IJCTA, 9(27), 2016, pp. 147-152 ISSN: 0974-5572
© International Science Press

Enhanced RSA Algorithm for Data Security in Cloud

D.I. George Amalarethinam* and H. M. Leena**

ABSTRACT

In the new era of Computing, the possibility of provisioning resources like operating system, computing power, memory space, software, platform, etc., on the basis of pay-on-demand came into existence through Cloud Computing. The rapid evolution of usage of resources based on the need of the users paved the way for seeking this new technology. Since all the users rush up in accessing the resources provided by the cloud, more complexity lies on storing the users' data in a secured way in clouds. Cloud Security issues force the users as well as providers to propose more security related solutions. Data Security is the most vital among all security issues in the cloud. This data security can be ensured by Confidentiality. To achieve this confidentiality, the data has to be encrypted before it is sent to the cloud environment. Cryptography is the methodology introduced in the last decades for attaining Information Security. To avoid the attacker or intruder to predicate the pattern used to secure the data, the speed of the encryption and decryption processes have to be increased, and the key used for the processes has to be strengthened. Two cryptographic mechanisms, namely, Symmetric Key and Asymmetric Key algorithms are used for encryption and decryption processes. Among these two, Asymmetric key cryptography also termed as Public key cryptography is widely used now-a-days because it is not necessary to prevent the key from the public whose performance and speed is more or less equal to that of symmetric key algorithms. RSA is one of the widely used asymmetric key encryption algorithm. The proposed work brings the data security in cloud by enhancing the RSA algorithm. It uses prime numbers for encryption and decryption processes. The proposed algorithm outperforms the standard RSA.

Keywords: Cloud Computing, Data Security, Confidentiality, Public Key Cryptography, RSA.

1. INTRODUCTION

Cloud computing architecture is a collection of interrelated or interconnected systems in a distributed manner with the provision of sharing resources like hardware, software, applications, memory, operating systems, etc., The current users of IT focuses on deploying these type of resources on pay from anywhere at any time. Since there is an increase in amount of users of cloud resources, the issues related to accessing these resources also increases. Some of the challenges like Security, Availability, Performance, Higher cost and lack of interoperability etc., exists more in clouds. Among these, security is the most important issue. Thus it decreases the usage of cloud. Since most of the IT users need more storage for storing their professional, organizational and personal data, they move to cloud. Security is the major issue with regard to storage. Data Security and Privacy, Identity and Access Management, Disaster Recovery/Business Continuity Planning etc., are some of the security concerns, related more with data called as Data Security. This issue becomes a serious one in the cloud computing environment, because data are scattered in different machines and storage devices including servers, PCs, and various mobile devices. Data security in the cloud computing is more complicated than data security in the traditional information systems [1]. Confidentiality plays a major role in providing data security. Confidentiality can be achieved through the process of encryption and decryption which can protect the data from unauthorized access and modifications. Cryptography is one the major mechanism used in the last decades for handling the security issues. The types of cryptographic

* Dean of Science & Director (MCA), Jamal Mohamed College, Trichy, Tamil Nadu, India.

** Assistant Professor, Department of Computer Science, Holy Cross College (Autonomous), Trichy, Tamil Nadu, India. leena_raja@yahoo.co.in

algorithms may be symmetric or asymmetric. Asymmetric key Cryptography also known as Public key Cryptography is more preferable than the Symmetric key Cryptography because it is not a matter to share the secret key to the other party who participate in communication. Public key cryptography includes Encryption algorithms like RSA, Digital Signature algorithms like Message Digest, Secure Hash, Hash-based Message Authentication Code, and other algorithms including Elliptic Curve, Elgammal etc., . RSA is considered as a primary one for accomplishing the task of protecting data stored in cloud.

2. RELATED WORK

RSA[2] is a widely used Public Key Cryptographic algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, the discoverers of the algorithm. RSA includes three parts : Key Generation, Encryption and Decryption. The key generation part generates two keys, namely, Public Key and Private Key. This Standard RSA algorithm is used by many researchers to protect the data stored in the cloud environment. The Public key is provided by the Cloud Service Provider. The data encryption is done by the Service Provider. Thus, only the authorized user can access the data [3].

Pallav Sharma et. al. [4] suggested a solution for data security problem by combining RSA algorithms with the other Symmetric Key Cryptographic algorithms. This hybrid approach made the encryption and decryption process stronger. RSA algorithm with 1024 bit key used with a block cipher algorithm provided more complex encryption method. RSA and Advanced Encryption Standard (AES) algorithms [5] are used as an integrated approach where data was encrypted with AES and private key can be encrypted with RSA algorithm. This lead to the increase in performance and compared with other techniques. The parameters like throughput, response time, overheads etc., were used as a performance measure. There exist many variants of RSA. One among them is Multi-prime RSA. It is an isolated version of RSA cryptosystem. This Multi-prime uses more than two prime numbers for increasing the speed of decryption time and the Chinese remainder theorem for decryption process [6]. This method was used to speed up the decryption procedure and in turn decreased the time spent for converting cipher text into plain text.

A new scheme[7] was proposed by combining the different variants of RSA such as DRSA and RePower RSA. This is semantically secure because randomness was added in the computation. It gives better encryption cost and the decryption time is also reduced. This scheme was proven to be better than RePower RSA as well as DRSA. The Key generation step of the RSA algorithm was optimized by using prime test. But this is very tedious when the key size is very large. This can be overwhelmed by Fermat's little theorem [8]. By the usage of this theorem, the complexity and the key generation time is reduced. It also increased the reliability of the encryption process.

RSA algorithm with two public keys and mathematical relation [9] was implemented by Narkhede et. al. The limitation in degree of Security in RSA was eliminated by a hybrid approach for providing data security in cloud. Nandita Sengupta et. al.[10] used Feistel Cipher Algorithm and RSA in two phases. Since two algorithms were used in two phases, the probability of man-in-the-middle attack was reduced.

Pachipala Yellama et. al. [11] discussed the encryption of RSA algorithm for the sensitive data that are to be stored in the cloud. When the authorized user request the data for usage then the data is decrypted and provided to the user. Nasrin Khanezaei et. al. [12] used a combination of asymmetric and symmetric encryption techniques (i.e., RSA and AES encryption methods) to achieve the assurances of cloud data security. Sarthak R Patel et. al. [13] suggested an algorithm called High Speed and Secure RSA algorithm. It used Random Numbers for encryption and decryption processes. Thus RSA algorithm is used to enhance the data security in cloud either individually or in an integrated manner.

3. PROPOSED METHODOLOGY

RSA algorithm involves two keys termed as public and private. The public key is used for encryption process and private key is used for decryption. Both the keys use the same computed 'N' value. The proposed Enhanced RSA (ERSA) algorithm uses two different 'N' values for encryption and decryption.

The three Stages of the ERSA algorithm:

Stage 1: Key Generation

Stage 2: Encryption

Stage 3: Decryption

Stage 1 : Key Generation involves the following steps.

STEP 1 : Select any two large prime numbers P and Q. Apart from these, choose two more prime numbers PR1 and PR2.

STEP 2 : Calculate the values of N1 and N2 by

$N1 = P * Q * PR1 * PR2$

$N2 = P * Q$

STEP 3 : Compute $\Phi(r) = (P-1) * (Q-1) * (PR1-1) * (PR2-1)$

STEP 4 : Choose the Public Key E, such that $GCD(E, \Phi(r)) = 1$.

STEP 5 : The Private Key D is computed from $D * E = 1 * mod(\Phi(r))$.

Thus, the Public key component has a pair of E and N1 and Private Key pair as D and N2.

Stage 2 : Encryption Process

The formula for generating a cipher text from the given plain text is $C = M^E$ mod (N1).

Stage 3 : Decryption Process

The Plain text can be found by using $M = C^D$ mod (N2).

The proposed algorithm ERSA used RSA algorithm with computations of two ‘N’ values. The calculated N1 and N2 values included prime numbers instead of two Random Numbers as in High Speed and Secure RSA algorithm. The ERSA algorithm increases the encryption speed and decreases the decryption time.

4. RESULTS AND DISCUSSIONS

ERSA algorithm has been implemented in Java version 7. The results show an improvement in both encryption and decryption process. Table 1 shows the Encryption and Decryption time for Standard RSA algorithm proposed by Ron Rivest, Adi Shamir, Len Adleman. High Speed and Secure RSA algorithm was proposed by Sarthak R Patel[12].

Table 1
Comparison of Encryption and Decryption time of various algorithms with different file sizes

FILE SIZE (KB)	*Encryption Time(ms)*			*Decryption Time(ms)*		
	Standard RSA	*High Speed and Secure RSA*	*ERSA*	*Standard RSA*	*High Speed and Secure RSA*	*ERSA*
4	16	15	15	15	16	15
8	31	47	15	16	16	16
16	47	62	43	16	16	15
32	78	109	69	47	31	31
64	218	202	187	47	47	47

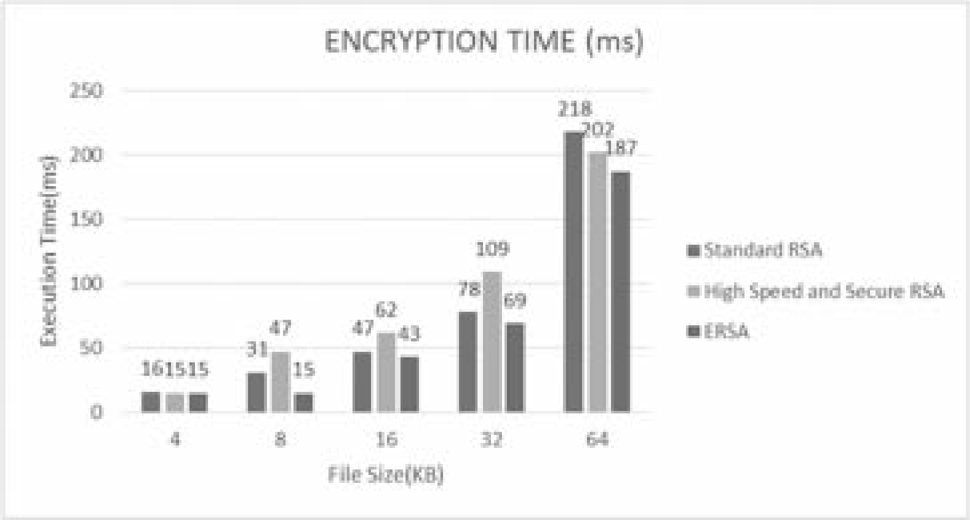

Figure 1: Comparison of Encryption Time with different file sizes

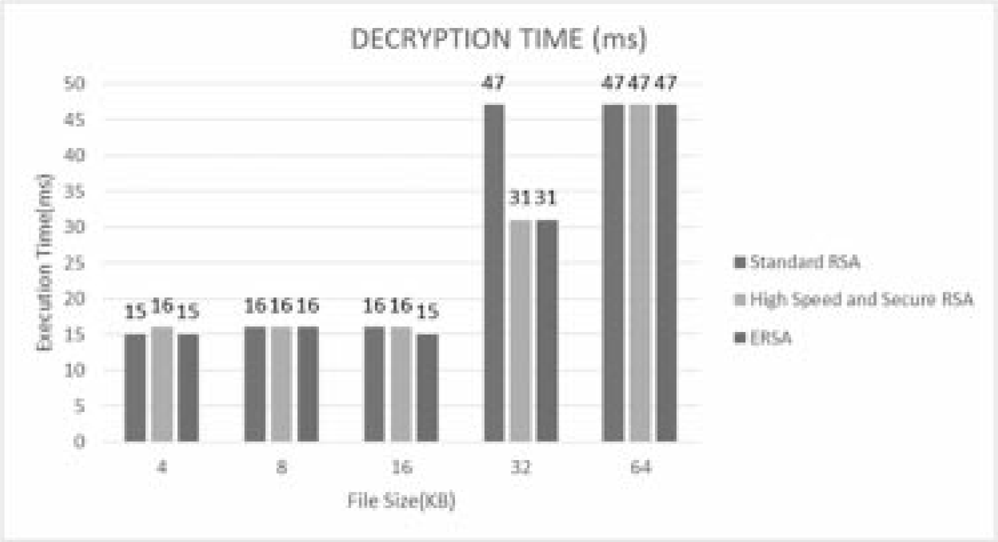

Figure 2: Comparison of Decryption Time with different file sizes

From the table, it is observed that the proposed ERSA algorithm outperforms the Standard RSA and High Speed and Secure RSA algorithms in encryption speed and decryption time.

Figure 1 and Figure 2 show the Encryption time and Decryption time respectively of all the three algorithms.

Table 2 reveals that the average time of both encryption and decryption process of ERSA has been condensed to a certain extent when compared to the other two.

Table 2
Comparison of average time of encryption and decryption of various algorithms

Average Time (ms)	*Standard RSA*	*High Speed and Secure RSA*	*ERSA*
Encryption	78	87	65.8
Decryption	28.2	25.2	24.8

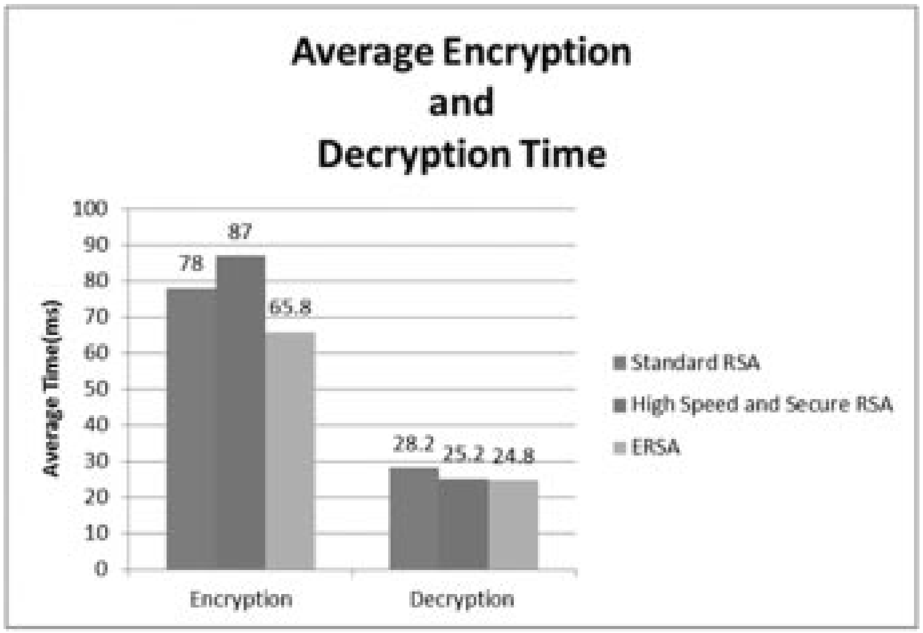

Figure 3: Comparison of Average Encryption and Decryption time of various algorithms

Concisely, it is exposed that the average encryption time of ERSA is so much reduced than High Speed and Secure RSA and to a certain extent than Standard RSA. With respect to decryption time, it shows the better results than Standard RSA.

Figure 3 depicts that the average encryption time of ERSA. It is lesser than Standard RSA and High Speed and Secure RSA. The average decryption time of ERSA is lesser than High Speed and Secure RSA.

5. CONCLUSIONS AND FUTURE WORK

This study shows that using prime numbers in public key cryptography algorithms enhances the security. Adding to its security, making the process of conversion of plain text to cipher text and vice versa is more complex because of the inclusion of two more prime numbers. The proposed algorithm ERSA has been implemented in such a way that it not only creates a complex calculation, but also increases the speed of encryption and decryption time to a certain extent with the help of two different 'N' values. It is observed that there is a small variation in decryption time when the file size is increased. In future, the Chinese Remainder Theorem can be applied in decryption process.

REFERENCES

[1] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu, "Data Security and Privacy in Cloud Computing", *International Journal of Distributed Sensor Networks*, doi.10.1155/2014/190903, 2014.

[2] Atul Kahate, Cryptography and Network Security, Tata McGraw Hill Education Private Ltd., New Delhi, 2010.

[3] Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm," *International Journal of Research in Computer & Communication Technology*, **1**, 2278-5841, 2012.

[4] Pallav Sharma, Varsha Sharma, Sanjeev Sharma and Jitendra Agrawal, "Data Protection in Clouds using Two Stage Encryption", *International Journal of Grid Distribution Computing*, **8**, 269-276, 2015.

[5] Navdeep Singh and Pankaj Deep Kaur, "A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks", *International Journal of Database Theory and Application*, **8**, 145-154, 2015.

[6] Suganya .N, N.Boopal M.E , Naveena .M, "Implementing Multiprime RSA Algorithm to Enhance the Data Security in Cloud Computing", *International Journal of Innovative Research in Science, Engineering and Technology*, **4**, 18954-18957, 2015.

[7] Seema Verma, Dr Deepak Garg, "Improvement in RSA Cryptosystem", *Journal Of Advances In Information Technology*, **2**, 146-151, 2011.

[8] Balkees Mohamed Shereek, ZaitonMuda, SharifahYasin, “ Improve Cloud Computing Security Using RSA Encryption WithFermat’s Little Theorem”, *IOSR Journal of Engineering (IOSRJEN)*, **4**, 01-08, 2014.

[9] V. P. Narkhede, P. S. Ajabe, S.M. Dandage, P. B. Zope, “A Review of Public Key Cryptography for Secure Communication Using RSA”, *International Journal of Advent Research in Computer and Electronics (IJARCE),* 01-04,2015.

[10] Nandita Sengupta,”Designing of Hybrid RSA Encryption Algorithm for Cloud Security”, *International Journal of Innovative Research in Computer and Communication Engineering,* **3**, 4146-4152, 2015.

[11] Pachipala Yellama, Challa Narasimham, Velagapudi sreenivas, “Data Security in Cloud using RSA”, IEEE, 1-6, 2013.

[12] Nasrin Khanezaei, Zurina Mohd Hanapi, “A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services”, IEEE, 58-62, 2014.

[13] Sarthak R Patel, Khushbu Shah, “Security Enhancement and Speed Monitoring of RSA Algorithm”, “*International Journal of Engineering Development and Research”*, **2,** 2057-2063, 2014.