International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 11 No. 2 Nov. 2014, pp. 439-444
© 2014 Innovative Space of Scientific Research Journals
http://www.ijisr.issr-journals.org/

Data Security for Cloud Computing Using RSA with Magic Square Algorithm

A. Dharini, R.M. Saranya Devi, and I. Chandrasekar

Assistant Professor, Department of Computer Science,
Sri Vijay Vidayala College of Arts & Science,
Dharmapuri, Tamil Nadu, India

ABSTRACT: Cloud computing is an up-and-coming technology and shared information, resources, software and hosting to customer on a pay-as-you-use basis. The major issues in cloud computing is the data protection security and it reduce the growth of the cloud computing. The security needs during the transmission of sensitive data and critical application to shared cloud environment. For secure communication over public network data can be protected by the method of encryption. So the proposed encryption techniques for secure data transmission, SSL over RSA with magic square provide add-on security to cryptosystem. To provide the confidentiality and integrity of data-in-transmission to and from cloud providers In this paper cryptographic methods RSA are discussed and combine Magic Square algorithm with RSA when implementing on data security in cloud computing.

KEYWORDS: Cryptography, Encryption, Decryption, Magic Square, RSA, Cloud computing.

1 INTRODUCTION

Cloud computing is used for group of virtualized and scalable resources and also competent of hosting application and providing required services to the users with the “pay only for use” basis. Using the internet cloud, users can access these services without having any previous knowledge on managing the resources involved. Cloud computing provides the ability to shared resources and common infrastructure, offering services on demand over the network to perform operations that meet changing business needs.

Cloud providers typically center on one type of cloud functionality provisioning: infrastructure, Platform of Software [1][2]. Cloud Infrastructure as a service provides processing, storage network bandwidth and other fundamental computing resources which allow customers to deploy and run operating systems or applications. For safe communication over public network data can be protected by the method of encryption. Encryption exchanges that data by any encryption algorithm using the key in twisted form. Only user can access the key used to decrypt the encrypted data [3]. The purpose of encryption is used to preventing leak or secrecy in communications [4]. Encryption algorithms play a huge role in providing data security against malicious attacks.

To encrypt the plaintext characters to cipher, their ASCII values are taken and if a character occurs in several places in a plaintext there is a possibility of same cipher text is produced. To overcome the problem, taking ASCII values for the characters to encrypt, preferably different numerals representing the position of ASCII values are taken from magic square and encryption is performed using RSA cryptosystem. This proposed research work provides the security using public key algorithm that ensures the security is improved and also compare these two algorithms and analysis which one is best for encryption in Cloud Computing.

The paper begins with a note on the related technology required in section 2. The detailed features of Cloud security is found in section 3. The Performance of two algorithms is in section 4. The result analysis of the two algorithms is in Section 5. Section 6 deals with the findings and future work of the paper.

2 BACKGROUND

Many works are carried out to implement data security in the Cloud Computing. Some of the earlier works are presented in this section.

In 2009 Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing analysed the basic problem of cloud computing data security. With the analysis of Hadoop Distributed File System (HDFS) architecture, they get the data security requirement of cloud computing and set up a mathematical data model for cloud computing. Finally they build a data security model for cloud computing [5].

In 2009 *Gopinath Ganapathy, and K. Mani* proposed another layer of security to any public key algorithms such as RSA, ElGamal etc., Since, this model is acting as a wrapper to a public key algorithm, it ensures that the security is enhanced. Further, this approach is experimented in a simulated environment with 2, 4, 8, and 16 processor model using Maui scheduler which is based on back filling philosophy [6].

In 2010 Amir Mohamed Talib Rodziah Atan, Rusli Abdullah & Masrah Azrifah Azmi Murad described on the theoretical concept and approach of a security framework as well as a Multi-Agent System (MAS)and architecture that could be implemented in cloud platform in order to facilitate security of Cloud Data Storage(CDS) [7].

In 2011, G. Jai Arul Jose, C. Sajeev Propose a model system in which cloud computing system is combined with Cluster Load balancing, Secure Socket Layer (SSL) over AES and secure session In this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system. Here cost is greatly reduced, Maintenance cost is reduced. The data is secured through SSL; AES based Cryptography, Server clustering and Server Load balancing [8].

In 2011 S. Praveen Kumar, K. Naveen Kumar, S. Sreenadh, B. Aravind, K. Hemnath Kumar proposed a work provides another layer of security to any public key algorithms such as RSA, Elgamal etc., Since, this model is acting as a wrapper to a public key algorithm, and it ensures that the security is enhanced. It attempts to augment the efficiency by providing add-on security to the cryptosystem [9].

3 SECURITY IN CLOUD

Cryptography is the study of mathematical techniques related to characteristic of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Modern encryption techniques such as RSA are discussed in brief in this section.

3.1 RSA

In the asymmetric method, private key and public key are used. Both the sender and receiver know the public key and it is used to encrypt the data. The owner of the private key can only decrypt the message. The public and private keys are always in pairs, it is difficult to derive at the private key from the public key which is shared. That is why this method is considered to be more secure than the symmetric method. RSA adopted public key cryptography algorithm [10]. RSA algorithm is developed by Rivest, Shamir and Adleman.

The encryption process can be done either at the customer's end or at the service provider's or at the vendor's end. The customer can do the encryption process and it will increase the computation time and usage which in turn increases the cost. Furthermore there may be no guarantee for the proper implementation of the encryption process. Because of these, it is appropriate to do the encryption process at the Client's end.

3.2 MAGIC SQUARE

A magic square is a square array of numbers consisting of the distinct positive integers 1, 2, …, *n*2 arranged such that the sum of the n numbers in any horizontal, vertical, or main diagonal line is always the same number. Given an n×n matrix of the integer 1 to n^2 such that the sum of every row, column and diagonal is the same. Then n rows the sum of all the numbers in the magic square must be n.M. But the numbers being added are 1, 2, 3, ... n2 , and so 1 + 2 + 3 + ... + n2 = n.M. In summation notation $\sum_{i=1}^{n^2} i = n.M$. Using the formula for this sum, $\mathrm{n.M} = \frac{n^2(n^2+1)}{2}$, and then solving for M gives $\mathrm{M} = \frac{n(n^2+1)}{2}$. Thus, a $^{3\times3}$ normal magic square must have its rows, columns and diagonals adding to $\mathrm{M} = \frac{3(3^2+1)}{2} = \frac{30}{2} = 15$ a $^{4\times4}$ to M = 34.The magic sum for an n×n normal magic square can be found by filling the n×n square with the numbers 1, 2, 3, ... n2 first going across the top row, then the second row, and so on and then adding the numbers along either of the diagonals. There are three types of magic squares:

- The odd order magic square are referred to M is an odd number M=2n+1 where n=0,1,2,3….
- The even order magic square are referred to M is an even number divisible by both 2 and 4 M=4(n+1) where n=0,1,2,3…
- The singly even order order magic square are referred to M is an even number divisible by 2 but not by 4 M=2(n+3) where n=0,1,2,3..

Method of Proposed Add-On Security Model

- Construct different doubly even Magic Square of order 16 as far as possible and each magic square corresponds to one ASCII set.
- To encrypt the character, use the ASCII value of the character to determine the *numeral in the magic square* by considering the position in it. Let NP and NC denote the numeral of the plaintext and cipher text respectively. Based on NP and NC values, all plaintext and cipher text characters are encrypted and decrypted respectively.

DATA SECURITY PROCESS

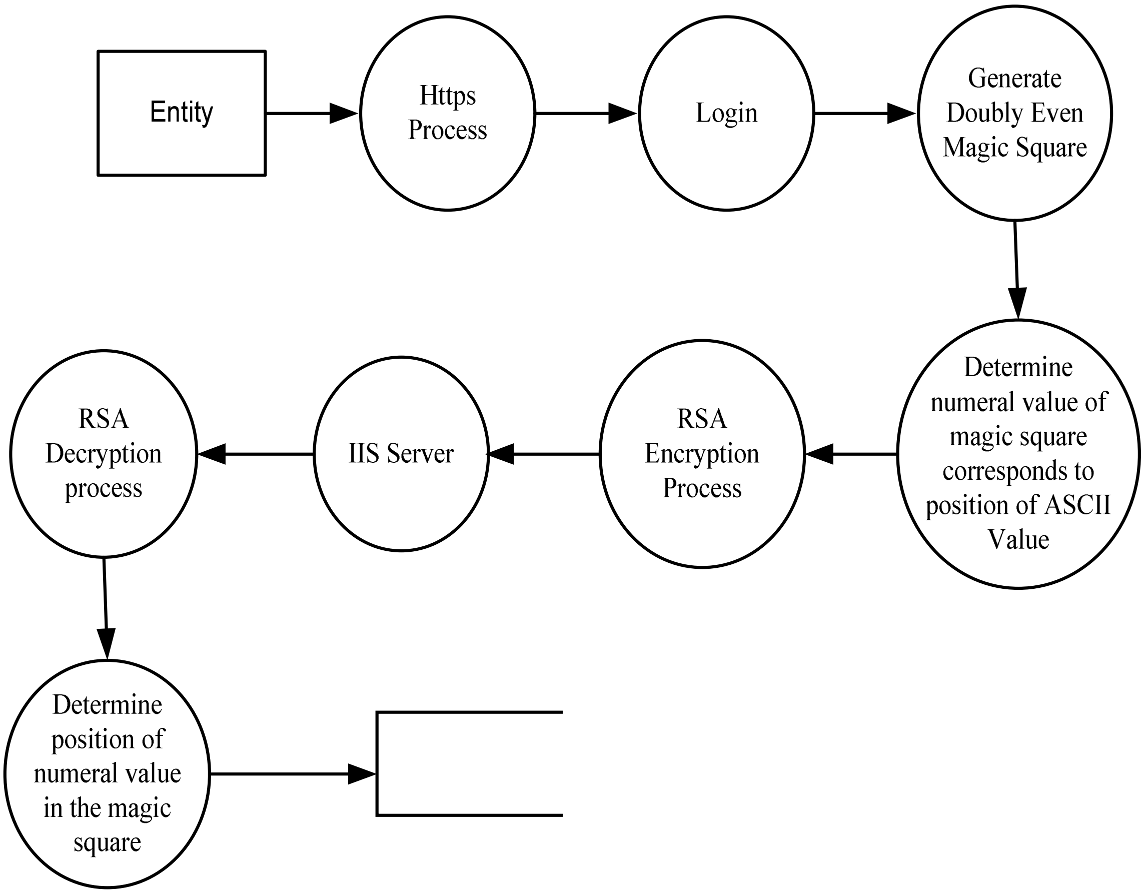
Entity
Https Process
Login
Generate Doubly Even Magic Square
Determine numeral value of magic square corresponds to position of ASCII Value
RSA Encryption Process
IIS Server
RSA Decryption process
Determine position of numeral value in the magic square

Fig.1. Data security Process

In data security process, the authenticated client has to login and the doubly even magic square has been generate the sequence of number that corresponds to ASCII value. By using that value RSA algorithm are used to encrypt the data. Afterwards the decryption of data has been done.

Context Level Diagram

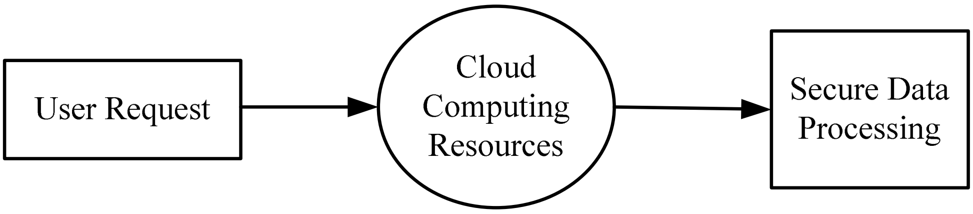

Fig.2. Context Level Diagram

Architectural Diagram

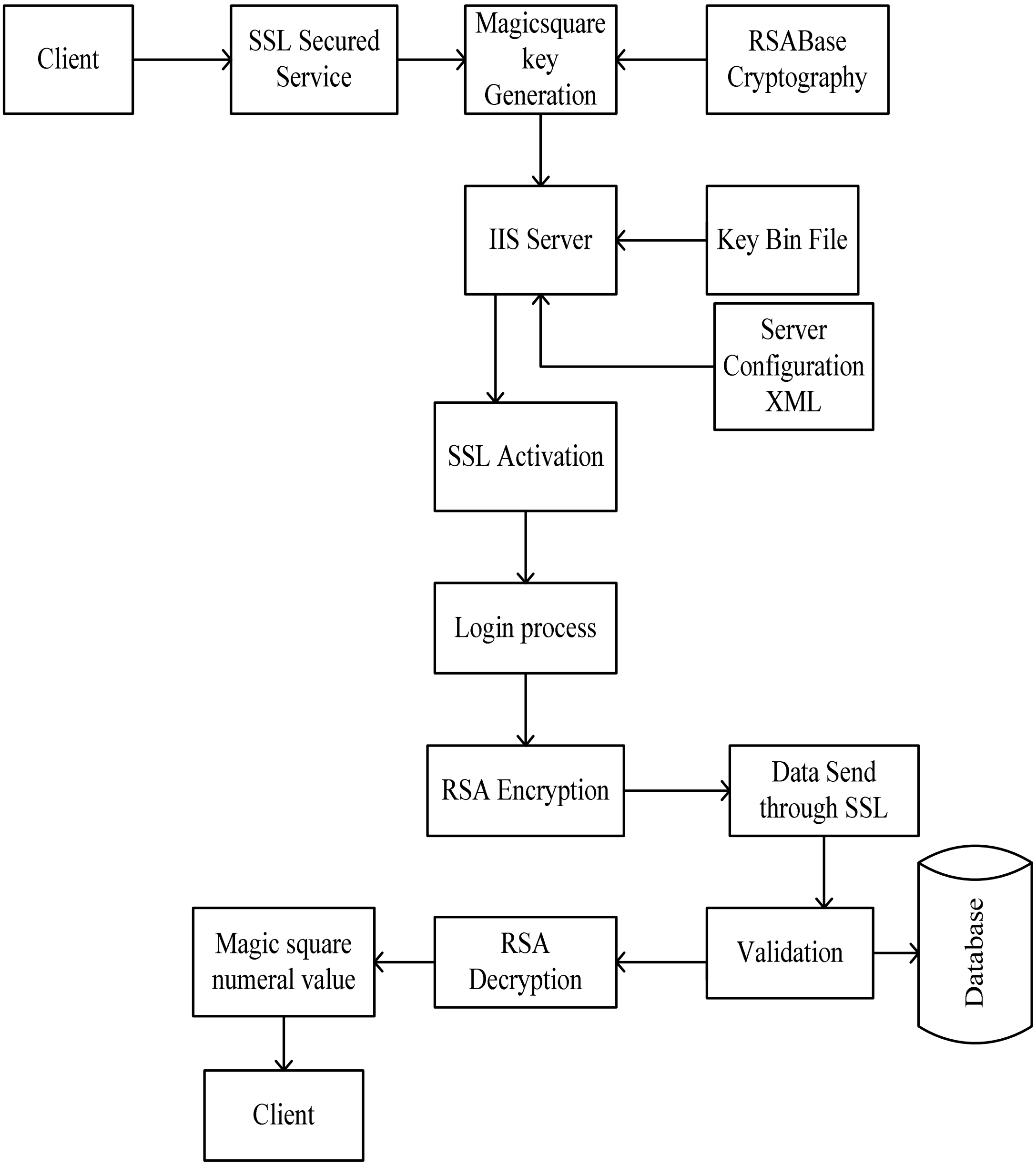

Fig.3. Architectural Diagrams

4 Result Analysis

The security analysis consists of analyzing various security properties such as Data Confidentiality, Authentication and Integrity of the data.

4.1 Security Analysis

- *Data Confidentiality* is analyzed by comparing it with various data Encryption algorithms such Advanced Encryption Standard or Data Encryption Standard which uses the symmetric key for encrypting the data. In our proposed scheme as the data is encrypted, hence the cloud service provider do not have any access to the data as the user do not know the key, and is only known to the data owner which ensures the Data Confidentiality.
- *Authentication: A* new user is added or it tries to access the data over a cloud, authentication is performed with the help of the password set by the user during registration.
- *Integrity:* Ensures that the data integrity is maintained and the data over the cloud is secured.

4.2 Algorithm Analysis

4.2.1 RSA Algorithm

In Table 1 is used to evaluate the RSA algorithm with the local and cloud environment analysis with different input file sizes. The algorithm RSA- an asymmetric encryption algorithm, is on an average the most time consuming. This is true in a local environment as well as cloud environment.

Table.1. Comparison of Mean Processing Time on the Cloud and on Local

Input file	RSA (Local)	RSA (Cloud)
2kb	678.4	380.2
5kb	747.3	309.2
10kb	796.8	400.9
20kb	853.4	429

4.2.2 RSA with Magic Square

The time taken for encryption and encryption of various file sized message in simulated parallel environment using RSA public key crypto system with magic square, illustrated in Table 2. In earlier system these algorithms are implemented on the single processor system but because of the availability of the fast and parallel computing resources, the better encryption and decryption techniques can be implemented by using these security algorithms in cloud network. The Maui Scheduler with back filling techniques are used to calculate encryption and decryption time.

Table.2.Encryption and Decryption time using RSA

File Size(MB)	Encryption Time(ms)	Decryption Time(ms)	Total Time
1	231	265	496
2	452	480	932
4	910	940	1850
8	1867	1888	3755

5 Conclusion

Finally conclude the RSA algorithm is very secure with the help of the magic square. The magic square boosts the add-on security to system. It will increase the Computational speed. It provides security to the files while transmitting the files. The efficiency of algorithm is based on the time take of the encryption and decryption produce the cipher text to clear text so the extensively RSA with magic square is handling ASCII character in the cryptosystem. Magic square deals with complexity in encryption and boosts the security in the cloud environment.

In the future work, at present a small data requires large amount of memory space for data so in future this can be further developed so that the memory space would be minimized into small area. Existing RSA allows only text content to be encrypted whereas further it can be enhanced so that image file and audio files shall also be encrypted.

ACKNOWLEDGEMENT

We would like to thank my respected research supervisor **Dr. S. SAGAYARAJ,** for the support of this research work. It is our privilege to thank my parents and friends for their encouragement and support in carrying out my research work well.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud dentition. SIGCOMM Comput. Commun. Rev.,39:50{55, December 2008.

[2] Srinivasa Rao V, Nageswara Rao N K, E Kusuma Kumari. Cloud Computing: An Overview, Journal Of Theoretical And Applied Information Technology-2005 - 2009 Jatit.

[3] Cloud Security Alliance (2010). Top threats to cloud computing, version 1.0.
http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[4] Anoop MS, “Public key Cryptography (Applications Algorithm and Mathematical Explanations)”.

[5] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing. Data Security Model for Cloud Computing. Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) *Qingdao, China, November 21-22, 2009.*

[6] Gopinanadh Ganapathi, and K.Mani, “Add on security model for public key Cryptosystem based on magic square implementation”, India, 2009.

[7] Amir Mohamed Talib Faculty of Computer Science & IT, University Putra Malaysia. Security Framework of Cloud Data Storage Based on Multi Agent System Architecture: Semantic Literature Review. Vol. 3, No. 4; November 2010, www.ccsenet.org/cis.

[8] G. Jai Arul Jose1, C. Sajeev2. Implementation of Data Security in Cloud Computing. *International Journal of P2P Network Trends and Technology- July to Aug Issue 2011.*

[9] S. Praveen Kumar, K. Naveen Kumar, S. Sreenadh, B. Aravind, K. Hemnath Kumar. Novel Advent for Add-On Security by Magic Square Intrication. Global Journal of computer science and technology. volume 11, issue 21, December 2011.

[10] R. Rivest, A. Shamir, L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems" z. Communications of the ACM, Feb 1978.