IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12108

Comparison between a Proposed Algorithm Based on Homomorphic Encryption and Elliptic curve with traditional Algorithms for security of data in cloud computing

MSC Rasha Falih Hassan

University of Information Technology and Communication (UOITC), Iraq

Abstract: A proposed algorithm based on Homomorphic Encryption built based on Homomorphic Encryption and Elliptic curve. In cloud computing, big amount of users 'data are allowed to de collected on cloud server storage for next use, and any computations on stored data will be implemented in the cloud. To keep the stored data that is on the cloud we necessities have to use an encryption system that can do computations on the encrypted data called homomorphic encryption. In this paper, Comparison between a Proposed algorithm Based on Homomorphic Encryption and Elliptic curve(PAHEEC) with traditional Algorithms for security of data in cloud computing ,", Elliptic curve cryptography used to generate algorithm's private key , A new algorithm reduces the time of processing, space of storage and make available high security because of its key generated depends on ECC. The use of 64-bit provides enough security to be used in a comparison.

Keyword: Security of cloud computing, Homomorphic Encryption, Elliptic curve.

1. INTRODUCTION

The strength of encryption algorithm rest on the strength of the keys used in the encryption and decryption, , if the key is short or weak this leading to produce weak encryption and vice versa, In this paper, key generation of a proposed algorithm depends on the elliptic curve, so the key strength depends on the ECDLP [1], An encryption contains three algorithms: Kegan, Encrypt and Decrypt [2], Elliptic curve cryptography along with its own specifications like homomorphism for encryption and decryption application will give us less computational complexity with same level of security similar to other algorithms. Elliptic curves if simulated with ElGamal, Paillier and RSA gives enhanced security with smaller key generation [3] .

2. RELATED WORK

In 2016, Ming-quan Hong, Wen-bo Zhao, Aimed at SMC difficult (computation and communication cost), proposed Elliptic Curve Cryptography (ECC) based homomorphic encryption scheme that is dramatically reduces & treats a problem. It displays that the system has advantages in energy ingesting, communication consumption and privacy protection through the comparison experiment between ECC based homomorphic encryption and RSA&Paillier encryption algorithm. Further evidence, the scheme of homomorphic encryption scheme based on ECC is applied to the calculation of GPS data of the earthquake and proves it is proved that the scheme is feasible, excellent encryption effect and high security [4].

In 2016, Mr. Manish M Potey, The cloud service provider stocks the plaintext format of data and user requests to use their own encryption algorithm to secure their data if required. The data requirements to be decrypted when it is to be treated .This paper stresses on loading data on the cloud in the encrypted format using fully homomorphic encryption. The data is kept in Dynamo DB of Amazon Web Service (AWS) public cloud. User's calculation is performed on encrypted data in public cloud storage. When deductions are required they can be copied on client machine. The many security issues associated with data security such as privacy, confidentiality, integrity and authentication desires to be mentioned[5].

In 2017, Xidan Song, Yulin Wang, Fully homomorphic encryption method has disadvantages of large key size and low calculation efficiency, and it is not practical for the secure cloud computing. In this paper, developed a hybrid cloud computing scheme based on the Paillier algorithm which is additively homomorphic, and RSA encryption algorithm

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12108

which is multiplicative homomorphic. Customer's calculation requests can be described as the combination of simple add and multiplicative operation and the operands. An Encryption Decryption Machine which running in the private cloud processes the encryption according to the type of the operation and upload the cipher texts to the public cloud. The public cloud process calculation without knowing the exact data. Then we run simulations and analyze the results, and the results show that the scheme is practical and efficient [6].

In 2019, Adi Akavia, Dan Feldman, Hayim Shaul, Secure report is hypothetically potential with Fully Homomorphic Encryption (FHE), In this paper, executed main reporting system in an open source library and can response such database queries when treating only FHE encrypted data and queries. The experimental results show that Implemented Secure report queries on billions records in minutes on an Amazon EC2 server, compared to less than a hundred-thousand in previous FHE based solutions [7].

In 2019, ---Ahmed El-yahyaoui , %Mohamed Dafir Ech-cherif El kettani, fully homomorphic encryption (FHE) is a intelligent type of encryption schemes that assists working encrypted form of data. It offers efficient techniques for outsourcing calculations over encrypted data to a distant. The resultant scheme is named Verifiable Fully Homomorphic Encryption (VFHE). Presently, it has been demonstrated by many existing schemes that the theory is feasible but the efficiency needs to be dramatically value-added in order to make it practical for real applications. One subtle difficulty is how to efficiently handle the noise. In this paper, present a well-organized and symmetric provable FHE based on a modern mathematic construction that is without noise, the noise is persistent and does not rest on homomorphic evaluation of ciphertexts. The homomorphy of our structure is gained from simple matrix operation processes (addition and multiplication). The running time of the multiplication process of our encryption scheme in a cloud environs has an order of a small number of milliseconds [8].

3. HOMOMORPHIC ENCRYPTION

In 1978 Ronald Rivest, Leonard Adleman and Michael Dertouzos submitted at the beginning the idea of Homomorphic encryption. Since then, a few evolutions have been prepared for 30 years. The encryption scheme of Shafi Goldwasser and Silvio Micali was suggested in 1982 was a provable security encryption method which reached a notable level of security, it was an additive Homomorphic encryption, however, it can encrypt just a single bit. In the same concept in 1999 Pascal Paillier was also suggested a provable security encryption system that was also an additive Homomorphic encryption. After few years later, in 2005, Dan Boneh, Eu-Jin Goh and Kobi Nissim designed a system of verifiable security encryption, by which we can do an unlimited number of additions with only one multiplication [9].

3.1 Idea of Homomorphic Encryption

Homomorphic Encryption systems permit to perform operations on encrypted data without knowing the private key (without decryption), When we decrypt the result of any operation, it is equivalent if the calculation carried out on the raw data [10], HE techniques are partial, somewhat and fully homomorphic encryption with the purpose of a secure store, transfer and dealing with ciphertext in a means that maintains the integrity and confidentiality of data [11].

3.2Functions of Homomorphic Encryption:

Homomorphic Encryption has four function of as in figure (1):

1. Function of KeyGen: It is an algorithm that takes parameter of security (SP) to generate secret key (sk) and public key (pk), (pk, sk) KeyGen (SP).

2. Function of Encryption (Enc): It is algorithm, it uses plaintext and (sk) to produce a ciphertext (c), c = Enc (sk, m).

3. Function of Evaluation (Eval): It is algorithm, the server uses function f designed for evaluating the ciphertext, and it's done with using function f and pk (Eval(f, pk, c)), where c= (c1, ... , ct) and t means the number of circuit inputs. Hence, Dec (sk, Eval (f, pk, c)) = C (m1, m2 …… mt), Where C is a computation executes in the plaintext.

4. Function of Decryption (Dec): It is algorithm produces a plaintext (m) that comes from ciphertext and sk m = Dec (c, sk), Hence, after evaluation, original text obtained as follows Dec(sk, Eval(f, pk, c)) as in Figure (3) [12]. Assume that (m1), (m2) ∈ M and (c1) and (c2) ∈ C then m1 = Dec (c1) and m2 = Dec (c2) and this lead to: Dec (c1*c2) = m1*m2, When multiplication operation group applied in C and M, consecutively [5].

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12108

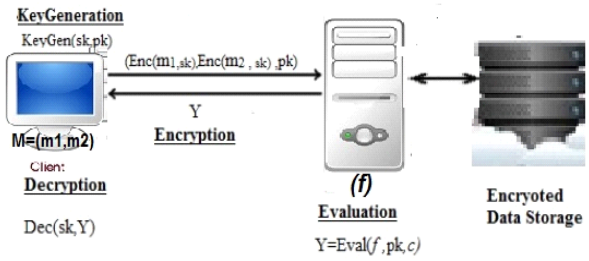


Figure 1: Homomorphic Encryption functions [4]

3.3 Homomorphic Encryption properties:

Assume that:
(m1, m2) ∈ M, (c1 and c2) ∈ C then
c1 = Enc (m1)
c2 = Enc (m2)
P is the prim number.

Additive Homomorphic Encryption

Enc (m1 + m2) mod p = c1 + c2 mod p.

Multiplicative Homomorphic Encryption

Enc (m1 * m2) mod p = c1*c2 mod p [13].

4. PARTIAL HOMOMORPHIC ENCRYPTION (PHE)

Partial Homomorphic Encryption allows users to apply a single mathematical operation on encrypted data by using either addition or multiplication [14]. Any encryption scheme which supports either multiplication or addition, but necessarily not both, is called a Partial Homomorphic Scheme [15].

4.1 Additive Homomorphic Schemes

A homomorphic encryption is named additive if there is an algorithm that can compute Enc(x+ y) from Enc (x) and Enc (y) without knowing x and y, such as algorithms of (Paillier and Goldwasser-Micali) [1].

4.1.2 Paillier Cryptosystem: The French (mathematician, Pascal Paillier), has suggested a new cryptographic algorithm called Paillier Cryptosystem Algorithm‖ in 1999. It is an additive homomorphic property. Paillier cryptosystem is on the base of decisional composite residuosity theory (DCRA). Hence, the Paillier cryptosystem has various applications, for example, e-voting systems, and threshold schemes.

4.1.3 Paillier Algorithm

1. Key generation

1.1 Select two large random primes'(p and q)
1.2 n = p*q
1.3 compute λ = lcm (p − 1, q − 1)
1.4 choose g ∈ Zn 2, n divides the order of g
1.5 Public-key => (g, n)
Secret-key => (p, q)

2. Encryption

2.1 M ∈ Zn
2.2 C = g m. r n (mod n2), r ∈ Zr is randomly chosen.

3. Decryption

3.1 M = (L (C2 (mod n2))) (L (g2
(mod n2)))-1 (mod n),
Where L (u) = (u-1) / n.

4.1.4Paillier Homomorphic Property:

Assume there are two ciphers (C1, C2) such that:
4.1 C1 = g M1 r1n (mod n2), C2 = g M2 r2n (mod n2)
4.2 C1·C2 = g M1 r1 n. g M2 r2 n (mod n2)

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12108

4.3 Additive Property is: g M1+M2 (r1 r2) n (mod n2) [15,1]

4.2 Multiplicative Homomorphic Schemes

A Homomorphic Encryption is named multiplicative if there is an algorithm that can compute Enc(x × y) from Enc (x) and Enc (y) without knowing x and y. Such as Algorithms of RSA and ElGamal [3].

4.2.1 RSA Cryptosystem: Rivest, Shamir, and Adleman presented their public key cryptosystem in (1978).

4.2.2 RSA Algorithm:

1. Key Generation

1-1 Select p, q big prime numbers

1-2 Calculate n = p. q,

Ø (n) = (p-1) (q-1)

1-4 Determine d, ensure that: (d * e) mod (ø (n)) = 1

- Public encryption key = (e, n)
- Private decryption key = (d, n) ø (n) = (p-1) (q-1)

2. Encryption

2-1 Plaintext M ∈ [0, n-1]

2-2 C = (M) e mod (n)

3. Decryption

3-1 M =(C) d mod (n)

4.2.3 RSA Homomorphic property:

Suppose C1 and C2 are two ciphertexts

4-1 C1 = M1e mod (n), C2 = M2e mod (n)

4-2 C1 · C2 = M1 e · M2 e mod (n)

4-3 Multiplicative property: (M1 · M2) e mod (n) [16,3]

4.3Elgamal cryptosystem

In 1984 ElGamal encryption algorithm is proposed by Tahir Elgamal, ElGamal Cryptosystem is (public key and multiplicative) Encryption algorithm .

4.3.1 ElGamal Algorithm:

1- Setup

A and B choose prime p and generator g as public key

2- Key generation

B: Chooses private x, and calculates Y = (g) x mod p, then send Y to A.

3- Encryption

A: Select a message M and Chooses random r and then calculates:

K = Yr (mod p)

C1= g r (mod p)

C2= M. K (mod p), Then send (C1, C2) to B

4- Decryption

B: Calculates K= C1 x (mod p) and recovers the message

M = K-1.

C2 (mod p), (where K-1 is the inverse of K (mod p)).

4.3.2 ElGamal Homomorphic Property: Given two encryptions:

(C11, C12) = (gr1, M1 y r1), (C21, C22) = (gr2, M2 y r2), Where r1, r2 are randomly chosen from {1, 2, …, q – 1 } and M1 , M2 ∈ G, one can compute :

(C11, C12) (C21, C22) = (C11C21, C12C22) = (g r1 g r2, (M1 y r1) (M2 y r2)) = (g r1+r2, (M1.M2) yr1+r2)

Multiplicative property: (M1. M2) y r1+r2 [45, 28].

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12108

5. ELLIPTIC CURVES

Elliptic Curve Cryptosystem (ECC) is a technique of public key cryptography, is based on the structure of algebraic and discrete logarithms of an elliptic curve over finite fields. Definitions of elliptic curve (EC) based on two kinds of finite field:
1-prime field Fp, where p is a large prime number
2-Binary fields [17,18].
The key sizes of ECC are smaller, faster encryption, more efficient and better security for the same level of security compared with other systems of public cryptography such as RSA [18].
Elliptic Curve Cryptography (ECC Compared to currently prevalent cryptosystems such as RSA, ECC offers the same security with smaller key sizes. By the help of table which provides approximate Comparable with key sizes for symmetric and asymmetric-key cryptosystems depended on the famous algorithms for attacking them [3].

5.1 Definition (ECDLP): The Elliptic Curve EC, let P, Q EC, recall that in the ECDLP, is to find an integer k Z where (1 k < n), such that KP= Q. It's easy to determine the points Q and P, but the difficulty deceits in finding integer k from multiple points of P*k, even if the knowledge of Q, P of EC. The ECDLP over Fq is more fixed than the DLP in Fq, This specify makes the cryptographic technique built on the ECDLP much more secure than that built on the DLP [19,18].

6. EVALUATION OF HOMOMORPHIC ENCRYPTION BASED ON ELLIPTIC CURVE

The security of Homomorphic Encryption based on ECC schemes to generate private key dependent on resolution of an basic principle mathematical problem named the Elliptic Curve Discrete Logarithm Problem (ECDLP).It's specifications is point doubling and point multiplication, Homomorphic property of an algorithm gives an advantage of making data even operate and effective after encryption over the networks [23].

The best significant advantages of elliptic curve cryptography are its ability to create same levels of security by much smaller keys, for instance, an RSA construction. This ability to utilize smaller keys signifies a computational support and time advantage with comparing by other asymmetric key systems. Also, accordingly an asymmetric key cryptosystem, it is generally safer than a symmetric key, because it is more difficult to decrypt without knowledge the private key. Generally Elliptic Curve Cryptography is very demanding computationally, this can be considered Disadvantages of Despite the fact elliptic curve cryptography is generally more secure in terms of its difficulty to break the cipher, this increased gradation of computation translates into a less time effective method of encryption, in general requiring more time than other encryption methods to run. Even though, elliptic curve systems generally run faster than RSA or Diffie-Hellman systems, they are still significantly slower than symmetric key systems, which is why many systems only use an asymmetric key system to distribute keys before finally utilizing a faster symmetric key system [21][12].

7. THE PROPOSED ALGORITHM DEPENDS ON

1. Key Generation:

- d= SHA-256 (e-mail + Password)
- k = d (G) where G is the base point, so G= (x, y)
- k = (k_1, k_2)
- We depend k_1 as the secret key, sk=k_1.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12108

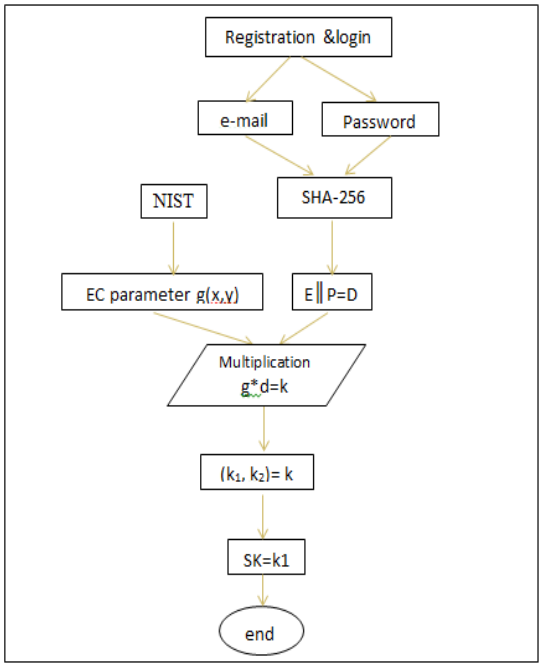


Figure2: key Generation process

2. Encryption

- Convert data chars (M) and SHA-256 (password) to ASCII where M= (m_1, m_2… m_n).
- $c_i = m_i * k_1$.
- C is the output of all encrypted attributes

3. Decryption

1. mi = c_i *
2. M is the output of all decrypted data

8.SECURITY OF DATA IN CLOUD COMPUTING

(Cloud computing) means one and only of the parts in information technology (IT) [13]. Data security that means different security things related to (integrity, privacy, confidentiality, and authentication) is a very important thing that needs to be remarked. Users want secure their data by using their own encryption algorithm to which stocks in a plaintext form if required by Cloud service provider and so this data essential designates decrypted whenever it is to be dealt with[22].

9.EXAMPLE OF IMPLEMENTED APROPOSED ALGORITHM IN SECURE CLOUD DATA STORAGE

If User e-mail= omer@gmail.com and password = Aa123123, user's data for instant is (Nowadays, there are many universities around the world and each of them may have up to 10 thousand students. To handle this large number of students may cause a problem especially in terms of the student attendance. Attendance is one of the important factors that affect the students' performance in class the attendance in the majority of) as show in Figure.

Step1: log in Secure Cloud Environment by using E-mail and password.
Step2: generate a secret key
SK = d*G (gx, gy) = (k_1 ,k_2)
Set k_1 as a secret key based on Elliptic curve used for encryption.
Step3: Encryption of data Based on partial Homomorphic Encryption (PHE)
Step5: Matching of evaluation of stored encrypted data and user's request encrypted data.
Step 6: if the matching is true, users' data is found then decrypted for user.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12108

10. PHASES OF IMPLEMENTED ALGORITHM STEPS

There are six phases (Setup, KeyGen, Encryption, Decryption, Evaluation and Matching) Figure 3.4shows these phases.

a) Setup (): It has an EC security parameter (SP) as an input, where it was based on the standard NIST values (p, a, b, G, n) and assigned to this function for use in generating the secret key in the Key Gen.

b) KeyGen (SP, S): It is accepted EC parameter domain SP, and some of the data (S), where S or (e-mail || pass), the outputs of this algorithm is the secret keys sk which associated with some Data S.

c) Encryption (sk, p, PT): This algorithm is used to encrypt all users Data (PT), so the input is PT, sk and p, the output is ciphertext C.

d) Decryption (sk, p, C): This algorithm is used to decrypt all encrypted Data. Input data is a ciphertext C, sk and p, the output is getting the original data (PT) as in Figure 3.4.

e) Plaintext Evaluation (e-mail||SHA-256(pass), pt, Mult-sk, Mult-pt, ouput): get result1 after applying computation on pt.

f) Ciphertext Evaluation (e-mailct||Pct, mulct, ouput): get a result2 after applying computation on ct.

G) Matching (e-mail, pass, e-mailct, Pct., true or false): Matching the resilt1 and result2 to be either true or false.

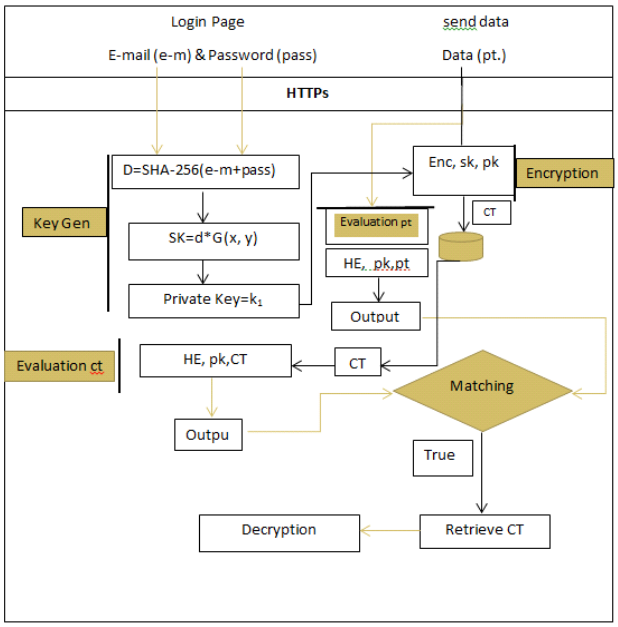


Figure 3: Phases of a proposed algorithm

11.COMPARISON BETWEEN A PROPOSED ALGORITHM AND (RSA, PAILLIER, ELGAMAL) IN EXECUTION TIME

The results of encryption, decryption and Evaluation specific length of text are presented in Figures (5,6and 7). The results were implemented in terms of execution time in millisecond. The proposed algorithm is used in encrypting the user Data. The proposed algorithm provides a high security compared with ElGamal, RSA and Paillier algorithm.

In this paper, 64-bits keys were utilized. The reason of choosing (64 bits) as a key size, that 64 bits requires a less storage space compared to the high keys; which require more storage space for encrypted data. Therefore, 64 bits can reduce the processing time to be used by (HE). So, in this thesis (64 bits) as a key size for the algorithm has been adopted.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

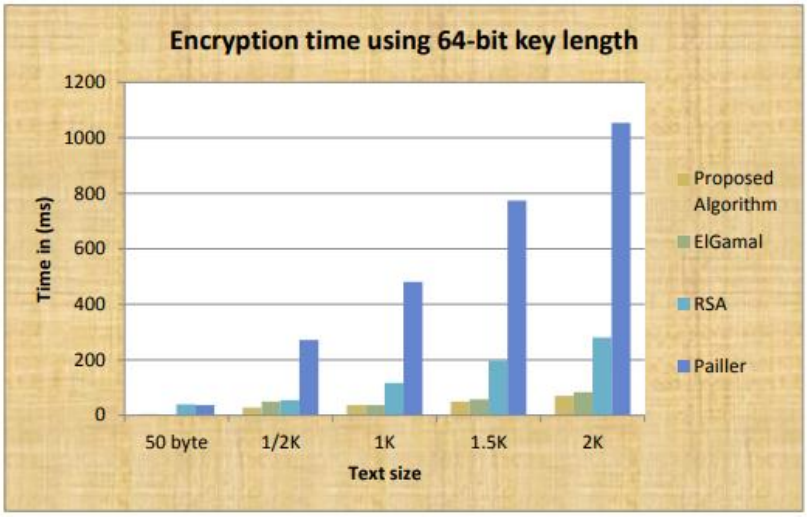
Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12108

Table 1: Times of encryption, decryption text and Evaluation Execution (64-bit)

Message In Byte	Time in ms and 64-bit key length											
	Proposed Algorithm			ElGamal Algorithm			RSA Algorithm			Pailler Algorithm		
	Enc.	Dec.	Eva.	Enc.	Dec.	Eva.	Enc.	Dec.	Eva.	Enc.	Dec.	Eva.
50	4	2	2	1	10	1	39	6	1	37	29	4
1/2K	28	26	8	49	146	4	55	101	33	271	199	65
1K	37	27	14	37	917	5	116	144	69	481	370	242
1.5K	49	44	17	57	3043	8	197	206	159	774	568	572
2K	70	67	22	83	8084	27	280	268	259	1054	791	901

Table (1) shows the time in millisecond of encryption/decryption and Evaluation of the proposed algorithm, (ElGamal, RSA and Paillier) algorithms execution using 64-bit as a size of key.



Figures (4) shows Encryption time results plot of the Table (1). The results presented in Table (1) shows acceptable execution speed suitable for the secure environment

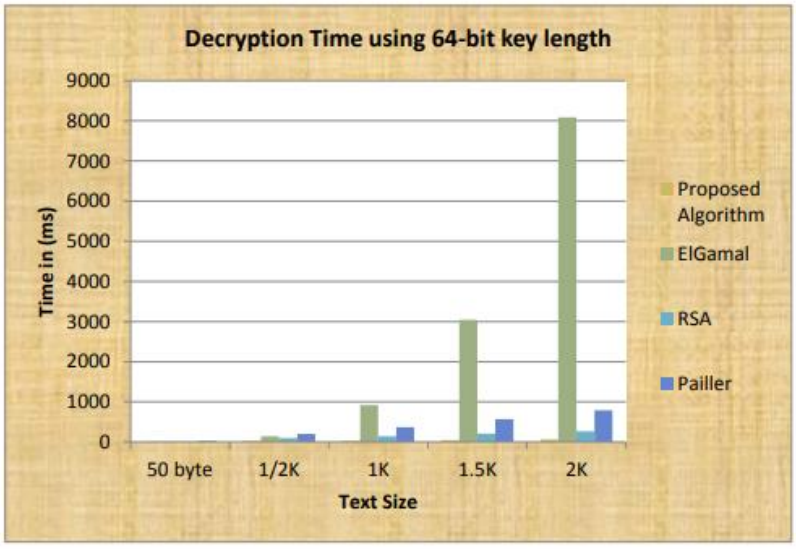


Figure 5:Time of Decryption Text by using 64-bit length of key

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 1, January 2025

DOI: 10.17148/IARJSET.2025.12108

Figure (5) shows Decryption time results plot of the Table (1). The results presented in Table (1) shows acceptable execution speed suitable for the secure system.

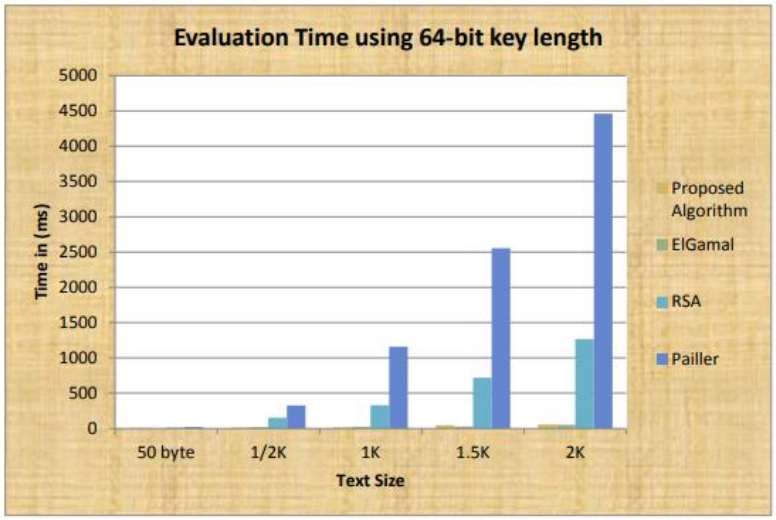


Figure 6: Time of Evaluation Text by using 64-bit length of key

Figures (6) shows Evaluation time results plot of the Table (1). The results presented in Table (1) shows acceptable execution speed suitable for the secure environment.

11.1 Encryption, Decryption and Evaluation Results

The results of encryption, decryption and Evaluation specific length of text are presented in Figures (4,5 and 6). The results were implemented in terms of execution time in millisecond. The proposed algorithm is used in encrypting the user Data. The proposed algorithm provides a high security compared with ElGamal, RSA and Paillier algorithm.

12. CONCLUSION

1-The use of homomorphic encryption (HE) in the secure cloud Environment provide great protection for user data that became completely encrypted and no one could know the information even if the server database was hacked by Hacker.

2- The security of the ECC algorithm depends on the difficulty of ECDLP. ECC currently appears to be implemented on a 64-bit to provide nearly the same security level against the attacks of hackers compared with algorithms like (RSA Elgamal, paillier). This variation in the length of the keys has led to improve and speed in performance and less storage requirements, table1present the comparison between proposed algorithm and RSA in terms of execution time.

3-The use of ECC means the powerful and efficient asymmetric algorithms for the given key length, and it is good, particularly for security applications where it restricted in power calculation and integrated circuit area, e.g. PC cards, wireless devices and smart cards.

REFERENCES

[1] Marwan Majeed Nayyef, Ali Makki Sagheer, Sara Shhab Hamad " Attribute Based Authentication System using Homomorphic Encryption", Journal of Engineering and Applied Sciences, 2018.

[2] Kalpana Gudikandula, P. Kumar,Ravilla VenkataKrish, "Homomorphic Encryption Environment-Service Provider based Encryption and Decryption Endpoints for Third-party Cloud Provider", Journal of Computer Science IJCSIS, Pennsylvania, USA Vol. 15No.7, 2017.

[3] Yong Ding, Xiumin Li," Policy Based on Homomorphic Encryption and Retrieval Scheme in Cloud Computing", International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), IEEE, 2017.

[4]. Mahesh U. Shankarwar, Ambika V. Pawar " Security and Privacy in Cloud Computing: A Survey ", ./----Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing, pp 1-11, Springer, 2014.

DOI: 10.17148/IARJSET.2025.12108

[5] Kamal Benzekki , Abdeslam El Fergougui, Abdelbaki El Belrhiti El Alaoui," A Secure Cloud Computing Architecture Using Homomorphic Encryption", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016.

[6] Xidan Song ,Yulin Wang,," Homomorphic cloud computing scheme based on hybrid homomorphic encryption", 3rd International Conference on Computer and Communications (ICCC) ,IEEE, 2017.

[7] Adi Akavia, Dan Feldman, Hayim Shaul," Secure Data Retrieval on the Cloud: Homomorphic Encryption meets Coresets ", IACR Transactions on Cryptographic Hardware and Embedded Systems, 80-106, 2019.

[8] Ahmed El-yahyaoui and %Mohamed Dafir Ech-Cherif EL kettani," A Verifiable Fully Homomorphic Encryption Scheme for Cloud Computing Security", Technologies, 7, 21, 2019.

[9] Maha Tebaa , Saïd El hajji, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering , U.K, London, 2012.

[10] Maha Tebaa, Said El hajji, "Secure Cloud Computing through Homomorphic Encryption ", International Journal of Advancements in Computing Technology (IJACT), Volume5, 2013.

[11] Prof.S.D.Pingle, "Survey of Latest Trends in Cryptography and Elliptic Curve Cryptography", International Journal of Scientific Research and Education, Volume 4, Issue 05, 2016.

[12]Yatao Yang, Shuang Zhang , Junming Yang, Jia Li, and Zichen Li, "Targeted fully homomorphic encryption based on a double decryption algorithm for polynomials", Tsinghua Science and Technology, Vol. 19, No. 5, pp. 478-485, 2014.

[13]. Jayachander Surbiryala , Chunlei Li , Chunming Rong, " A framework for improving security in cloud computing", 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China, IEEE, 2017.

[14] Pallavi, "Homomorphic Encryption Schemes: Steps To Improve the Proficiency" International Journal of Science Technology and Management, Vol.No5, Issue No.02, 2016.

[15] Payal V. Parmar, Shraddha B. Padhar, Shafika N. Patel, Niyatee I. Bhatt , Rutvij H. Jhaveri" Survey of Various Homomorphic Encryption

[16] Dave Thompson" ELLIPTIC CURVE CRYPTOGRAPHY", partial fulfillment of the requirements for Departmental Honors in the Department of Mathematics Texas Christian University Fort Worth, Texas , 2016.

[17] Sarita Kumari" A research Paper on Cryptography Encryption and Compression Techniques ", International Journal Of Engineering And Computer Science ,Volume 6, Page No. 20915-20919 , 2017 .

[18] Sunuwar, Rosy and Suraj Ketan Samal. "Elgamal Encryption using Elliptic Curve Cryptography", Cryptography and Computer Security, 2015.

[19] Patel, Sankita J., Ankit Chouhan and Devesh C. Jinwala, "Comparative evaluation of elliptic curve cryptography based homomorphic encryption schemes for a novel secure multiparty computation", Journal of Information Security, Vol. 5, No. 1, 2014.

[20] Sneha Patil, Vidyullata Devmane "A review on Elliptic Curve Cryptography and Variant", International Research Journal of Engineering and Technology (IRJET) , 2018.

[21] Tong Li, Elda Paja, John Mylopoulos, Jennifer orkoff ,Kristian Beckers," Security attack analysis using attack patterns",IEEE, 2016.

[22] Manish M. Potey, C.A. Dhote, Deepak H. Sharma, "Homomorphic Encryption for Security of Cloud Data ",/ 7th International Conference on Communication, Computing and Virtualization, Elsevier, 2016.

[23]. Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris, " Survey on the Cryptographic Encryption Algorithms", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 11, 2017.

