GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

AN HYBRID APPROACH FOR EFFICIENT DATA ENCRYPTION AND DECRYPTION FOR DATA SECURITY IN CLOUD COMPUTING

Kulwinder Kaur
Research Scholar, Punjabi University Patiala, India

ABSTRACT

In this paper, a hybrid encryption is proposed using combination of two asymmetric schemes. The existing schemes are lacking in encrypting large data files, there time complexity may worsen with size. In this work the homomorphic algorithm is used along with RSA, to enhance the encryption and decryption time. The evaluation study has been done between AES, 3DES, DES and proposed algorithm on basis of their time complexities. Our proposed work has very least complexity for both encryption and decryption. Proposed scheme is also highly secure as it involves 2 encryption and decryption rounds.

I. INTRODUCTION

Cloud computing is a model that provides on-demand computing resources through network technologies. This model is a combination of remote servers and software networks that allow users to store, process and access data. Cloud user can use any of services as per their requirement. Cloud service provider will charge according to use. Different services provided by cloud are servers, storage, software platforms, and applications. Cloud computing has five essential characteristics i.e. on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

In the era of growing technologies, all IT industries outsource their confidential data to cloud in order to save their cost spent on infrastructure. So to keep outsourced data confidential, data should be encrypted using different cryptographic algorithmsso that data that resides on cloud could not accessed by unauthorized user or cloud service provider.

Cryptographic Algorithms involves two types of algorithm:

i. Symmetric algorithm also called secret key cryptography as it use the same *key* for both *encryption* anc decryption. For e.g. DES, AES, BLOWFISH, IDEA.
ii. *Asymmetric* algorithms also called public *key* cryptography as it use two *keys – private key for encryptior and public key* for decryption. For e.g. RSA, Diffie-Hellman.

Based on combination of above cryptographic algorithms different type of encryption algorithms exists tc implement security in cloud storage. Some of them are discusses as follows:

II. DATA ENCRYPTION STANDARD(DES)

DES is 64-bits symmetric-key Encryption algorithm that takes plaintextblock wise that means encryption is done block wise not bit by bit. Block are further divided into two half of 32 bits, on one half Feistel function is applied. After applying function it is XOR with other half. Further each of these blocksgoes through 16 rounds of permutation and substitution using secret key.In this way we get encrypted data. In order to decrypt data, whole encryption process done in reverse order. DES is not so effective encryption algorithm as the key length used is of 64 bit, out of which eight bit used for parity checks so 56 bit left. So using brute force attack maximum of 2^56 attempts required to find correct key.

1. Advanced Encryption Standard(AES)

AES is 128-bits symmetric-key Encryption algorithm that overcomes the disadvantage of DES algorithm of small key length. In AES number of rounds varies according to the length of secret. It takes 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.Each round consist of different processes i.e. byte substitution, row shifting, MixColumns resulting in 4 x 4 matrix that are XORed with 128 bits of the round key. This process continues till the last round .After last round we get encrypted data.In order to decrypt data, whole encryption process done in reverse order.

2. Blowfish

Just like DES, blowfish is also 64-bits symmetric-key Encryption algorithm with variable key length ranging between 32 bits to 448 bits. It works in two parts: one is key expansion part in which keys are pre computed and another one is data encryption part in which data encrypted using Feistel network of 16 rounds. Keys are computed using P-array of 18 32-bits sub keys and 32-bits S-boxes that accept 8-bit input and produce 32-bit output.The F-function used in Feistel network divides the input into four 8-bit quarters which serves as input to the S-boxes. The outputs that we get are XORed and at the end we get encrypted 32-bit output.

3. Diffie-Hellman Algorithm

Diffie-Hellman is asymmetric key exchange algorithm, also called exponential key exchange, is a method of digitalencryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming.

4. *Rivest–Shamir–Adleman(RSA)*

RSA is asymmetric encryption algorithm that means two keys are used one is private key used for encryption and another one is public key that is used for decryption. In this algorithmusing Rabin – miller algorithm two large prime number are generated. After taking modulus of both the large prime number private and public keys are generated.

III. LITERATURE REVIEW

Ratnadewi et al. had proposed various algorithms DES, 3DES and AES for encryption in near field communication [1]. The process of encryption in used in NFC to protect information against various vulnerable attacks. The user as soon enter in NFC the information is send to server in an encrypted form, which later send by server to the end destination. The destination is challenged for the decryption as if user is already in database, they can decrypt. All these algorithms are applicable on ACOS3. The encryption and decryption time is some time very time consuming task. This is one of the major bottleneck of the system.

Akashdeep Bhardwaj et al. had done the comparison study of various security algorithms [2]. In this paper, three algorithms DES, 3DES and AES are compared on basis of their encryption and decryption time which is computed. The author use the symmetric ways of encryption which involve only single key. The performance is evaluated for the time taken to encrypt and decrypt the data. The performance of DES is quite better than AES algorithm also the performance of 3DES lies in between both. This is the reason, author stressed on using symmetric algorithms.

AdilJamilZaru et al. had performed a literature study of cryptography [3]. The cryptography is a field of data hiding to preserve the data from various modification attacks. The data integrity and authentication are most important factors for data transfer. The cryptography uses two type of techniques for data encryption. They are categorised as asymmetric and symmetric techniques. The symmetric algorithms involves only single key which is private key. Asymmetric algorithms need two keys for encryption and decryption i.e. public and private key. This scheme is more secure than using symmetric scheme.

Vignesh. M et al. had proposed an algorithm for images encryption and decryption [4]. This algorithm works well with heavy data. The AES scheme is used for encryption which is asymmetric method and involves public and private keys. The author proposed the method of divide and share, which works exactly like divide and conquer. In this scheme the data for encryption is divided into two parts. This avoid large complexity and time. Once the both parts are encrypted they are combined to form the original data block again.

M.Keerthika at al. had done survey study of public key cryptography i.e. symmetric way of encryption also on email [5] [6]. In this paper various algorithms are discussed some are based on asymmetric and other symmetric method. The block cipher is generated using various key combinations like 64 bit and 256 bit. The brute force attack is highly possible. In [7] author perform same study and validate.

In [8] author study various genetic algorithms to perform encryption and decryption. The proposed method by author is also based in genetic properties. The modification of RSA is done with defined properties to overcome gap of time. In [9] this scheme is implemented based on key exchange. In [10] homomorphic encryption is used which randomly shuffle the data operation and this is done by cloud and not stored on it. These operation are only stored at user end and passed to cloud when needed.

IV. PROPOSED WORK

The encryption and decryption are used in this work, based on a hybrid method. The goal is to reduce the complexity time of the encryption and decryption operation. There exist many algorithms like AES, DES and 3DES which are used, but there time complexity is increasing with file payload. In this work a hybrid approach which combine functionality of two algorithms. Our proposed scheme is using dual encryption for better security also it does not add on into time complexity. The first round of encryption is done using RSA algorithm and in second round of encryption EIGamal algorithm is used. The decryption process is reverse of encryption.

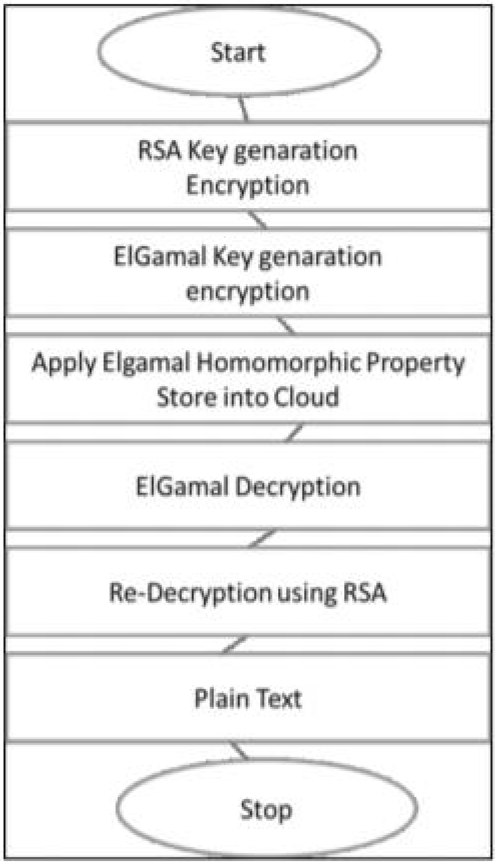


Figure 2 Proposed Scheme

Round 1: RSA is asymmetric encryption algorithm, which uses two keys public and private for encryption and decryption.

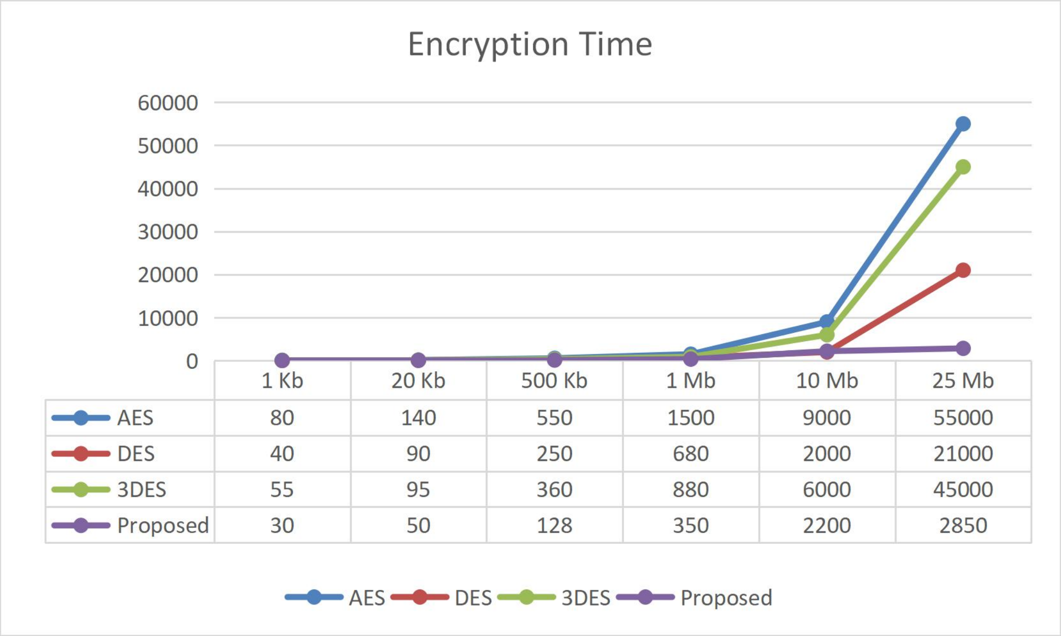
a) Initially the combination of two prime numbers is selected say ‘A’ and ‘B’.
b) Modulus of A and B is calculated using variable M, defined as M = A x B.
c) Compute Euler function using $\phi(M) = \phi(A) * \phi(B) = (A-1) * (B-1)$
d) Another integer is selected in a way that previously computed $\phi(M)$ and integer I are co-prime.
e) Compute Multiplicative inverse of Integer I using $D * I \equiv 1 \pmod{\phi(M)}$
f) Generate public key using mod ($\phi(M)$) and private key using mod ($\phi(D)$) and ($\phi(M)$).
g) After this perform RSA algorithm producing output ‘P’.

Re – Encryption Round:

a) Fetch public key from previous RSA encryption, consist of output, number, multiplicative denoting P, A, D.
b) Select an integer ‘n’.
c) Fetch previously encrypted text as plain text ‘T’.
d) Evaluate $x = A^n$mod P.
e) Evaluate $y = (D^k * M)$ mod P.
f) Produce Cipher C = (x,y).

V. RESULTS

The proposed scheme is evaluated on bases of encryption and decryption time. The values are represented in Figure 2 below is for four different algorithms. The AES, DES, 3DES and proposed are evaluated. The encryption time for proposed is least in contrast with other algorithms. The time complexity of other algorithms is enhancing with increase in data. Our proposed scheme is very efficient in encrypting large data files.



	1 Kb	20 Kb	500 Kb	1 Mb	10 Mb	25 Mb
AES	80	140	550	1500	9000	55000
DES	40	90	250	680	2000	21000
3DES	55	95	360	880	6000	45000
Proposed	30	50	128	350	2200	2850

VI. CONCLUSION

The encryption and decryption need to be done in lesser time to reduce the overall complexity. The proposed hybrid scheme is highly secure and efficient in contrast with existing schemes. The proposed scheme uses dual encryption i.e. two rounds of encryption are performed. The decryption again repeat the reverse process. This is asymmetric type of encryption as two keys are used for encryption and decryption process. The Elgmal with various homomorphic operations is combined with RSA. The overall performance is evaluated on basis of encryption and overall time. Our algorithm is quite efficient and secure

REFERENCES

1. *Ratnadewi, R. P. Adhie, Y. Hutama, A. Saleh Ahmar, and M. I. Setiawan, "Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC)," J. Phys. Conf. Ser., vol. 954, no. 1, 2018.*
2. *A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, and H. Sastry, "Security Algorithms for Cloud Computing," Procedia Comput. Sci., vol. 85, no. Cms, pp. 535–542, 2016.*
3. *G. Chandhiny and S. Vairamuthu, "Securing financial database using partial homomorphic encryption," Int. J. Pure Appl. Math., vol. 119, no. Special Issue 7A, pp. 21–29, 2018.*
4. *A. G. Sawant, "Advanced Encryption Standard Block Cipher Algorithm," vol. 7, no. 3, pp. 366–371, 2018.*
5. *R. Jhingran, "A Study on Cryptography using Genetic Algorithm," vol. 118, no. 20, pp. 10–14, 2015.*
6. *A. M. Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," no. June, 2017.*
7. *A. Shukla, A. Mohite, and A. S. Rawat, "Encrypted Email System," vol. 3, no. 1, pp. 46–52, 2018.*
8. *J. Athena and V. Sumathy, "Survey on Public Key Cryptography Scheme for Securing Data in Cloud Computing," Circuits Syst., vol. 08, no. 03, pp. 77–92, 2017.*
9. *M. Vignesh, P. A. Raihana, S. Hakkim, and S. Sukanya, "An Efficient K-N Secret Sharing Image and AES Encryption Algorithm in Visual Cryptography," pp. 233–239, 2018.*
10. *A. Zaru and M. Khan, "General Summary of Cryptography," vol. 08, no. 02, pp. 68–71, 2018.*