Ekoloji 28(107): 665-677 (2019)

Environmental Benefits of Enhanced Hecc- Elgamal Cryptosystem for Security in Cloud Data Storage Using Soft Computing Techniques

T. Devi [1]*, R. Ganesan [2]

[1] Research Scholar, SCSE, Vellore Institute of Technology, Vandalur – Kelambakkam Road, Chennai, Tamil Nadu – 600 127, INDIA

[2] Associate Professor, SCSE, Vellore Institute of Technology, Vandalur – Kelambakkam Road, Chennai, Tamil Nadu – 600 127, INDIA

* Corresponding author: devi.janu4u@gmail.com

Abstract

Cloud services is used by many organizations and it has captured a major segment of the competitive market today. The green, or eco-friendly, aspect of the cloud is one of the most multifaceted advantages of cloud computing. The environmental advantages of cloud services include: reducing a firm's carbon footprint, data center efficiency, dematerialization, saving green, educed electricity use and so on. Even with its unprecedented growth, the question of security is also of paramount concern among the users of cloud services. There is a huge demand for new protocols and tools in order to enhance and assess the security strength of its service. Notwithstanding the present methods used for encrypting the files in cloud they are not highly efficient. Hence this enhanced technique is proposed to overcome all these challenges and improve the environmental benefits. In this method, initially the authentication of the user is verified. Once the authentication of the user is verified successfully dual encryption is performed on the cloud stored files using ElGamal cryptosystem and Hyper Elliptical Curve Cryptography (HECC). The aim for using the proposed system is for analysis of security which can be enhanced through the technique of sharing many keys amongst the two parties. Integer selection is an important attribute which defines the proper security to the cloud storage. For ensuring high security, this integer selection is performed by utilizing BAT algorithm. After the encryption, the suggested technique uses the HECC algorithm. In HECC, key generation is done by point addition and point doubling based elliptic curve cryptography. The dual encryption in this method provides efficient security to the cloud data. The proposed technique performance is evaluated in reference with environmental protection, storage cost, computation cost and execution time and is implemented in JAVA. The experimental results show the efficacy of the system as it utilizes only less time for both encryption and decryption of sensitive data.

Keywords: environmental benefits, cloud services, ElGamal cryptosystem, Hyper Elliptical Curve Cryptography, BAT algorithm, point addition, point doubling and elliptic curve cryptography

Devi T, Ganesan R (2019) Environmental Benefits of Enhanced Hecc- Elgamal Cryptosystem for Security in Cloud Data Storage Using Soft Computing Techniques. Ekoloji 28(107): 665-677.

INTRODUCTION

Cloud Computing evolved through the distributed software architectures scalability and extensibility (Khan and Al-Yasiri 2016). According to the National Institute of Standards and Technology (NIST) definition, "the cloud computing is a model for enabling convenient, resource pooling, ubiquitous, on-demand access which can be easily delivered" (Singh et al. 2016b). It is transforming ways to hardware and software design and procurements activities. Services without cost, elasticity of resources, accessibility through internet etc. are some of the benefits that cloud technology offers. With all of the recent buzz about cloud computing, companies have learned that by switching to a public cloud, they can gain flexibility and scalability while simultaneously cutting costs. But what they may not realize is that the cloud not only benefits their workplace, but also, the environment. Managing and processing data on a local server greatly increases carbon emissions. Almost all enterprises (big or small) are aiming towards enhancing businesses and tie-ups with other enterprises through the use of cloud technology (Vurukonda and Rao 2016); SaaS, PaaS, Iaas and Private, Public, and Hybrid are the service and deployment models respectively. One of the key reasons why it faces more security problems is due to high availability to end users. So, security issues from cloud provider send and security issues from

Received: 4 Aug 2017 / Accepted: 2 Jul 2018

Customers end are the two types of security related problems (Manogaran et al. 2016). Confidentiality of data comprises of data privacy of only valid and authorized access of data that are sensitive. Data integrity comprises of data content which can be achieved only through consistency and accuracy. Fool proof storage, type of storage, plans for disaster recovery and backup are covered under data availability (Shaikhand Sasikumar 2015a, Al-Sharif, 2017).

Hence, organizations that implement Cloud Computing and Big Data are faced with critical issues of security, trust, privacy and environmental issues. While businesses are aiming to achieve both cost and operational efficiencies through cloud, it is paramount to enforce the system design and deployment based on current security practices (Chang et al. 2016). Hence the importance of security concerns on the development and exploitation of information systems has never stopped growing. Today, the very fact that information Systems are used everywhere have made them more vulnerable to information security attacks. It is obvious that this kind of attack would result in heavy loss of money, time and other precious resources (Jouini and Arfa Rabai 2016). With an aim to tackle such security challenges, the European Network and Information Security Agency (ENISA 2009) made a survey. And loss of governance and compliance risks was among the two key risks to such vulnerability (Rasheed 2014). Data security can be ensured through customers handle processes such as control of access, management of key, encryption, and decryption (Wei et al. 2014). Prior to outsourcing to the cloud, sensitive data are supposed to be encrypted for the privacy of users (Gupta 2014, Eryılmaz and Ece 2016).

Climate impact is greatly reduced by the clouds improvement in energy efficiency as a result of fewer carbon emissions. According to AWS, "the average corporate data center has a dirtier power mix than the typical large-scale cloud provider." AWS, in combination with other cloud providers, use a 28% less carbon-intense power mix. This also affects climate control costs, since it is much more expensive to run machines at peak performance levels in perfect temperature levels. The cloud eliminates this wasteful spending due to the use of energy efficient equipment and fewer carbon emissions. For data operations and transmissions, security measures must be established otherwise data are considered to be at very high risk. Accessibility of stored data is granted for a group of users and hence possibility of having high data risk is more (Rao and Selvamani 2015). Prior to running Map Reduce tasks, the Hadoop security makes it mandatory for a user to log on to each cluster. This process is apparently not convenient for the users. Therefore, a common solution is very much necessary for concealing the particulars of the system's architecture and also not to burden the users with such tedious tasks (Zhao et al. 2014). Thus, software security engineering is supposed to be a promising service which will fulfill such requirements. It aims to provide security measures such as methods and tools, design, examination of vulnerability, testing and metrics (Ramachandran 2016). Notwithstanding the aforementioned points, the cloud service providers (CSP) security measures are usually obvious to the organizations. The occurrence of large numbers of users that are not related to the organizations further exacerbates the concern (Ali et al. 2015). Finally, a trust model comprising of trust value is proposed by researchers in order to enable estimation of the strength of cloud service security. Arecord of parameters covering all appropriate features of security helps in the evaluation of trust value (Shaikh and Sasikumar 2015b). Hence security is provided to the data stored in cloud.

LITERATURE SURVEY

To assess the environmental impact of cloud computing, Microsoft engaged with Accenture—a leading technology, consulting and outsourcing company— and WSP Environment & Energy—a global consultancy dedicated to environmental and sustainability issues—to compare the energy use and carbon footprint of Microsoft cloud offerings for businesses with corresponding Microsoft on-premise deployments. The analysis focused on three of Microsoft's mainstream business applications—Microsoft Exchange®, Microsoft SharePoint® and Microsoft Dynamics® CRM. Each application is available both as an on-premise version and as cloud-based equivalent. 2 The team compared the environmental impact of cloud- based vs. on-premise IT delivery on a per-user basis and considered three different deployment sizes—small (100 users), medium (1,000 users) and large (10,000 users). The study found that, for large deployments, Microsoft's cloud solutions can reduce energy use and carbon emissions by more than 30 percent when compared to their corresponding Microsoft business applications installed on-premise. The benefits are even more impressive for small deployments: Energy use and emissions can be reduced by more than 90 percent with a shared cloud service.

Several key factors enable cloud computing to lower energy use and carbon emissions from IT:

• Dynamic Provisioning: Reducing wasted computing resources through better matching of server capacity with actual demand.

• Multi-Tenancy: Flattening relative peak loads by serving large numbers of organizations and users on shared infrastructure.

• Server Utilization: Operating servers at higher utilization rates.

• Data Center Efficiency: Utilizing advanced data center infrastructure designs that reduce power loss through improved cooling, power conditioning, etc.

Though large organizations can lower energy use and emissions by addressing some of these factors in their own data centers, providers of public cloud infrastructure are best positioned to reduce the environmental impact of IT because of their scale. By moving applications to cloud services offered by Microsoft or other providers, IT decision- makers can take advantage of highly efficient cloud infrastructure, effectively "outsourcing" their IT efficiency investments while helping their company achieve its sustainability goals. Beyond the commonly cited benefits of cloud computing— such as cost savings and increased agility—cloud computing has the potential to significantly reduce the carbon footprint of many business applications.

RDA method proposed by Sookhak et al. (2016) was based on features of algebraic signature. The cost of computation and communication incurred are minimum. Divide and Conquer Table (DCT) presented by them could sustain dynamic data operation and applicable even for data storage in a comprehensive way. The proposed RDA techniques have proven to be more enhanced in terms of security and efficiency with least cost of computation and communication on the server and the auditor.

The cryptography approach proposed by Rohini et al. (2017) impedes cloud service operators to get to the partial data directly. In this approach, file is divided and subsequently data is stored separately. In order to find whether the data packets require to be divided for reducing operation time, an alternative approach was developed.

Zhang et al. (2016) proposed a method named match-then-decrypt. As the name indicates, an additional phase called as a matching phase was introduced prior to the decryption phase. That technique worked by computing special components in cipher texts, which were used to perform the test that if the attribute private key matched the hidden access policy in cipher texts without decryption. The purpose of this process was to expedite the process of decryption by facilitating the pairing aggregation. An anonymous ABE construction was proposed and a security-enhanced extension was then obtained. During the process of attribute matching, the cost involved for computation was less than decryption operation.

The aim of the method proposed by Batista et al. (2016) was to define QoS-driven approaches for cloud environments depending on the performance evaluation results wherein security procedures of different types were employed. An extra overhead was forced upon as part of security mechanism. In spite of the overhead imposed, results prove that cloud environment was feasible to sustain the service performance. This was accomplished through a change in the virtualized computational resources directly affecting the response variables.

Yang et al. (2016) studied the GNFS algorithm in cloud with the primary focus was on solving large and sparse linear systems over GF (2). And to make communication cost more efficient, the Parallel block Wiedemann algorithm was then proposed. For accelerating different steps, the proposed algorithm comprises of strip, cyclic and improved strip partitioning. The proposed algorithm showed enhanced performance of GNFS in regards to execution time and speedup.

The primary focus of Singh and Pasupuleti (2016a) was the third party data-integrity verification for the client's data on cloud storage server (CSS). The cloud storage server is vulnerable to malicious insiders attack and hence the third party auditing protocol was enhanced to make it resistant to such attacks. A protocol was also proposed which can execute operations at block-level and fine-grained dynamic-data update. Analysis on the proposed method proved that it works efficiently for such attacks.

A multilevel classification model was presented by Hussain et al. (2016). The proposed model encompassed Low, medium and high levels of risks related to various cloud services. The cloud layers position determined the intensity of those risk levels with lower layers prone to more severe attacks. BAT algorithm (VenkateswaraRao and Venkateswarlu 2017) stands as one of the important optimization techniques available in literature.

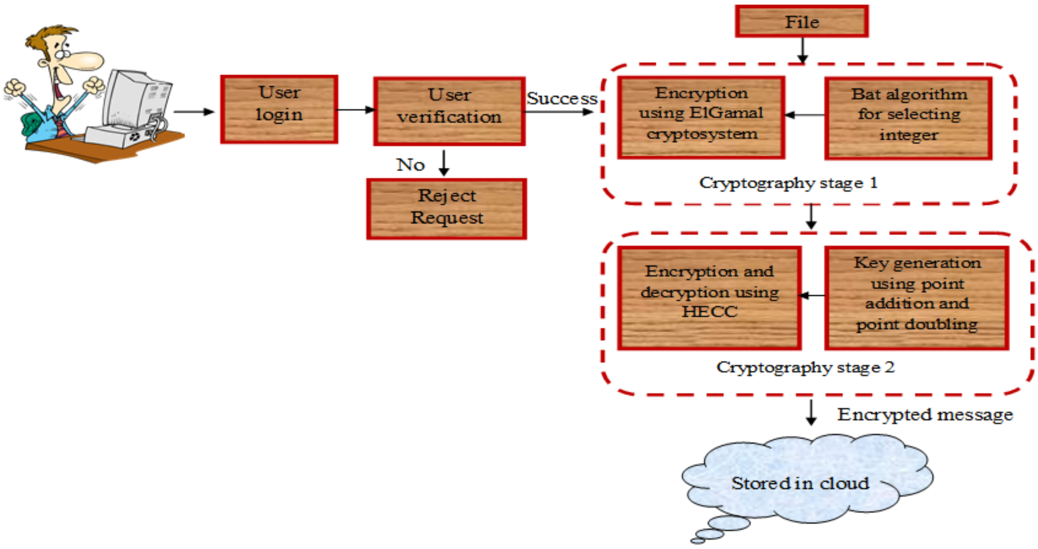
File
User login
User verification
Success
No
Reject Request
Encryption using ElGamal cryptosystem
Bat algorithm for selecting integer
Cryptography stage 1
Encryption and decryption using HECC
Key generation using point addition and point doubling
Cryptography stage 2
Encrypted message
Stored in cloud

Fig. 1. The semantic structure of recommended technique

PROPOSED METHODOLOGY

Virtualizing makes cloud computing very cost efficient and has made it very promising for the research communities. Today, the world of core business processes has a lot of dependency on Cloud computing. But it is very vulnerable to attacks since it is internet based. Therefore the issue of security is of paramount concern. That is why Cloud security has attracted attention of the research community. With ElGamal cryptosystem, data owner will first encrypt the index that is searchable and for double encryption the Hyper Elliptical Curve Cryptography is utilized. In ElGamal cryptosystem the integer selection is an important attribute which defines proper security to the cloud storage. For ensuring high security, this integer selection is performed by utilizing BAT algorithm which is an optimization approach. Further for encryption and decryption, the hyper elliptical curve cryptography and ElGamal cryptosystem are incorporated. In ElGamal cryptosystem we employ an additional divisor factor which aids to enhance security along with the normal curve equation. The explicit formula for point doubling and point addition in HECC is subjected to modification in hyper elliptic curve. The suggested technique overall semantic architecture is shown in **Fig. 1**.

The new-fangled technique flows through two main process such as the authentication and dual encryption. In the authentication process, the user authentication is examined. Thereafter, the input message is subjected to dual encryption by means of the ElGamal and HECC technique. The total process of the dual encryption is broadly discussed as follows.

ElGamal Cryptosystem for Encrypting Messages

ElGamal cryptosystem provides the advantage of encrypting large messages. In a large prime modulus, the process of encryption depends on the challenge of computing discrete logs. And every time it is encrypted, cipher text given varies by the same plaintext. The ElGamal cryptosystem operates as follows,

In ElGamal cryptosystem every user chooses their own secret keys such that,

$$k_i \in [1, n-2) \tag{1}$$

where,

n - Prime number

The associated public key is then indicated by,

$$p_k = c^{k_i} mod n \tag{2}$$

where,

c - Primitive root or generator

For encrypting a large message using ElGamal cryptosystem, the sender calculates s and t as follows,

$$s = c^j mod n \tag{3}$$

$$t = M.p_k{}^j mod n \tag{4}$$

where,

$$j \in [1, n-2)$$

Now for decryption the receiver can decrypt the cipher s and t by computing,

$$M = t.(s^{k_i})^{-1} mod n \tag{5}$$

Depending on the aforementioned steps, ElGamal cryptosystem functions. And to make the phenomena

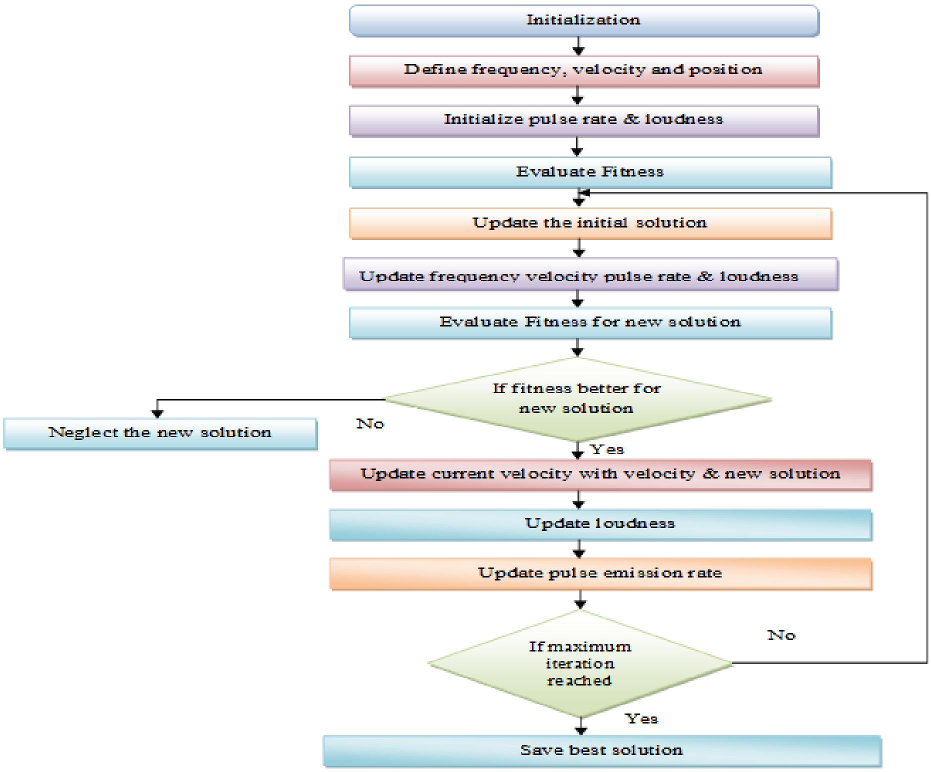
Initialization
Define frequency, velocity and position
Initialize pulse rate & loudness
Evaluate Fitness
Update the initial solution
Update frequency velocity pulse rate & loudness
Evaluate Fitness for new solution
If fitness better for new solution
No
Neglect the new solution
Yes
Update current velocity with velocity & new solution
Update loudness
Update pulse emission rate
If maximum iteration reached
No
Yes
Save best solution

Fig. 2. Flowchart of Bat algorithm

more secured we have utilized some changes in normal ElGamal steps by utilizing an optimization algorithm. In our technique, for choosing the integer values in the process of ElGamal encryption we have used bat algorithm to optimize the selected values which will help in securing the message more. The detailed explanation of this algorithm is as follows:

Bat Algorithm (BA)

Optimization algorithms are necessary to find local minimum and extends the analysis to global minimum. One of the novel evolutionary algorithm that is based on population and at the same time utilizing the echolocation behavior of bats is BAT algorithm. The prey of bats can be reached based on the distance calculated using the echolocation activities of bats. As every bat produces some sound and regulates the coldness of the prey by means of the echo (high frequency ultrasonic sound) from that prey.

Hence BA exploiting such echolocation feature depends on certain significant parameters like frequency, velocity, pulse rate and loudness. The BA transforms to the optimal solution by updating the current position with the fittest solutions velocity. In each iteration, the emission rate of pulse as well as loudness becomes efficient. Some of the expectations were predefined depending on the characteristics features of bats for achieving the BA.

Assumption:

Several assumptions are made inside the Bat Algorithm (BA). The expectations made are jagged here,

- All bats are capable of differentiating between background and Prey.

- Echolocation property is utilized to sense the distance.

- All bats fly unsystematically with velocity V_k at position y_k and emits some sound pulses with fixed minimum frequency $\lambda_{\min}$, fluctuating wavelength ω and loudness L_k.

- Frequency (or) wavelength varies established on the vicinity of the target particle.

- Furthermore, emission rate of pulse may be varied between the range of 0 and 1 based on the target location.

- Loudness L_k congregates among the maximum loudness L_0 to constant minimum loudness $L_{\min}$.

The whole flow illustration for the Bat Algorithm used for Optimization purpose of the integer value is assumed by the succeeding **Fig. 2**.

Steps involved in the BA optimization:

Assumption of the steps tangled is in the underneath segment.

Step 1: Initialization

Initially, a random number of population will be engendered for the inputs. In our suggested technique, the primary value is integer value from ElGamal encryption.

Step 2: Initialize Frequency and Velocity

Frequency, wavelength and the velocity values were well-defined for the input solution.

Step 3: Initialize Rate of Pulse Emission and Loudness

Likewise, emission rate of pulse and the loudness for the initial solution can also be calculated at each and every iteration.

Step 4: Fitness Evaluation

Previously, the fitness will be assessed for each solution to get the preeminent solution. Currently, the fitness is resulted as the solution with maximum popularity.

$$FF = max\ popularity \tag{6}$$

Step 5: Generate new solution

In step 5, new solutions were then produced arbitrarily. The solution generation is enlarged through the succeeding associations.

$$V_k{}^x = V_k{}^{x-1} + (I_k{}^{x-1} - I_*)\, f_k \tag{7}$$

where, I_*- Current best solution

In the above equation, the frequency f_k is signified as below:

$$f_k = f_{min} + (f_{max} - f_{min})\chi \tag{8}$$

where, χ - Uniform random number amid [0, 1]

Furthermore, the subsequent equation helps in the estimation of the present particle location:

$$I_k{}^x = I_k{}^{x-1} + V_k{}^x \tag{9}$$

The velocity may also be indicated as the product of frequency and wavelength. The velocity is denoted by the below equation:

$$V_k = f_k w_k \tag{10}$$

where, f -frequency and ω - wavelength

Hence, the velocity can be changed by varying the frequency term or the wavelength constituent.

Furthermore, the new solution is fitness assessed. Equally if the newly produced solution fitness value is improved, the initial solution will be substituted with the newly calculated solution. The finest solution is efficient in terms of velocity, the present position of the bat is updated with the newly calculated solution velocity depending on the fitness value calculated.

Step 6: Solution Updation:

In this stage a random number is produced and assessed. If the random number produced is more to that of rate of pulse emission, the updation of the solution is calculated. The solution updating is made through the subsequent equation:

$$I_{new} = I_{old} + \mu L^x_k \tag{11}$$

where, μ ∈ [1, 1]

Step 7: Loudness Updation:

Similarly, the loudness is also updated for the current best solution as per the below mentioned equation:

$$L_k^{x+1} = \eta\, L_k^x \tag{12}$$

where, η - constant value

Step 8: Pulse Emission rate Updation:

It is furthermore updated via the below equation:

$$E_k^{x+1} = E_k^0[1 - exp(-\zeta \times x)] \tag{13}$$

where, ζ - constant

Step 9: Termination:

If maximum iteration is attained, the procedure of updation will be terminated.

So by utilizing the above method the integer for encrypting the messages using ElGamal cryptography is chosen which aids in additional security of data. The proposed ElGamal cryptography encryption pseudo code is shown below,

```
pseudo code for Optimal ElGamal encryption
Input- Input message (M)
Output- Encrypted data

1. Key Generation

Input: Select the random prime numbers.
Output: Public key ($p_k$) and private key ($k_i$).
Procedure:
  •  Select the random prime number (n)
  •  Choose a generator number (C)
  •  Select the integer as secret key $k_i \in [1, n-1)$
// Here the integer value is optimally selected using bat algorithm
Steps for bat algorithm

Input: Random integer value
Output: Optimal integer value

Begin
Initialize the bat population $k_i$ (i = 1, 2, ..., n-1) and velocity
Define pulse frequency ($f_k$) at $k_i$
 Initialize pulse rates ($E_k$) and the loudness ($L_k$)
 Evaluate the fitness by using equation (6)
While (1< Max generation)
Frequency adjusted resulting in new solution,
 and updating velocities using the equation (7)
 Evaluate the fitness by using equation (6)
If (rand >$E_k$)
Out of the best solution is chosen
From the selected best ones, generate a local solution
End if
haphazard flying generates new solution
If (rand <$L_k$&If (new fitness>old fitness)
 New solutions accepted
 Increase $E_k$ and reduce $L_k$
End if
Bats are ranked and the current best identified
End while
End
  •  Generate the public key $p_k = C^{k_i} mod$ n
2. Encryption

Input: User input message (M).
Output: Cipher text s and t.
Procedure:
  •  Obtain the user input message M.
  •  Compute cipher text by splitting (s and t),
$s = C^j mod\ n$
$t = M.p_k^j mod\ n$; where $j \in [1, n-2)$
3. Decryption

Input: Cipher text sand t.
Output: Plaintext message M.
Procedure:
  •  Get s and t.
  •  Estimate plaintext,
$M = t.(s^{k_i})^{-1} mod\ n$
```

As mentioned earlier we use double encryption process for securing the message. Hence after the ElGamal encryption of message, we further perform hyper elliptic curve cryptography for further security.

Hyper Elliptic Curve Cryptography (HECC)

The encrypted message from the ElGamal cryptosystem is then subjected to the above encryption process. The encryption process in HECC is as follow,

Select a random prime number for the set r,

$$k_A \in r \tag{14}$$

k_A-Represents the private key of user

And then generates the cipher text using the equation (15), as shown below,

$$c_m = M + k_A p_B \qquad (15)$$

where, $P_B = K_B * G$, is the public key, G is the base point of HEC.

Here the user represents M as the message by adding $k_A * p_B$. Now in our proposed system we have modified the HECC algorithm by including an auxiliary input considered as a key for encrypting the message. The expression is given by,

$$C_m = M + \alpha(k_A P_B) \qquad (16)$$

where,

α - Auxiliary input (additional key)

The key generation is made more effective by utilizing the addition and doubling of point using the elliptic curve cryptography. It is based on the elliptic curves which is algebraic in nature over finite fields. Compared to non-ECC cryptography, it requires smaller keys to provide equivalent security. The private and public keys produced by the ECC method make the encrypted data safer. The general equation is given below,

$$y^2 = x^3 + ax + b \ (modp) \qquad (17)$$

Here $a, b \ and \ p$ are random numbers and x ranges from $0 \ ton - 1$.

By substituting the above values we could get different values of y. Hence we could get different points. From these points we select private key. Public key is also calculated from private key. The formula for public key is indicated as follows,

$$public \ key = private \ key * p \qquad (18)$$

Hence public key is calculated. Using these keys various group operations are performed on elliptic curves and they are,

- Point addition
- Point doubling

Point Addition

The process of addition of two points to generate a new point is called as point addition.

Point Addition $M + N$, denoting the group operation with the symbol " + " "Addition" means that given two points and their coordinates lies in the curve E, say $M = (X1, Y1,) \ and \ N = (X2, Y2)$. In this case we compute $R = M + N \ and \ M \neq N$. A tangent is drawn through the points M and N and obtain the third meeting point. R' is reflected on the X axis to obtain the point R on the curve.

Simple steps for point addition is as follows,

- Let $M + 0 = 0 + M$ for all $M \in E(Z_M)$.
- If $M = (X, Y) \in E(Z_M)$, then $(X, Y) + (X, -Y) = 0$. (The point $(X, -Y)$ is denoted by $-M$ and called the negative of M; observe that$-M$ is a point on the curve).
- Let $M = (X1, Y1) \in E(Z_M)$ and $N = (X2, Y2) \in E(Z_M)$, where $M \neq -N$. Then $M + N = (X3, Y3), where$

$$X3 = λ^2 - X1 - X2 \bmod M$$

$$Y3 = λ(X1 - X3) - Y1 \bmod M$$

where,

$$\lambda = \frac{Y_2 - Y_1}{X_2 - X_1} \ modP, if \ M \neq N \qquad (19)$$

Point Doubling

It is important if two points are added are identical, i.e.

$$R = M + M$$

The formula for point doubling is,

$$\lambda = \frac{3X_1^2 + a_1}{2Y_1} modP, if \ M = N \qquad (20)$$

Based on the above process we calculate the key value. Once the key value is selected the coordinate is calculated and the cipher text for transmitting is selected. The above process ensures that the message is highly secured and these secured message is then stored in the cloud. The below process would enable user for decryption,

$$Decryption(D) = C_m - k_B P_A$$

$$Decryption(D) = M + α(k_A P_B) - k_B P_A$$

$$\begin{aligned} D = M + αk_A P_B - k_B(αk_A G), Where \ [P_A = αk_A G]D \\ = M + αk_A(k_B G) - k_A(αk_B G) \end{aligned}$$

$$D = M \qquad (21)$$

Using the above expression we can decrypt the message from the cloud storage. The proposed process pseudo code is shown below,

```
Pseudo code for Hyper elliptic curve encryption
Input- Encrypted data from ElGamal encryption
Output- Dual encrypted data

Procedure:
    • Select the random number ($k_A$)
    • Generate the public key $p_B = k_B * G$

Encryption
    • Compute cipher text $C_M = M + \alpha(k_A p_B)$
// Here $\alpha$ value is selected with the help of Elliptic curve cryptography
Initialization: The general equation of the elliptic curve, $y^2 = x^3 + ax + b\ (mod\ p)$
        Where $a, b\ and\ p$ are random numbers and x ranges from0 $ton - 1$.
    • Generate the public key $public\ key = private\ key * p$
 // Using these keys various group operations performed in ECC
Point addition
$\lambda = \frac{Y_2 - Y_1}{X_2 - X_1} mod\ P, if\ M \neq N$
Point doubling
$\lambda = \frac{3X_1^2 + a_1}{2Y_1} mod\ P, if\ M = N$
Decryption
    • Estimate plaintext $Decryption(D) = C_m - k_B P_A$
```

Table 1. Storage cost, computational cost and time and usage of memory for different number of files

No of files	Storage cost (KB)	Computation cost(sec)	Memory usage (KB)	Computational Time (s)
10	130	36860	401545	2001
20	378	62126	518454	2092
40	613	93125	639654	3295
50	719	109607	755112	3356

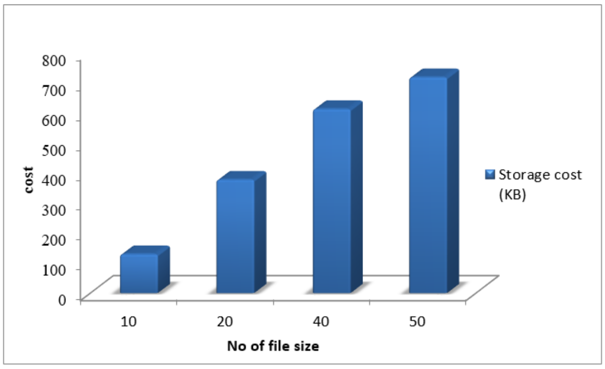

Fig. 3. Graphical representation of Storage cost for different files

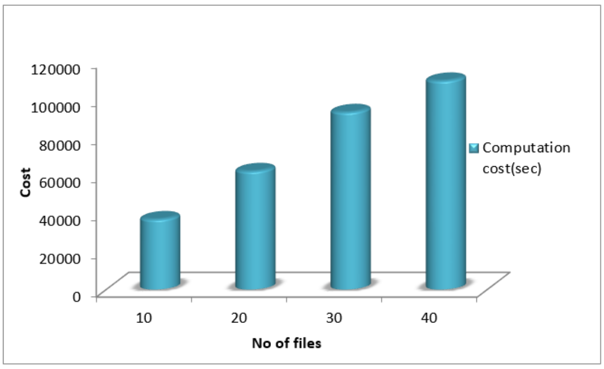

Fig. 4. Graphical representation of computation cost for different files

The above process secures the message to a higher extend as the key are more secured to the user and cannot be utilized by any unauthorized users.

RESULTS AND DISCUSSIONS

This section encompasses results of the proposed security system in cloud. We have proposed an efficient security system for cloud data storage where encryption and decryption processes of ElGamal and HECC are used. The proposed system is implemented in the working platform of JAVA. Calculation of storage, computational cost and time, usage of memory and the obtained values are shown in **Table 1**.

When analyzing **Table 1**, here we are varying the number of files and evaluate the storage cost, computational cost and time and usage of memory. **Fig. 3** shows the graphical representations for the storage cost for different files. X-axis represents the file size and Y-axis represents the cost of storage of files.

Similarly the graphical representation for and computation cost with respect to different sizes are represented graphically in the **Fig. 4**, X-axis represents the file size whereas the Y-axis represents computation cost.

Fig. 5 shows the graphical representations for the memory usage for different files. X-axis represents file

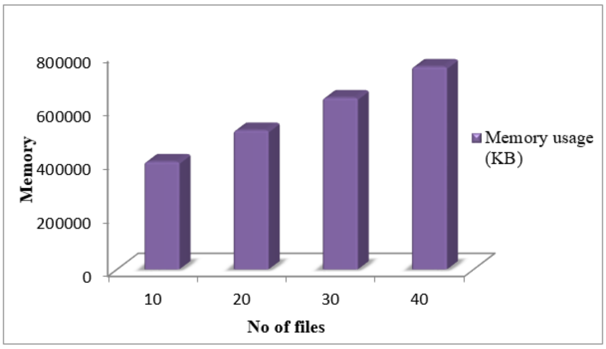

Fig. 5. Graphical representation of Memory Usage for different number of files

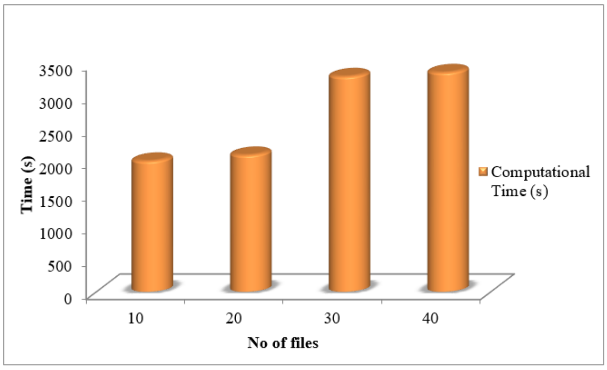

Fig. 6. Graphical representation of Computational time for different number of files

Table 2. Encryption and Decryption time for various file sizes

File size	Encryption time	Decryption time
10 kb	140	152
20 kb	210	189
30 kb	254	229
40 kb	351	295

size and Y-axis represents the corresponding memory usage. The proposed technique usage for 10 file is 401545kb. For the 20 files, the suggested technique takes the memory usage of 518454kb. For 30 and 40 files, the recommended technique takes the memory usage of 639654kb and 755112kb respectively.

Similarly the graphical representation for and computation time with respect to different sizes are represented graphically in **Fig. 6**. X-axis represents file size and Y-axis represents corresponding computational time.

In our suggested technique, to complete the process for 10 files it takes 2001 seconds. For completing the number of files 20, 30 and 40 the suggested technique takes the computational time of 2092s, 3295s and 3356s respectively. **Table 2** shows the time obtained for various file sizes used in our proposed method.

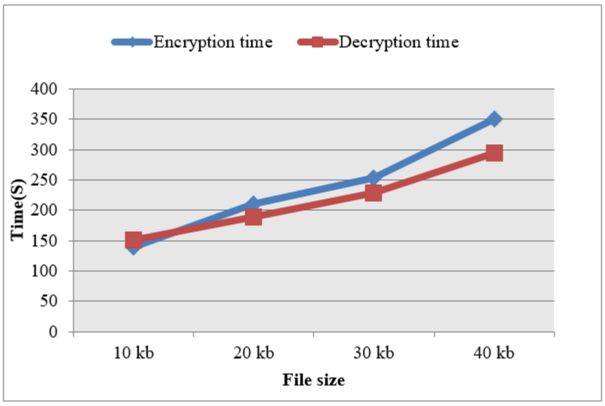

Fig. 7. Encryption and decryption time for various file sizes

Table 3. Comparison results of proposed and existing method

Metrics	Proposed method [ElGamal(BAT)+ HECC(ECC)]	Existing method [ElGamal(MCS)+ HECC(GSO)]	Existing method [ElGamal + HECC]
Storage Cost (KB)	441.5	468.25	499.5
Computational time (s)	41.28	44.14	105.99

Fig. 7 shows the graphical representation time for various file sizes. X-axis represents file size and Y-axis represents corresponding encryption and decryption time.

There is a comparison of the discussed method with that of existing technique's performances to prove the robustness of the proposed method. The storage cost and the computational time for different number of files are estimated and are compared for both proposed and the existing method as shown in the **Table 3**. Here we are considering the existing methods for encryption [ElGamal (MCS) +HECC (GSO)] and another method for the comparison [ElGamal + HECC] (see **Table 3**).

The graphical representation for the above comparison table is shown in **Fig. 8** and **9** as given below. From the graph it is clear that the method we discussed in this work has delivered improved storage cost and the computational time for different number of files. In **Fig. 8**, X-axis represents existing and proposed methods whereas the Y-axis represents the corresponding storage cost. In **Fig. 9**, X-axis represents existing and proposed methods whereas the Y-axis represents the corresponding computational time.

In **Fig. 8** the proposed storage cost is compared with the existing methods. Here the existing technique

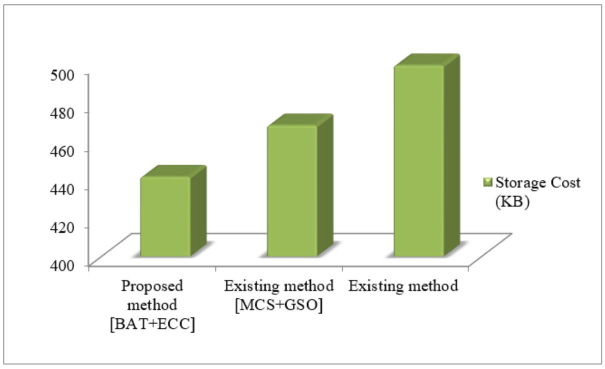

Fig. 8. Graphical representation of storage cost for proposed and existing methods

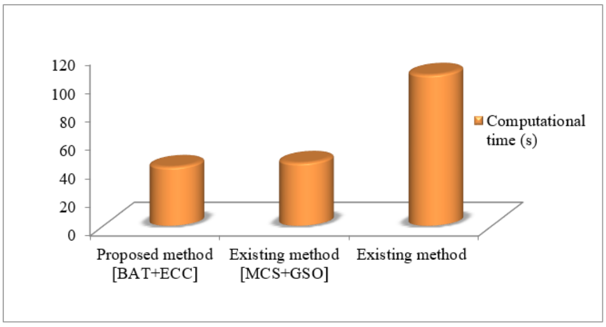

Fig. 9. Graphical representation of computational time for proposed and existing methods.

reaches the storage cost value at 499.5 and 468.25 which is maximum value when compared to our recommended technique. The suggested technique attains the store cost at 441.5. Thus our proposed technique takes minimum storage cost. The comparison result of computational time is shown in **Fig. 9**.

In **Fig. 9** the proposed computational time is compared with other methods presently available. Here the existing technique takes the computational time 105.99s and 44.14s which is the maximum value when compared to our recommended technique. The suggested technique takes the computational time 41.28, so our proposed technique takes minimum computational time.

Table 4 shows the comparison result for proposed method and existing method. When analyzing **Table 4**, the minimum encryption time is achieved by the proposed technique as compared to the method available. For encrypting the file size 10 kb, 20kb, 30kb and 40kb the proposed technique takes 140s, 210s, 254s and 351s which is minimum value than the existing method. For decrypting the file size 10 kb, 20kb, 30kb and 40kb the proposed technique takes 152s, 189s, 229s and 295s which is minimum value than the existing method. The key positive point of the recommended technique is the dual encryption. It is highly secured and hence message decryption becomes challenging. Proposed model is compared with the existing methods and shows significant improvement in securing data in cloud. Thus the proposed method serves the best security and results show that it has high security, minimum storage cost and minimum computational cost and time than the existing methods.

Table 4. Time comparison results of proposed and existing method

File size	Proposed [ElGamal(BAT) + HECC(ECC)]		Existing [ElGamal(MCS) + HECC(GSO)]	
	Encryption time (s)	Decryption time (s)	Encryption time (s)	Decryption time (s)
10 kb	140	152	148	158
20 kb	210	189	212	196
30 kb	254	229	261	238
40 kb	351	295	363	313

CONCLUSION

What will be the environmental impact if cloud-based solutions are widely adopted by businesses to replace current on-premise deployments? To illustrate the findings from this study in an example, it is possible to estimate the potential carbon savings assuming all US companies with 100 to 10,000 employees were using Microsoft Exchange and would switch from on-premise email servers to the corresponding cloud solution. 17 For this scenario, the reduction of carbon emissions would be equivalent to the emissions saved from permanently removing about 100,000 passenger cars from the road.

In this paper, secure storage of data in cloud is offered based on double encryption of ElGamal and HECC algorithms. ElGamal and HECC are utilized in our proposed method for encryption and decryption with some modification to normal process. The use of double encryption enhances data security as the security of sensitive data from unauthorized access is essential requirement of cloud environment. We have utilized BAT algorithm for integer selection in ElGamal cryptosystem. And for key generation in HECC, we have utilized addition and doubling of point using elliptic curve cryptography. The user secures the input message with ElGamal and HECC cryptosystem algorithms. The proposed method performance analysis is done in regards to storage cost, computation cost and execution time. Results indicate that our proposed data security model is more efficient with regards to storage and computation cost and minimum time than the existing methods.

REFERENCES

Ali M, Khan SU, Vasilakos AV (2015) Security in cloud computing: Opportunities and challenges. Information Sciences, 305: 357-383.

Al-Sharif, F. M (2017) Correlation between serum alanine aminotransferase activity and immunologic response and body mass index in obese patients with chronic hepatitis B virus infection. European Journal of General Medicine, 14(2), 34-37. doi: 10.29333/ejgm/81879

Batista BG, Gomes Ferreira CH, Marim Segura DC, Leite Filho DM, Maciel Peixoto ML (2016) A QoS-driven approach for cloud computing addressing attributes of performance and security. Future Generation Computer Systems, 68: 260-274.

Chang V, Kuo Y-H, Ramachandran M (2016) Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57: 24-41.

Eryılmaz D, Ece A (2016) Evaluation of Follow-up Results in Children with Henoch-Schönlein Purpura. J Clin Exp Invest, 7(4):269-77. doi: 10.5799/jcei.328558

Gupta PC (2014) Evaluation of Antifertility Potential of Ficusbengalensis (Linn.) in Male Albino Mice. International Journal of Pharmacy Research & Technology, 4: 05-09.

Hussain SA, Fatima M, Saeed A, Raza I, Khurram Shahzad R (2016) Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics: 1-9.

Jouini M, Arfa Rabai LB (2016) Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems. Procedia Computer Science, 83: 1084-1089.

Khan N, Al-Yasiri A (2016) Identifying cloud security threats to strengthen cloud computing adoption framework. Procedia Computer Science, 94: 485-490.

Manogaran G, Thota C, Kumar MV (2016) Meta Cloud Data Storage architecture for Big Data security in cloud computing. Procedia Computer Science, 87: 128-133.

Ramachandran M (2016) Software security requirements management as an emerging cloud computing service. International Journal of Information Management, 36(4): 580-590.

Rao RV, Selvamani K (2015) Data security challenges and its solutions in cloud computing. Procedia Computer Science, 48: 204-209.

Rasheed H (2014) Data and infrastructure security auditing in cloud computing environments. International Journal of Information Management, 34(3): 364-368.

Rohini S, Sharanya M, Vidhya A, Viji S, Poornima P (2017) Proximity Coupled Microstrip Antenna for Bluetooth, WIMAX and WLAN Applications. International Journal of Communication and Computer Technologies, 5: 48-52.

Shaikh R, Sasikumar M (2015a) Data classification for achieving security in cloud computing. Procedia computer science, 45: 493-498.

Shaikh R, Sasikumar M (2015b) Trust model for measuring security strength of cloud computing service. Procedia Computer Science, 45: 380-389.

Singh AP, Pasupuleti SK (2016a) Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing. Procedia Computer Science, 93: 751-759.

Singh S, Jeong Y-S, Park JH (2016b) A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75: 200-222.

Sookhak M, Gani A, Khan MK, Buyya R (2016) Dynamic remote data auditing for securing big data storage in cloud computing. Information Sciences, 380: 101-116.

VenkateswaraRao N, Venkateswarlu Ch (2017) Hybrid ABC optimization based interference cancellation in MIMO-OFDM. 2017 2nd International Conference on Communication and Electronics Systems (ICCES).

Vurukonda N, Rao BT (2016) A study on data storage security issues in cloud computing. Procedia Computer Science, 92: 128-135.

Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV (2014) Security and privacy for storage and computation in cloud computing. Information Sciences, 258: 371-386.

Yang LT, Huang G, Feng J, Xu L (2016) Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing. Information Sciences: 1-27.

Zhang Y, Chen X, Li J, Wong DS, Li H, You I (2016) Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Information Sciences, 379: 42-61.

Zhao J, Wang L, Tao J, Chen J, Sun W, Ranjan R, Kołodziej J, Streit A, Georgakopoulos D (2014) A security framework in G-Hadoop for big data computing across distributed Cloud data centres. Journal of Computer and System Sciences, 80(5): 994-1007.