Received: January 1, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Ensuring Security for Data Storage in Cloud Computing using HECC- ElGamal Cryptosystem and GSO Optimization

Devi Thiyagarajan[1*] **Ganesan Ramachandrarao[1]**

[1]*Vellore Institute of Technology University, Chennai, India*
* Corresponding author's Email: devithiyagarajan0884@gmail.com

Abstract: Cloud computing is a popular subject across the IT industry, but many risks associated with this relatively new delivery model is not yet fully understood. Cloud computing is an budding information technology of data storage, of local networks (infrastructure) as well as software and has its advantages of scalability, reliability, high performance and comparatively low cost feasible solution contrast to committed infrastructures. Here, initially the data owner will encrypt the searchable index with ElGamal cryptosystem utilizing Hyper Elliptical Curve Cryptography for double encryption. The ElGamal cryptosystem is utilized for security analysis where in sharing of multiple keys between two parties are performed aiming for better security. The random integer selection in the ElGamal cryptosystem is modified based on optimization process using Modified cuckoo search (MCS). Further Hyper elliptical curve cryptography is incorporated with ElGamal cryptosystem which is utilized for encryption and decryption. Also, the hyper elliptic curve cryptography is modified using auxiliary input in the divisor calculation in order to improve security. For selecting keys, we have used Gravitational search algorithm (GSO). The retrieval process will take a two-round communication between the cloud server and the data user. The experimental results shown that, the recommended technique attains minimum storage cost and minimum computation time when compared to the existing technique.

Keywords: ElGamal cryptosystem, Hyper elliptical curve cryptography, Cuckoo search and gravitational search algorithm.

1. Introduction

Cloud computing has been envisioned as the next generation architecture of the IT enterprise due to its long list of unprecedented advantages in IT: on demand self-service, ubiquitous network access, location-independent resource pooling, rapid resource elasticity, usage-based pricing, and transference of risk. One fundamental aspect of this new computing model is that data is being centralized or outsourced into the cloud [1]. In cloud data is stored at remote location and available on demand. It allows clients to use applications without installation the file at any computer with internet facility. By data outsourcing user can get the information from anywhere more efficiently and has no burden on data storage and avoid the extra expenses on software, hardware, and information resources and data maintenances and used more efficiently [2]. With the increasing popularity of cloud storage, the risks for security, data integration, and confidentiality of data is implicitly increasing. Therefore, the cloud provider must consider the security and confidentiality as the challenging factors for data sharing functionality [3].

Cloud adoption will have its own positive and negative effects on the data security of consumers. It is virtually not possible for the data owner to confirm security conditions of all the server locations that might be used to house the data. In cloud computing environment data and application is controlled by service provider which leads to its safety concerns from internal as well as external sources [4].

In cloud storage system, however, it is inappropriate to let either side of cloud service

providers or owners conduct such auditing, because none of them could be guaranteed to provide unbiased auditing result. In this situation, third party auditing is a natural choice for the storage auditing in cloud computing. The associate economical and secure information sharing theme for groups inside the cloud is not a straightforward task due to the following troublesome issues.

- Identity privacy is one altogether the foremost necessary obstacles for the wide activity of cloud computing.
- It is extraordinarily prompt that any member in a passing cluster needs to be ready to completely get pleasure from the knowledge storing and sharing services provided by the cloud, that's printed as a result of the multiple-owner manner.
- Groups are typically dynamic in follow. The changes of membership build secure information sharing very powerful [5].

One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [6]. Cloud computing relies on large data centres consisting of thousands of servers and all application processing and resources are centralized in data centres. Security issues have been the top concerns in cloud computing 0. Since cloud servers are operated by commercial providers who are usually outside of the trusted domain of users, they are not entitled to access the confidential data [7].

Cloud computing is used in a number of applications. The cloud computing model shifts the computing infrastructure to third-party service providers that manage the hardware and software resources with significant cost reductions. Cloud computing has shown great potential to enhance collaboration among different healthcare organizations and to fulfil the common requirements, such as scale, agility, cost effectiveness, and availability [8]. Cloud computing scenario has also been utilized in the mobile computing as well. The mobile cloud computing scenario is therefore exacerbating the mobile privacy problem, which turns the risk of implicit total surveillance of individuals even more into a reality [9]. Another application is in the form vehicular cloud computing. A VC can be formed on-the-fly by dynamically integrating resources and collecting information. Vehicles can access the cloud and obtain, at the right time and the right place, all the needed resources and applications that they need or want. Obviously, security and privacy issues need to be addressed if the VC concept is to be widely adopted. Conventional networks attempt to prevent attackers from entering a system [10].

The overall objective of the suggested technique is secure data storage in cloud computing. In order to attain the objective effective cryptographic algorithm is examined in our proposed technique. For encryption, optimal ElGamal and hyper elliptic cryptographic algorithm is utilized. The main advantage of the proposed technique is minimizing the storage cost and computation time with more secure when compared with existing technique.

The rest of the paper is organized as follows: Section 2 gives a brief discussion on various recent researches done on the cloud security field. Section 3 explains about the proposed technique for Ensuring security for data storage in cloud computing using HECC- ElGamal cryptosystem. Section 4 gives the detailed explanation about the results obtained and the section 5 concludes our proposed methodology.

2. Related work

Numerous researches have been done in the field of ensuring data security to cloud system. Some of the recent researches in the respective area are reviewed in this section which are discussed as follows

ElGamal cryptosystem occupies very important position in network security and it has wide application. Compared with RSA algorithm, elliptic curve encryption algorithm has significant advantages, and it is suitable for application in the environment with limited resources. Wang and Sun [11] have proposed ElGamal cryptosystem based on elliptic curve. The two schemes are compared in security and calculation performance. Despite a little more calculation, the scheme could improve the safety and expand the application field of ElGamal based on elliptic curve cryptosystem.

Secure and efficient data storage was needed in the cloud environment in modern era of information technology industry. The cloud verifies the authenticity of the cloud services without the knowledge of user’s identity. The cloud provides massive data access directly through the internet. Centralized storage mechanism was followed here

for effective accessing of data. Cloud service providers are normally acquires the software and hardware resources and the cloud consumers are avail the services through the internet access in lease basis. Cloud security was enhanced through cryptography technique applied to the cloud security to avoid vulnerability. The intractable computability was achieved in the cloud by using the public key cryptosystem. Selvi and Ganesan [12] have proposed the approach of applying hyper elliptic curve cryptography for data protection in the cloud with the small key size. The proposed system has the further advantage of eliminating intruder in cloud computing. Efficacy of the system was to provide the high security of the cloud data.

Cloud computing was a latest computational system which could be used for big data processing. Huge amount of unstructured, structured and semi structured data could be called as big data. Map-Reduce and the Hadoop facilitate an affordable mechanism to handle and process data from multiple sources and store the big data in distributed cloud. Jose and shine [13] have explained the secured and cost minimizing approach to move and store very large amount of data to cloud. Hyper elliptic cryptography was introduced to provide encryption to the huge amount of data arriving to the cloud. In addition to cryptography, data download module was included.

Cloud Computing was a computing model which provides ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that could be rapidly provisioned and released with little or no up-front IT infrastructure investments costs. Cloud computing moves the application and data to the cloud storage where the management of the data and services might not be fully trustworthy. Therefore, there was a need for cloud service providers to provide a sufficient level of integrity for the client's data. Samson and Kayode [14] have proposed a data security scheme using Signcryption and hyper elliptic curves as a single logical step. Signcryption schemes based on hyper elliptic curves saves more computational time and communication cost.

Cloud computing was arguably one of the most significant advances in information technology (IT) services today. Several cloud service providers (CSPs) have offered services that have produced various transformative changes in computing activities and presented numerous promising technological and economic opportunities. However, many cloud customers remain reluctant to move their IT needs to the cloud, mainly due to their concerns on cloud security and the threat of the unknown. Pichan and Soh [15] have systematically surveyed the forensic challenges in cloud computing and analyze their most recent solutions and developments. In particular, unlike the existing surveys on the topic, they have described the issues in cloud computing using the phases of traditional digital forensics as the base. For each phase of the digital forensic process, they have included a list of challenges and analysis of their possible solutions.

Wei *et al.* [16] have proposed a privacy cheating discouragement and secure computation auditing protocol, or Sec Cloud, which was a first protocol bridging secure storage and secure computation auditing in cloud and achieving privacy cheating discouragement by designated verifier signature, batch verification and probabilistic sampling techniques. The detailed analysis was given to obtain an optimal sampling size to minimize the cost. Another major contribution was that they build a practical secure-aware cloud computing experimental environment, or Sec HDFS, as a test bed to implement Sec Cloud. Further experimental results have demonstrated the effectiveness and efficiency of the proposed Sec Cloud.

From the literature survey, they mainly focused on the security of data storage with the help of hyper elliptic curve algorithm. The main drawbacks of the existing algorithm achieves the maximum computation time and storage cost with poor security of data storage. So that the suggested technique is using the optimal dual encryption algorithm for secure data storage with minimum storage cost and minimum computation time.

3. Proposed methodology

Cloud computing is becoming the most important distributed computing paradigm, more and more researchers and developers are interested in it. The full resources of the system must cooperate to respond to a client request which requires intercommunication between various components of the system to design a component or subset of components to deal with the request which can lead to bottlenecks in the network. With Cloud Computing rapidly gaining popularity, it is important to highlight the resulting risks. As security and privacy issues are most important, they should be addressed before Cloud Computing establishes an important market share.

3.1 Data privacy threat in cloud

The main threat on data privacy roots in the cloud itself.

- Even in the encrypted data utilization, users still need to communicate with the cloud and allow the cloud operates on the encrypted data, which potentially causes leakage of sensitive information.
- Keyword-based retrieval is a typical data service and widely applied in plaintext scenarios, in which users retrieve relevant files in a file set based on keywords. However, it turns out to be a difficult task in cipher-text scenario due to limited operations on encrypted data.
- Data confidentiality appears as the biggest concern for users of a cloud storage system.

These are the main drawbacks of various existing works, which motivate us to do this research on cloud security. We are intended to propose a suitable method to achieve securing data provenance in cloud computing.

The block diagram for our proposed security system is shown in the Fig. 1 below,

Here, initially the data owner will encrypt the searchable index with ElGamal cryptosystem utilizing Hyper Elliptical Curve Cryptography for double encryption. The ElGamal cryptosystem has the advantage of encrypting large message which prompted us to utilize the encryption method in our proposed system.

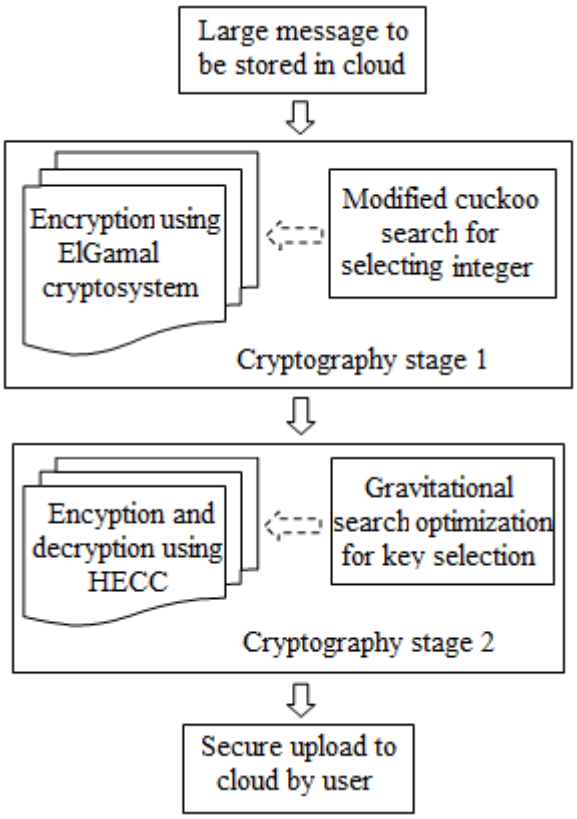

Figure.1 Block diagram for our proposed method

The ElGamal cryptosystem is utilized for security analysis where in sharing of multiple keys between two parties are performed aiming for better security. The random integer selection in the ElGamal cryptosystem is modified based on optimization process using MCS. Further Hyper elliptical curve cryptography is incorporated with ElGamal cryptosystem which is utilized for encryption and decryption. Also, the hyper elliptic curve cryptography is modified using auxiliary input in the divisor calculation in order to improve security. When the cloud server receives a large query message consisting of multi-keywords, it will compute the score from the encrypted index stored on cloud and then will return the encrypted scores of files to the data user. Subsequently, the data user will decrypt the scores and select out the top-k highest scoring files identifiers to request to the cloud server. For selecting keys, we have used Gravitational search algorithm (GSO). The retrieval process will take a two-round communication between the cloud server and the data user.

3.2 ElGamal cryptosystem for encrypting messages

ElGamal cryptosystem provides the advantage of encrypting large messages. This encryption system provides users with the option of sending any type of messages with more secured access between the users. The ElGamal cryptosystem operates as follows,

In ElGamal cryptosystem each user selects their own secret keys such that,

$$k_i \in [1, N-2) \quad (1)$$

Where,

N- Prime number

The related public key is then given by,

$$p_k = c^{k_i} \, mod \, N \quad (2)$$

Where,

c - Primitive root or generator

For encrypting a large message using ElGamal cryptosystem, the sender computes the cipher text *s* and *t* as follows,

$$s = c^j \, mod \, N \quad (3)$$

$$t = M.p_{k^j} \, mod \, N \quad (4)$$

Where, $j \epsilon [1, N-2)$

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

$$M = t.(s^{k_i})^{-1} mod \, N \quad (5)$$

Based on the above process the ElGamal

cryptosystem works and in order to make the encryption process more secure we have utilized some modification in normal ElGamal process by incorporating optimization process. In our technique for the selection of the integer values in the process of encryption we have used Modified cuckoo search algorithm to optimize the selected values which will help in securing the message more. The process of optimization is explained in the below section,

3.2.1 Optimization using modified cuckoo search algorithm

The Cuckoo search algorithm represents a biologically inspired algorithm. Its origin is owed to the breeding conduct of the cuckoos and it is easy to implement. Each egg signifies a solution and an egg of cuckoo corresponds to a novel solution. The novel and superior solution is replaced by the worst solution in the nest. A brief justification of diverse steps that are involved in the modified cuckoo search algorithm are given below

Step 1: Initialization Phase

Population ($P_{i,}$ where i=1, 2, N) of host nest is initialized at random.

Step 2: Generating New Cuckoo Phase

With the help of the levy flights a cuckoo is selected randomly which generates novel solutions. Subsequently, the engendered cuckoo is estimated by employing the fitness function for ascertaining the excellence of solutions.

Step 3: Fitness Evaluation Phase

The fitness function is evaluated in accordance with Eq. (6) and Eq. (7) shown hereunder, followed by the selection of the best one.

$$F_m = \frac{P_C}{p_N} \tag{6}$$

Where,

F_m- Fitness or maximum popularity

P_c- signifies the selected population

P_N- represents the total population

Step 4: Updation Phase

In the beginning, the solution is optimized by the levy flights by employing the cosine transform. By estimating the superiority of the fresh solution, a nest is chosen at random among them. If the new solution in the elected nest is superior and advanced to the previous solution, it is restored by the new solution (Cuckoo). Otherwise, the preceding solution is considered as the finest solution. The levy flights employed for the general cuckoo search algorithm is expressed by the Eq. (7) shown below,

$$Lf_i^* = Lf_i^{(n+1)} = Lf_i^{(n)} + \alpha \oplus Lvy(N) \tag{7}$$

In modified cuckoo search, the above levy flight equation is modified by incorporating the Gaussian function for updation which is given in Eq. (8) below,

$$Lf_i^* = Lf_i^{(n+1)} = Lf_i^{(n)} + \alpha \oplus \eta_g \tag{8}$$

$$\eta_g = \eta_0 \exp(-\mu C) \tag{9}$$

η_0, μ - Constants

C - Current generation

Step 5: Reject Worst Nest Phase

In this section, the worst nests remain unobserved, considering their possibility values thereby creating fresh ones. Consequently, the best solutions are ranked based upon their fitness function. Thereafter, the best solutions are distinguished and marked as optimal solutions.

Step 6: Stopping Criterion Phase

Based on the termination criteria, the above process is repeated until the best solution is reached.

So, by utilizing the above optimization technique the integer for encrypting the messages using ElGamal cryptography is selected which aids in more security of data. 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.

3.3 Encryption and decryption using hyper elliptic curve cryptography

Before cloud storage the user further encrypts the message using the hyper elliptic curve cryptography. The encrypted message from the ElGamal cryptosystem is then subjected to hyper elliptic curve cryptography encryption process. The encryption process in HECC is as follow,

Select a random prime number for the set N, (i.e.)

$$h \in N \tag{10}$$

The coordinate C is given by,

$$C = hD \tag{11}$$

Where,

D- Divisor of HEC

Now in our proposed system we have modified

the HECC algorithm by including an auxiliary input which is regarded as a key for encrypting the message. The expression is given by,

$$C = \alpha[hD] \quad (12)$$

Where,

α - Auxiliary input (additional key)

The key selection is made more effective by utilizing the optimization technique. Here we use GSA for selecting the key which is explained in the below section.

3.3.1 Gravitational search optimization for fuzzy rule optimization

Gravitational search optimization (GSO) is a metaheuristic optimization algorithm, which is depending on the Newton's law of gravity and the law of motion. In GSO, the fitness of the result is deliberate by the weight. The weight of an entity is predictable by regard as the possessions like, location, inertial weight, dynamic gravitational weight and inactive gravitational weight.

Similarly, PSO (Particle Swarm Optimization) algorithm, the GSO also modernizes the existing location by the finest fitness result during the velocity estimate. Additionally, the quickening value is calculated by exploiting the Newton's Law of Motion earlier than the velocity updation.

The step by step procedure about the GSO algorithm is detailed in the upcoming section.

Step 1: Initialization

The preliminary result is the location of the input entity (agent), which is specified by the subsequent Eq. (13) as,

$$T_y = (t_y^1, \ldots\ldots, t_y^p, \ldots\ldots, t_y^m) \quad (13)$$

Where,

Y= 1,2,..,*M*

t_y^p - Position of y^{th} agent in P^{th} dimension

m- Space dimension

Step 2: Fitness Evaluation

At this point, the fitness of every mediator will be assessed. Consequently, the velocity ($V_y^p(x)$) will be primarily prepared to zero. Afterward, the finest and nastiest fitness assessment is prepared for every one of the mediator. The finest and the nastiest fitness will be assessed by the next equations.

For Minimization Problems

The finest and nastiest fitness is assessed for the minimization troubles are specified by the subsequent Eq. (14) and Eq. (15).

$$B(x) = \min_{z\xi\{1,..,M\}} FF_z(x) \quad (14)$$

$$W(x) = \max_{z\xi\{1,..,M\}} FF_z(x) \quad (15)$$

For Maximization Problems

Additionally, the finest and nastiest fitness is assessed for the minimization troubles are specified by Eq. (16) and Eq. (17).

$$B(x) = \max_{z\xi\{1,..,M\}} FF_z(x) \quad (16)$$

$$W(x) = \min_{z\xi\{1,..,M\}} FF_z(x) \quad (17)$$

Where,

$FF_Z(x)$- Fitness of the Z^{th} agent for *x* iteration

The Fitness of the Z^{th} agent for *x* iteration can also be computed by means of reducing the Mean Square Error (*MSE*) values.

$$FF_z(x) = \min(MSE) \quad (18)$$

Step 3: Compute Gravitational Constant

In step 3, the gravitational invariable will be modernized. The Gravitational invariable updation is completed by Eq. (19).

$$H(x) = H_0 exp\left(-\beta \frac{x}{X}\right) \quad (19)$$

Where,

x- Current iteration

X- Maximum number of iteration

β , H_0- Constants

Step 4: Update Gravitational Mass & Inertial Mass

The Gravitational mass and the inertial mass will be updated through the following Eq. (20) & (21).

$$G_{Ay} = G_{Py} = G_{yy} = G_y \quad (20)$$

Where, *y*=1,2,….,*M*.

$$G_y(x) = \frac{g_y(x)}{\sum_{z=1}^{M} g_z(x)} \quad (21)$$

Where, $g_y(x)$ is represented by the below Eq. (22).

$$g_y(x) = \frac{FF_y(x) - W(x)}{B(x) - W(x)} \quad (22)$$

Step 5: Compute Force

The force is calculated by the following Eq. (23).

$$F_y^p = \sum_{z\xi sbest \neq y} rand_z F_{yz}(x) \quad (23)$$

Moreover, the force acting on y^{th} agent by Z^{th} agent is determined by the following Eq. (24).

$$F_{yz}^{p}(x) = H(x)\frac{G_{Py}(x)\times G_{Ay}(x)}{E_{yz}(x)+\xi}(t_{z}^{p}(x) - t_{y}^{p}(x)) \quad (24)$$

$E_{yz}(x)$- Euclidean distance between y^{th} agent and Z^{th} agent

ξ - Constant

The Euclidean distance between y^{th} agent and Z^{th} agent is understood by the following Eq. (25).

$$E_{yz}(x) = (\|T_{y}(x), T_{z}(x)\|_{2}) \quad (25)$$

Step 6: Estimate Acceleration

Since the laws of gravity, the acceleration of y^{th} mediator is predictable. The acceleration is signified by the subsequent Eq. (26).

$$A_{y}^{p}(x) = \frac{F_{y}^{p}(x)}{G_{yy}(x)} \quad (26)$$

Step 7: Estimate Velocity

Additionally, the velocity determine is intended by the laws of motion. The velocity working out is signified by the subsequent Eq. (27).

$$V_{y}^{p}(x+1) = rand_{y} \times V_{y}^{p}(x) + A_{y}^{p}(x) \quad (27)$$

Step 8: Update Position

In this pace, the situation of the mediator will be modernized by the estimated velocity among finest result at the existing location. The situation updation is prepared by the subsequent Eq. (28).

$$t_{y}^{p}(x+1) = t_{y}^{p}(x) + V_{y}^{p}(x+1) \quad (28)$$

Step 9: Repeat

Reiterate the procedure up to the greatest iteration is attained.

Step 10: Terminate

Formerly the greatest iteration is accomplished, extinction will be completed.

Once the auxiliary input is selected the coordinate is calculated and the cipher text for transmitting is selected.

$$p_{h} = [\alpha h]p_{r} \quad (29)$$

$$C_{t} = \{C, M + p_{h}\} \quad (30)$$

Where,

P_r- is the receiver's public key

C_t- Cipher text to send

The above process ensures that the message is highly secured and these secured message is then stored in the cloud. The user can decrypt the message by the below process,

$$M + hp_{r} - qr(C) = M \quad (31)$$

Using the above expression we can decrypt the message from the cloud storage. 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.

4. Result and discussion

This section gives a detailed view of the results that are obtained using our proposed security system in cloud. We have proposed an efficient security system for cloud data storage where ElGamal and HECC encryption and decryption are used. The proposed system is implemented in the working platform of JAVA. The performance evaluation of our proposed method is done by calculating the storage, computation cost along with the memory usage and Computational time and the obtained values are shown in the below Table 1.

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

No	Storage cost (KB)	Computation cost(sec)	Memory usage (KB)	Computational Time (s)
10	132	36887	2154981	101451
20	395	62231	2235451	112524
40	621	93254	2469574	136995
50	725	109683	2658715	154682

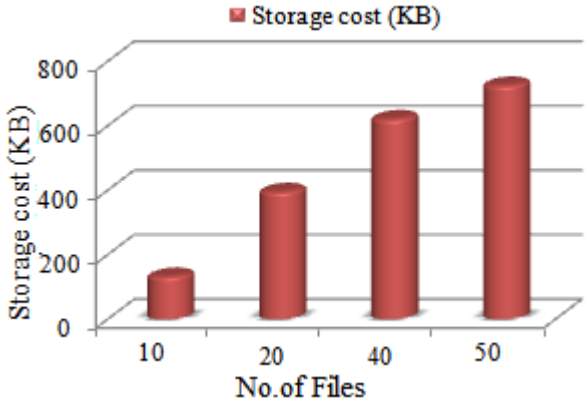

Figure.2 Graphical representation of Storage cost for different number of files

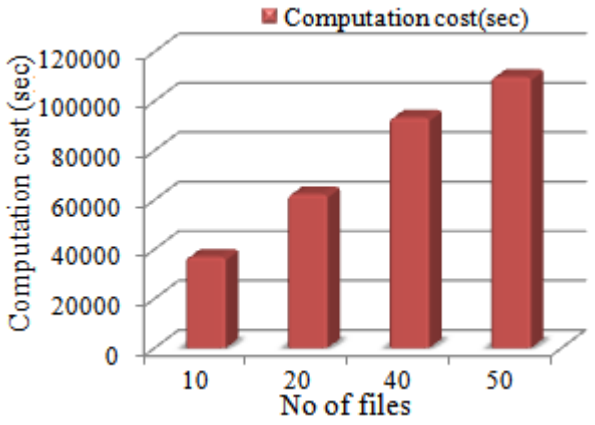

Figure.3 Graphical representation of computation cost for different number of files

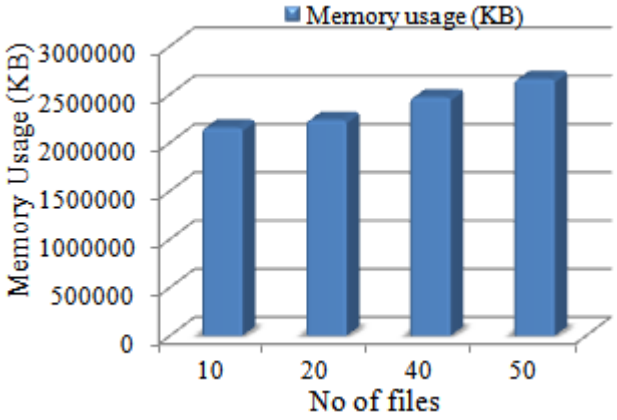

Figure.4 Graphical representation of Memory Usage for different number of files

For the above parameters, i.e. for different file sizes the corresponding storage, computational costs are plotted. The graphical representations for the storage for different files are shown in Fig 2.

Similarly, the graphical representation for and computation cost with respect to different sizes are represented graphically in the Fig. 3 above.

Also for the above parameters, i.e. for different file sizes the corresponding memory usage and Computational time are plotted. The graphical representations for the memory usage for different files are shown in Fig. 4. Similarly, the graphical representation for and computation time with respect to different sizes are represented graphically in the Fig. 5 below. The Table 2 given below shows the Encryption and decryption time obtained for various file sizes using our proposed method. The Fig. 6 given below shows the graphical representation of encryption and decryption time for various file sizes.

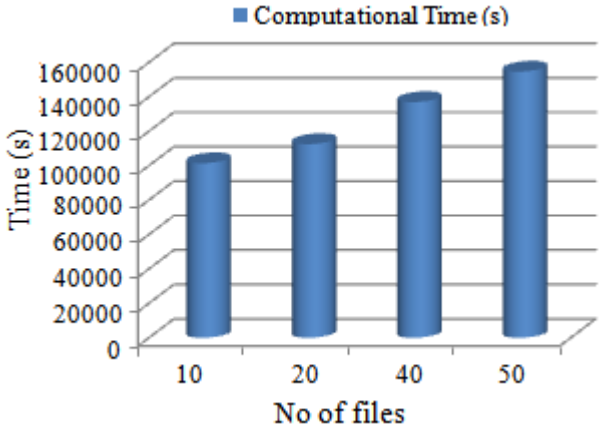

Figure.5 Graphical representation of Computational time for different number of files

Table 2. Encryption and decryption time for various file sizes

File size	Encryption time	Decryption time
10 kb	4562	3654
20 kb	7562	6242
30 kb	9546	8745
40 kb	10255	9995

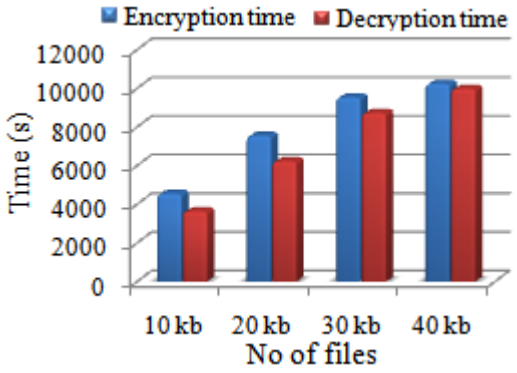

Figure.6 Graphical representation of encryption and decryption time for various file sizes

Table 3. Comparison of proposed and existing method

Methods	Storage Cost (KB)	Computational Time (s)
Proposed method	12.2	4147
Existing method (GA)	12.8	5412
Existing (Hyper elliptic curve) [13]	12.71	4354

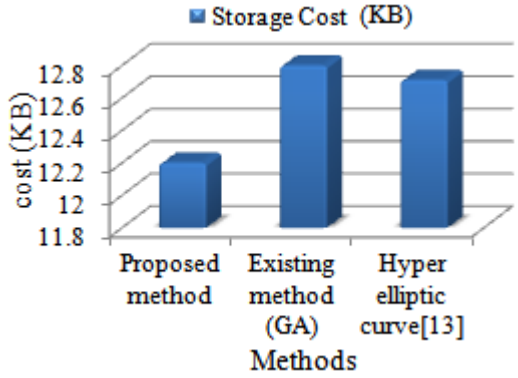

Figure.7 Graphical representation of storage cost for proposed and existing methods.

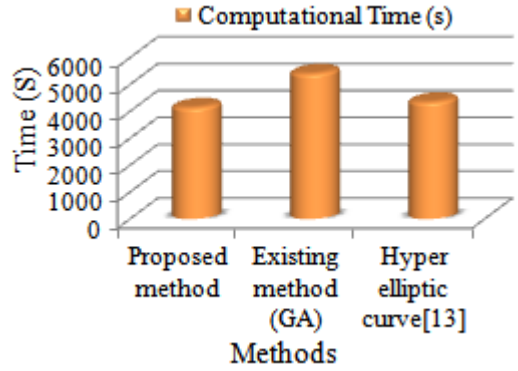

Figure.8 Graphical representation of computational time for proposed and existing methods

The performance of our proposed method is compared with existing technique in order to prove the effectiveness of the proposed technique. 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.

The graphical representation for the above comparison table is shown in the Fig.7 and Fig. 8 given above. From the graph, it is clear that our proposed method has delivered improved storage cost and the computational time for different number of files.

5. Conclusion

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 by giving some modification to normal process. We have utilized MCS algorithm for integer selection in ElGamal cryptosystem and also for key selection in HECC we have utilized GSO algorithm. The user secures the input message with the aid of ElGamal and HECC cryptosystem algorithms. Even large images can be processed since we use ElGamal cryptosystem as it supports encryption of large images. From the experimental results the suggested technique attains the storage cost of 12.2 and the existing method achieves 12.8 and 12.71 for GA and Hyper elliptic curve which is maximum value when compared to the proposed storage cost. The computational time for the recommended technique is 4147s which is minimum value when compared to the existing methods. From the result, we obtained that our proposed data security model is more efficient in terms of storage and computation cost. In future, the researcher will have sufficient opportunities to perform efficient data storage security by means of various cryptographic algorithms.

Reference

[1] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services", *IEEE Network*, Vol.24, No. 4, 2010.

[2] J. P. Kaur, and R. Kaur, "Security Issues and Use of Cryptography in Cloud Computing", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, No. 7, 2014.

[3] S. P. Tenginkai and K. S. Vani, "Cryptographic Algorithms for Efficient and Secure Data Sharing in Cloud Storage", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 4, No. 2, 2015.

[4] S. A. Shinde, and V. Chavan, "Data Security in Cloud Computing: Major Concerns and Implications", *In.proc.of National Conference on Emerging Trends: Innovations and Challenges*, Vol. 19, 2013.

[5] M. R. K. Selvi, "Secure Data Sharing for Dynamic and Large Groups in the Cloud", *International Journal of Innovative Research in Computer and Communication Engineering* Vol. 2, No. 1, 2014.

[6] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", *IEEE Transactions on Parallel And Distributed Systems*, Vol. 24, No. 6, pp. 1182-1191, 2013.

[7] H. He, R. Li, X. Dong, and Z. Zhang, "Secure, Efficient and Fine-grained Data Access Control Mechanism for P2P Storage Cloud", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 4, pp. 471-484, 2013.

[8] A. Abbas, and S. U. Khan, "A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds", *IEEE Journal of Biomedical and Health Informatics*, Vol. 18, No. 4, pp. 1431-1441, 2014.

[9] C. A. Ardagna, M. Conti, M. Leone, and J. Stefa, "An Anonymous End-to-End Communication Protocol for Mobile Cloud Environments", *IEEE Transactions on Services Computing*, Vol. 7, No. 3, pp. 373-386, 2014.

[10] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security Challenges in Vehicular Cloud Computing", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 14, No. 1, pp. 284-294, 2013.

[11] H. Wang, and Z. Sun, "Study on the Improvement of ElGamal Cryptosystem Based on Elliptic Curve", *Journal of Networks*, Vol. 9, No. 11, pp. 3025-3029, 2014.

[12] S. Selvi, and R. Ganesan, "A Secured Cloud System using Hyper Elliptic Curve Cryptography", *International Journal of Scientific & Engineering Research*, Vol. 6, No. 1, 2015.

[13] J. Jose, and S. N. Das, "Hyper Elliptic Curve Encryption and Cost Minimization Approach in Moving Big Data to Cloud", *International Journal of Scientific Research Engineering & Technology (IJSRET)*, Vol. 4, No. 5, 2015.

[14] S. B. Akintoye, and K. A. Akintoye, "Data Security Scheme for Cloud Computing Using Signcryption Based on Hyperelliptic Curves", *Journal of Research and Development*, Vol. 2, No. 7, 2015.

[15] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis", *Digital Investigation*, Vol. 13, pp. 38-57, 2015.

[16] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing", *Information Sciences*, Vol. 258, pp. 371-386, 2014.