International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 12 No. 1 Nov. 2014, pp. 336-345

http://www.ijisr.issr-journals.org/

Performance Evaluation of RSA Algorithm in Cloud Computing Security

Asma Khatoon[1] and Dr. Ataul Aziz Ikram[2]

[1]Software Engineering,
Department of Computing and Technology, Iqra University,
Islamabad, 2014, Pakistan

[2]Electrical Engineering,
Department of Electrical Engineering, National University of Computer & Emerging Sciences (FAST-NUCES),
Islamabad, 2014, Pakistan

ABSTRACT: In this research we propose a security algorithm for handling the security issues in cloud environments. Cloud computing is a large pool of easily and accessible virtualized resources, such as hardware, development platforms and services. Since Cloud Computing stores the data and provides resources in the open environment, therefore security has become the main obstacle which is hampering the deployment of Cloud computing framework. To ensure the security of data in cloud environment, we proposed a method by implementing RSA algorithm. After implementing 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, Security, RSA Algorithm, Time complexity, Space complexity, Throughput.

1 INTRODUCTION

Cloud Computing is the key driving force in many small, medium and large sized companies [7-8]. Cloud computing has three delivery models named as Saas, Iaas, Paas and four deployment models such as private cloud, public cloud, hybrid cloud and community cloud as illustrated in figure 1.

As many cloud users seeks the services of cloud computing, the major concern is the security of their data in the cloud [13]. Data security is always of vital importance and plays an important role in trust worthiness of computing [10]. Due to the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important [9]. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services [14].

Security and privacy are always a major concern in cloud computing environment [15]. Some of the security issues are Privacy and Confidentiality, Data integrity, Data location and Relocation, Data Availability, Storage, Backup and Recovery [16-17].

Corresponding Author: Asma Khatoon

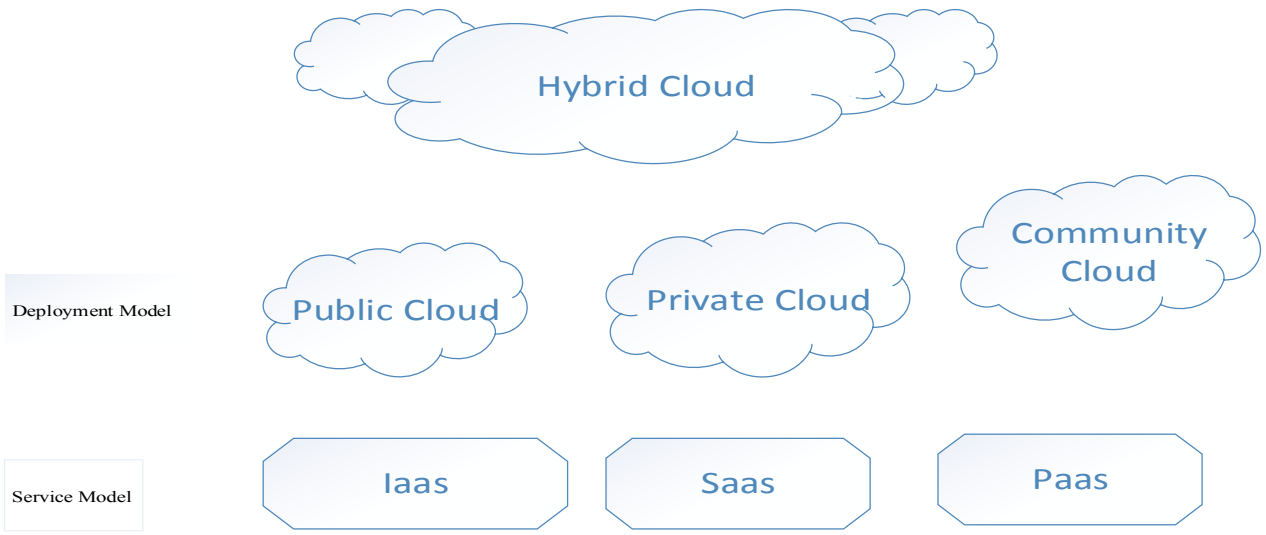

Figure 1: Cloud computing Deployment model & Service model

In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it [11-12]. 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.

2 PROBLEM STATEMENT

The security of data of the user is prime responsibility of cloud provider. So, for efficient data security we need a mechanism that provides secure data encryption as well as secure shield against data theft. Different researches have focused on the fact that user generally has to access large volumes of data from the cloud in a secured manner. We need some algorithm that will help in efficient and speedy secured data access. In this study we do research on data security issues in cloud and provide a mechanism which ensures data security in cloud in an efficient way.

3 RESEARCH OBJECTIVES

- To develop a system that will Provide Security and Privacy to Cloud Storage.
- To establish an Encryption Based System for protecting Sensitive data on the cloud and Structure how owner and storage Service Provider to operate on encrypted Data.
- To create a System where the user store its data on the cloud the data is sent and stored on the cloud in encrypted form. As in normal cases in cloud computing when a user login to the cloud and they store data on cloud storage device the data stored on the server cloud is not much secure as it can be readable to anyone who has permission to access and leaving data vulnerable.
- To develop a retrieval System in which the data is retrieved by the user in encrypted form and is decrypted by the user at its own site using a public and private key encryption.

This paper discussed security issues in the cloud environment and our proposed solution. In related work we described how other people used security techniques in cloud and the analysis of success and failure they achieved. In fifth section of the paper we discussed overview of the proposed system which is followed by technique used for our experiment and experimental results. Conclusion, future work and references are given at the end.

The research paper has organized as; Section 1 elaborates Introduction and security issues in cloud. Section 2 elaborates problem statement. Section 3 discussed research objectives. Section 4 elaborates related work. In this section, we provide some related work in the area of cloud computing security. Section 5 elaborates our proposed work. In this section, we proposed a security technique which provides user with a secure way for his data on cloud. Section 6 discusses the Implementation and Results and the paper is concluded in section 7.

4 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.

Arockiam, et al [1] proposed technique which emphasizes on improving classical encryption techniques by integrating substitution cipher and transposition 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.

Yang Xu, et al [4] proposed an agent-aid model by combining multi-agent system and decision-making theory toward working load balancing problem in large clouds. 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.

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

Tirthani, et al [6] have contemplated a design for cloud architecture which ensures secured movement of data at client and server end. They used the non-breakability of Elliptic curve cryptography for data encryption and Diffie Hellman Key Exchange mechanism 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.

Veerraju Gampala, et al [5] explore data security of cloud in cloud computing by implementing digital signature and encryption with elliptic curve cryptography. In their work authentication and encryption for secure data transmission from one cloud to other cloud is presented that 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.

5 PROPOSED WORK

In proposed work, we have to implement RSA algorithm and then analyze its performance based on different parameters such as Time complexity, Space complexity and through put. The proposed work will be carried out in two steps. First we will program the algorithm in Eclipse IDE with Java to get the results for different evaluation parameters and then we use Matlab to plot the results for these parameters. The obtained graphs will help us to study and analyze the efficiency of RSA algorithm for the above mentioned parameters. The implementation of RSA algorithm involves following steps:

- Key Generation
- Encryption
- Decryption

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA uses modular exponential for encryption and decryption. RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is ciphertext, then at encryption n is a very large number, created during key generation process.

The RSA algorithm is a secure, high quality, public key algorithm. Following are the steps involved in key generation, encryption & decryption of system.

A) RSA Encryption

PLAIN TEXT : $M < n$

CIPHER TEXT : $C = Me \bmod (n)$

B) RSA Decryption

CIPHER TEXT: C

PLAIN TEXT: $M = Cd \bmod (n)$

Encryption/Decryption Equation of RSA

Key Generation

- Choose 2 large prime numbers, p & q
- Compute $n=p*q$
- Compute $\Phi(n) = (p-1) *(q-1)$.
- Choose e, relatively prime to $\Phi(n)$.
- Find d, such that $e*d=1 \bmod \Phi(n)$.

($e*d \bmod \Phi(n) = 1$ i.e.[$(e*d) / \Phi(n)$] reminder =1)

- The Public key is (n, e).
- The Private key is (n, d),

Key Generation steps of RSA Algorithm

In order to implement RSA in Eclipse software first of all a flow chart for the required algorithm was designed. This flow chart is given below:

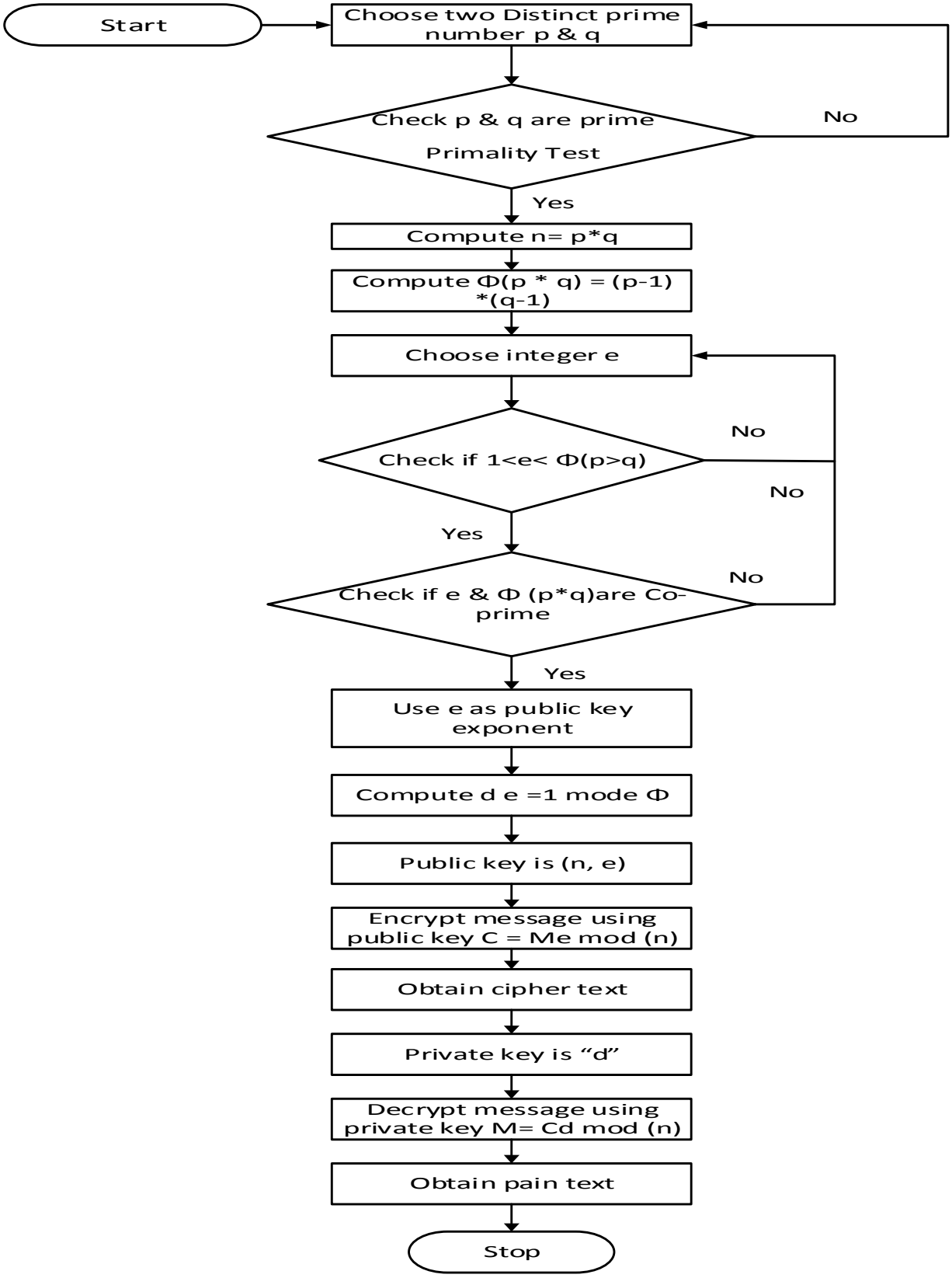

Figure 2: Flow chart of RSA Algorithm

The RSA encryption/decryption is just a modular exponentiation operation. This mathematical operation is represented as C=Me mod n, where C is cipher text, M is plain text, e is the public key exponent, and n is the modulus.

6 IMPLEMENTATION AND RESULTS

In this section we have evaluate our algorithm on parameters such as Time complexity, Space complexity and through put which will help us to analyze the efficiency of algorithm based on these parameters. These parameters can be used to check the effectiveness of RSA algorithm.

6.1 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

Private key length(bits)	Time in (ms)
64	86.00
128	91.33
256	110.33
512	142.67
1024	363.67
2048	2784.67

Graph can be shown as:

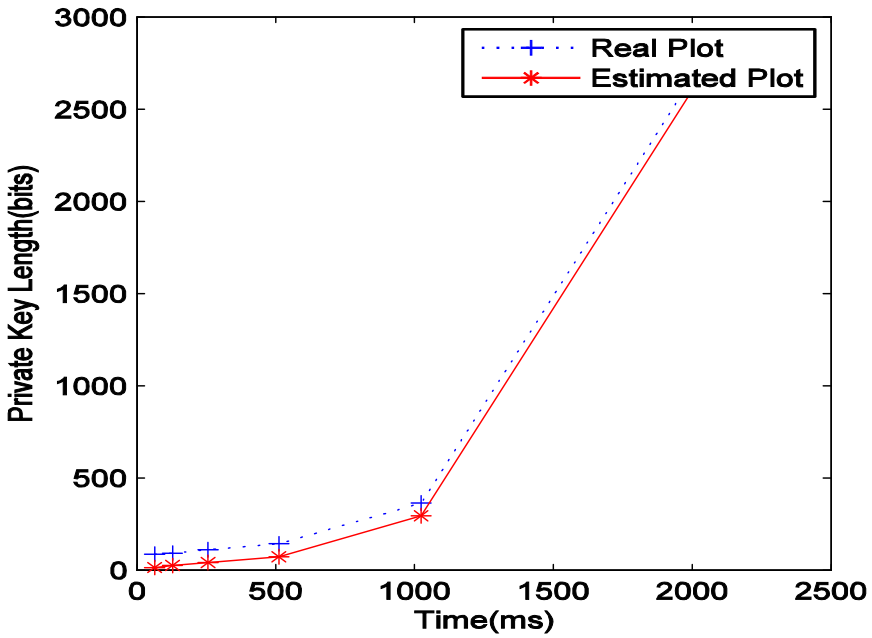

Figure 3: Time Complexity

Figure 3.shows the plot for Time vs Cipher length in bits for RSA algorithm. In order to find the relationship between time and Cipher length a polynomial equation of order two is proposed and was also compared with the original graph. As we can see that the estimated equation follows the simulated plot with very less error therefore 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.

6.2 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

Private key length (Bits)	Run time memory
128	345128
256	347224
512	347320
1024	348040
2048	348608
4096	349488
8192	351048

The graph plotted between Run time memory and Private Key length is shown in figure 4. As seen from the plot as length of private key increases the run time memory increases gradually. When the relationship is estimated 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)

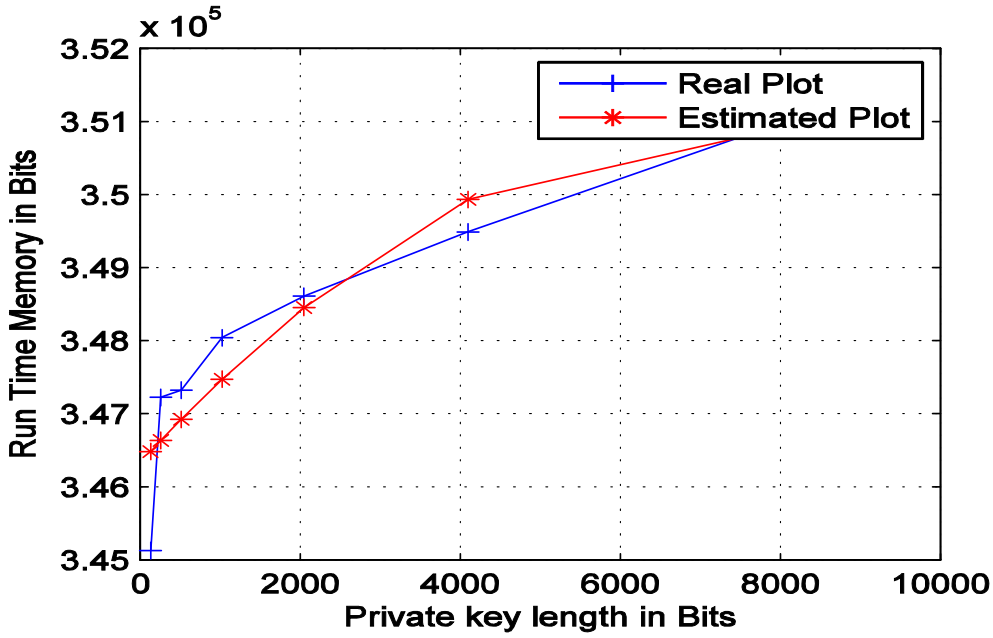

Figure 4: Run Time Memory Vs Private Key length plot of RSA algorithm

6.3 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 Ciphertext compared with the Plaintext, more secure is the Ciphertext against any Brute-Force attack. The table below gives us the throughput for different data length.

Table 3: Throughput

	Throughput for different Private Key Length					
Data Bits	**128 bits key length**	**256 Bits key length**	**512 bits key length**	**1024 bits key length**	**2048 bits key length**	**4096 bits key length**
32	205.13	186.04	136.75	102.56	48.854	7.120
64	457.14	372.09	256	205.13	71.99	10.82
128	914.28	684.49	514.056	315.27	182.33	16.77
256	1641.02	1361.70	1094.02	684.49	443.67	0.095

When we analyze the data from the above table we see that there is a tradeoff between through put and Private Key length. If we want to increase the throughput we have to decrease the Private key length and hence have to make compromise on the security of the data. The plot given below gives us a comparison for throughput for different data sizes.

The graph plotted for 32, 64,128 and 256 bytes of messages.is shown in figure 5. As seen from the plot it is clear that there is a tradeoff between through put and Private Key length. If we want to increase the throughput we have to decrease the Private key length and hence have to make compromise on the security of the data.

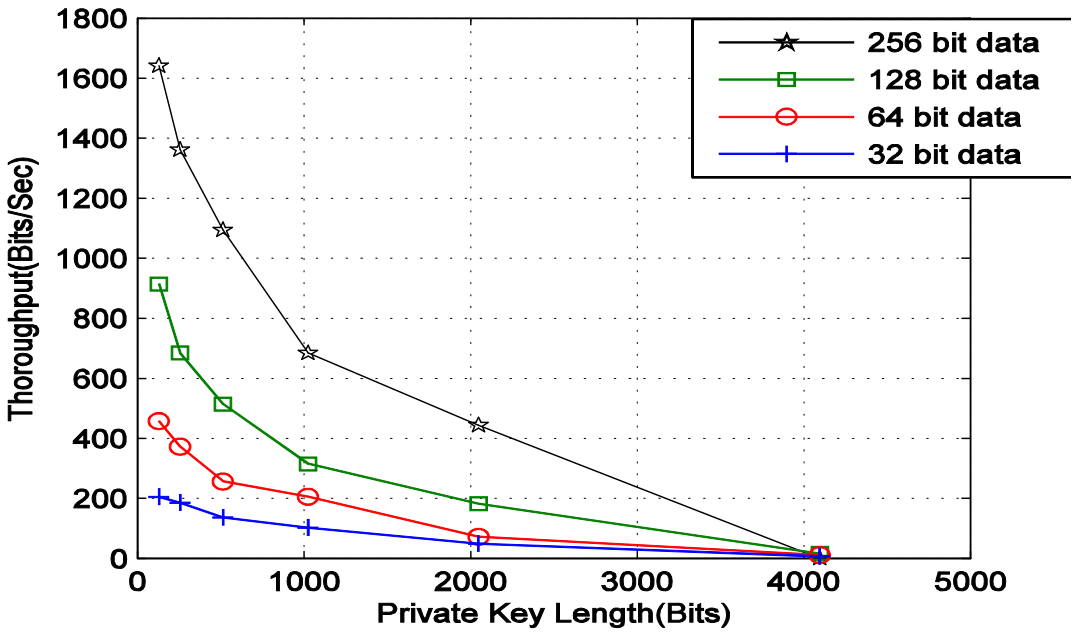

Figure 5: Throughput for 32, 64,128 and 256 data sizes

7 CONCLUSIONS

In this research paper we have discussed the security issues of cloud computing in detail. We have also discussed different encryption systems which are being proposed to address the security problem in cloud computing. Then we have proposed and implemented a security system based on RSA algorithm. We have evaluated its performance based on different parameters such as space complexity, time 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 stated safely that RSA encryption algorithm is a feasible solution for secure communication in cloud computing.

ACKNOWLEDGMENT

First, I am thankful to Allah Almighty, whose support and strength helped me in bringing this work to the end. After that I am thankful to my teacher Dr Ataul Aziz Ikram for his support and guidance.

Finally, thanks to my parents who endured this long process with me, always offering support and love. Without their support I would not be able to complete this work.

REFERENCES

[1] Dr. 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 2013.

[2] Dr. Mohammad V. Malakooti, NilofarMansourzadeh, "A Robust Information Security Model for Cloud Computing Based on the Scrambling Algorithm and Multi-Level Encryption", Proceedings of the International conference on Computing Technology and Information Management, Dubai, UAE, 2014, Islamic Azad University, UAE branch, Dubai, UAE.

[3] EmanM.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby, "Enhanced Data Security Model for Cloud Computing", The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May, Cloud and Mobile Computing Track.

[4] Yang Xu, Lei Wu, Liying Guo, Zheng Chen, Lai Yang, Zhongzhi 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).

[5] Veerraju Gampala, SrilakshmiInuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[6] NehaTirthani, Ganesan R, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography", School of computing Science and Engineering, VIT, Chennai campus.

[7] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for Cloud Computing". The University of Texas at Dallas, USA, International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.

[8] Anup R. Nimje, "Cryptography In Cloud-Security Using DNA (Genetic) Techniques", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue5, pp.1358-1359, September- October 2012.

[9] Danish Jamil, Hassan Zaki, "Cloud Computing Security", International Journal of Engineering Science and Technology (IJEST).

[10] RachnaArora, AnshuParashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, www.ijera.com , Vol. 3, Issue 4, pp.1922-1926, Jul-Aug 2013.

[11] Li Dongjiang, Wang Yandan, Chen Hong, "The research on key generation in RSA public- key cryptosystem", Department of Computer Science, North China Electric Power University, Beijing, China, Fourth International Conference on Computational and Information Sciences 2012.

[12] Ahmed E. Youssef, ManalAlageel, "A Framework for Secure Cloud Computing", Dept. of Information Systems, King Saud University, Riyadh, 11543, KSA.

[13] Engr: Farhan Bashir Shaikh, SajjadHaider, "Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates.

[14] Dr. P. Dinadayalan, S. Jegadeeswari, Dr. D. Gnanambigai, "Data Security Issues in Cloud Environment and Solutions", World Congress on Computing and Communication Technologies 2014.

[15] NatanAbolafya, Secure Documents Sharing System for Cloud Environments, Master of Science Thesis Stockholm, Sweden 2012.

[16] Abdullah Al Hasib, AbulAhsan Md. MahmudulHaque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography", Third International Conference on Convergence and Hybrid Information Technology, 2008.

[17] Cloud Security Alliance, (2009) Security Guidance for Critical Area of Focus in Cloud Computing V2.1. [Online]. Available: https://cloudsecurityalliance.org/csaguide.pdf , accessed on Feb 2012.