Homomorphic Encryption Using Bio-Inspired Method

Satmeer Kaur[1], Inderdeep Kaur[2]
[1]*Student*, [2]*Assistant Professor*
GGS College Kharar, Mohali (Punjab)

Abstract - Cloud computing may be described as a distributed design that is accessible to different forms of security intrusions. An encoding technique named homomorphic encoding is used for the encoding of entities which are utilized for the accession of data from cloud server. The main problems of homomorphic encoding scheme are key organization and key allocation. Because of these issues, effectiveness of homomorphic encryption approach decreases. The encoding procedure requires the generation of input, and for this, an approach named Particle swarm optimization is implemented in the presented research study. PSO algorithms are nature encouraged meta-heuristic algorithms. These algorithms are inhabitant reliant. In these algorithms, societal activities of birds and fishes are utilized as an encouragement for the development of a technical mechanism. Relying on the superiority of computations, the results are modified with the help of algorithms which are taken from arbitrarily allocated pattern of particles. With the movement of particles around the searching area, the spontaneity is performed by utilizing a pattern of arithmetical terminology. For the generation of permanent number key for encoding, optimized PSO approach is utilized. MATLAB program is used for the implementation of PSO relied homomorphic algorithm. The investigating outcomes depicts that this technique proves very beneficial on the requisites of resource exploitation and finishing time. PSO relied homomorphic algorithm is more applicable in terms of completion time and resource utilization in comparison with homomorphic algorithm.

Keywords - Particle swarm optimization, Homomorphic, Key management, Nature Inspired, Resource utilization

I. INTRODUCTION

A number of security methodologies implemented various cryptographic approaches [4]. The implementation of cryptographic approaches is necessary for ensuring the protection inside obscure. For the encoding and decoding of information, an input is necessary in this system. This is necessary for maintaining the reliability and privacy of information. With the help of these mechanisms, data sharing in the cloud can be performed with security. This data can also be stored in more secure manner with the help of these techniques. The cryptography is known as a technique which deigns ciphers. A lot of cryptographic approaches have been already projected these days. These approaches are classified in terms of balanced and unbalanced approaches. The keys are utilized in these algorithms by diverse methods [5]. In the symmetric or balanced input encoding, a familiar undisclosed key is shared amid senders and receivers. The secrecy of the key must be implemented in both sides. The information can be decoded or encoded with the help of this secret key via both sides. In unbalanced or asymmetric key encoding, two dissimilar keys are utilized. Two different keys are used in these algorithms during encoding and decoding procedure. In a case, when personal or confidential key is unidentified and the accessibility of undisclosed key is in the hand of user, then for the implementation of definite functions, an approach named homomorphic encoded technology is used [6]. Just like computations applied on unprocessed information, the outcomes of any kind of procedures may be decoded at this point. In this approach without implementing previous decoding, calculations on encoded information can be executed. When the encoded outcomes are converted into decoded data after the implementation of procedure, an authentic outcome is obtained. In the obtained outcomes, the recognition of authentic plain content is not possible. While Enc (f (a, b)), is calculated through Enc (a) and Enc (b), then this type of encoding is called homomorphic encoding. The function f can be described in the form of +, x, $\oplus$. No personal key is involved in this case. For maintaining, segregation between homomorphic encoding, a number of procedures are applied on the given unprocessed information. During the implementation of additive homomorphic encoding technique, the unprocessed supplies are included. The multiplication of unprocessed products can be performed only in case of multiplicative homomorphic encoding [7]. A complete description of both the algorithms is given below where the key utilization in encoding technique is named as E k while D k represents decoding approach.

$$D_k (E_k (n)\times E_k (m))=n\times m \quad \text{OR} \quad Enc(x\otimes y)=Enc(x)\otimes Enc(y) \quad \dots (1)$$

$$D_L (E_L (n)\times E_L (m))=n+m \quad \text{OR} \quad Enc(x\oplus y)=Enc(x)\oplus Enc(y) \quad \dots (2)$$

For performing cloud computing, the presented research work is associated with homomorphic encoding technique. The detailed information associated with homomorphic technique is applied in the first phase. For the description of earlier tasks performed by writers, the associated work is applied in section 2. The third phase depicts the projected method in association with flowchart and algorithm. The outcomes and the study are

presented in association with graphical investigation in the third part.

II. RELATED WORK

The author proposed a hybrid cloud computing approach based on Paillier algorithm [8]. This is a multiplicative homomorphic algorithm which includes homomorphic and RSA encryption algorithm. The integration of simple addition and multiplicative operation and operands can be termed as the description of client's calculation requests. Depending upon the types of operations, the encryption is processed by the encryption decryption machine which runs in private cloud. The cipher texts are uploaded to the public cloud further. Without knowing the actual plain text, the calculation is processed by the public cloud. Several simulations are performed and results are analyzed in this paper, which shows that the proposed approach is more practical and efficient in comparison with several traditional approaches. The author proposed a novel approach such that higher speed and enhanced performance can be achieved which ensures that it is possible to implement this algorithm feasibly in applications [9]. The proposed algorithm is named as Artificial Bee Colony Random Number Generator – ABCRNG. Inside up and down approach and above and below mean method, the Run test is performed such that the randomness of random numbers created by proposed approach might be evaluated. It is seen that with the help of proposed approach, the strength and security of systems are improved along with the achievement of completely random and non-repeating final keys. Various applications that need random numbers utilize this proposed approach. The author proposed a homomorphic signature mechanism along with Identity Management (IDM) sever to provide security environment within the cloud applications [10]. The real or fake users can be distinguished by applying the implicit authentication approach. This helps in accurately authenticating the users within the system. The IDM is used as medium to authenticate the user. During the complete authentication process, no password is utilized. Thus, at the end of this process, the client is authenticated safely through this approach. The author proposed the design of a novel communication protocol which can be applied in a distributed measuring system to provide authenticity, integrity and privacy of data [11]. For securing the data, some techniques like processing method, integer arithmetic and multi-threading are used. Further, to a higher factor, the 32 and 64-bit arithmetic operations are enhanced in this approach. To provide privacy in terms of design, this improved algorithm is integrated with cloud computing architecture. The time based constraint issues related to smart meter gateway tariffs are resolved with the help of resulting parallelized algorithm. As per the conclusions it is seen that the demands of real world applications are met with the help of this fully homomorphic encryption library.

The author proposed an Optimal Asymmetric Encryption Padding (OAEP) which is used along with Hybrid Encryption algorithm such that the user's data can be encrypted. A function can be calculated by multiple parties on their inputs through this approach along with the insurance of integrity and confidentiality of the systems. The multi-party calculation is integrated along with homographic encryption to propose a novel approach here through which calculations of encrypted data are performed and no decryption technique is required here [12]. Further, the description of various cryptographic techniques implemented in the cloud model is provided here. Comparisons are performed amongst various approaches in terms of overhead for the evaluation of proposed approach performance. The author proposed a fully homomorphic encryption mechanisms based on the attribute encryption in association with LSSS matrix. A fine-grained and flexible access control is provided with the help of "Query-Response" mechanism such that the required data can be extracted from the cloud servers in an effective manner [13]. In order to avail certain privileges from users without providing any update to the key client, higher flexibility is provided by this approach. This helps in minimizing the client's pressure to some extent.

III. PROPOSED METHODOLOGY

A number of encoding schemes are available for ensuring the protection of clouds. For this purpose a "completely Homomorphic" approach is very trustworthy. In comparison with "Full Disk Encryption", this approach provides better confidentiality and protection. The major issues associated with completely Homomorphic encoding scheme are key storage, key organization, admittance control and maintenance of information accruement catalog. In the past years, a lot of techniques have been proposed for the settlement of issues like key organizing and key allocation. These techniques are vulnerable against these intrusions. There are chances of failing third party investigation system, in case of third party compromise and malevolent state. Therefore an effective system will be designed by user for key allocation and key organization. For the attainment of effective key organizing scheme, particle swarm optimization approach in association with homomorphic encoding approach is implemented. PSO algorithms are nature encouraged meta-heuristic algorithms. These algorithms are inhabitants reliant. In these algorithms, societal activities of birds and fishes are utilized as an encouragement for the development of a technical mechanism. Relied on the superiority of computations, the results are modified with the help of algorithms which are taken from arbitrarily allocated pattern of particles. With the movement of particles around the searching area, the spontaneity is performed by utilizing a pattern of arithmetical terminology. With the implementation of easy and basic arithmetical terminology, some inter- particle interactions are carried out. For the swarm, the movement of every particle is

recommended towards the finest recognized location. Presence of arbitrary apprehensions is also identified here. But there is a scarcity of some variants which uses different up gradation policies. An effective description of PSO algorithm's aiming operation is given here. For this purpose, a comparison between present and conventional iterations is performed on the foundation of swarm value. For the identification of aiming operation, swarm value containing maximum iteration is considered [15]. The definition of vibrant aiming function is presented by the equation 3. Its value changes after every iteration.

$$v_{i+1} = v_i + c * rand * (p_{best} - x_i) + c * rand * (g_{best} - x_i) \quad \text{- - - - -} (3)$$

As described in equation, speed of elements is represented by V_i, the maximum value between existing options is represented by p_{best} and random value is represented by rand. X value is used for the implementation of every characteristic of website while c value is utilized for the description of whole characteristics of website. p_{best} is the best value recognized from every inhabitants and the best value recognized from every iteration is represented by g_{best}. After the finalization of aiming function and quality negotiation, the obtained value is added in equation as shown below:

$$x_{i+1} = x_i + v_{i+1} \quad \text{- - - -} (4)$$

Position vector is represented by x_{i+1}. PSO algorithms are utilized for the elimination of multi aiming optimization problems. Some vibrant aiming functions are included in PSO algorithms. These functions are used for the enhancement of system effectiveness in association with finest computed value [16]. Input data is used by particle swarm optimization for encoding and generated an advanced value which will be used as a key for encoding.

E-Homomorphic Encryption Algorithm ()

1. Input: Data for encryption
2. Output: Encrypted Data
Logic
Key Generation ()
I=Input Data
For I = 1 to it_Max
For each particle p in P do
Fp=f(p)
If fp is better than f(pBest)
pBest=p;
end
end
gBest=best p in P
For each particle p in P do
*V=V+Cl*rand*(pBest-p)+c8*rand*(gBest-p)*
P=p+v
End
End
3. Key for Data encryption =P
4. If (user enter key=P)
Decrypt data;
Else
Display message wrong password
5. End

IV. PROPOSED FLOWCHART

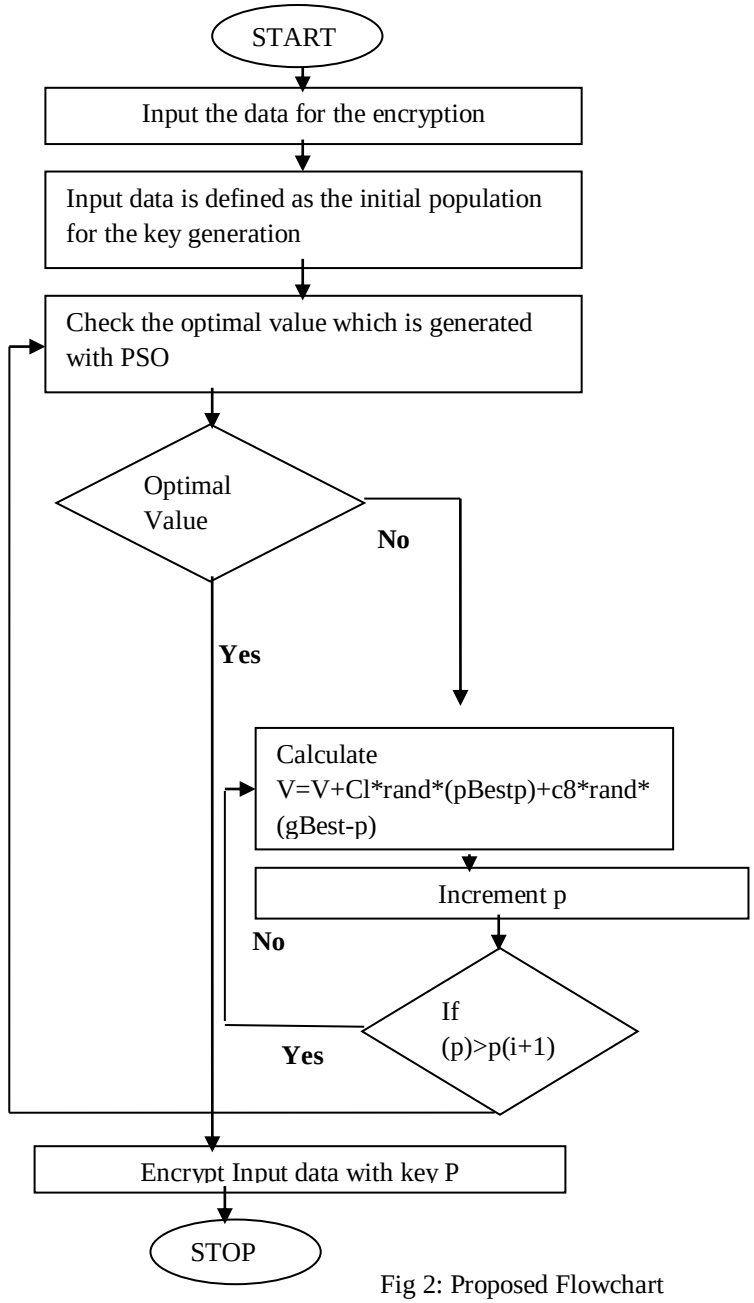

Fig 2: Proposed Flowchart

For encoding, input data is taken in the form of a picture in the presented approach as shown in fig 2. Balanced cryptography is used by the homomorphic encoding system. Particle swarm optimization approach is utilized for the generation of keys which are used for picture encoding

V. RESULT AND ANALYSIS

MATLAB programming is used for encoding of data in cloud system in this approach. Input is applied in the form of a picture. For performing the encoding and decoding of cloud information, balanced encoding algorithm is utilized. An advanced key is generated by PSO approach. This key is used for the encoding of information in association with homomorphic system. Two parameters named as execution time and resource consumption are used for investigation of projected scheme presentation. The reproduction outcomes are presented in table 1. An operating system named Xnon in data sample is applied on every fundamental mechanism. Every fundamental mechanism contains 5GB RAM and total 7 fundamental machines are used. Total numbers of pictures are 80 and every picture has a dimension of 256*256.

Parameter	Values
Operating System	Xnon
Number of virtual machines	7
Number of hosts	10
RAM	5 GB
Input Data	Image Data
Image size	256*256
Number of Images	80

Table 1: Simulation Parameters

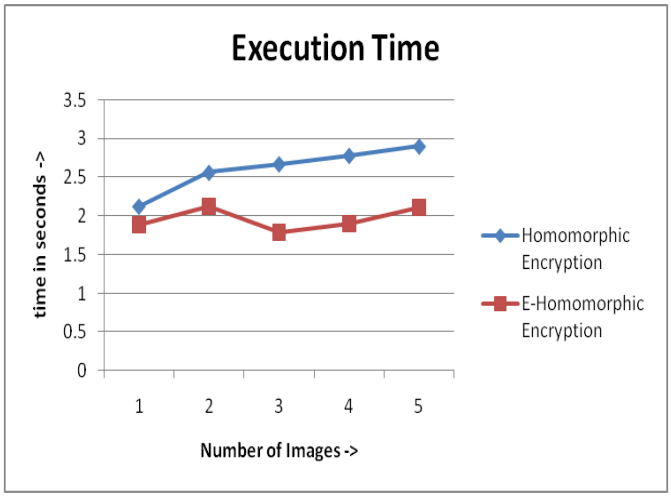

Figure 3: Execution Time

Figure 3 depicts a comparison between presented and previous algorithm implementation time. The existing algorithm is of homomorphic encoding type while the projected algorithm is a modified version of homomorphic encoding system.

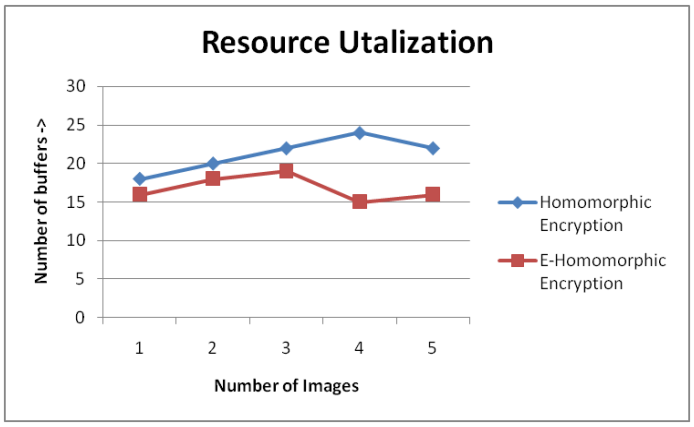

Figure 4: Resource Utilization

A comparison between existing homomorphic encoding system and modified homomorphic encoding system is performed for the identification of resource exploitation in figure 4 scheme. After investigation, it has been proved that the resource exploitation is less in case of proposed homomorphic approach.

Parameter	Homomorphic Encryption	E-Homomorphic Encryption
Execution Time	3.8 seconds	2.2 seconds
Resource Utilization	18 Buffers	12 Buffers

Table 2: Comparison of Techniques

. The table no 2 shows a comparison between homomorphic encoding and enhanced homomorphic approaches by means of resource exploitation. Various comparative results proved that the enhanced homomorphic encoding approach performed well on all parameters.

VI. CONCLUSION

The encoding of cloud information is performed by homomorphic encoding system. Two main problems associated with homomorphic encoding approach are key allocation and key organization. For the generation of key for encoding, PSO advanced algorithm is implemented. For the generation of encoded data, this key is applied as input to the

homomorphic encoding system. MATLAB programming is utilized for the implementation of presented approach, and the outcomes are investigated by means of resource exploitation and implementation time. It is analyzed that the resource exploitation and exploitation time of enhanced homomorphic algorithm is minimum in comparison with presented homorphic encoding system. For ensuring the information reliability in cloud surroundings, this approach will be enhanced more in future.

VII. REFERENCES

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, U.S. Department of Commerce, September 2011.

[2] R. Kanagavalli and Dr. Vagdevi S, "A Mixed Homomorphic Encryption Scheme for Secure Data Storage in Cloud", IEEE Intemational Advanced Computing Conference IACC2015, 2015

[3] K. Lauter, M. Nachirg, V. Vaikuntanathan, "Can Homomorphic Encryption be Pratical?," CCSW'11,October 21,2011, Chicago, Illinois, USA, pp.113-124.

[4] M.TEBAA and S.ELHAJII, "Secure cloud computing through Homomorphic Encryption", International Journal of Advancements in Computing Technology, Vol.5,No.16, 2013,pp.29-38.

[5] Payal V. Parmar, et.al, "Survey of Various Homomorphic Encryption algorithms and Schemes", International Journal of Computer Applications (0975-8887), Vol.91, No.8, April 2014, pp.26-32.

[6] M. Ogburn, C. Turner, P. Dahal, "Homomorphic Encryption In Complex Adaptive Systems", Publication 3, Baltimore,MD,Elsevier,2013,pp.502-509.

[7] R. Rivest, A.Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communication of the ACM,21(2):120-26,1978.ComputerScience,Springer,1999,pp.223- 238.

[8] Xidan Song, Yulin Wang, "Homomorphic Cloud Computing Scheme Based on Hybrid Homomorphic Encryption", 2017, 3rd IEEE International Conference on Computer and Communications

[9] J.Sai Geetha and D. I. George Amalarethinam, "ABCRNG - Swarm Intelligence in Public key Cryptography for Random Number Generation", Intern. J. Fuzzy Mathematical Archive, Vol. 6, No. 2, 2015, 177-186

[10] Lim Tsu Chean, Vasaki Ponnusamy, Suliman Mohamed Fati, "Authentication Scheme using Unique Identification method with Homomorphic Encryption in Mobile Cloud Computing", 2018, IEEE

[11] Alexander Oppermann, Federico Grasso Toro, Jean-Pierre Seifert, "Secure Cloud Computing: Communication Protocol for Multithreaded Fully Homomorphic Encryption for Remote Data Processing", 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications

[12] Debasis Das, "Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi-Party Computation", 2018, IEEE

[13] Yong Ding, Xiumin Li, "Policy Based on Homomorphic Encryption and Retrieval Scheme in Cloud Computing', 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)

[14] George Anescu, Ilie Prisecaru, "NSC-PSO, a novel PSO variant without speeds and coefficients", 2016, 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing Ajith Abraham, Tarun Kumar Sharma, Millie Pant, "Blend of Local and Global Variant of PSO in ABC", 2013, IEEE

[15] Shailesh Tiwari, K.K. Mishra, and A.K. Misra, "Test Case Generation for Modified Code using a Variant of Particle Swarm Optimization (PSO) Algorithm", 2013 10th International Conference on Information Technology: New Generations

[16] Satvir Singh, Shivangna, Etika Mittal, "Range Based Wireless Sensor Node Localization using PSO and BBO and its variants", 2013 International Conference on Communication Systems and Network Technologies