International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Enhancement in Homomorphic Encryption Scheme of Cloud Computing to Isolate DOS Attack

Jaspreet Kaur[1], Dr. Gurjit Singh Bhathal[2]

[1]Research Scholar, Dept. of Computer Science and Engineering, Punjabi University, Patiala, India
Email: *jasspreet87270[at]gmail.com*

[2]Department of Computer Science and Engineering, Punjabi University Patiala, India
Email: *gurjit.bhathal[at]gmail.com*

Abstract: ***Cloud computing (CC) is a kind of a distributed design which can be accessed through dissimilar forms of security intrusions. An encoding method recognized as homomorphic encoding is adopted to encode the entities which assist in acquiring the data from the cloud server. The key organization and key allocation are the major issues that often occurred in the homomorphic encoding method. These problems lead to alleviating the efficiency of HEA (homomorphic encryption algorithm). The input must be generated in the encoding process. Thus, this study makes the utilization of PSO (Particle swarm optimization) to achieve this. The PSO algorithms have an influence on nature based meta - heuristic algorithms. These algorithms are inhabitant reliant. These algorithms employ the societal activities of birds and fishes as a motivation to construct a technical technique. On the basis of the supremacy of computations, the algorithmic approaches generated from arbitrarily allocated patterns of particles are exploited to modify the outcomes. As the particles move around the searching area, a pattern of arithmetical terminology is deployed to carry out the spontaneity. The permanent number key is produced to perform the encoding, using optimized PSO (Particle swarm optimization). The homomorphic algorithm based on PSO is implemented on MATLAB. The results reveal that the introduced method proves is efficient for resource usage and finishing time. This approach is more adaptable with regard to completion time and resource usage as compared to homomorphic algorithms.***

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

1. Introduction

Different cryptographic techniques are utilized in several security mechanisms [4]. The deployment of cryptographic techniques is required to ensure the protection inside obscure. A system requires input in order to encode and decode the information. This process is essential to keep the information secure and reliable. Such techniques are assisted in sharing the data in a secure manner. These mechanisms are also useful to store the data with privacy. The cryptography is a technique in which the ciphers are designed. In recent times, various cryptographic techniques are developed. These methods have two categories: balanced and unbalanced approaches. Different schemes are employed to exploit the keys in these mechanisms [5]. The balanced input encoding shares a familiar undisclosed key from senders to receivers. Both the ends keep the key confidential. These sides utilize this secret key with the purpose of encoding or decoding the information. The latter category deploys two diverse keys. The information is encoded and decoded applying two diverse keys in these algorithms.

When the personal or secret key is not recognized and only user can access the confidential key, the definite functions are employed using a technique known as homomorphic encoded technology [6]. Similar to execution of computations on the unprocessed information, the decoding of the results of any kind of procedures is performed at this point. This technique can compute the encoded information without any execution of earlier decoding. The valid results are acquired after employing the procedure for transforming the encoded outcomes into decoded data. The attained results do not facilitate to recognize the valid plain content. Enc (a) and Enc (b) are assisted in computing the Enc (f (a, b)). Thus, such a encoding is named as homomorphic encoding. The function f is defined in the form of +, x, ⊕. This case has not utilized any personal key. In order to maintain the segregation among homomorphic encoding, various processes are implemented on the given unprocessed information. The unprocessed supplies are considered while deploying an additive homomorphic encoding method. The unprocessed products are multiplied only in case of multiplicative homomorphic encoding [7]. The algorithms are defined comprehensively in the given equation at which E k denotes the key exploitation in encoding method and the D k is the decoding approach.

$D_k (E_k (n) \times E_k (m)) = n \times m$ OR $Enc (x \otimes y) = Enc (x) \otimes Enc (y)$ … (1)

$D_L (E_L (n) \times E_L (m)) = n+m$ OR $Enc (x \oplus y) = Enc (x) \oplus Enc (y)$ … (2)

In order to perform the CC (cloud computing), the suggested research work is conducted on the basis of homomorphic encoding method. The initial stage has depicted the comprehensive information related to homomorphic encoding method. The section stage discusses about the detailed review of precious works that researchers have done. The third stage demonstrates the introduced technique on the basis of flowchart and algorithm. This stage also defines the outcomes and the study depending upon the graphical investigation.

2. Related Work

The author suggested a hybrid CC (cloud computing) technique on the basis of the Paillier algorithm [8]. It was a multiplicative homomorphic algorithm in which homomorphic and RSA encryption algorithm were contained. The simple addition and multiplicative operation and operands were integrated and called as the description regarding the calculation requests of client. The encryption

decryption system whose execution was done on cloud was implemented to process the encryption on the basis of kinds of operations. Moreover, the uploading of cipher texts was performed to the public cloud. The public cloud executed the computation without any knowledge related to the public cloud. Various simulations were conducted and the analysis of results was carried out. The results demonstrated that practicality and efficiency of the suggested technique over the conventional methods. An innovative technique was put forward by the author for attaining higher speed and improved performance [9]. This ensured that the introduced technique was feasible in applications. The introduced technique is recognized as ABCRNG (Artificial Bee Colony Random Number Generator). The up and down technique and above and below mean scheme carried out a run test for computing the randomness of random numbers which was generated using introduced technique. The evaluation indicated that the introduced technique had potential for enhancing the strength and security of systems and acquiring the random and non - repeating final keys in comprehensive way. Several applications, in which random numbers were required, made the deployment of this technique. The author projected a homomorphic signature system along with IDM **(**Identity Management) sever to keep the environment secure in the cloud applications [10]. The implicit authentication technique was implemented to differentiate the real users from the forged ones. The users were authenticated in the system. The Identity Management was adopted as medium for validating the user. There was not any password employed in the entire authentication procedure. Therefore, at the completion of this procedure, the projected system authenticated the client in secure manner. The author focused on developing a new communication protocol whose implementation was done in a distributed measuring system to keep the authenticity, integrity and privacy of data [11]. The data was kept secured using some schemes such as processing method, integer arithmetic and multi - threading. Moreover, this protocol aided in improving arithmetic operations of 32 and 64 - bit at a higher factor. The privacy was attained with regard to design by integrating this enhanced algorithm with CC (cloud computing) architecture. The resulted parallelized algorithm was useful for tackling the time based constraint issues about the smart meter gateway tariffs. The developed FHE (fully homomorphic encryption) library was capable of fulfilling the requirements of real world applications.

An OAEP (Optimal Asymmetric Encryption Padding) technique was established by the author that was employed with the Hybrid Encryption algorithm with the objective of encrypting the data of user. Multiple parties computed a function on their inputs with the deployment of established approach and ensured the integrity and secrecy of the systems. A new mechanism was suggested by an author by integrating multi - party calculation with HE (homographic encryption) [12]. This approach was valuable to quantify the encrypted data. The decryption method was not necessitated in the suggested approach. Moreover, diverse cryptographic methods executed in the cloud model were described in this approach. A number of methods were compared with regard to overhead in order to compute the suggested approach. The author investigated a FHE (fully homomorphic encryption) on the basis of the attribute encryption related to the LSSS matrix. The Query - Response system was put forward to offer a fine - grained and flexible access control with the purpose of extracting the required data from the cloud servers efficiently [13]. This approach was flexible for attaining certain privileges from users for which it had not offered any update to the key client. The investigated approach was useful to diminish the pressure of the client to some extent.

3. Proposed Methodology

There are various encoding technique are present which ensure the security of clouds. To achieve this, a completely Homomorphic technique is effective and reliable. Unlike the Full Disk Encryption, this technique offers higher privacy and protection. This technique has faced diverse issues such as to store the key, organize the key, to control the admission and maintain the information accruement catalog. Over the past decades, a number of schemes have been suggested to deal with these issues related to organize the key and allocate the key. These methods have susceptibility against these intrusions. The third party investigation system may be faced failure in case of third party compromise and malevolent state. Thus, the user focuses on developing an effectual system with the objective of allocating and organizing the key. An efficient key organizing system can be generated using PSO (particle swarm optimization) based homomorphic encoding approach. PSO algorithms are meta - heuristic having influence of nature. These algorithms make the deployment of societal activities of birds and fishes as a basis of construct a technical method. The supremacy of computations is considered for the modification of outcomes using the algorithms which are developed from arbitrarily allocated pattern of particles. As the particles move around the searching region, a pattern of arithmetical terminology is exploited to perform the spontaneity. The simple and basic arithmetical terminology assists in accomplishing some inter - particle interactions. For the swarm, the movement of every particle is suggested to the finest recognized locality. It is also determined that the arbitrary apprehensions are present or not. Some variants, in which various up - gradation policies are deployed, are lacked.

In this, the aiming operation of particle swarm optimization algorithm is discussed efficiently. To achieve this, the present iteration is compared with the traditional one with regard to the swarm value. The aiming operation is recognized considering the swarm value having greatest iteration [15]. The equation 3 is expressed to define the vibrant aiming function. Its value changes after every iteration as:

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

In this, V_i denotes the speed of elements, the p_{best} is the maximum value among existing options and the rand illustrates the random value. X value is utilized to implement every characteristic of website. c value is used to define the entire characteristics of website. p_{best} represents the best value whose recognition is done from every inhabitants and g_{best} depicts the best value recognized from every iteration. When the aiming function and quality negotiation are finalized, the obtained value is inserted in the equation as:

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

In this, x_{i+1} denotes the position vector. Particle swarm optimization algorithm is adopted to remove the multi aiming optimization issues. The PSO algorithms are consisted of some vibrant aiming functions. These functions assist in improving the efficiency of the system with regard to the finest computed value [16]. The PSO algorithm deploys the input data to perform the encoding and generates an advanced value that can be employed as a key for encoding.

E - Homomorphic Encryption Algorithm (HEA)

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

Proposed Flowchart

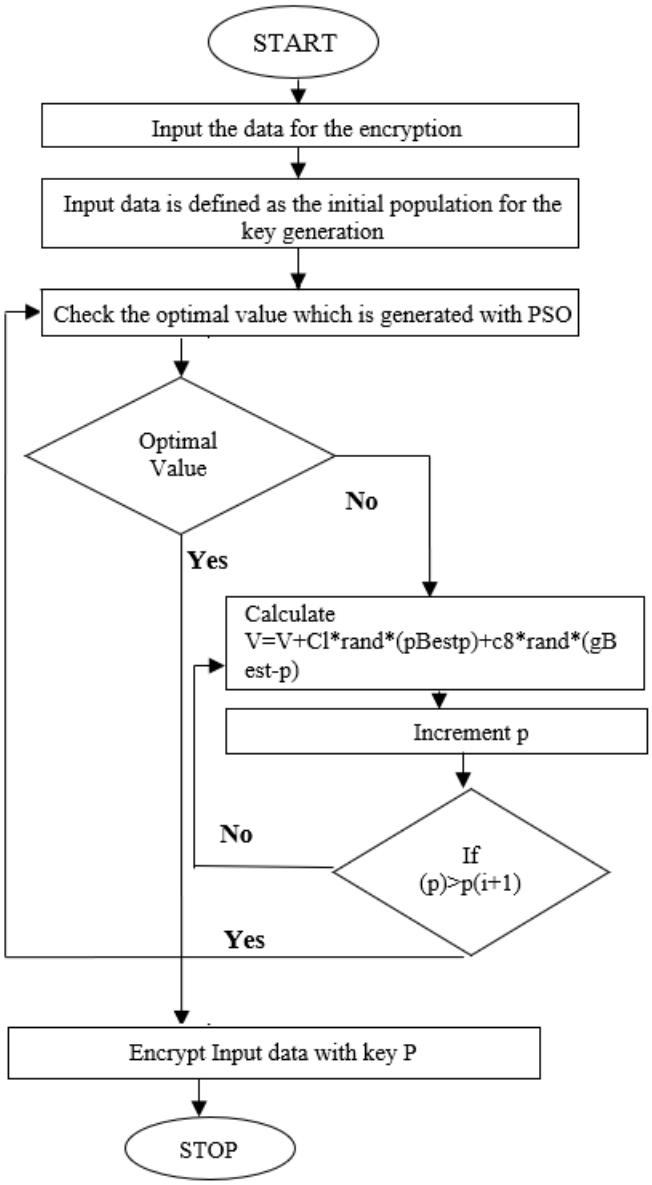

Figure 2: Proposed Flowchart

The figure 2 illustrates that the input data is taken in the form of an image in the introduced technique in order to perform the encoding. The homomorphic encoding system implements the balanced cryptography. PSO is adopted to create the keys that are useful to encode the picture.

4. Result and Analysis

MATLAB is executed in order to encode the data in cloud system in the introduce approach. An image is utilized for the input. The cloud information is encoded and decoded using the balanced encoding algorithm. The particle swarm optimization is implemented to produce an advanced key. This key is helpful to perform encoding of information with the help of homomorphic system. The introduced method is quantified on the basis of two metrics namely execution time and resource usage. The table 1 illustrates the reproduction results. An operating system recognized as Xnon in data sample is deployed on every fundamental system.5GB RAM is included in every fundamental system and total seven fundamental machines are utilized. Overall eighty images are employed and each image has a dimension of 256*256.

Table 1: Simulation Parameters

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

Figure 3: Execution Time

Figure 3 illustrates that the introduced approach is compared with existing algorithm with regard to the implementation time. The existing algorithm is a kind of homomorphic encoding on the other hand, the projected algorithm is an enhancement of homomorphic encoding system.

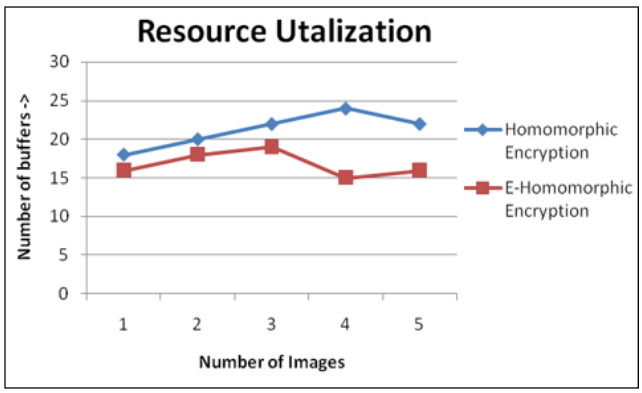

Figure 4: Resource Utilization

Figure 4 represents that the existing system is compared with the introduced in order to determine the resource usage. The investigation reveals that the introduced system provides lower resource exploitation.

Table 2: Comparison of Techniques

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

The table 2 depicts that a homomorphic encoding is compared with the enhanced homomorphic technique concerning the resource usage. Diverse results indicated that the enhanced homomorphic encoding technique offers higher performance with regard to all metrics.

5. Conclusion

The homomorphic encoding system is utilized to encode the cloud information. The major concerns related to this system are to allocate the key and organize the key. The key is produced to carry out the encoding using PSO, an enhanced algorithm. This key is deployed as an input in the homomorphic encoding system in order to create the encoded data. The projected system is implemented on MATLAB. The resource employment and execution time are considered for analyzing the outcomes. This exhibits that the projected algorithm provides lower resource usage and execution time in contrast to existing algorithm. The future work would emphasize on improving this system to ensure that the information is reliable in cloud surroundings.

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