ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 1, pp: (38-43), Month: January - March 2020, Available at: www.researchpublish.com

DEPLOYMENT OF HYBRID SYMMETRIC ENCRYPTION ALGORITHM IN CLOUD DATA SECURITY AND PRIVACY

[1]Dawson john kwao, [2]Dr. Thomas Yeboah, [3]Michael Osei Boakye

[1]Kwadaso College of Agriculture, Kumasi, Ghana
[2]Christ Apostolic University,
[3]NJUST

Kwaodawson1@yahoo.com, thomyebs24@gmail.com, Michael.ob@njust.edu.cn

Abstract: **In this paper, a hybrid algorithm has been proposed, which is based on RSA algorithm and Delta encoding technique with the aim of improving security issues and also bring about a total reduction in execution time in message encryption and decryption in cloud computing environment. Security was enhanced by increasing the level of encryption and decryption of messages stored in the cloud at two levels thus making it heterogeneous. The reduction in the total execution time was observed after comparing Key generation time, Encryption time and the Decryption time of the traditional RSA algorithm and the proposed hybrid algorithm based on different exponent sizes of 256, 512, 1024 and 2048. Also, common attacks of the traditional RSA algorithm have been considered to find out the resistance of the proposed hybrid algorithm against these possible attacks.**

Keywords: **RSA, Delta Encoding, Heterogeneous.**

I. INTRODUCTION

Cloud computing as used in information technology environment refers to the delivering of services which has been hosted over internet. This system enables clients from their offices to access services such as Software-as-a-Service (SaaS), Infrastructure-as-a-service (IaaS) and Platform-as-a-service (PaaS) (Rouse, 2016). With the introduction of cloud computing, issues of security and data privacy has become more important due to the sharing vulnerabilities associated with the documents involved by attackers both from the inside and outside of organizations.

In cloud computing environment, security should be provided for both known and unexpected intrusion that can corrupt and delete essential data by employing appropriate cryptographic technologies. RSA encryption technology is one of many popularly used public-key cryptosystem schemes which utilizes integer factorization problem in the encryption and decryption process. RSA is an asymmetric cryptosystem, which implies that the scheme is made up of double arithmetical transformations: an encryption function E, and a decryption function D (Rivest et al, 1983).

The study has expanded the level of encryption to two, thus making the encryption process heterogeneous.

II. RELATED LITERATURE

As per Dharini (2014), cloud computing is a rising innovation which utilizes shared data, assets, programming and facilities to client on a pay as you utilize base. For secure communication over public network to have the capacity to secure information a strategy for encryption is required. As a result the proposed encryption strategy for securing information transmission is by joining RSA and Magic Square to give an extra security to the cryptosystem.

According to Sudhansu (2014), the most appropriate approach to encrypting the cloud, is through the combination of RSA algorithm and MD5 hashing. In this mechanism RSA algorithm is used to secure communication (Kaliski, 2003), data scramble and unscrambling purposes while MD5 algorithm is aimed at providing digital signature as well as for protecting data that are in tabular forms against illegitimate clients (Rivest , 1992).

As indicated by Arora, (2013), the combination of RC4, SHA and RSA algorithm were proposed to be utilized to secure information in the cloud.

According to Amro, (2014), in cloud computing, all that you can do is currently based on the web as opposed to being desktop based. The proposed algorithm integrates AES and RSA algorithms for securing data and connections in view of various keys in encryption and decoding and again utilized SHA1 algorithm to secure the hash table of data.

III. METHODOLOGY

The proposed hybrid algorithm works using five phases;

PHASE 1: Obtain the integer values.

PHASE 2: Apply Newton Forward Differential on the message to obtain the encoded form by using the formula (Ripa N, 2010): $C_t = P_t$

$P_t^{+1} = C_t^{+1} - C_t^0$

PHASE 3: Encode the message with the public key by employing the RSA encryption algorithm.

PHASE 4: Decrypt the message by employing the private key of RSA algorithm

PHASE 5: Apply again Newton Backward Differential on the initial Newton Encoded message output to decrypt the message by using the formula (Adhikary, 2013): $C_t = P_t$

$P_t^{+1} = C_t^{+1} + C_t^0$

STEPS OF THE PROPOSED ALGORITHM :

The proposed hybrid algorithm for cloud data security and privacy involves six steps. This combines the RSA algorithm and Delta Encoding Techniques. These steps are Decimal Message, Encoded form (Newton Forward), Key generation, Encryption, Decryption and Newton backward.

Steps I, II and VI are the Delta Encoding Technique while Steps III, IV and V are the RSA algorithm. The combination of all the steps gives the hybrid symmetric encryption algorithm.

Step I: Decimal message

Obtain the decimal of the message entered.

Step II: Encoding (Newton Forward)

Encode message (Integer values) using Newton Forward differential.

Step III: Generation of Key

- Two distinctive prime numbers are chosen as g and j.
- Compute $k = g * j$
- Compute $\varphi(k) = (g-1) * (j-1)$
- Choose h so $1 < h < \varphi(k)$ and also e as well as k are co-prime numbers.
- Compute the significance of **d** when $(t * h) \% \varphi(k) = 1$
- Therefore the following are valid
- Public key then is (h , k)
- Private key then is (t , k)

Step IV: Encryption Stage

$C(f) = F^h \pmod k$

Step V: Decryption

$F(c) = c^t \pmod k$

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 1, pp: (38-43), Month: January - March 2020, Available at: www.researchpublish.com

Step VI: Encoding (Newton Backward)

Apply Newton Backward differential.

EXPERIMENTAL OBSERVATION OF THE PROPOSED HYBRID ALGORITHM:

PHASE: I

The message to be encoded and decrypted is 'Hello'

Table 1: Integer values of alphabets

Message	H	e	l	l	O
Integer Value	72	101	108	108	111

PHASE II: Apply Newton Forward Differential

Using the formula

$C_t = P_t$,

$P_t^{+1} = C_t^{+1} - C_t^0$

Table 2: Results of Newton Forward Differential

Integer Value	72	101	108	108	111
NFD	72	29	7	0	3

PHASE III:

Apply RSA on the encoded message

STEP A: Key generation

- Choose two distinct prime numbers. That is g = 3 and j = 11
- Compute k = g*j. k = 3 *11 = 33
- Calculate Euler's totient function, Ø(k) = (g-1)(j-1), Ø(k) = (3-1)(11-1)

  = 2*10 = 20
- Choose any integer h, such that 1<h<20, that is gcd (7) = 7.

  7 therefore is chosen.
- Calculate d such that (t*h) % Ø(k) =1.Using Extended Euclidean algorithm. That is t = 3
- The public key is (h,k) = (7, 33).

  The private key is (t,k) = (3,33).

STEP B: SCRAMBLING

- The public key (7, 33)
- $C = m^h \bmod k = C = 30172809$

STEP C: UNSCRAMBLING

- $m = C^t \pmod k$

  =30172809 = 629703

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 1, pp: (38-43), Month: January - March 2020, Available at: www.researchpublish.com

STEP D: Newton backward differential

Apply the Newton Backward Differential on the encoded message using the formula

$P_t^{+1} = C_t^{+1} + C_t^0$

Table 3: Results of Newton Backward Differential

Decrypted message	6	29	7	0	3
Newton backward	72	101	108	108	111

IV. RESULTS AND DISCUSSION

Comparison of key generation time and total execution is as shown in figure 1.

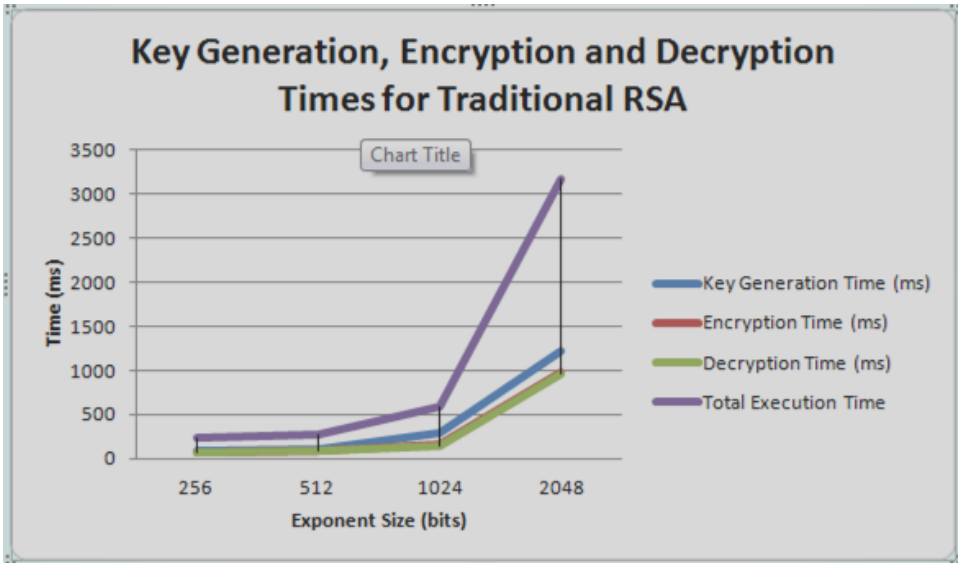

Figure 1: Key Generation, Encryption and Decryption Times for original RSA (milliseconds).

From figure 1 the encryption time, key generation time and the decryption time for the proposed hybrid algorithm was always lesser than the traditional RSA algorithm when the exponent sizes 256, 512 and 1024 bits were used.

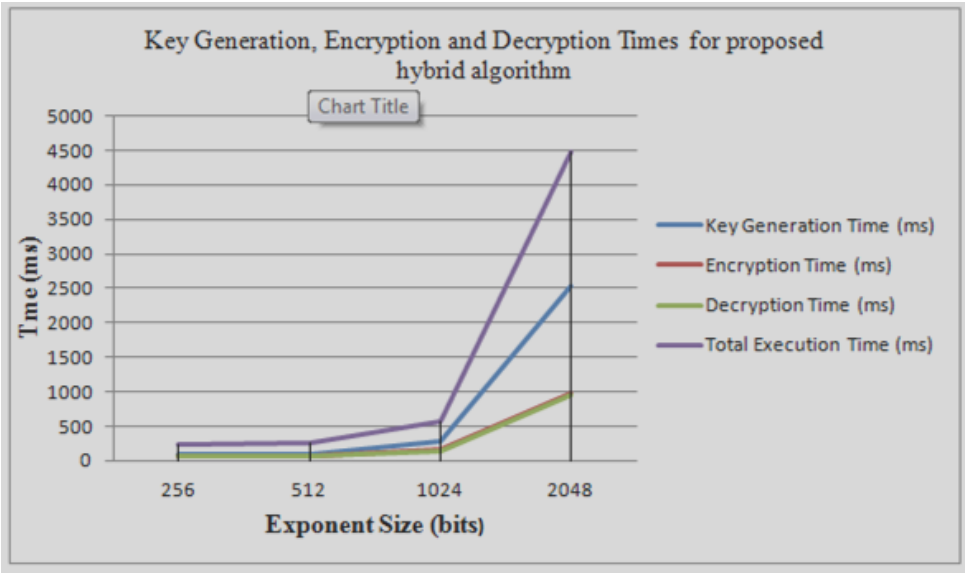

Figure 1: Key Generation, Encryption and Decryption Times for proposed hybrid algorithm (ms)

The key generation time of the proposed hybrid algorithm and the traditional RSA algorithm show that there was an increment in the key generation time because higher exponent was used which resulted in an increase in the total execution time for the proposed algorithm against the traditional RSA algorithm. On the other hand the encryption and decryption time for the proposed hybrid algorithm was lesser than the traditional RSA algorithm because of the employment of the Delta encoding technique.

V. THE SECURITY ANALYSIS

The security analysis of the proposed hybrid algorithm and the original RSA is investigated with regards to three attack approaches. These are, Brute Force, Mathematical Attacks and Timing Attacks.

- Mathematical Attacks

Mathematical attack is based on attacking from the underlying structures of the RSA function. The first approach is to factor the modulus T. Since been able to identify the factorization of T, it is easy to obtain K(T) from which L can be determined by using the equation D = 1/L mod K(T). In original RSA because it is homogenous in nature it is easily to factor the modulus T whiles in this proposed algorithm it is heterogeneous in nature and therefore make it difficult to factor the modulus.

- Brute Force attacks

In brute force attacks you need to explore all the possible combinations to guess the private key. In the proposed algorithm the attacker has to guess the encoded private key and the original private key which makes it difficult to guess as compare to the original RSA which requires the attacker to only guess the original private key.

- Timing Attacks

In any cryptographic security plan, there is dependably timing attack which is a side channel attack where the intruder endeavors to bargain the cryptosystem by investigating the time taken to finish the cryptographic calculation. Timing attack on unique RSA algorithm can be counteracted by the acquaintance of an irregular postponement with the exponentiation algorithm or by the augmentation of the figure content with any arbitrary number while the heterogeneous encryption algorithm, for example, the proposed hybrid algorithm will shield the exchanged message from the planning attack and not as a matter of course to multiply the cipher text.

VI. CONCLUSION

With the passage of time cloud computing has been on high demand due to its cost and high reliability along with high security and scalability. Cloud computing helps pooled materials such as software, resources and other information to be made available to computers and other devices as a utility. However it is observed that there are still limitations regarding security and privacy issues when it comes to cloud computing.

In this work the encryption algorithm employed is an adjustment and an addition on the RSA algorithm. In RSA algorithm the data to be protected do not go through any form of transformation or encoding before it is protected which makes the encryption process homogeneous. In this research, an extended level of encryption is employed which converts the homogeneous nature of the RSA and make it heterogeneous.

REFERENCES

[1] Adhikary K, 2013. On Equality of Newton's Forward, Newton's Backward and Lagrange's Interpolation Formula. *International Journal of Applied Mathematics and Statistical Sciences (IJAMSS),* 2(4), pp. 63-68.

[2] Amro A,Abutaha M, 2014. Using AES, RSA, SHA1 for Securing Cloud. *International Conference on Communication, Internet and Information Technology,*, Volume ICCIIT.

[3] Arora D,Smriti s, 2013. Ensuring Data Security for Secure Cloud Hybrid Framework. *international Journal of Engineering Research and Applications*, 3(4), pp. 2217-2212.

[4] Dharini A, Saranya Devi R M,Chandrasekar I, 2014. Data Security for Cloud Computing Using RSA with Mag. *International Journal of Innovation and Scientific*, 11(235-8014), pp. 439-444.

[5] Kaliski B, 2003. *The Mathematics of the RSA Public Key Cryptosystem*, RSA Laboratories: s.n.

[6] Ripa N, 2010. Analysis of Newton's Forward Interpolation Formula. *International Journal of Computer Science and Emerging Technolodies* , 1(4), pp. 2044-6004.

[7] Rivest R, 1992. *MD5 Message- Digest Algorithm,* MIT Laboratory for Computer Science: s.n.

[8] Rivest R,Shamir A,Adleman L, 1983. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM,* 26(CACM), pp. 96-99.

[9] Rouse M, 2016. *Searchcloudcomputing.* [Online] Available at: http://searchcloudcomputing.techtarget.com/definition/cloud-computing [Accessed 23 June 2016].

[10] Sudhansu R, Biswaranjan N., 2014. Enhancing Data Security in Cloud Computing using RSA Encryption and MD5 Algorithm. *International Journal of Computer Science Trends and Technology (IJCST),* 2(3) pp.60-64.

AUTHORS PROFILE:

Mr, John Kwao Daswson received the Bachelor's Degree in Information Technology from University of Education, Kumasi campus in 2010. He acquired his Master of Philosophy in Information Technology from Kwame Nkrumah University of Science and Technology in 2017. He is a tutor in the Agricultural Economics and Extension Department of the Kwadaso College of Agriculture. His research interest includes Network securities, Cloud computing and Algorithms design.