Heterogeneous Security Determination System Inculcating Elgamal Cryptosystem

Angel Rubavathy B[1], B Rebecca Jeyavadhanam [2]
[1] Research Scholar, Department of Computer Science, SRMIST,KTR, angelrub@srmist.edu.in
[2] Assosiate Professor, Department of Computer Applications, SRMIST, KTR, rebeccab@srmist.edu.in

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

ABSTRACT: ElGamal public key cryptosystem secures data using multiple output and inputs using efficient cryptosystem which provides ciphertext from plain text execution. There are many existing efficeint and modified Elgamal cryptosystem that implements different text size and data with efficient expansion time and rate. In our proposed security system heterogeneous determination of Elgamal cryptosystem inculcates various methodologies proceeding conversion of text data into binary files, arithmetic operations accomplished and it will be stored as metadata. That metadata converted into binary file and that will be stored inside the actual data. Final output will be encrypted using ElGamal algorithm using attribute based key from both encryptor side and decryptor side. Machine learning for this heterogeneous security methods will be prompted with one time three key encryption system along with fussy level selection of security implementation. Limitations assigned for file segments, user selection, key generation ranges and compacted machine learning in ElGamal algorithm endows privacy, security, robust and accuracy in data security.

Keywords : ElGamal Cryptosystem Algorithm, Heterogeneous Security Determination (HSD), Attribute based key generation, Fussy level selection and Machine Learning.

I. INTRODUCTION

Internet has been incorporated into almost all fields of economy, society, and life. The fast improvement of the Internet has added approximately a lot comfort to every day life, however additionally poses a risk to community protection. Various malicious community assaults can emerge in an limitless stream. Current global technology are continuously converting and developing. There also are a few issues with all technological developments. Also, net packages are greater widespread, and protection is the largest problem of those packages. So, to make those packages greater stable, new algorithms and strategies are being established. At this point, software program designers have to attempt to use new strategies and then, in the event that they succeed, they are able to observe those strategies to their very own electronic mail packages, that are now extensively utilized in today's global. This trial has been first of all used on the American Defense Ministry in 1970, which presents stable and short verbal exchange that everyone wants.

Many approaches are actually executed with the aid of using sending mails together with commercial enterprise corresponding or the world over corresponding. Besides that, there are different considerable traits of sending mails that are their cost, speed, and affectivity. Therefore, software program sending mails with the above-cited traits entice human with negative intentions. So, to shield our software program from such assaults, a robust encryption set of rules is recommended to be used. As well as, new techniques should be derived from antique algorithms in which the improvement of recent easy-to-use packages with new technology via coding in well-built programming languages will resolve a few protection issues. For all above-cited reasons, this studies proposes a change of the ElGamal cryptosystem with a purpose to be cited as the proposed Modified ElGamal Cryptosystem (MEC). It comprises of 3 steps: key pair era set of rules, encryption set of rules, and decryption set of rules.

The cryptographic metrics together with encryption time, decryption time, and enlargement rate measured to assess the proposed MEC. Different report sizes are used because the take a look at sample. The outcomes have been in comparison with the conventional EC and confirmed that the proposed MEC outperforms the conventional EC in phrases of execution time and enlargement rate. In 1985, [2] ElGamal Cryptosystem (EC) became at first presented. It is an extension of the Diffie-Hellman key settlement protocol and one of the few probabilistic schemes. Its safety relies upon at the difficulty of fixing the discrete logarithm problem.

The rest of this paper is organized as follows: Section II briefly reviews the related works. The detailed proposal of Heterogeneous security determination method is described in Section III. Section IV describes the deatils about the proposed algorithm. Section V presents the result and discussion. At the end of this paper, we provide our conclusion in Section VI.

II. LITERATURE SURVEY

Discrete logarithm hassle happens whilst the general public key (p, g, y) is given then, finding the personal key x such that: gx = y(mod p) The essential disadvantage of EC is the rate due to the fact there may be always a trade-off among safety and performance. [4] Sharma et al. claimed that EC is likewise sluggish due to the fact whilst exclusive information is encrypted, it generates multiple public keys. Thus, recently many researchers have taken into consideration flows of EC to enhance its safety both via way of means of combining it with the alternative modern public key cryptosystems or via way of means of editing its cryptosystem. A changed ElGamal cryptosystem changed into provided via way of means of [5]Sharma et al. to enhance the safety for encrypting lengthy messages and stable towards mathematical and brute-pressure assault in addition to Low-Modulus and Known-Plaintext assault on ElGamal.

ElGamal cryptosystem changed into reviewed via way of means of [6] Rosly et al. to decide how the information is secured for the duration of the encryption and decryption manner withinside the 32-bit computation. Based on their experiments, the most wide variety that may be computed the use of ElGamal in 32-bit computation is constrained to the wide variety below 232. ElGamal encryption scheme changed into recommended via way of means of [7] Kumar et al. that converts plaintext to factors at the elliptic curve via way of means of one to one correspondence the use of ASCII characters. They added Fibonacci Q-matrix to enhance the safety stages which can be tough to crack via way of means of recognised attacks. A key technology set of rules changed into proposed via way of means of Iswari [8] that is a aggregate of RSA and ElGamal set of rules to provide a double layer of safety.

A new ElGamal public key cryptosystem changed into evolved via way of means of [9] Inam & Ali primarily based totally at the matrices over a grouping. The underlying difficult hassle for his or her cryptosystem is the conjugacy seek hassle. They have changed the exponentiation of factors via way of means of conjugacy. A changed ElGamal Cryptosystem changed into provided via way of means of Ordonez et al. [10] in order that a couple of senders can encrypt a exclusive message the use of a couple of personal keys meant via way of means of a single receiver for decryption. Most of the preceding works have targeting enhancing the safety aspect of the conventional EC. To the first-class of our knowledge, none of the preceding works taken into consideration the hassle of low performance for the ElGamal cryptosystem.

III. PROPOSED METHODOLOGY:
HETEROGENEOUS SECURITY DETERMINATION (HSD) METHOD

ElGamal cryptosystem is uneven cryptosystem which its protection is predicated on the problem of discrete logarithm problem. It comprises of 3 phases: key pair era algorithm, encryption algorithm, and decryption algorithm. This procedure generates required keys (private key and public key) for each encryption and decryption procedure. The encryption procedure is finished the use of the general public key statistics. The following steps are taken into consideration to encrypt a exclusive message: The sender gets the general public key statistics only, which will allow her to encrypt. The sender encodes the message via way of means of changing its string illustration to its corresponding numerical value. The decryption procedure is done the use of the non-public key statistics.

In our proposed HSD method various conversions, storage, attribute based and user selctions are inculcated to prevail secured data environment. All the steps are inculcated with machine learning technique to automate security system strongly and efficiently. HSD process will be first stepup with conversion of text file into binary file. The odd number or even number from binary data will be chosen randomly by HSD and eventually manipulated with arithmetic operations such as addition, subtraction and multiplication.

The manipulated data will be stored as metadata that is text file. That too will be converted into binary and added some randomly chosen number from the allotted range of numbers. The binary converted metadata will be inserted into the original binary converted data. The eventual output file will be encrypted using ElGamal algorithm. This ElGamal algorithm is usually attribute based key cryptosystem. These keys will be assigned either from user side or encryptor or decryptor side. Other wise the determinant can assign key attributes from both encryptor and decryptor side.

The transferring file can be of any number of splits so that each segment can be separately assigned with preferred level of security. For each segment the complete HSD process will be implied according to the required level of security to each data segment. According to the security requirements user or encryptor or machine automatically assigns random number which will be generated from given range of numbers and deterrmine their attributes.

Once the encryption procedure accomplished using HSD method three keys will be sent to decryptor for enabling data decryption. If same key used twice then it will not be validated, once if three keys barred then that will be invalidated and other set of three keys will be sent to their mail id. After each generation and usage of three keys they are not valid anymore. Each time when three keys sent the instructions for applying them also will be sent like reverse of the key or straight key or the key place values from and to will be defined. This type of security provided only for high level secured data and will not be applied for low level or medium level data security. Moreover in high level security the keys and its instructions to enter will be sent one by one and not all at once.

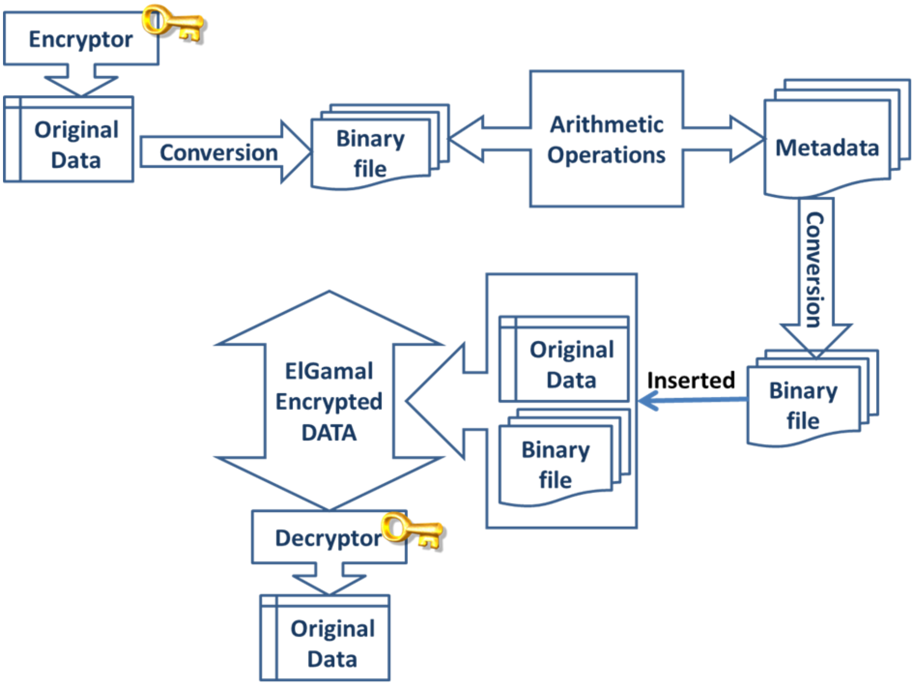


Fig. 1. Generic design of proposed methodology

In high level security pattern the security provided for more than one number of file or more than one number of segments then the splitting will be randomly shuffled as metadata and attach those parts like from part 1 to part n (1....n). The limitations can be determined such as any number files, its assembling techniques and file split ups accomplished. Automation of efficient security provided by machine learning which will be verified from the users perception. Machine learning process keenly notices and analyzes the patterns of selction of users, attributes, key generation ranges, number of split-ups or segments of files and level of security assigned to each file or segment. Thus attains efficient and feasible automated security of data. Fig.2 shows the traces of generic design

IV. SECURITY LEVELS WITH ELGAMAL PERFORMANCES

The essential security provided based on majority of security requirements it involves encryption, decryption and attribute based key authentication etc. In HSD system heterogeneous security will be implemented to secure data. Many data split ups involved chooses and computes various algorithm system with performance oriented data security. Elgamal is the existing highly secured technique whereas, we inculcate elgamal crytosystem along with various binary converted security implementation using metadata methodologies. In such asymmetric cryptosystem which relies on arithmetic computation alomg with discrete problems to generate keys either from encryptor side, or it randomly choses according to user requests. The proper encryption and decryption algorithm proceeds generating public key and private key where the algorithm for heterogeneous determination of security provies cryptographic secured data.

The user data U_d initialized which will be split up into segments and one specific segement loops and determines the level of security. Threshold (T) for acceleration of execution system along with its rate of number of rounds (N_r) will be set as the range value to perform process of converting metadata. As the preliminary process of decryption the text file will be converted in to binary data (B_c) and the random number (R_s) either odd or even will be selected for further manipulation. The binary data will be done with arithmetic operation (A_o) with addition, subtraction or multiplication. The created data file is considered as metadata (M_d) and this metadata will be again converted into binary file.

This metadata binary conversion (M_d B_c) include its manipulated binary converted data into the original existing binary file (IM_d). After all these steps of heterogeneous binary converted decrypted data will be undergone attribute based key setting A_k where the Elgamal encrytpion cryptosystem which is one of the efficient security system is inculcated and implemented for providing high level secured data. The security operations performed with integrity and random numbers will be chosen from the provided range of values. It would be either selected from encryptor side or decryptor side else the uer requests responded dynamically for selction of range values using conditions within the key range of values. Thus the secured cryptographic data output file will be sent to the destination. There the decryptor will be provided with different types of key generation according to the level of security the user has set. Table.1 encloses pseudo code for the propounded algorithm

.

Table 1.Pseudo code of the proposed algorithm.

```
Algorithm 1 Algorithm for heterogeneous security determination
Input: $U_d$ //User data
Output: cryptographic secured data
Initialization:
$U_d \leftarrow$ User data
While ($N_r < T$)// Number of rounds lesser than threshold
    $B_c \leftarrow$ Binary conversion of user data
    $R_s \leftarrow$ Random number selection
    $A_o \leftarrow$ Arithmetic operation
    $M_d \leftarrow$ Create metadata
    $M_d B_c \leftarrow$ Meta data binary conversion
    $A_o \leftarrow$ Arithmetic operation
    $IM_d \leftarrow$ Include metadata with existing binary data
    $E_e \leftarrow$ Elgamal encryption
    $A_k \leftarrow$ Attribute based key setting

    If ($S_l > 2$) then//high security level
        $D_s \leftarrow$ max data split up
        $R_{sf} \leftarrow$ random shuffling of split up
        $M_{sd} \leftarrow$ Merge shuffled data
        $E_{app} \leftarrow$ Elgamal application
    End if

    If ($S_l == 2$) then//medium security level
        $D_s \leftarrow$ medium data split up
        $M_{sd} \leftarrow$ Merge shuffled data
        $E_{app} \leftarrow$ Elgamal application
    End if

    If ($S_l < 2$) then// low security level
        $D_s \leftarrow$ data split up
        $M_{sd} \leftarrow$ Merge shuffled data
        $E_{app} \leftarrow$ Elgamal application
    End if
End while
```

The data split-ups will be segmented as various parts and the public key or private key sets for the HSD decrypted data. The sender of data can only have access to encrypt and send data thus the decryptor side couldnt decrypt easily without much knowledge about decryption technique. The encryption and decryption algorithm inculcates various other different conversions and manipulations to provide high security. The level of security provided will be determined by the segments and each segement can be collocated and categorized according to its level of security requirement. Security level (S_l) determined by the system and the low level security will have very less data split ups which will be shuffled and merged into different parts where the HSD and Elgamal security algorithm is implemented. In medium level moderately obscured data split ups and segments done and SD process inculcated along with Elgamal. In high level security Maximum data segments will be done ad randomly shuffled parts will be set within provided range of values determined by the users.

The main advantage of providing security is that can be selected and chosen from encryptor side or users can directly chose their requirement. The number of segments will not be the major size or performance factor as the selection of security level need to be provided for each segment can be determined individually. Thus for parts or segments with high secured data only will be accomplished with all manipulations and process of high level HSD secured encryption. Other segments will be assigned medium or low level encryption according to their requirement thus to save size, increase speed and thus effectuate efficeint data security.

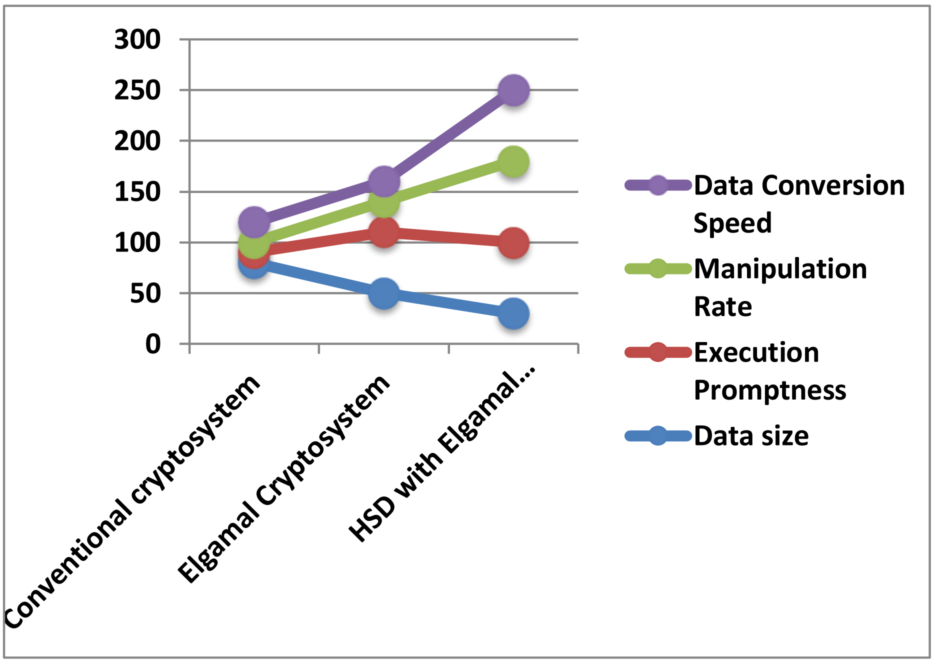
V. RESULT ANALYSIS

In the result analysis, where the evaluation parameters for providing secured cryptosystems the implemented heterogeneous Secured determination system inculcating the Elgamal cryptosystem. The various security parameters and manipulations such as text into binary conversion, arithmetic operations, execution of arithmetic operations and metadata processing and manipulaions are involved to accomplish data encryption and decryption efficiently. Analysing results provided with experimental analysis of our proposed system can be determined using factors like size of data used, execution promptness, rate of manipulation, speed of data conversion etc. Fig.3 potrays the graphical comparision of the cryptosystem.

	Data size	Execution Promptness	Manipulation Rate	Data Conversion Speed
Conventional cryptosystem	80	10	10	20
Elgamal Cryptosystem	50	60	30	20
HSD with Elgamal cryptosystem	30	70	80	70

Table 2. Comparability between the Three different Cryptosystem

The Conventional cryptography system, Elgamal cryptosystem and our proposed Heterogeneous security determination system which inculcates Elgamal analysed and determined. The conversion of text file to binary and the metadata conversion speed for each system where the proposed HSD method has higher speed than compared with other methods. The manipulation of various arithmetic operations also done effectively compared with other conventional cryptography. Prompt execution of encryption and decryption key generation and various process accomplished perfectly in HSD based cryptosystem.



.

Fig. 3. Juxtaposition between Conventional cryptosystem, Elgamal cryptosystem and HSD wth Elgamal cryptosystem

From all the above factors the size of data for HSD with Elgamal cryptosystem is very less as the manipulations and converted metadata occupies lesser space. Thus the performance based on above factors states the efficiency and vehemently our proposed Heterogeneous security determination along with Elgamal security cryptosystem is best machine learning security system.

VI. CONCLUSION

The paper confronts highest level of security from super high level security, high level security, medium level security and low level security. Heterogeneous type of security will be determined using various encryption and attribute based key techniques and inculcates ElGamal algorithm. Various types of key generation used for securing various segments of data files sent and those segments or split-ups also determined by HSD method to achieve efficient security to data. The promptness, speed of execution and efficient security of proposed system provides strong security method than conventional methodologies. From our proposed method it assures strong robust and secured data files by huge inculcation of strong techniques.

REFERENCES

1. Okeyinka AE. Computational complexity study of RSA and Elgamal algorithms. Transactions on engineering technologies. San Francisco (CA); 2017. p. 233–243.
2. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory. 1985;31(4):469– 472.
3. Mahajan S, Singh M. Analysis of RSA algorithm using GPU programming. arXiv preprint arXiv. 2014.
4. Sharma A, Attri J, Devi A, et al. Implementation & Analysis of RSA and ElGamal algorithm. Asian Journal of Advanced Basic Sciences. 2014;2(3):125–129.
5. Sharma P, Sharma S, Dhakar RS. Modified elgamal cryptosystem algorithm (MECA). 2nd International Conference on Computer and Communication Technology (ICCCT). Allahabad, India; 2011. p. 439– 443.
6. Rosly NA, Aziz MZ, Hashim H, et al. Cryptographic computation using ElGamal algorithm in 32-bit computing system. Third International Conference on Control, Automation and Systems Engineering (CASE-13). Atlantis Press; 2013.
7. Kumar BR, Sekhar AC, Naidu GA. A Novel ElGamal encryption scheme of elliptic curve cryptography. International Journal of Computer Trends and Technology. 2015;20(2):70–73.
8. Iswari NM. Key generation algorithm design combination of RSA and ElGamal algorithm. International Conference on Information Technology and Electrical Engineering (ICITEE); Yogyakarta, Indonesia; 2016.
9. Inam S, Ali R. A new ElGamal-like cryptosystem based on matrices over grouprings. Neural Comput Appl. 2018;29(11):1279–1283.
10. Ordonez AJ, Medina RP, Gerardo BD. Modified El Gamal algorithm for multiple senders and single receiver encryption. IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). Penang, Malaysia; 2018. p. 201–205.
11. Okeyinka AE. Computational speeds analysis of RSA and ElGamal algorithms on text data. Proceedings of the World Congress on Engineering and Computer Science. San Francisco (CA); 2015. p. 115–118.
12. Patil P, Narayankar P, Narayan DG, et al. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Comput Sci. 2016;78:617–624.