimated equation follows the simulated plot with very less error so it can be stated that the time complexity of RSA is O(n^2). It is also seen that as the size of Private key length increases the increase in time is nonlinear and exponential.

Space Complexity

Apart from Time complexity, space complexity is also an important measure to judge the performance of an algorithm. It is the amount of memory which the algorithm needs for performing its computations. A good algorithm keeps the amount of memory as small as possible. The way in which the amount of storage space required by an algorithm varies with the size of the problem it is solving. Space complexity is normally expressed as an order of magnitude, e.g. O(N^2) means that if the size of the problem (n) doubles then four times as much working storage will be needed.

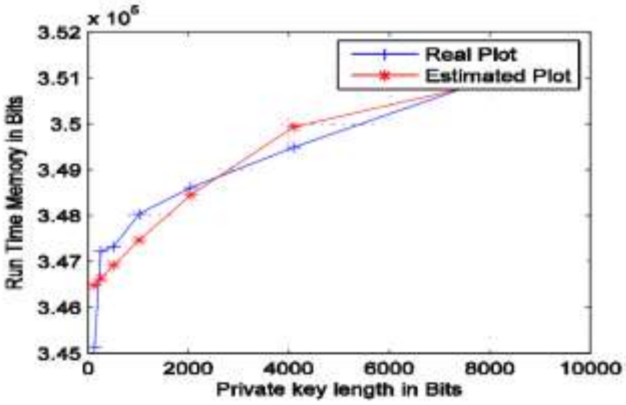
We have analyzed the space complexity between private key length which is in bits and run time memory consumed by system. A summary of the different Private Key length in bits and run time memory taken by the system is given below in table 2.

Table 2. Space Complexity

Length of Private key (bits)	Memory Consumed
128	345130
256	347225
512	347530
1024	348542
2048	348815
4096	349485
8192	351346

Graph is shown below:

Space Complexity



From the plot we see that when length of private key increases then the run time memory increases gradually. When we estimate the relationship between the private key length and run time memory it is found to be a polynomial equation of order 2 from which we can deduce that the space complexity of RSA can be expressed as S(n)=O(n^2).

Throughput

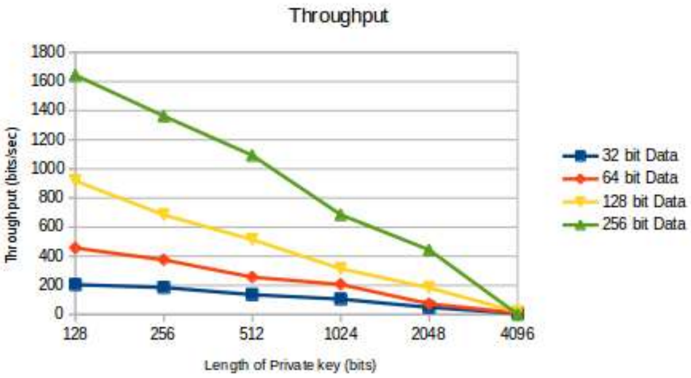
In communication systems throughput is the rate of successful data delivery over a noisy communication channel. Throughput is usually measured in bits per second and sometimes we measure it in terms of packets per second. We have calculated the throughput of the algorithm by dividing the total data in bytes by encryption time. Higher the throughput higher is the efficiency of the system. Table given below gives us the comparison between the throughput and the message signal.

We have calculated the throughput for 32, 64, 128 and 256 bytes of messages. In any cryptographic algorithm, it is essential to understand the size of the input and the size of output as this is one of the important property of an avalanche effect. Larger the size of the Cipher text compared with the Plain text, more secure is the Cipher text against any Brute-Force attack. The Table 3 below gives us the throughput for different data length.

Table 3. Throughput

	Throughput for different Private Key Length					
Data bits	**Key length 128 bits**	**Key length 256 bits**	**Key length 512 bits**	**Key length 1024 bits**	**Key length 2048 bits**	**Key length 4096 bits**
32	205.17	185.03	136.23	105.33	48.75	8.12
64	456.13	375.09	256	206.03	73.35	10.75
128	917.28	683.37	514.029	314.19	183.37	16.80
256	1643.02	1362.35	1092.20	685	443.23	0.098

The Graph, shown below, gives us a comparisons for throughput for different data sizes.



V. CONCLUSION

This paper describes the Advanced RSA cryptosystem. The proposed algorithm has speed and performance improvement on the decryption side of RSA algorithm by using the concept of Chinese remainder theorem and the method also improves the security of Cloud computing environment. The proposed method is also analysed in terms of three significant evaluation parameters namely Time complexity, Space complexity and Throughput. We have observed each efficiency parameter in detail by varying message packet length and private key length of our encryption scheme. By studying the obtained results and graphs it can be stated safely that Advanced RSA encryption algorithm is a feasible solution for secure communication in cloud computing.

VI. REFERENCES

[1] N. Somani, D. Mangal, "An Improved RSA Cryptographic System" International Journal of Computer Applications, Vol.105**,** Issue.16, pp.18-22, 2014.

[2] M. V. Malakooti, NilofarMansourzadeh, “A Robust Information Security Model for Cloud Computing Based on the Scrambling Algorithm and Multi-Level Encryption”, In the Proceedings of the International Conference on Computing Technology and Information Management, Dubai, UAE, 2014.

[3] Yang Xu, Lei Wu, Liying Guo, Zheng Chen, Lai Yang, Z. Shi, “An Intelligent Load Balancing Algorithm Towards Efficient Cloud Computing”, AI for Data Center Management and Cloud Computing: Papers from the 2011 AAAI Workshop (WS-11-08).

[4] L. Arockiam, S. Monikandan, “Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm”, International Journal of Advanced Research in Computer and Communication Engineering, Vol.2, Issue.8, August 2015.

[5] E. M. Mohamed, H. S. Abdelkader, S. EI-Etriby, “Enhanced Data Security Model for Cloud Computing”, In the Proceedings of the International Conference on Informatics and Systems (INFOS2012), Tel Aviv, Israel, 2012.

[6] V. Gampala, SrilakshmiInuganti, S. Muppidi, “Data Security in Cloud Computing with Elliptic Curve Cryptography”, International Journal of International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Vol.2, Issue.3, July 2012.

[7] N. Tirthani, R. Ganesan, “Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography”, School of computing Science and Engineering, VIT, Chennai campus.

[8] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm," In the Proceedings of the IEEE International Conference on Advanced Computer Science Applications and Technologies, pp. 402-408, 2012.

[9] W. Diffie and M. Hellman, "New Direction in Cryptography", IEEE Transaction on Information Theory, Vol. 22, pp. 644-654, 1976.

[10] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signature and Public-key Cryptosystems", Communications of the ACM, Vol. 21, Issue. 2, pp. 120-126, 1978.

CITE AN ARTICLE

Dey , S., & Basak, S. (n.d.). ACHIEVING SECURITY IN CLOUD COMPUTING THROUGH ADVANCED RSA ALGORITHM AND PERFORMANCE ANALYSIS. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *6*(12), 519-525.