International Journal of Advanced Science and Technology
Vol. 29, No. 10S, (2020), pp. 8736-8749

Elliptic Curve - Homomorphic ElGamal Based Mutual Authentication Scheme in Cloud Computing

V. Biksham[1], and D. Vasumathi[2]

[1]*Research Scholar, Dept. of CSE, JNTUH, Hyderabad, India.*
[2]*Professor, Dept. of CSE, JNTUHCEH, JNTUH, Hyderabad, India*
[1]*vbm2k2@gmail.com*, [2]*rochan44@gmail.com*

Abstract

Cloud computing is an extensive technology from which the client could access several services through a remote server. Authentication of the remote services needs a common key between the client and the server in a secured manner. The existing key agreement protocols utilized various techniques for the preservation of the data security. The proposed work attempted to provide a high secure data by optimizing the key generation for encryption and decryption process. Hybridization of a novel ECC (Elliptic Curve Cryptography) algorithm and homomorphic ElGamal algorithm for encryption and decryption and also employment of a bio-inspired Genetic algorithm for the generation of maximum secured key is performed. A random 128-bit hash have been developed for the generation of two input points to run the homomorphic property in the ElGamal algorithm secures the key and make it as a non-breakable one. The integrated property of ECC and the ElGamal associated with the Genetic algorithm makes the key more stabilized and a confidential one that is more resistant to the various kinds of attacks. The performance analysis depicted that the proposed technique outperforms the existing with respect to computational time.

Keywords: *Cloud computing, ElGamal, Elliptic Curve Cryptography, Genetic algorithm, cryptographic attacks, homomorphic property.*

1. Introduction

Cloud computing incorporates its role in analyzing, storing and maintaining, sharing and backing up several confidential information in all the fields. The major advantages of employing the cloud computing is its flexibility, scalability, minimized cost and time, efficient way of communication etc. Apart from that it Cloud Computing includes some of the computational operations through the cloud service provider. The accessions of mutual pool of resource on the demanded network have also accomplished. In recent years, industrial and academic sector widely utilize this Cloud Computing services. Privacy preservation is the method of preservation of data security in the cloud environment. For such preservation, there is need of authentication process like generation of key followed by encryption and decryption. In spite of various privacy preserving mechanism for protecting the sensitive information, no optimized secured encryption and decryption process had been developed yet.

The limitations of accession by multiple users, maintenance problem, insufficient storage of big data and cost efficiency must be overcome for better cryptographic results[1]. In this paper a kind of multi cloud setting that holds the confidential data have been set up. And also the public domain stores the information in the form of authentication. For the purpose a completely homomorphic encryption concept under ElGamal algorithm was enabled for the protection of highly sensitive data in the cloud. The method permitted few arithmetic operations such as multiplications and addition on the plain text thereby the encrypted data are manipulated.

ISSN: 2005-4238 IJAST

Homomorphic characteristics of cryptographic technique was utilized now a days in several security contexts like ElGamal based processing system, image sharing[2], ECC based data integration, computer distortion methods etc. In specific ElGamal and RSA possess homomorphic multiplication whereas Paillier and ECC possess homomorphic additions. The method of additive homomorphism have a wide use like reduction of average pixel and privacy preservation in the video through achieving wide ranged images and provide security in outsourced computation in cloud computing.

The figure 1 depicted the fundamental encryption and decryption process involved in the cryptographic communication.

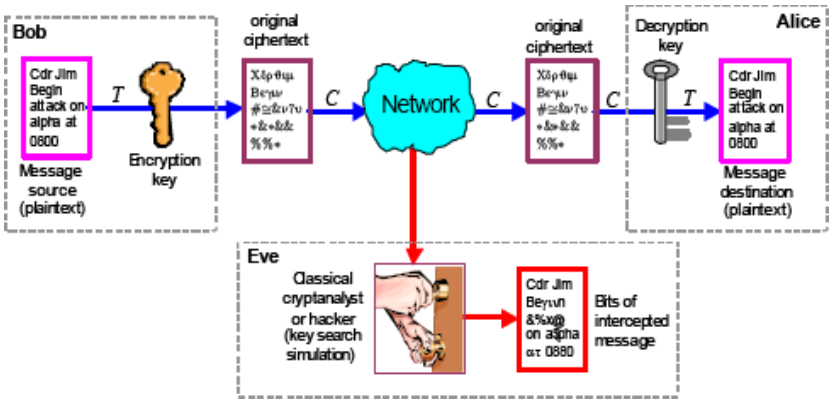

Figure 1. Cryptographic communication of data

1.1. Objective

- To provide a highly secured data with an optimized encryption and decryption process
- To hybridize novel ECC and homomorphic ElGamal algorithm for optimized encryption and decryption process.
- To utilize Genetic algorithm for key generation with better coefficient of autocorrelation and fitness function.
- To increase the efficiency by overcoming the cryptographic attacks like brute force attack, CPA,CCA and CCA2.

1.2. Organization of the paper

Initial section in this paper gives the detailed preview of why and what for the encryption and decryption is being used; Next section gives the survey of the existing literatures with reference to the development, evolution, and utilization of cryptographic technique with respect to ECC and homomorphic ElGamal algorithm; The third section gives the glimpse of the methods that were considered base for the extension and implementation of the proposed methodologies; Fourth section includes the crucial area of our proposed methodology with reference to cryptographic attacks; Fifth section gives the drawn conclusions out of the optimization/classification on the whole with reference performance metrics and future directions; and Final section discusses the references for the used texts and referred works.

2. Review of Existing Work

The section comprises a review of the existing works regarding the proposed system.

[3]presented a homomorphic scheme that supported a random arithmetic operation. The author of this paper aimed to transfer an input ciphertext to encrypted form with the

same plaintext with a greater modulus. The applications are further improved by still more optimizations. The research also attempted to optimize by taking advantage of NTT (Number Theoretic Transform) for rapid polynomial multiplication. [4] In this study, secure outsourcing of images is mainly focused. A secure architecture collected by two clouds first cloud is a private cloud dedicated for encryption/decryption and a second cloud is dedicated for storage. The first cloud was implemented for using open stack as a service concept in respecting the encryption. While applying the Watermarking algorithm the test of homomorphic property has been done. [5]This research utilized the ElGamal algorithm and RSA algorithm for homomorphic encryption. By using this method, the information was very confidential and secure. In homomorphic operation, the RSA was done for encryption and ElGamal strategies was done for decryption process. It takes more time for encrypting the information but it produces high security. In cloud, the data contains more secure by using hybrid encryption approach. [6]Investigated an arithmetic methodology which could perform homomorphic multiplication and addition calculation on the basis of ElGamal cryptographic system. The overall results when compared with the HElib stated that eventhough the processing duration for homomorphic addition raised by thirty-five percentage, the process time for homomorphic multiplication have been decreased to 1.8% and finally the time for calculation the variance was reduced to 15%. [7, 8]The demonstration of how to merge a fully homomorphic encryption scheme with linear decryption and a linearly homomorphic encryption scheme to acquire new properties. The first scheme is created with message-to-ciphertext length ratio and the scheme is based on hardness of Learning with Errors (LWE). The first general purpose secure function protocol preprocessing model is the additive factor of optimal insecure protocol. Fully-Homomorphic Time-Lock Puzzles construct for the first time-lock puzzle, from traditional principles, where one can test some task over a series of puzzles without solving them. [9]In this study the author propose a scheme for performing arbitrary depth homomorphic evaluations with the help of a special recryption box for module. Homomorphic encryption scheme performs until the noise in ciphertexts reaches a critical point. The researcher describes two different insanitation for recryption box to assist homomorphic evaluation arbitrary depth. The recryption box is used to boost the performance of encrypted operations. The 40 core Intel server can perform encrypted search in a table around 20 seconds. The implementation without recryption box is faster than 20 times approximately. [10] A feasible attack against a variant of recently proposed E1Gamal encryption scheme has been shown in this paper. Any adversary who has access to the underlying group's in the ElGamal encryption scheme would be able to mount such an attempt, culminating in the distributed cryptosystem being completely exposed to the secret key. [11] explored the homomorphic property and signified the observation of the suggested partition based cryptographic system. The paper attempted to reduce the computational time and compared it with the state of art methods. [12] currently, the fully homomorphic encryption approach has drawbacks of broad key size and poor calculation performance, and for safe cloud computing and this is not feasible. The suggested work developed a hybrid Cloud Computing method on the basis of additively homomorphic paillier algorithm and homomorphic RSA(multiplicative) encryption algorithm. A better encryption and decryption process that operates cloud by procedure form and uploads the ciphertexts to the public cloud. Calculation of the public cloud process, without knowing the exact data. The suggested works then conducts calculations and analyze the results and the results indicate the system is realistic and effective. [13]The goal is to provide security during client communication in the business organization where project information is performed by secured device. The sender needs to know the receiver's identity but not other information, such as a public key or certificate etc. the receiver

should have two components to decode a cryptographic code. Initially, the hidden key of the receiver contained in the computer system and second is some of the special hardware device and user, access to secure data with symmetric key is achieved. The proposed system used Elliptic curve cryptography to define two-factor authentication protocol is secure. The protocol provides participant mutual authentication. The consequence is that ciphertext can't be decrypted without these two restrictions. [22][23][24] presents survey of fully homomorphic encryption scheme since from privacy homomorphism of Rivest et al.[25] to post Gentry's FHE [26] scheme and also represent their significant somewhat homomorphic scheme's algorithm ,experimental results and security.

3. Proposed Methodology

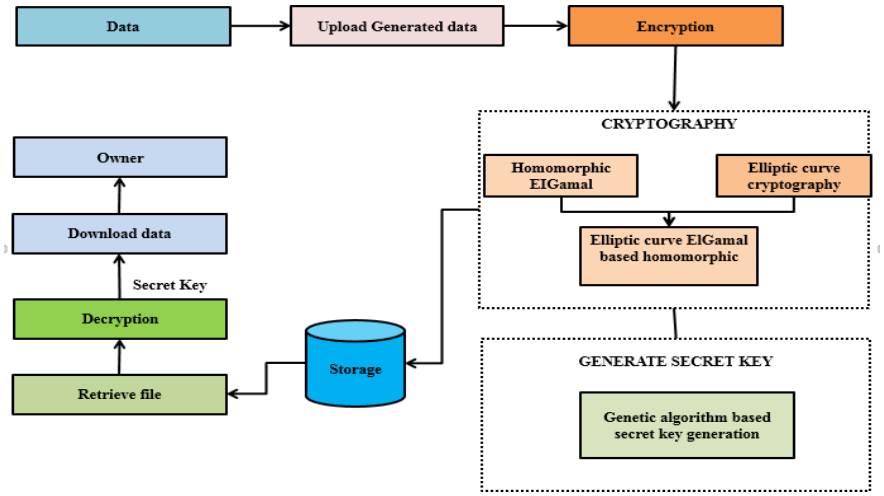

Figure 2. Overall proposed methodology of ECC-Elgamal technique

The figure 2 depicts the overall flow of proposed system. The proposed cloud system performs from data user side and service provider side. The service provider takes the overall responsibility for cloud environment. In this flow, the dataset is uploaded to cloud with more privacy. To achieve the highest security, the proposed system explicates with cryptography concept. In this concept, the encryption is done by using homomorphic ElGamal and Elliptic curve cryptography, which combines with Elliptic curve ElGamal based homomorphic method. This hybrid method processes with the secret key generation by using genetic algorithm. Our proposed novel ECC algorithm develops a random 128 bit hash that is involved in the generation of two input points (termed as elliptical curve point) that is used to run the elliptical curve. This Genetic algorithm method generates the secret key to access the document. The Genetic algorithm generates a six array in the form of random prime number that functions as initial seed value that is to be passed on to the Genetic algorithm. After encryption process the overall data is stored in cloud storage. To retrieve the file from data owner sider, the decryption process is required with secret key. Final download the data and sent to data owner.

3.1. EC Elgamal

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

The elliptic curve $y^2 = x^3 + ax + b$ over a point P could be denoted as $EC_p(a,b)$ is an abelian group. If the point $U = (x_u, y_u), V = (x_v, y_v)$ are

on $EC_p(a,b).W = U + V = (x_w, y_w)$. The addition of points on $EC_p(a,b)$. is equated in Eq (2)-(5) to be make $EC_p(a,b)$ into an abelian group. If U=V then W= 2U and for negative point U is calculated as $U = (x_u - y_u)$

$$x_w = (\lambda^2 - x_u - x_v) \bmod p \tag{2}$$

$$y_w = (\lambda(x_u - x_w) - y_u) \bmod p \tag{3}$$

$$\lambda = ((y_u - y_v)/(x_u - x_v)) \bmod p \; if \; U \neq V \tag{4}$$

$$\lambda = ((3x_u^2 + a)/(2y_u)) \bmod p \; if \; U = V \tag{5}$$

The equation 6 and 7 illustrate $Ej = njH$ in which $nj \in P$, $j = 1,2,\ldots.n.$ the additive homomorphic property (AHP), P–Prime finite field Fp. Because the n decryption a complex task that is equal to solve ECDLP(Elliptic curve discrete logarithm problem) the AHP of $E = nH$ may not possess practical implementation. Dec(x) denoted the decryption of x. Here

E – Ciphertext

E' and E" –ciphertext points of E. N – Plaintext

N' and N" – decrypted version of N T – Public Key point

T –Private key

H –Base point and $S1, S2 \cdots Sn$ are the integers of base points

$$\begin{aligned}(S' = S_1 + S_2 + \cdots Sn)\, E_1 + E_2 + \cdots + E_m &= n_1 H + n_2 H \cdots + n_m H \\ &= (n_1 + n_2 + \cdots n_m)H \\ &= Ct(n_1 + n_2 + ...n_m)\end{aligned} \tag{6}$$

$$\begin{aligned}Dec(E_1 + E_2 + \cdots + E_m) &= Dec\,(C_m(n_1 + n_2 + \cdots n_m)) \\ &= n_1 + n_2 + ...n_m\end{aligned} \tag{7}$$

The results specified the points on similar elliptic curve.

Encryption: $E' = N + sT, E'' = sH$ (8)

Decryption: $N' = E' - tE''$ (9)

In equation 8 the encryption of the similar plaintext point will develop ciphertext points with the use of various S, and hence the EC –ElGamal is efficient than other existing methods. The process in EC- ElGamal based on addition (between two points) is

$$\begin{aligned}&E_1 + E_2 + \cdots + E_m \\ &= (N_1 + s_1T, s_1H) + (N_2 + s_2T, s_2H) + \cdots + (N_m + s_mT, s_mH) \\ &= (N_1 + s_1T + N_2 + s_2T + \cdots + N_m + s_mT, s_1H + s_2H + \cdots + s_mH) \\ &= (N_1 + N_2 + \cdots + N_m + s_1T + s_2T + ...s_mT, s_1H + s_2H + ... + s_mH) \\ &= (N_1 + N_2 + ...N_m + (s_1 + s_2 + \cdots s_m)T, (s_1 + s_2 + \cdots + s_m)H) \\ &= (N_1 + N_2 + \cdots + N_m + s'T,\ s'H)\end{aligned} \tag{10}$$

$$\begin{aligned}Dec(E_1 + E_2 + .\cdots + E_m) &= Dec(N_1 + N_2 + .\cdots N_m + s'T, s'H) \\ &= N_1 + N_2 + \cdots + N_m + s'T - ts'H = N_1 + N_2 + \cdots . + N_m\end{aligned} \tag{11}$$

The elliptic curve describes an abelian group and various elliptic curves define various abelian groups. Based on the closure property of abelian group, when combining X and Y in same abelian group, also X + Y in group with respect to addition rules. Consider the X and Y in various abelian groups as group 1 and group 2, Z = X + Y combines to neither group 1 nor group 2. It proved that the contradiction method when Z∈ group 1, Y = Z – X

= Z + (-X), then R∈ group 1 that is conflicted with R ∈group 2. Likely, it proved that Z does not comprises in group 2. So, the additional point on different elliptic curves is not effective. So we consider only the additional points on same elliptic curves that has effective abelian property. For $C_i = (P_i + s_i Q, s_i S)$ is not point on $EC_P \pi(m,n)$ then the points are defined $P_i + s_i Q$ and $s_i S$ that not combines same elliptic curve but it contain another elliptic curve (c, d). Then c_i is decrypted, but $N_1, N_2, ...N_n$ does not contains same elliptic curve $C_1, C_2 ...$, establishes various elliptic curves and does not establishes in same abelian group. Therefore, the image pixel values transferred into the similar elliptic curve points before the use of additive homomorphism.

Assign u =11, a =1, b=6, that means the elliptic curve $y^2 = x^3 + x + 6 \ (mod\ 11)$.

And $H = (2, 7), N_1 = (5, 2), N_2 = (8, 3)$ were the two points a located on the curve $EC_{11}(1, 6)$.

Assumption of the *privatekeyt* $= 6$, obtained the public key point $T = 6H = 2(H + 2H)$ bythe above equation (2)-(5).

The following described the steps in detail.

For solving2H, compute

$$\lambda = ((3x_H^2 + a)/(2y_H))\ mod\ p = \left(\left(3(2^2)+1\right)/(2*7)\right) mod 11 = 8.$$

$$x_2 H = \left(\lambda^2 - x_H - x_H\right) \bmod p = \left(8^2 - 2 - 2\right) \bmod 11 = 5$$

$$y_2 H = \left(\lambda(x_H - x_{2H}) - y_H\right) \bmod p (8(2-5)-7) \bmod 11 = 2$$

For solving $3H = H + 2H$, calculate

$$\lambda = \left((y - y_2 H)/(x_H - x_2 H)\right) mod\ p = \left((7-2)/(2-5)\right)\ mod\ 11 = 2$$

$$x_3 H = \left(\lambda^2 - x_H - x_{3H}\right) mod\ p = \left(2^2 - 2 - 5\right) mod 11 = 8$$

$$y_{3H} = \left(\lambda(x_H - x_{3H}) - y_H\right) mod\ p = \left(2(2-8)-7\right)\ mod\ 11 = 3$$

For solving $T = 6H = 2(3H)$, compute

$$\lambda = \left(\left(3x_{3H}^2 + b\right)/\leq (2x_{3H})\right) mod\ 11 = (193/6)\ mod\ 11 = (6/6)\ mod\ 11 = 1$$

$$x_T = \left(\lambda^2 - y_{3H} - y_{3H}\right) \bmod q = \left(1^2 - 8 - 8\right) \times mod\ 11 = (-15) mod 11 = 7$$

$$y_T = \left(\lambda(y_{3H} - y_T) - x_{3H} mod\ q\right) = \left(1(8-7)-3\right)\ mod\ 11 = 9$$

Likewise, computation of for addition was also performed accordingly. The random number $s1 for N1 is 5, s2 for N2 is 7. Dec(y)$ denotes the decryption ofy

$$N_1 + N_2 = (5,2) + (8,3) = (3,6)$$

$$E_1 = (N_1 + s_1 T, s_1 H) = \left((5,2) + 5(7,9), 5(2,7)\right) = \left((7,9),(3,6)\right)$$

$$E_2 = (N_2 + s_2 T, s_2 H) = \left((8,3) + 7(7,9), 7(2,7)\right) = \left((7,9),(7,2)\right)$$

$$E_1 + E_2 = \left((7,9) + (3,6)\right) + \left((7,9),(7,2)\right)$$

$$= \left((7,9) + (7,9), (3,6) + (7,2)\right) = \left((2,4),(2,4)\right)$$

$$Dec\ (E_1 + E_2) = E1 - t * E2 = (2,4) - 6 * (2,4)$$

$$= (2,4) - (7,2) = (2,4) + (7, -2)$$

$= (2,4)+(7,9) = (3,6)$

Hence , $N_1 + N_2 = Dec(E_1 + E_2)$.

$N_3 = (1, 2)$ does not represented the curve point $C_{11}(1,6)$ and hence 22 (mod 11) (13+1 +6) mod 11, assumption of random number s3 for N3 is 2. $N_1 + N_3 = (5,9)$ also does not represented the curve point. $E_{11}(1,6)$. Likewise with the previous points T and H to encrypt N3, achieved $E_3 = (M_3 + r3K, r3G) = ((1,9),(5,2))$

$Dec(E_3) = (1, 9) - 6(5, 2) = (1, 2)$.

$E_1 + C_3 = ((3,2)),(7,2)), Dec(E_1 + E_3) = (3,9)$

$N_1 + N_3 \neq Dec(E_1 + E_3)$

The above example gives an illustration to the show that the additive homomorphism is only satisfied for the points on the same elliptic curve.

3.2. Genetic Algorithm

The Genetic Algorithm is an adaptive exploratory search technique which is based on mechanism of natural genetics and selection. It is used to evaluate the answers for many unsolved problems based on biological concepts such as crossover, inheritance, selection and mutation. Here, the cryptography is a traditional technique for safeguarding the data with parameters such as public key is used for encryption process and private key is used for decryption process. The genetic algorithm is implemented here to calculate the fitness value which is used in key generation.

Step 1. Initial generation of population:

A Genetic Algorithm starts with an indiscriminately developed individual set that is termed as initial population. This initial population array possess 192 bit and every bit have been assigned 1 or 0 value with respect to random development. If the value created from the generator is higher than 50 then the bit value 1 have been consigned or else 0 is assigned. The size of the chromosome cell showed the length of the key. The whole 192 bits were assigned randomly. The initial two dimensional population size greatly depends on the Max_populaiton value that is defined as macro. The following are the data structures involved:

initPop [MAX_POPULATION][192], final Pop [MAX_POPULATION][192]

Step 2. Estimation of Chromosomal number and Threshold checking:

All the chromosome must achieve a threshold standard, that depict that the above average chromosome must possess large number of population copies, whereas the below chromosomes have been deleted on the basis of threshold.

For all the chromosome, a particular number have been estimated, and if the value id more than the threshold value the respective chromosome have been chosen otherwise it is rejected. Such threshold checking was done in the upcoming stages also.

Step 3. And now occurs the entering of GA into a loop. At the iteration end, a set of new population is being synthesized by the application of some stochastic operators to the earlier population. Every kind of such iteration have been termed as a generation.

Step 4. Process of Selection and Crossover:

Initially an operator for selection have been applied, from which the 2 parents have been chosen arbitrarily from the initial population. The chosen parents have been utilized for the production of individuals for the upcoming generation by applying the crossover operator.

In case of binary string individuals, single point, two point and uniform crossover have been frequently utilized. For the application of crossover operator, the parents are joined

together with one point ring crossover. These two parents have been joined in ring form and the generation of random cut point have been generated. As per the cutting point (C1[ ] array) (one of children)was generated in a clockwise and the other(C2[ ] array) have been created in the anticlockwise direction. All the position of the child should regain a value present in the respective position and the corresponding child should be a valid permutation. When the crossover is complete the threshold check is done.

Step 5. Mutation:

The application of mutation operator where the child is changed randomly from what the corresponding parents have been generated in crossover. The number of mutation have been estimated with the above equation. So the number of Mutation = (192 * 200 * 0.5) ÷ 200 = 96

Step 6. Estimation of key Fitness:

The previous steps have been repeated till the final population array becomes full. The chromosomes in the end population have been ordered as per the fitness values and the chromosome with the high value of fitness was chooses.

Recovery of the key: Among the quantum algorithms a third root time algorithm was impacted by the combinatorial attack. Hence the proposed algorithm must be sufficient to rule out such combinatorial attacks.

3.3. Cryptographic Attacks

The following section presents the proposed system is secure from the following attacks observed in the experimental results

A. Brute Force attacks

It is a type of attack which gains the access to any password protected server or websites by using different combination of passwords or username repeatedly until the site or server opens up. It is similar to an military attacking a fort.

B. Passive attacks

It is type of network attack where the system is scanned to find open vulnerabilities and ports. It is mainly to gain knowledge on the target instead of editing or distributing the target.

C. CPA

CPA is expanded as Chosen Plaintext attacks which assumes that, the hacker gain information which minimizes the designed encryption . Since the proposed system is implemented on the basis of ECC and ElGamal cryptosystem, it is highly complex for the illegal user for the computation of secret key of user using the equation (4) and(5).Another complexity have also been found for the intruder in obtaining the system developed randomized number r_1 and r_2 from the following two equations, which are $xw = (r_1 - x_u - x_v) \bmod p \; y_w = (r_2 (x_u - x_w) - y_u) \bmod p$ .The complexity depends on the evaluation of discrete algorithm over the finite area.

If few pairs of plaintext and ciphertext (N_j, E_j) is being known by the intruder ,they could achieve .But there exists complexity for the intruder to derive x_w *and* y_w. Apart from that the intruder could not able to achieve x_w and hence y_w.The system security depends upon the complexity in the determination of composite add operation. Hence λ is a nonlinear equation, the hackers may possesses complexity the plaintext pieces in spite of the availability of (N_j, E_j).These analysis reviewed that our proposed method is against such described attacks.

D. CCA

CCA is Chosen Cipher text attack where the generic cryptanalysis check the feasibility of attacks at the decryption stage and the possibility of information gathered at a time of decryption. By this, he guides his team to produce a strong key and maintain it as secret for decryption. It is depicted that proposed work obtains indistinguishability under adaptive CCA attack. MAUC be a message authentication scheme, ASYM - encryption scheme.

For any number also, t,N',N,

$Adv^{cca}_{MAUC}(t,q,\mu,N) \le Adv^{ASYM}(t_1,0,N)$

$Adv^{cca}_{MAUC}(t_2,q,\mu,N) \le Adv^{MAUC}(t_3,q-1)$

In which

$t1 \in O\left(t + TIME\uparrow + TIMEMAUC : gen(m')\right)$,

t2 ∈ O(t + TIME ASYM:enc(N) +TIME MAUC:gen(N')),

$t3 \in O(t + TIME + TIME\ MAUC : gen(N') + TIME\ ASYM : enc(N) + q)$.

Assuming ASYM and MAUC are secured,H is the hard core with CCA attack. Adverse A defeats CCA2 security.

If g^v represents the recipient public key

$y = N \| E' \| tag'$ is the challenge ciphertext where the A algorithm is in the guess stage. Considering

Type 1 query as $N \| E' \| tag'$ and

Type 2 query as $N \| E' \| tag'$ (Here $N \neq N'$)

Considering 2 cases that depends on the condition, whether the result/output of H seems random and If there is y^0 (Type 1 query) to ASYM.decsk which means ASYM.decsk ($(y') \neq BAD$)

Case 1

If the output of H is randomized and there is y^0 (Type 1 query) to ASYM.decsk which means ASYM.decsk $(y') \neq BAD$. Here an adversary F is presented that is involved in the breakage of MAC. Case 2

If the output of H is randomized and there is y^0 (Type 1 query) to ASYM.decsk which means ASYM.decsk $(y') \neq BAD$. Here an adversary B is presented that is involved in the breakage of ASYM.

E. CCA2

It is an adaptive form of CCA, here the hacker sends a code to be decryption and utilizes the output of a target followed by repeated queries until it reveals or enables its access.

F. Device anonymity absence

Leakage of the data that are device specific could enable the attacker for tracking the login history and present location of the device. Further, the anonymity property would make the authentication process stronger. In general, the anonymity could be preserved by concealing the valid identity of the invention. But Kalra and Sood's method is breakable mainly due to that the attacker may be able to track the logging device had been monitored by the login request message.

G. Offline password guessing attack

If an attacker was supposed to get a cookie data C'k from Edi(the embedded device).Assumed the attacker interrupts the response message of the CS' as depicted in the figure 3.

It is found that the by means of intercepted information from an open channel (P3 ,Ti, P4), the attacker could achieve the Pwi(obtain Edi 's password).

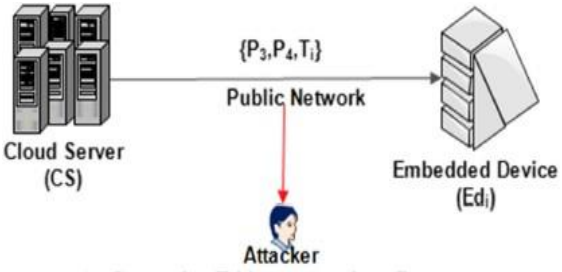

Figure 3. Offline password guessing attack

H. Insider attack

The cloud server developed a discrete password for all the Edi during the registration and consequently there exists a chance of misusing it, which is termed as an insider attack.

I. Stolen-verifier attack

The attacker may hack the database record from the cloud server and could use the data for mounting server impersonation attack. When Edi passes the information to the corresponding cloud server, the attacker attempts to interrupt and block the data from reaching the server. In due course, the attacker chose a random ra and evaluated the {P3a, P4a, Ti} to Edi. From this information, the password could be easily generated by the attacker. The attacker is thereby successful in the imitation as a server with the use of stolen verifiers of Edi.

J. Ruling out combinatorial attacks

When the encrypted information is provided with the corresponding noise value is utilized for recovering the secret key. Apart from that, a birthday algorithm may also exhaustively permit the recovery of the key. Among the quantum algorithms, a third root time algorithm was impacted by the combinatorial attack. Hence the proposed algorithm must be sufficient to rule out such combinatorial attacks.

4. Results and Discussion

The implementation of the proposed work is performed in Windows 8.1 Pro N with Intel(R) Core (TM) i3-7100 CPU@ 3.90GHz,8 GB RAM and a system type of 64-bit operating System (x64 – based processor) and developed in PYTHON 3.6 with ANACONDA navigator.

4.1. Performance analysis for uploading speed and security overhead

In general the uploading speed has been calculated as the time taken for the transmission of data files from the personal computer to the internet. In the study, the uploading speed is estimated by the transmission of encrypted data to the cloud by the Cloud Unit. On the basis of the rate of bandwidth(100 mpbs), the speed from uploading differ under various traffic load. The upload speed is estimated for the file size ranging from 0.1 to 500 MB. The estimated upload speed for the proposed system ranges from 9.05 to 12.9(Mb/s). The above description is clearly shown in the figure 4 and table 1.

Table 1. Uploading speed for the proposed and the existing system

Uploading speed (Mb/s)		
File size (MB)	Existing work[14]	Proposed work(Mb/s)
0.1	11.5	9.05
0.5	12	10
1	11.9	10.2
10	12.92	11.3
50	12.5	11
100	13	12.8
250	13	12.8
500	13	12.9

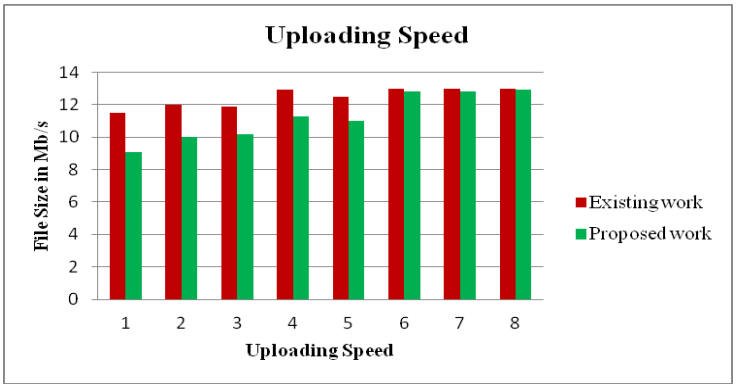

Figure 4. Uploading speed for the proposed and the existing system[14]

Table 2. Security overhead of the proposed and the existing system

Security overhead (%)		
File size (MB)	Existing work[14]	Proposed work
0.1	19	18.8
0.5	18.8	18
1	18	18
10	15	15
50	14	14
100	13	13
250	13	13

In any ECC technique, there exists a delay over TTP-CS(Trusted Third Party – Cryptographic server) side because of the security overhead(SO). The SO in percentage is termed as the security operation time which divides the transmission time of the file. The Table 2 and figure 5 displayed that the percentage is constant for more number of files. The observed results showed that the larger the size of the file, the smaller the SO with respect to percentage.

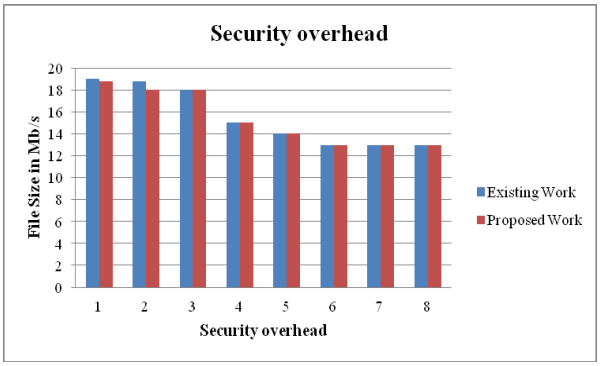

Figure 5. Security overhead of the proposed and the existing system [14]

Table 3. Comparative analysis of approximate costs of the selected schemes including proposed Scheme

Schemes	**Authentication phase**	
	Client	Server
[15]	$4T_{EM}+4T_H$	$4T_{EM}+5T_H$
[16]	$3T_{EM}+5T_H$	$3T_{EM}+5T_H$
[17]	$2T_{EM}+2T_{EM}+3T_H$	$T_{EM}+T_{EM}+2T_H$
[18]	$3T_{EM}+2T_H$	$2T_{EM}+2T_H$
Proposed	$3T_{EM}+T_H$	$2T_{EM}+T_H$

The provided framework utilizes the Elliptical Curve Cryptography with 256 bits with no timestamps so that additional time synchronization complexity between the server and the client is prevented. Let TH, TEM and TME be the cost of doing one hash computation, one ECC point multiplication operation and one modular exponentiation operation respectively. The cost of doing the operation is negligible. Then, TME > TEM > TH. Nonces have been employed for the reply attack prevention. From the table 3 the provided method possesses considerable reduction of cost when compared with the other existing system. From the results it is proved that the authentication phase of the proposed system seems to be better than the existing methods.

Table 4 provides the comparison of the generation of key with various technique namely AES method, CL-PRE scheme, PRE scheme certificateless encryption. Overall findings from the figure depicted that the proposed system efficiently reduced the time taken for the processing the data.

Table 4. Observation of the time consumption for key generation

Number of users	**Methodologies time in seconds)**					
	CLPRE [19]	Certifice Less Encryption [20]	PRE [20]	AES[21]	EC [14]	Proposed
10	1.494	1.594	1.534	0.004	0.00212	0.00211
20	1.598	1.741	1.606	0.00425	0.00235	0.00223
30	1.673	2.321	1.684	0.00476	0.00286	0.00266
40	1.791	1.888	1.799	0.005	0.00302	0.00282
50	1.907	1.952	1.866	0.00512	0.00328	0.00305
60	1.954	2.193	1.923	0.0055	0.0035	0.00319
70	1.994	2.286	2.034	0.00598	0.00398	0.00348
80	2.092	2.694	2.129	0.00632	0.00427	0.00389
90	2.401	2.827	2.388	0.00664	0.00463	0.00428
100	2.495	2.887	2.545	0.00697	0.00499	0.00476

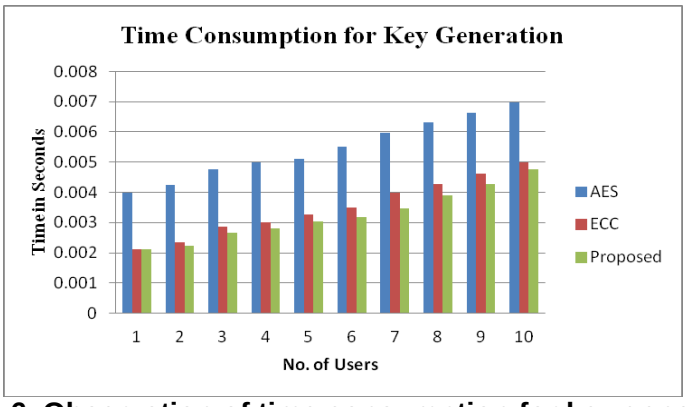

Figure 6. Observation of time consumption for key generation

5. Conclusion

A security scheme for data sharing through the cloud served system was formulated in this paper. The proposed methodology used novel ECC algorithms that have been integrated with the homomorphic properties of ElGamal algorithm. The advantages of both the algorithm provided an opportunity for the synthesis of novel unbreakable key from encryption and decryption process. A bio inspired genetic algorithm was employed for the key generation thereby the overall combination prevents the cryptographic attacks like brute force attack, CPA, CCA and CCA2. The performance analysis of the proposed system outperforms the existing in terms of computational time. The future work deals with the implementation of the proposed cryptographic technique for multimedia data.

References

[1] S. Prakash, N. Andola, and S. Venkatesan, "Secure access of multiple keywords over encrypted data in cloud environment using ECC-PKI and ECC ElGamal", In 2017 International Conference on Public Key Infrastructure and its Applications (PKIA), **(2017),** pp. 49-56.
[2] K. El Makkaoui, A. Beni-Hssane, and A. Ezzati, "Cloud-ElGamal and Fast Cloud-RSA Homomorphic Schemes for Protecting Data Confidentiality in Cloud Computing", International Journal of Digital Crime and Forensics (IJDCF), vol. 11, **(2016),** pp. 90-102.
[3] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers", in International Conference on the Theory and Application of Cryptology and Information Security, **(2017),** pp. 409-437.
[4] M. Ibtihal and N. Hassan, "Homomorphic encryption as a service for outsourced images in mobile cloud computing environment", in Cryptography: Breakthroughs in Research and Practice, ed: IGI Global, **(2020),** pp. 316-330.
[5] D. Chandravathi and P. Lakshmi, "A New Hybrid Homomorphic Encryption Scheme for Cloud Data Security", Advances in Computational Sciences and Technology, vol. 10, **(2017),** pp. 825- 837.
[6] T. Jogan, T. Matsuzawa, and M. Takeda, "Acceleration of Homomorphic Arithmetic Processing Based on the ElGamal Cryptosystem", Communications and Network, vol. 11, **(2019),** pp. 1.
[7] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain", IEEE Access, vol. 6, **(2018),** pp. 20632-20640.
[8] Z. Brakerski, N. Döttling, S. Garg, and G. Malavolta, "Leveraging linear decryption: Rate-1 fully-homomorphic encryption and time-lock puzzles", in Theory of Cryptography Conference, **(2019),** pp. 407-437.
[9] S. S. Roy, F. Vercauteren, J. Vliegen, and I. Verbauwhede, "Hardware assisted fully homomorphic function evaluation and encrypted search", IEEE Transactions on Computers, vol. 66, **(2017),** pp. 1562-1572.
[10] F. Y. Rao, "On the security of a variant of ELGamal encryption scheme", IEEE Transactions on Dependable and Secure Computing, **(2017).**
[11] A. Chatterjee and I. Sengupta, "Sorting of Fully Homomorphic Encrypted Cloud Data: Can Partitioning be effective", IEEE Transactions on Services Computing, **(2017).**

[12] X. Sun, P. Zhang, J. K. Liu, J. Yu, and W. Xie, "Private machine learning classification based on fully homomorphic encryption," IEEE Transactions on Emerging Topics in Computing, **(2018).**
[13] A. L. E. Britto and N. U. Maheshwari, "Enhanced multicomponent data secure mechanism for cloud storage system using elliptical curve cryptography", Advances in Natural and Applied Sciences, vol. 11, **(2017),** pp. 520-528,
[14] V. S. V. Hema and R. Kesavan, "ECC Based Secure Sharing of Healthcare Data in the Health Cloud Environment", Wireless Personal Communications, vol. 108, **(2019),** pp. 1021-1035,
[15] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers", Pervasive and Mobile Computing, vol. 24, **(2015),** pp. 210-223,
[16] M. Qi and J. Chen, "An efficient two-party authentication key exchange protocol for mobile environment", International Journal of Communication Systems, vol. 30, **(2017),** pp. e3341,
[17] B. L. Chen, W. C. Kuo, and L. C. Wuu, "Robust smart-card-based remote user password authentication scheme", International Journal of Communication Systems, vol. 27, **(2014),** pp. 377- 389.
[18] S. Chatterjee and S. G. Samaddar, "ECC Based Remote Mutual Authentication Scheme for Resource Constrained Client in Cloud", In International Conference on Computational Intelligence, Communications, and Business Analytics, **(2018),** pp. 374-387.
[19] L. Xu, X. Wu, and X. Zhang, "CL-PRE: a certificateless proxy re-encryption scheme for secure data sharing with public cloud", in Proceedings of the 7th ACM symposium on information, computer and communications security, **(2012),** pp. 87-88.
[20] S. H. Seo, M. Nabeel, X. Ding, and E. Bertino, "An efficient certificateless encryption for secure data sharing in public clouds", IEEE Transactions on Knowledge and Data Engineering, vol. 26, **(2013),** pp. 2107-2119.
[21] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, et al., "SeDaSC: secure data sharing in clouds", IEEE Systems Journal, vol. 11, **(2015),** pp. 395-404.
[22] V. Biksham and D. Vasumathi, "An efficient symmetric algorithm for data security in cloud computing security using Homomorphic Encryption scheme", International Journal of Applied Engineering Research(IJAER), vol. 12, no. 21, **(2017),** pp. 10477-10484.
[23] V. Biksham and D. Vasumathi "Homomorphic Encryption Techniques for securing Data in Cloud Computing: A Survey", International Journal of Computer Applications (IJCA), vol. 160, no .6, **(2017),** pp. 1-5. DOI: 10.5120/ijca201791306
[24] V. Biksham and D. Vasumathi, "Query based computations on encrypted data through homomorphic encryption in cloud computing security", International Conference on Electrical, Electronics, and Optimization Techniques(ICEEOT), Chennai, **(2016),** pp.3820-3825.doi:10.1109/ICEEOT.2016.7755429.
[25] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms", Foundations of secure computation, vol. 4, no. 11, **(1978),** pp**.** 169-180.
[26] C. Gentry, "Fully homomorphic encryption using ideal lattices", In STOC, vol. 9, no. 2009, **(2009),** pp. 169-178.