MULTI KEY RSA ALGORITHM WITH VARYING KEY SIZES FOR DATA SECURITY IN CLOUD COMPUTING

[1] Miss Arpita Shukla, [2] Dr. Pratima Gautam
[1]Research Scholar, [2]Dean of Computer Science and Information Technology
[1]Computer Science and Information Technology, [2]Computer Science and Information Technology
[1]Rabindranath Tagore University, Bhopal, India

Abstract

Cloud computing has come to be on the top of any list of topics in the fields of computer because of its cost effectiveness. Storage and maintenance of large amount of data used to be a nightmare of the end users, but the advent of cloud computing gave them breathers because of its third party computing capabilities, thereby cutting the cost of infrastructure and man power. Moreover cloud computing has greater flexibility and reliability. Since it has effected a paradigm shift in the whole field of computing, it has become an unavoidable concept with any government in the field of e-governance and rural development in the developing world, shifting the entire concept of computing from the user-owned network infrastructure to the third party computing capability, sourcing data from a server situated not in the user's location but somewhere else. At the same time a word of caution becomes inevitable on the security aspect of the stored data which is kept in the open environment. This paper explores the possibility of securing the users' data more effectively using MRSA algorithm.

Keywords Cloud Computing, data security, ERSA algorithm, MRSA algorithm, Encryption, Decryption.

I Introduction

In the modern world of computing and e-governance both in the private and public sectors including various governmental departments and organizations, cloud computing has become a keyword. Cloud computing means storing once data in a rented server thereby saving on the infrastructure cost and the cost of man power. Although the future of computer lies in cloud computing, a major concern is the security of user data since it is kept in an open environment. Security of the data is of paramount importance because of ever growing use of data and the tremendous competition brewing among the software and hardware manufacturers and users. Therefore, there is a major concern of data security and privacy which is impeding the expected growth of the field of cloud computing. Since many users upload their data to the same cloud server there is danger of pilferage of data. So computer based security measures should emphasis on user authorization and authentication.

When the client uploads his data to the cloud server, it should be with proper security measures to ensure that the access to his data will be restricted to the authorized access. In other words a cloud space client should be cent-percent assured as to the security of his data and the related privacy policies and legalities.

II Problem Statement

The future of computing lies in cloud computing. But as the demand for cloud computing Client of cloud computing increases, so is the security threat for client-data. Therefore along with the space for cloud

computing ensuring data security is very significant. So more complex methods are to be advised for ensuring data security which can take the clients into confidence.

III Research Methodology

Our methodology working on 5 key for encryption and decryption also this algorithm decreasing time and increasing security and computation time is low

For security point of view, we use MRSA cryptography algorithm in this research to convert plain text to cipher text then that code is converted to cipher text and follow this procedure security level becomes very high.

IV Related work

Srinivasan Nagaraj et al. proposed that the randomness of the key generated increased the security of the data from unauthorized users and also the encryption process consumed significant amount of resources. They suggested that this can be enhanced by encrypting multimedia data which needs secured transmissions over unsecure channels.[1]

Prakash G L et al. Discussed an encryption methodology which uses 256 bit symmetric key with rotation. Data users can reconstruct the requested data from cloud server using shared secret key. This algorithm protects the outsourced sensitive data in cloud environment.[2]

Gayathri Devi P. discussed that the RSA algorithm is the base for many algorithms. So many algorithms can be combined with RSA algorithm to improve the productivity of RSA in the consideration of time, cost etc.[3]

A different stronger procedure is used to enhance the security of RSA scheme. This procedure selects alternative public keys when there is a possibility of getting an equality of the original message with the cipher text. In order to select an alternative public key, the proposed system searches for the nearest secure public key within a set of all valid keys.

Dr. D.I. George Amalarethinam and H.M. Leena proposed use of two additional prime numbers in standard RSA algorithm which increases the security of the data. Also the encryption process consumes significant amount of resources[5]. They used pseudo code for calculating private key and public key[1]. Such as off-line generators, on-line proxy generators and so on.

Gayathri Devi P. [3] discussed that the RSA algorithm be the base for many algorithms. So many algorithms can be fetched from RSA algorithm to improve the productivity of RSA algorithm.

A different and stronger procedure [4] is used to enhance the security of RSA scheme. This procedure selects alternative public keys when there is a possibility of getting an equality of the original message with the cipher text. In order to select an alternative public key, the proposed system searches for the nearest secure public key within a set of all valid keys.

The time spent for encryption and decryption processes is mostly lesser than with random numbers [6]. This work still enhances the speed of encryption and decryption processes by dividing the files into blocks that are to be encrypted.

V Proposed work

Multi key RSA algorithm is a asymmetric key algorithm which have four different keys for encryption and decryption processes. The key size can vary to make the encryption and decryption process strong. Hence it is difficult for the attackers to intrude in to the data. The increasing key size correspondingly increases the time taken for encryption a little bit, but not for decryption process. The proposed algorithm increases the security of data or message by dividing the file into blocks thereby enhancing the strength of the algorithm by increasing the key size.

MRSA algorithm uses the same key size for encryption and decryption process. Varying key size makes the encryption processes stronger. This makes it difficult for the attackers to thieve and / or abuse the data. The increasing key size correspondingly increases the processing time for encryption but not at all in the case of decryption. But the slight increase in the processing time for encryption is amply compensated by reducing the risk of data-hacking.

The proposed multi key algorithm (MRSA) uses three additional prime numbers in standard RSA algorithm. This is an improved version of ERSA algorithm which uses random numbers for key generation process.

MRSA Algorithm

Stage 1: Key generation involves the following steps.

Step 1: Select any two prime numbers P and Q Apart from these; choose three more prime numbers PR1, PR2 and PR3.

Step 2: Calculate the values of N by N = (P*Q*PR1*PR2*PR3)

Step 3: Compute Ø(r) = (P-1)*(Q-1)*(PR1-1)*(PR2-1)*(PR3-1)

Step 4: Choose the public key E, such that GCD (E, Ø(r)) = 1

Step 5: The private key D is computed from D*E = 1* mod (Ø(r)).

Thus, the public key component has a pair of E and N and private key pair as D and N.

Stage 2: Encryption process

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

Stage 3: Decryption process

The plain text can be found by using $M=C^D$ mod (N)

This is done with a view to increasing the complexity of the encryption.

The Pseudo Code of MRSA Algorithm is given below. It is combination of three stages.

Stage 1: This stage is used for generating two keys, namely, Public Key E and Private Key D. Generally RSA algorithm uses two prime numbers. In addition, three more
Prime numbers, namely, PR1 and PR2, PR3 are included in the proposed algorithm MRSA. The next step of the algorithm computes N value. Five prime numbers are multiplied and computed as N. This is done to increasing the complexity of the encryption part. The third step of the stage 1 calculates Euler Totient value of r. The public key E is chosen in such a way that the GCD of E and the Euler Totient value of r are equal to 1. The final step of stage 1 computes the private key D.
Stage 2: This stage does the process of converting plain text to cipher text. This process uses the Public key E and N values, where N is a product of five prime numbers. Thus the cipher text C is generated after the completion of Stage 2.
Stage 3: In stage 3, the original plain text is retrieved by using the values of cipher text, decryption key D and N. The calculated N value is used for encryption process as public key pair (E, N). For the decryption process the private key pair composed of D and N is used. The usage of prime numbers instead of random numbers showed the strength of encryption process. Because it is difficult to identify a prime number rather than a random number it gives a way to improve the strength of the key. The proposed work still enhances the security of encryption and decryption processes by dividing the files into blocks which are to be

encrypted**.** George Amalarethinam D I et al. [5] suggest an equation for the block size. The same equation is considered for calculating the block size in the proposed MRSA algorithm. The equation is given below:
Block Size = (2 * Key Size) -1 …… (1)
The values calculated using the equation (1) is used to divide the block with different key sizes. Since the block size depends on the key size, blocks with different sizes are generated for the same file size.

Example

Step 1 select primes : P = 3 and Q = 5,PR1 = 7,PR2 = 11,PR3 = 13;

Step 2 compute N = P*Q = 3*5*7*11*13 = 15015;

Step 3 compute $\phi(N)$ = (P-1)(Q-1)(PR1-1)(PR2-1)(PR3-1) = 2*4*6*10*12=5760;

Step 4 select GCD(E,5760) = 1, we choose E = 17;

Step 5 compute D, DE = 1 mod 5760 and D<5760, so D = 2033;

Step 6 **Encryption** Cipher = $(\text{message})^E$ mod N, cipher = $(3)^{17}$ mod 15015 = 11163

Decryption Message = $(\text{cipher})^D$ mod N, message = $(11163)^{2033}$ mod 15015 = 3

In MRSA algorithm we take 5 prime keys 3,5,7,11,13 then with the help of prime keys compute N=15015 and ϕ = 5760, after calculation we got public key E=17 and private key D=17. After calculating keys we send message and convert it to cipher text using ASCII value this is called encryption again send cipher text and again we got plain text or message this is called decryption.

VI RESULTS AND DISCUSSIONS

Result - The algorithms are executed in the python Frame work 3.7.0. Our main focus is on security and speed which are very important features for any algorithm. In our algorithm we used five keys for encryption. Our encryption time is slightly greater than ERSA algorithm but its main focus is on the security aspect. On the other hand for decryption we used 5 keys which are more than what is used in the ERSA algorithm (two keys). But our decryption time is much less than ERSA.

Table I shows
The Encryption and Decryption time for ERSA and MRSA algorithm for execution time in milliseconds. The proposed work shows an improvement in secure encryption and decryption.

COMPARISON OF ENCRYPTION AND DECRYPTION TIME OF TWO ALGORITHMS WITH DIFFERENT KEY SIZES

TABLE I

KEY SIZE (bits)	BLOCK SIZE(bits)	Encryption Time (ms)		Decryption Time (ms)	
		ERSA	MRSA	ERSA	MRSA
128	255	1489	9703.217	1823	15.59
256	511	1283	9001.215	3454	15.59
512	1023	1730	8892.015	4773	15.60

1024	2047	7581	8892.015	7519	15.60

Proposed algorithm MRSA performs better than ERSA algorithm from the point of view of the security of data. In this algorithm we have given more weight age to security of data. So we have used 5 keys. Our encryption time is slightly more than ERSA algorithm but the decryption time comes down significantly. On the other hand for decryption we used 5 keys which is more than ERSA algorithm (two keys).

Below figure represent the time in encryption and decryption according to MRSA and ERSA.

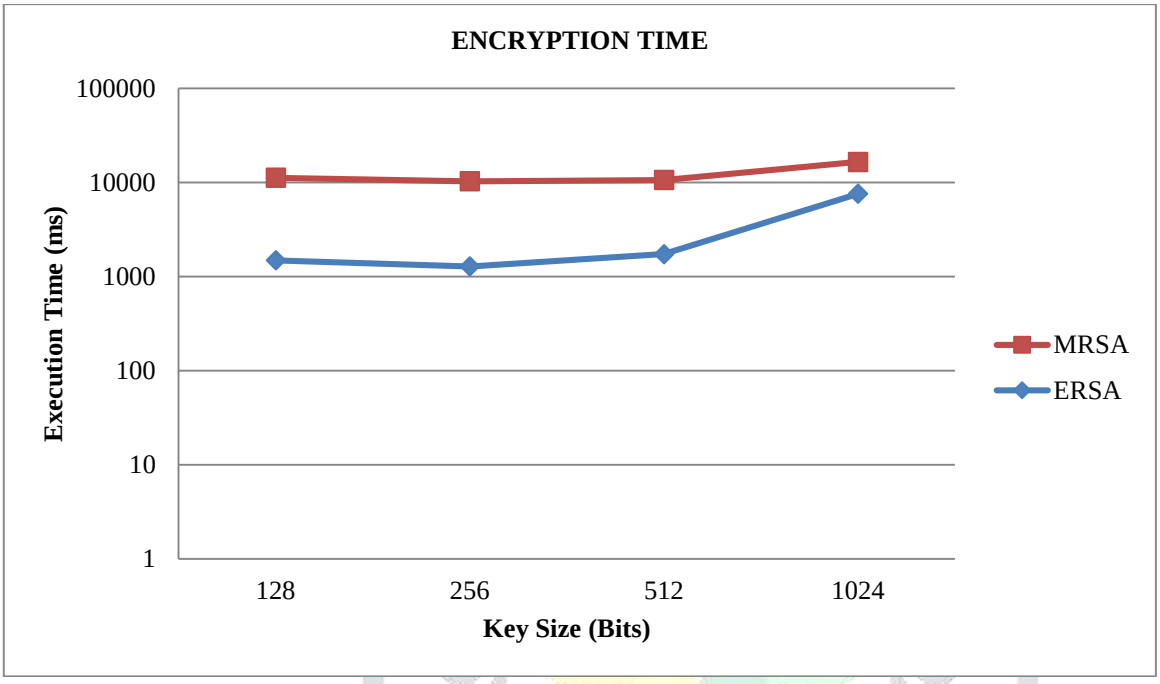

Fig. 1 Comparison of Encryption Time with same Key Size

This figure clearly reveals that MRSA algorithm performs better than ERSA in the matter of security since use of more keys makes it complex for the attackers.

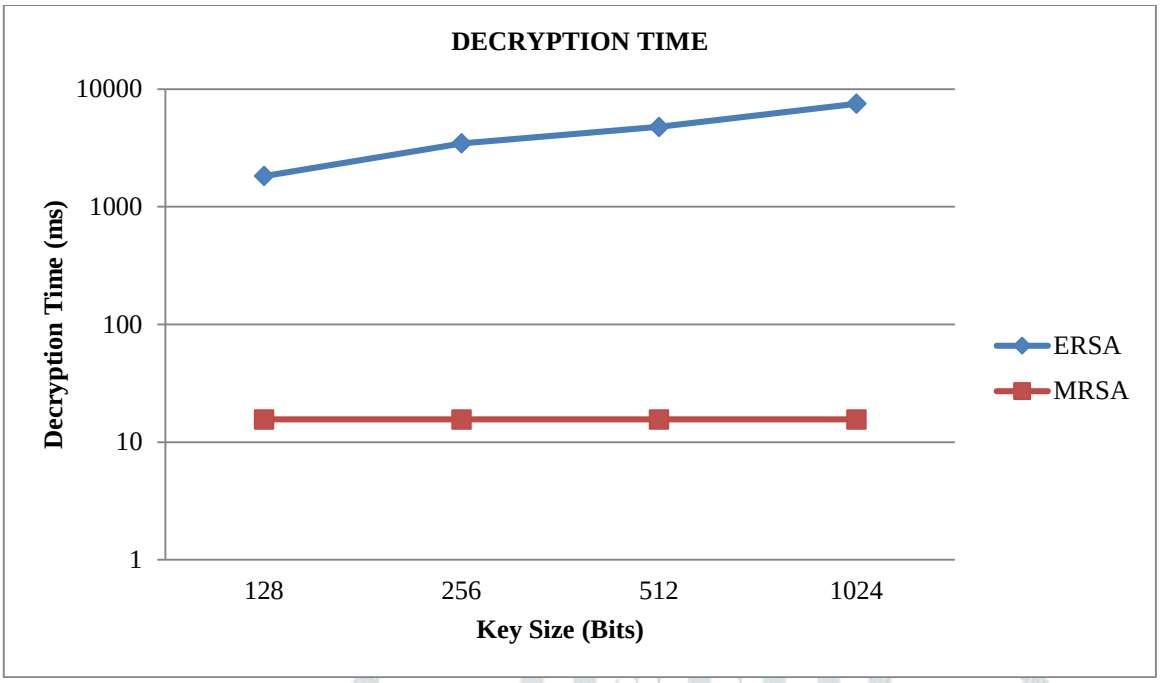

Fig 2 Comparison of Decryption Time with different Key Sizes

This figure clearly reveals that MRSA algorithm performs better than ERSA in the matter of security and time since use of more keys makes it more complicated for the attackers.

Table II Exposes
The average time (in ms) for encryption and decryption processes of MRSA and ERSA.

TABLE II

Algorithm	Average Encryption Time (ms)	Average Decryption Time (ms)
ERSA	3020.75	4392.25
MRSA	9122.115	15.595

It is revealed that the average encryption time of MRSA is so much more condensed than ERSA. Regarding decryption time, the ERSA shows better results than the other.
Figure given below depict the variation in the average time of Encryption and Decryption processes of two different algorithms namely, ERSA and the proposed algorithm MRSA. It is denoted that the average speed of Encryption and Decryption processes of MRSA algorithm is higher than the ERSA algorithm.

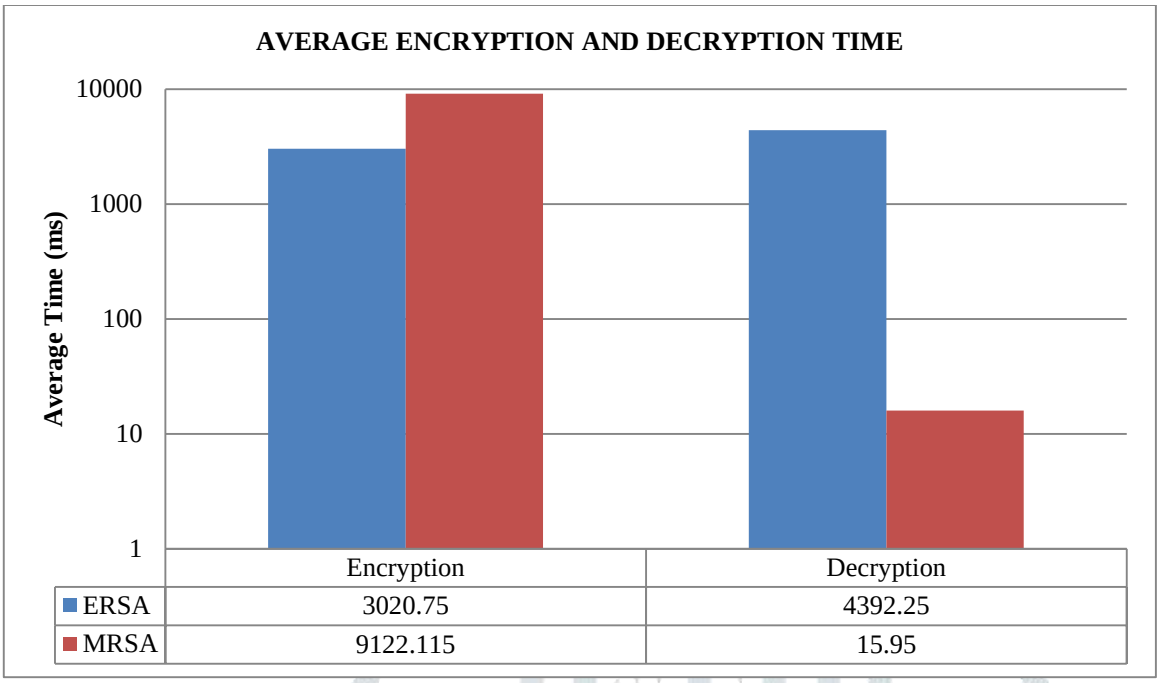

Fig. 3 Comparison of Average Time of Encryption and Decryption processes with different key sizes

VI CONCLUSION AND FUTURE WORK

We use multiple prime numbers as a concept of private key which increases security for encryption and decryption. MRSA algorithm is based on unique key concept. In MRSA we use multiplication of prime numbers. We will further enhance data security in the future experiment. We may use different key size, block size in future because data security and speed are very important in cloud computing. It is an ongoing process.

The usage of prime numbers instead of random numbers in the proposed system improves the speed of encryption and decryption. This speed is still enhanced in the proposed algorithm MRSA by dividing the file into several blocks. Apart from increasing the speed, the implementation of MRSA algorithm also makes the computation a complex one thereby increasing data security. In future, the time spent for encryption and decryption can still be improved by using the concept of Addition chaining. The security level of the algorithm can also be tested using statistical methods to find the strength of security.

VII REFERENCES

[1] Srinivasan Nagaraj, Dr.G.S.V.P.Raju, V.Srinadth, "Data Encryption and Authentication Using Public Key Approach", Elsevier Procedia Computer Science 48, pp. 126 – 132, 2015.

[2] Prakash G L , Dr. Manish Prateek, Dr. Inder Singh, "Data Encryption and Decryption Algorithm used Key Rotations for Data Security in Cloud System", International Journal Of Engineering And Computer Science, Vol. 3, No. 4, pp. 5216-5223, 2014.

[3] Gayathri Devi P, "Overview of RSA and its enhancements", International Journal of Innovative Research and Development, Vol. 2, No.11, pp. 306-310, 2013.

[4] Motasem A. Abu-Dawas, Abdulameer K. Hussain, "Enhancement of RSA Scheme using Agreement Secure Information for Nearest Parameters", International Journal of Computer and Information Technology, Vol. 4, No. 2, 2015.

[5] George Amalarethinam D I, Leena H M, "Enhanced RSA Algorithm for Data Security in Cloud", International Journal of Control Theory and Applications, ISSN 097-45-572(Accepted).

[6] Sarthak R Patel, Khushbu Shah, "Security Enhancement and Speed Monitoring of RSA Algorithm", "International Journal of Engineering Development and Research", vol. 2, 2057-2063, 2014.