International Journal of Scientific Research in Science, Engineering and Technology (www.ijsrset.com)
© 2020 IJSRSET | Volume 7 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
DOI : https://doi.org/10.32628/IJSRSET207264

Fast Hybrid Cryptosystem for Enhancing Cloud Data Security Using Elliptic Curve Cryptography and DNA Computing

Souad Hafidi[1], Fatima Amounas[1], Lahcen El Bermi[2], Moha Hajar[3]
[1]R.O.I Group, Computer Sciences Department, Faculty of Sciences and Technics, Moulay Ismaïl University, Errachidia, Morocco
[2]GL-ISI, Computer Sciences Department, Faculty of Sciences and Technics, Moulay Ismaïl University, Errachidia, Morocco.
[3]R.O.I Group, Mathematical Department, Faculty of Sciences and Technics, Moulay Ismaïl University, Errachidia, Morocco

ABSTRACT

Now a day's Security in cloud computing is one of the broad areas for researchers. Cloud computing is a term that involve to deliver the services over the Internet. So, it requires the security upgrade in data transmission approach. One of the ways by which data in the Cloud be secured is cryptography. In fact, the high-quality cloud security can be achieved by efficient encrypting techniques. This paper investigates how the integrity and secure data transfer are improved based on the Elliptic Curve cryptography and DNA computing. Many researchers have tried to exploit the features of ECC field for security applications. In this paper, we attempt to develop a fast hybrid cryptosystem based on Elliptic Curve and DNA computing for providing security service such as confidentiality in the cloud services. The security of the proposed scheme is based on Elliptic Curve Discrete Logarithm Problem (ECDLP). Existing DNA based cryptography technique need more computational power and more processing time with larger key sizes to provide higher level of security. The main goal of our construction is to enhance the security of elliptic curve cryptosystem using DNA Computing. In this approach data stored on the cloud server in the encrypted form and even if data is accessed by the attacker, the attacker can't get the current data.

Keywords : Data Security, Cloud Computing, Elliptic Curve Cryptography, Code computing, DNA encoding.

I. INTRODUCTION

Cloud computing is one of today's hottest research areas due to its ability to reduce costs associated with computing while increasing scalability and flexibility for computing services. Cloud computing platform is a combination and evolution of existing technologies which can be physical machines or virtual machines [1]. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them [2]. Further, Cloud computing is a model for enabling convenient, ubiquitous, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal effort or service provider interaction. The massive pool of configurable resources in Cloud is available to consumers as service.

These services are generally partitioned into three main categories: Software-as-a-Service (Saas), Platform-as-a-Service (PaaS) and Infrastructure-as-a-

Service (IaaS) as showing in Figure 1. Cloud Computing has its own attractive characteristics, they are On-Demand Self Service, Broad network access, Resource pooling, Rapid Elasticity and Measured Service [3].

Recently, cloud security can be achieved by cryptographic system [4]. The major functions of cryptographic system are encryption and decryption. So, for efficient data security and reliability we need mechanism which provides secure data encryption, decryption technique. Many problems like Data Security, Cloud Security issues and different cryptographic algorithms are discussed in literature review [5-8].

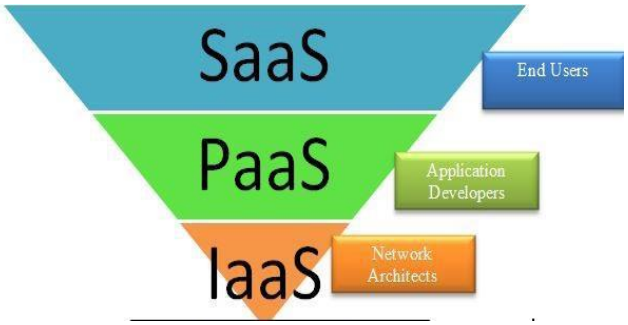

Figure 1. Cloud services

RSA algorithm is the most widely used public key cryptography algorithm for encryption and decryption today. This is the first generation algorithm that was used for providing data security. In today's world Elliptic Curve Cryptography (ECC) is a secure and more efficient encryption algorithm than RSA as it uses smaller key sizes for same level of security as compared to RSA. For e.g. a 256-bit ECC public key provides comparable security to a 3072-bit RSA public key [9].

The aim of this work is to provide better cloud data security in cloud computing using Elliptical Curve Cryptography which gives more secure data transmission, storage, authorization, and authentication process over the cloud. The proposed work uses the variants of ECC algorithms, thus ensuring a greater security with the benefit of smaller keys, providing perfect Forward Secrecy and less consumption of time and memory. To enhance security, the key matrix will be encrypted using code computing.

The rest of this paper is organized as follows: we start in section 2 with some basics notions on elliptic curve cryptography and DNA computing. Section 3 is devoted to proposed approach. The security analysis of the proposed scheme will be discussed in section 4. Finally, the concluding remarks will be in the last section.

II. BACKGROUND INFORMATION

In this section we provide some basic details required in the proposed method.

A. Elliptic Curve Cryptography

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller.

An elliptic curve over a field K is a nonsingular cubic curve in two variables, f(x,y) =0 with a rational point (which may be a point at infinity). The field K is usually taken to be the complex numbers, reals, rationals and algebraic extensions of rationals, or a finite field. Elliptic curves groups for cryptography are examined with the underlying fields of F_p (where p>3 is a prime) and $F2^m$ (a binary representation with 2^m elements).

An elliptic curve is a plane curve defined by an equation of the form:

$$y^2 = x^3 + ax + b \pmod p \qquad (1)$$

Where $a, b \in F_p$, $p \neq 2, 3$ and satisfy $\Delta = 4a^3 + 27b^2 \neq 0$. The set $E(F_p)$ consist of all point (x, y) that satisfy the elliptic curve E along with a point at the infinity O. The set of points on $E(F_p)$ also include point, which is

the point at infinity and which is the identity element under addition. The addition operator is defined over $E(F_p)$ and it can be seen that $E(F_p)$ forms an abelian group. The basic operations on elliptic curves are addition and doubling [10].

The addition of points follows specific rules indicated below:

- Identity law: P + O= O + P= P for every P∈E
- Inverse law: P + (-P)= O for every P∈E
- Associative law: (P + Q) + R= P + (Q + R)
  P, Q, R∈E
- Commutative law: P + Q = Q + P for all P, Q ∈E

The Rules for Addition

Let $E: y^2 = x^3 + ax + b$ be an elliptic curve and let $P_1=(x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E, where $P_1 \neq P_2$
and λ is an integer. Adding the two points P_1 and P_2 giving a point P_3 that should lie on the same curve E.

$$P_3 = P_1 + P_2 = (x_3, y_3)$$

where

$$x_3 = \lambda^2 - x_1 - x_2 \quad (2)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (3)$$

With λ define by:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if\ P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1} & if\ P_1 = P_2 \end{cases}$$

It is know that rational points form an additive group in the addition over the elliptic curve shown in the following figure:

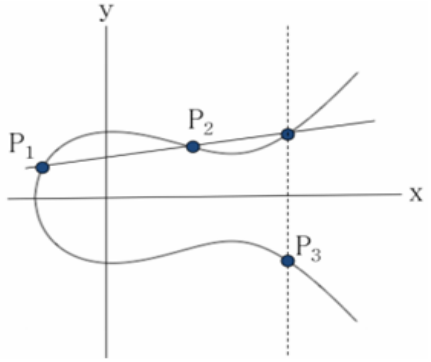

Figure 2. Addition of points on elliptic curve

Elliptic Curve Discrete Logarithm Problem (ECDLP)

ECC is a public-cryptosystem defined over finite fields on the basis of algebraic structures of the elliptic curves [11]. The Elliptic curve cryptography is defined on the supposition that the elliptic curve discrete logarithm problem (ECDLP) is very difficult. ECDLP is determining the integer k, given a rational point P on the elliptic curve E and the value of Q=k*P. Elliptic curve cryptosystems rely on the hardness of solving the ECDLP.

ElGamal Encryption using ECC

In 1985, ElGamal [12] proposed a public key cryptosystem, which gained a lot of attention in the field of Cryptography. The key idea behind the cryptosystem is the use of the discrete logarithm problem. It is hard to find the solution for a discrete logarithm problem.

The EC-ElGamal is an alternative of the ElGamal algorithm which based on ECPLD. The security of EC-ElGamal is higher than the other classical systems. The specific encryption and decryption processes of EC-ElGamal are performed as follows:

Step 1: Generation of keys for receiver:

- The elliptic curve equation Ep:$y^2=x^3+ax+b$, prime p and basic point P are selected. E and a point P are publicly known, as is the embedding system $m \rightarrow P_m$ which imbed plain text on an elliptic curve E [13].
- Private key d is set by receiver, then Q is calculated by Q=dP.
- public Keys Ep, p, P, Q are exposed.

Step 2: Encryption processes of transmitter:

- The plaintext is known as M, and it is converted to point P_M on the elliptic curve field.
- Private key k is set by transmitter, then C1=kP and C2= P_M +kQ, where "+" denotes addition operation on elliptic curve.
- Transmit encrypted data C1, C2 to receiver.

Step 3: Decryption processes of receiver:

- According to the private key d of receiver, P_M is given by

$$P_M = C2 - dC1$$
$$= (P_M + kQ) - d(kL)$$
$$= P_M + (k \cdot dL - d.kL) = P_M,$$

where ''-'' is the inverse addition operation on elliptic curve.

- Reverses the embedding to get back the original message M.

B. DNA Computing

The DNA cryptography is an emerging field in the area of DNA computing research. Some algorithms that are available in DNA Cryptography have limitations in that they still use modular arithmetic cryptography at their encryption and decryption processes.

1. DNA map rules

DNA sequence contains four nucleic acid bases A (Adenine), C (Cytosine), G (Guanine) and T (Thymine), where A, T, C and G are complementary pairs. In the binary system, 0 and 1 are complementary, 00 and 11, 10 and 01 also are complementary. If 00, 11, 10 and 01 are encoded with nucleic acid bases A, C, G and T, we can get 4!=24 kinds of encoding schemes. Due to the complementary relation between DNA bases, there are eight kinds of encoding combinations satisfying the principle of complementary base pairing, which are shown in Table 1.

TABLE 1. DNA MAP RULES

	A	T	G	C
R_1	00	11	01	10
R_2	00	11	10	01
R_3	01	10	00	11
R_4	01	10	11	00
R_5	10	01	00	11
R_6	10	01	11	00
R_7	11	00	01	10
R_8	11	00	10	01

b. Code Computing based DNA Encoding

There are different processes to encode data and different DNA cryptography methodology that are used for secure data transmission like bio-molecular, one-time-pad [14]. The sender chooses a secure key. Instead of giving DNA map rule directly, secure key is mapped with DNA molecule to provide greater level of security which is not known to the eavesdropper who always tries to retrieve the secret. DNA sequence is generated by combining DNA molecules such as Adenine (A), Thymine (T), Guanine (G) and Cytosine(C) as shown in Table 1. In our case, the secure key is imbedded into code point that can be converted into data sequence. Then, the data sequence is mapped with DNA nucleotide using the Table 1. Inversely, the DNA sequence can be decoded into a code point. In DNA encoding, Code subtraction is the reverse operation of code addition[15].

If the DNA encoding rule R_1 is adopted, the code operation can be expressed as shown in Table 2.

Table 2. (a) Code Addition operation

+	A	G	C	T
A	G	C	T	A
G	C	T	A	G
C	T	A	G	C
T	A	G	C	T

(b) Code subtraction operation

-	A	G	C	T
A	T	C	G	A
G	A	T	C	G
C	G	A	T	C
T	C	G	A	T

III. PROPOSED APPROACH

The cloud computing is a virtual environment that requires transfer data throughout the cloud. To preserve security of the cloud, the provider should

include the following solutions: encryption, authentication and access control and Intrusion detection [16].

The proposed approach involves major stakeholders who operate on the data in a cloud environment such as the Data Owner who sends the data to the Data User when he/she requests for. The proposed algorithm is structurally and functionally divided into two basic parts as showing in Figure 3. The first part deals with the key generation using ECC technique based on data matrix. The second part of the algorithm deals with ECC encryption and decryption processes. To enhance security, the key matrix will be encrypted using code computing. The authorized user can also download any of the uploaded encrypted files. The proposed approach upholds the data confidentiality in a cloud environment with utmost security. It makes it harder to break up by involving the code computing and ECC technique, which are highly randomized in the proposed mechanism.

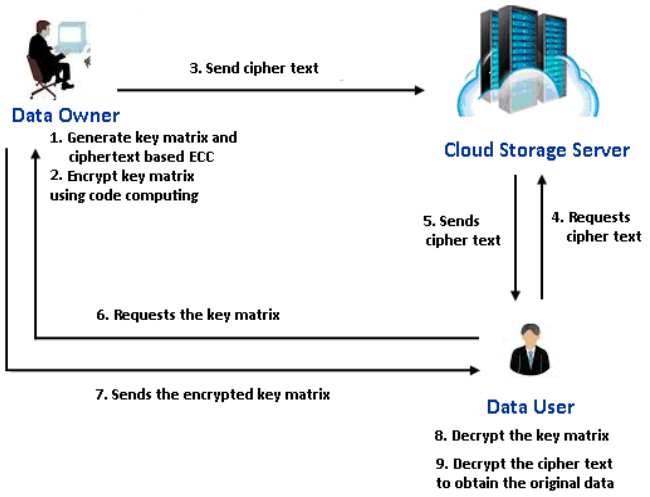

Figure 3. Model proposed of data storage in cloud computing

a. Key generation

- The data Owner chooses a random integer k_B, and publishes the point $P_B = k_B P$ (while k_B remains secret).
- The data user chooses a random integer k_A, and publishes the point $P_A = k_A P$ (while k_A remains secret).
- The data Owner computes the point $Q = k_A P_B$ and generates key matrix based on ECC technique.

$$K = (P_i),\ i=1, 2, \ldots$$

- The data Owner encrypts the key matrix using code computing operation.

b. Encryption/Decryption process

The proposed algorithm is structurally divided into two basic parts. The first part deals with the encryption process as follows: the data Owner encrypts the data using EC-ElGamal cryptosystem based on matrix approach. Next, the key matrix is encrypted using code computing. The Cipher text is sent to the cloud storage on completion of the encryption process. The pseudo code for the encryption process is given in Algorithm 1. The second part deals with the decryption process as follows: the Data User requests the cipher text to cloud. So, it checks the Data User and sends the corresponding cipher text. The Data User requests for the key matrix to the data Owner, which is decrypted with Code computing. The cipher text is received from the cloud storage server and is decrypted using the EC-ElGamal decryption process. The pseudo code for the encryption process is given in Algorithm 2. These algorithms use the following functions which are shown in Table 3.

TABLE 3. FUNCTIONS USED IN ENCRYPTION AND DECRYPTION

Function	Description
IMBED (M)	it imbeds each character into point on elliptic curve.
ENC-ELGAMAL (Pi, Ki)	it encrypts each point Pi using Elgamal cryptosystem.
SIZE(F)	returns the number of the characters in the plain text file F.

CADD (K'i, Q)	it permits to encode the key using code addition operation.
Send-to-Cloud (F')	it sends the encrypted file F' in cloud storage
CSUB (K'i, Q)	it permits to decode the encrypted key using code subtraction operation.
DEC-ELGAMAL (C_i, K_i)	it decrypts each point Ci using Elgamal decryption process.

- **Algorithm 1: Encryption**

```
Encryption (F) {
for i=1 to SIZE(F)
      Pi=IMBED(Mi)
// the results points are stored into data matrix PM
for i=1 to SIZE (K)
   for j=1 to SIZE (K)
      { Cij=EC-ELGAMAL( Pi, Ki) }
//insert the result sequence into file text F'
//Encrypt key matrix using code addition operation
for i=1 to SIZE(K)
{     // CADD: Code Addition operation
     K'i=CADD (Ki, Q)
}
Send-to-Cloud (F')
}
```

Algorithm 2: Decryption

```
Decryption (F'){
Download the encrypted file from cloud storage
// the obtained points are stored into data matrix PM
PM=(Pi), i=1, 2, ...
Compute Q= kBPA
//Decrypt key matrix using code substraction
operation
for i=1 to SIZE(K)
 {  // CSUB: Code Substraction operation
        K'i=CSUB(K'i, Q)
 }
for i=1 to SIZE (K)
   for j=1 to SIZE (K)
      { Pij=DEC-ELGAMAL( Pi, Ki)
 }
Reverse-Imbed (Pi, Mi)
}
```

IV. RESULTS AND ANALYSIS

A. Implementation and results

This section demonstrates the proposed approach in practical aspect using Netbeans 7.1. The implementation of the proposed approach has been done in a private cloud with the sufficient number of nodes (owners/users). The node which initiates to upload a file will be the owner, who encrypts and shares the key matrix to the user. The node which initiates to download the file will be the user, who decrypts the data in order to access it. The time taken to encrypt and decrypt the data is dependent on the size of the plaintext. The implementation results highlights the time of encryption/decryption process with time of execution in upload and in download of files with different sizes. Table 4 shows the execution time required by different size text files for encryption and decryption process.

The various metrics analyzed in our proposed algorithm and the results obtained are emphasized below.

TABLE 4. EXECUTION TIME FOR ENCRYPTION AND DECRYPTION PROCESS BY FILE SIZE

File size	Time in Encryption (ms)	Time in Upload (ms)	Time in Decryption (ms)	Time in download (ms)
64	18	105	48	210
128	25	202	64	422
256	48	406	80	845
512	65	810	127	1690

1024	128	1620	201	3380
2048	319	3280	437	6770

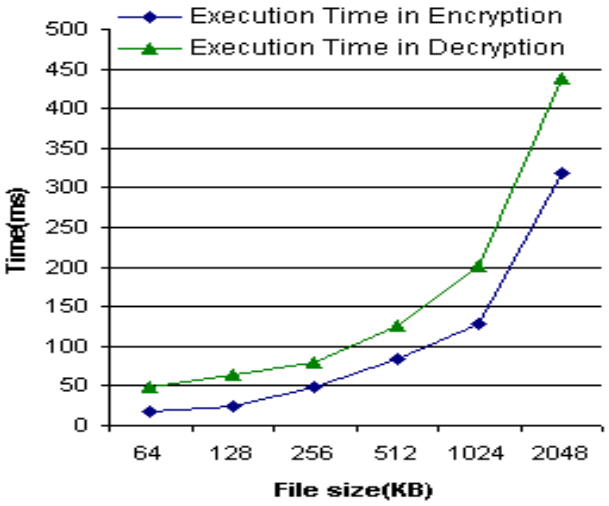

Figure 4. Graph of time execution for encryption and decryption process

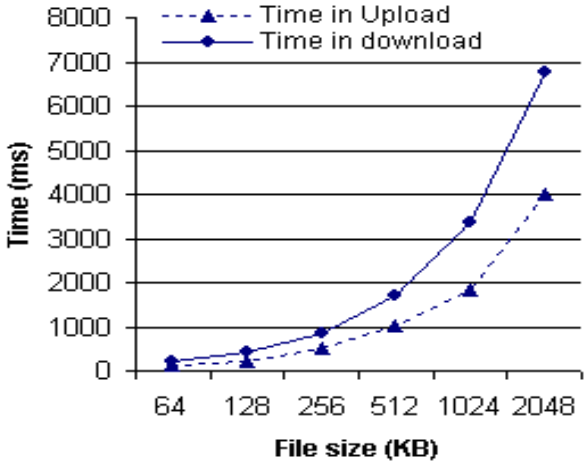

Figure 5. Graph of time execution in Upload and download of our algorithm by File size

Here, the decryption time is greater than the encryption time. This is explained by the addition of key recovery time.

The algorithm is giving hopeful results for various size files. From the results, it is found that the encryption time increases linearly with increase in the size of text files, but the time taken to decrypt is lesser than the encryption time. Similarly, when the file size increases, the time taken for encryption and decryption also increases. It proves that the computational complexity is less, as shown in Figures 4 and 5

B. Comparison with other algorithms

The most popular among cloud service providers is AES algorithm and used in many security applications. Many authors have proposed to apply double level of encryption using AES algorithms in integrated manner [17-19]. In this section we have performed a comparison of our proposed hybrid algorithm with AES algorithm for performance measurements.

The experiment is performed for the text files of various sizes. The experiment results are very satisfactory for the proposed hybrid algorithm as depicted in Table-5 given below. The results are also presented separately in the graphs shown in Figure 6 and Figure 7. According to the graph, it can be clearly seen that our proposed algorithm takes much less time for encryption and decryption as compared to AES. The security level achieved using elliptic curves and code computing, is far better than AES.

TABLE 5. RESULTS COMPARISON WITH AES ALGORITHM BY FILE SIZE

		File size (KB)			
		1024	2048	4096	8192
Enc. (ms)	AES	165	640	724	860
	Prop. Alg.	128	320	418	526
Dec. (ms)	AES	354	576	752	983
	Prop. Alg.	202	438	687	865

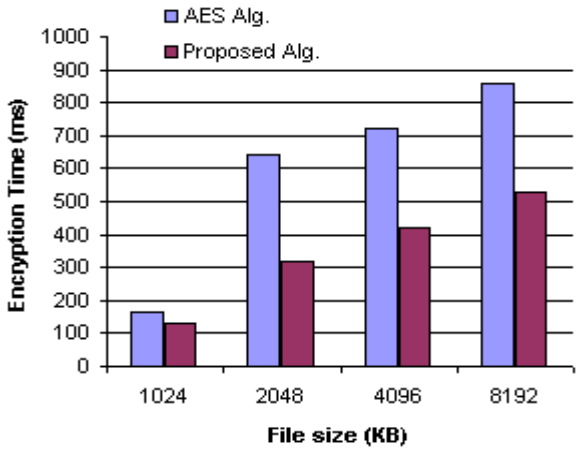

Figure 6. Comparison of Encryption Time among our algorithm and AES

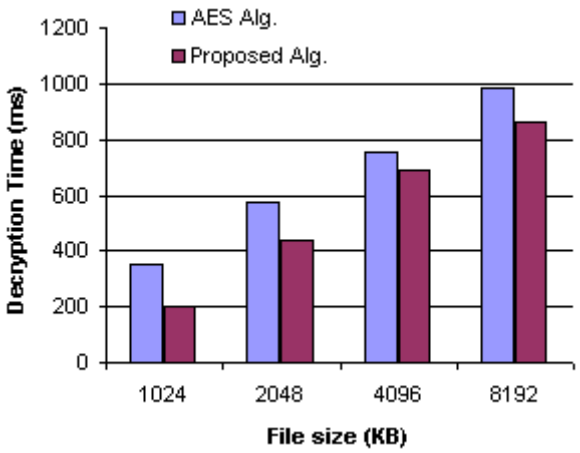

Figure 7. Comparison of Decryption Time among our algorithm and AES

V. CONCLUSION

Cloud Computing provides a platform with an enhanced and efficient way to store data in the cloud. In this paper, a fast hybrid algorithm based on EC-ElGamal cryptosystem and code computing is proposed. The Strength of the algorithm due to the difficulty level used in computing discrete logarithm and code computing based DNA encoding. Also Integration of Elliptic curve cryptosystem and code computing has improved the security level provided to the user's data in the Cloud. From the experiments, it is proved that the system is highly secure and hard to perform a cryptanalysis attacks. Similarly, the proposed approach provides data confidentiality for the data transferred between the Data Owner and the Data User in a cloud environment. The results of experiments and security analysis show that the proposed encryption scheme can achieve a good encryption result and can resist against common attacks.

In the future, it can be enhanced by making this method compatible to encrypt image, multimedia data which have to be transmitted securely over unsecured channels.

VI. REFERENCES

[1] L. Kacha and Abdelhafi Zitouni, “An Overview on Data Security in Cloud Computing,” Cybern. Approaches Intell. Syst., Vol. 661, pp. 250-261 (2017).

[2] Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication, September (2011).

[3] D. Lin and A. Squicciarini, "Data protection models for service provisioning in the cloud," Proceedings of the 15th ACM symposium on Access control models and technologies, pp. 183-192 (2010).

[4] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, “Data Security in Cloud Computing,” in Future Generation Communication Technologies (FGCT), pp. 55-59 (2016).

[5] Ravi Gharshi, Suresha, “Enhancing Security in Cloud Storage using ECC Algorithm”, International Journal of Science and Research (IJSR), Vol 2, Issue 7 (2013).

[6] Ms. Nikita N Chintawar, Ms. Sonali J Gajare, Ms. Shruti V Fatak, Ms. Sayali S Shinde, “Enhancing Cloud Data Security Using Elliptical Curve Cryptography”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 3 (2016).

[7] Parsi Kalpana , Sudha Singaraju, Data Security in Cloud Computing using RSA Algorithm, International Journal of Research in Computer

and Communication technology, ISSN 2278-5841, Vol 1, Issue 4 (2012).

[8] S. Arun, M.E., N. R. Shanker, "Data Security in cloud storage using Elliptical Curve Cryptography", International Journal of Pure and Applied Mathematics, Vol 120, No. 6, pp.27-38 (2018).

[9] C. Varma, "A Study of the ECC, RSA and the Diffie-Hellman Algorithms in Network Security," in 2018 International Conference on Current Trends towards Converging Technologies, pp. 1-4 (2018).

[10] F. Amounas and E.H. El Kinani, Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography", International Journal of Information & Network Security, Vol.1, No.2, pp. 54-59 (2012).

[11] Darrel Hankerson, Alfred Menezes and Scott Vanstone, "Guide to elliptic curve cryptography", Springer-Verlag (2004).

[12] T.ElGamal, A public key cryptosystem and signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31, pp. 469-472 (1985).

[13] Ahmad Steef and M. N. Shamma, "A secure approach for embedding message text on an elliptic curve defined over prime fields, and building 'EC-RSA-ELGamal' Cryptographic System", International Journal of Computer Science and Information Security, Vol. 15, No. 6 (2017).

[14] Ubaidur Rahman, N.H., Balamurugan, C.,Mariappan, R.: "A novel DNA computing based encryption and decryption algorithm", In Proceedia Computer Science, International Conference on Information and Communication Technologies, pp. 463-475 (2015).

[15] Grasha Jacob and Annamalai Murugan, "A Hybrid Encryption Scheme using DNA Technology", The International Journal of Computer Science and Communications Security, Vol. 3, pp. 61-65 (2013).

[16] G. Sakthivel, P. Madhubala, "Hybrid Elliptic Curve Cryptography for Secured Cloud Computing", International Journal of Computer Sciences and Engineering", 7(1), pp. 707-719 (2019).

[17] S. Kumari, Princy, Reema, and S. Kumari, "Security in Cloud Computing using AES & DES," Int. J. Recent Innov. Trends Comput. Commun., vol. 5, no. 4, pp.194-200 (2017).

[18] Tamilselvi.S, "Data Storage Security in Cloud Computing Using AES", International Journal of Advanced Networking & Applications, Vol. 8, Issue: 5, pp. 124-127 (2017).

[19] Dewi, "Data security in cloud computing using AES under HEROKU cloud", The 27th Wireless and Optical Communications Conference, (2018).

Cite this article as :

Souad Hafidi, Fatima Amounas, Lahcen El Bermi, Moha Hajar, "Fast Hybrid Cryptosystem for Enhancing Cloud Data Security Using Elliptic Curve Cryptography and DNA Computing ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 2, pp. 336-344, March-April 2020. Available at doi : https://doi.org/10.32628/IJSRSET207264
Journal URL : http://ijsrset.com/IJSRSET207264