

Enhancing Encryption in Cloud Computing and Reducing Energy Usage by Using PSO-ALO Algorithm to Improve Homomorphic Encryption Technique

MSc Research Project
Cloud Computing

Adwait Sawant
Student ID: x21127409

School of Computing
National College of Ireland

Supervisor: Adriana Chis

National College of Ireland
Project Submission Sheet
School of Computing



Student Name:	Adwait Sawant
Student ID:	x21127409
Programme:	Cloud Computing
Year:	2022
Module:	MSc Research Project
Supervisor:	Adriana Chis
Submission Due Date:	15/12/2022
Project Title:	Enhancing Encryption in Cloud Computing and Reducing Energy Usage by Using PSO-ALO Algorithm to Improve Homomorphic Encryption Technique
Word Count:	6561
Page Count:	22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	15th December 2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project , both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Encryption in Cloud Computing and Reducing Energy Usage by Using PSO-ALO Algorithm to Improve Homomorphic Encryption Technique

Adwait Sawant
x21127409

Abstract

In recent times, cloud computing has emerged as an innovation with the most potential. While using it, security concerns still exist in relation to vital data. However, the most widely used solution for bridging this gap is the utilization of data encryption techniques. The homomorphic encryption technique is an encoding technique that helps in the encoding of data that needs to be stored on the cloud. However, the homomorphic encryption technique has a few drawbacks such as the generation of a key at a faster rate and its optimal utilization. This issue decreases the effectiveness of the technique making it less favorable for encryption. Thus it is vital to achieve a better optimal key that can be utilized for the encryption of data in such a way that it maintains the integrity of data and avoids its exploitation. In this research paper, we proposed a novel encryption technique called Modified Particle Swarm Optimization Algorithm which would assist in the generation of the best key in a way that minimizes the execution time for encryption as well as decreases resource utilization. The research is focused on enhancing the existing encryption technique for faster encryption by combining the Ant-Lion Optimization algorithm with the existing PSO algorithm, further the concept of RandomWalkOfAnts is used to find an optimal key for encryption. The implementation of the proposed research is performed using Matlab. Furthermore, the outcomes of the simulation state that the proposed encryption technique is better in terms of execution time and resource utilization as compared to the existing homomorphic encryption technique.

1 Introduction

Cloud computing, the long-awaited recognition of computing as a utility, has the potential to radically disrupt the IT sector by enhancing the attraction of a software-as-a-service model and impacting the production and acquisition of IT equipment. The phrase "cloud computing" refers to the hardware and operating system used within data centers to operate applications that are offered as services over the Internet. Moreover, there are multiple cloud providers within the market so the customer has a variety of options to pick from. The way we create, deploy, scale, update, manage, and pay for applications and the infrastructure on which they run has changed as a result of cloud computing. Due to these advantages of cloud computing, it is necessary to have a dynamic security

system that is both effective and flexible in order to guarantee the security of user data in the cloud. Alam (2020)

Furthermore, as the concept of cloud computing started becoming increasingly popular, a huge number of organizations started to move their infrastructure to a cloud environment as an Operational Expenditure model was much more efficient as compared to the existing Capital Expenditure model. Nevertheless, the security of the data on the cloud has always been a vital issue of concern for individual entities opting for cloud or Cloud Service Providers. Numerous encryption techniques are proposed to achieve faster and more efficient encryption of data in the cloud. Encrypting the data such that operations and computations can be performed on that data without being decrypted has been a prominent area of research in cloud security. Much research has been made in this domain by various researchers by creating algorithms to obtain the best key for the encryption of data. Several attempts have been also made where various meta-heuristic techniques have been compared to achieve an optimal solution to this problem of encryption. Atayero & Feyisetan (2011)

However, all of the previous research that has been made using hybrid techniques have left some kind of drawbacks such as a longer time required for execution and a greater amount of resources utilized during the process. So with respect to the proposed research, more emphasis is given to improving the performance of encryption techniques by reducing the execution time and resource utilization.

1.1 Motivation for Research and Background

A method for medical cloud computing was developed to resolve the issues of CSP privacy by (Kocabas & Soyata 2020). The suggested approach made it possible to compute sensitive patient data without reviewing it. The research was successful in ensuring the security and secrecy of data were maintained. However, a longer amount of encryption time was required for performing encryption. Additionally, (Shankar & Lakshmanaprabu 2021) proposed a similar approach of using ALO for enhancing the security of the image. The model successfully achieved the goals and had brilliant advantages over other encryption techniques. Nevertheless, no attempts were made to generate the key at a much faster rate or reduce resource utilization. Also, there were no attempts made to specifically combine Particle Swarm Optimization with Ant-lion Optimization techniques to find the best optimal solution. Thus, the proposed research was motivated as there were no earlier attempts made by combining the PSO with ALO to find the best solution in the search area and to overcome the challenges faced by existing Homomorphic encryption.

1.2 Research Question

The proposed research question is as follows - "To what extent does a Modified Particle Swarm Optimization algorithm in Homomorphic encryption improve the quality of service parameters in cloud computing?" .

1.3 Research Objectives

- Implementation of a modified algorithm by combining the Particle Swarm Optimization and Ant-Lion Optimization Algorithm.

- To obtain the best optimal key for encryption and to reduce the execution time and resource utilization of encryption.
- Performing comparative analysis of the proposed encryption technique with existing homomorphic encryption technique.

1.4 Structure of Document

This research report is broken further into six sections. Section 2 describes earlier work in the domains of homomorphic encryption and meta-heuristic algorithm modification. In Section 3, the research methodology including the methods and algorithms used is described. Section 4 discusses the planned research’s design specifications. Section 5 details the suggested encryption algorithm’s step-by-step implementation. Finally, sections 6 and 7 include the experimental results and conclusion, respectively.

2 Related Work

Homomorphic encryption has been used in numerous research to conserve the privacy and security of cloud data. Moreover, various meta-heuristic algorithms are also used to find the best possible solutions. The below section focuses on some of the studies performed earlier which are relevant to my proposed research.

2.1 Homomorphic Encryption in Cloud Computing

(Halder & Newe 2022) built a method labeled SmartCrypt to maintain and exchange information which provided scalable analytics across time-series data that was encrypted. Users were able to improve and secure the procedure for sharing encrypted data thanks to this solution. When unauthorized parties were present, the designed system maintained the data’s confidentiality. For this, to attain end-to-end encryption, the SHE (symmetric homomorphic encryption) approach was used. In order to test whether the system could securely store and share IIoT (Industrial Internet of Things) data streams, a real-time dataset was used in the testing. The results showed that the system may be used to reduce query time by up to 17%, increase throughput by about 9%, and scale up to 20%.

(Alabdulatif et al. 2020) developed a cloud-based decentralized analytics platform for large datasets that maintains anonymity. Fully homomorphic encryption (FHE), one of the emerging as well as widely used cryptosystems that may perform analyses on encrypted data, was used in this research. This method moves quickly and maintains accuracy while processing the encrypted data more effectively. Individual execution of portions of the analytical computations and data is possible thanks to the distributed technique’s scalability. They introduced a revolutionary distributed big data analytics platform in this study that safeguards privacy. The study showed how end-to-end information integrity can be provided by entirely homomorphic encryption while automating analysis procedures safely. The evaluated results showed that the proposed architecture was effective with respect to analysis performance and accuracy when developing a secure analytics solution powered by the cloud.

(Kocabas & Soyata 2020) suggested a cutting-edge method for medical cloud computing that does away with issues related to cloud provider privacy. The suggested method made use of Fully Homomorphic Encryption (FHE), which made it possible to compute

sensitive medical data without necessarily viewing the raw data. They provided a functional implementation of a long-term cardiovascular healthcare monitoring application utilizing an existing open-sourced FHE library for a feasibility report. The findings of the suggested technique confirmed that such operations may be carried out homomorphically, ensuring the security and secrecy of the data were maintained.

(Chen & Zheng 2022) investigated how machine learning functions took advantage of the processing power and storage capability of CC by routinely uploading data and patterns to a 3rd party server. Moreover, 3rd party servers could experience confidential data leakage during the cycle of data collection, storage, and utilization, specifically in the sectors such as financial services, healthcare, and biometrics. The homomorphic encryption (HE) technique made ciphertext computations independent of decoding possible. This innovation could be used to forecast the ciphertext domain and train the machine learning architecture. This research used the SEAL homomorphic encryption repository to recreate the linear regression process. Six data sets were used for the tests, and the performance was assessed in light of security.

2.2 Particle Swarm Optimization for data encryption

(Ahmad et al. 2018) suggested an image encryption technique that is designed for secure picture-based communication. A chaotic map and an optimal encryption effect were obtained using the method, which used particle swarm optimization. The method initially produced a number of encrypted images as well as a chaotic logistic map, where the session key for the map's beginning conditions was made contingent upon a forthcoming plain image. Then, in order to carry out optimization through PSO, the encrypted images were provided as components and a starting assemblage. The correlation coefficient relevant to adjacent pixels that represents the optimal encrypted image serves as its fitness function. The simulation outcomes of the suggested encryption method showed that the encrypted pictures had outstanding encryption properties such as flat histograms, entropies, net pixel change rates, etc, in addition to high de-correlation of nearby pixels.

(Zeng & Wang 2021) suggested a hyperchaotic picture encryption system based on cellular automata(CA) and the particle swarm optimization method (PSO). The initial conditions of the hyperchaotic system are created by the hash function value that is closely related to the plaintext picture that needs to be encrypted, which increases the system's immunity to plaintext attacks. Moreover, the correlation coefficient among neighboring pixels within the image determines the PSO's fitness. Additionally, cellular automata technology is used based on hyperchaotic systems, that can improve the randomness of population distribution and raise the diversity as well as the complexity of the population, thereby enhancing the safety of the encryption system and preventing it from settling into a local optimum. The outcomes of the simulations and the security analysis of the suggested encryption technique show that the proposed encryption technique for images has a high level of immunity with respect to statistical attacks as well as plaintext attacks.

(Ahmad et al. 2020) created an effective method for the development of cryptographic highly nonlinear substitution boxes as an alternative to random, chaotic, or algebraic-based construction methods. Additionally, they developed the proposed method using the particle swarm optimization technique inspired by nature, in which the initial population is produced using a straightforward but dynamic Renyi map. Different situations, including population size changes, changes in the number of repetitions, and linear increases in inertial weight, were evaluated for the projected technique. The proposed method

was determined to be superior to several recent optimization-based S-box methods and to have outstanding cryptographic properties based on the performance evaluation of created S-boxes under accepted criteria. In order to assess the proposed S-boxes' appropriateness and applicability for picture-based security applications, an image encryption application was also recommended.

(Elhoseny et al. 2020) used a cutting-edge cryptographic model with optimization techniques to look at the security of medical images in IoT. Maintaining the security of the data is essential because the majority of the patient data was housed on cloud servers in the hospital. In order to strengthen the security of the encryption and decryption processes, elliptic curve cryptography employs a hybrid swarm optimization strategy that integrates grasshopper optimization and PSO to choose the optimum key. The outcomes were contrasted with published optimized encryption approaches that were already in use.

(Khan et al. 2021) developed an image encryption technique based on MOPSO, a DNA encoding sequence, and a 1-D Logistic map. To begin, the key in this paper was composed of a particle swarm optimization (PSO) sub-key sequence, a plaintext image hash value, and a shuffle mark bit. Utilizing logistic maps and DNA encoding, they generated random DNA mask pictures. Used it in conjunction with the plaintext DNA encoding sequence that was block-shuffled to create an encryption scheme. The iterative PSO algorithm is based on information entropy and correlation coefficient; in PSO, a particle's location value corresponds to a location in a plaintext picture. Lastly, the optimal ciphertext was acquired and the value of the optimal particle was returned. The correlation coefficient and entropy of ciphertext were outstanding, and simulations results and security analyses demonstrated that it was able to withstand all common types of attacks and had better encryption effect.

2.3 Encryption of data using Ant-Lion Optimization technique

(Shankar & Lakshmanprabu 2021) suggested a homomorphic encryption method that offered the best key for the image's security. The concept of histogram equalization was additionally introduced to change the intensities of pictures to enhance contrast. An image's histogram typically conveys information about the relative frequency of occurrence of the various gray levels in the image. Additionally, the Ant Lion Optimization (ALO) technique was given priority to raise security. The experiment showed outstanding results, and it was determined that the proposed model had a significant advantage over other encryption techniques. However, the research by any means is not focused on the factor of faster of key generation or reduced encryption time as proposed in my research.

(Kakkottakath Valappil Thekkepurayil et al. 2021) suggested an improved scheduling method that will shorten the execution time and lower the cost. In the proposed research, the prominent particle swarm optimization (PSO) algorithm was combined with the antlion optimization (ALO) approach to optimize a workflow schedule designed specifically for the cloud. Furthermore, when scheduling was done, cloud data was encrypted using the Data Encryption Standard (DES) concept. The goal of the research was to improve workflow scheduling while ensuring greater safety than current frameworks. The research was evaluated based on a number of criteria, including cost, load, and makespan. Additionally, simulations were run using the CloudSim simulation program. The results showed that the suggested strategy decreases cost by 10% of PSO and 20% of ALO, although the suggested method's load balancing and makespan decrease by 20% of PSO

and 20% of ALO.

(Paramarathi & Rao 2022) suggested and developed an obfuscation-based technology for secure data transmission in the cloud, known as the AROA-based BMCG method. By combining the ALO and ROA, the new algorithm known as AROA is created. In the privacy-preserving stage, OB-MECC Encryption is additionally utilized to guarantee the data's security. Additionally, a bilinear map co-efficient was created and used to manage both confidential material and utility information. Metrics including accuracy and information loss were used to measure the performance and conduct a comparative analysis of the proposed AROA-based BMCG technique. With the suggested AROA-based BMCG technique, maximum accuracy was 94%, and there was only 6% information loss.

(Mirjalili 2021) proposed to solve complex and advanced engineering problems with the help of the Antlion Optimization (ALO) algorithm. The ALO algorithm imitates an antlion's natural hunting strategy. Three stages were used to benchmark the proposed algorithm. Initially, 19 mathematical operations were used to test various ALO traits. Additionally, ALO successfully solved three well-known engineering issues, including the construction of a three-bar truss, a cantilever beam, and a gear train. In the research report, ALO also helped in the improvement of the propellers of two ships. The outcomes of the test functions demonstrate that the suggested algorithm is capable of delivering very superior performance in terms of enhanced discovery, local optima prevention, and convergence. The resolution provided for ship propellers suggested that the proposed approach might be used to solve actual issues with unknowable search areas. Hence, to obtain the more accurate and best key in terms of encryption I utilized the ALO technique in my research work.

2.4 Summary of the Literature Review

The literature review focused on three areas in which previous research was performed. The first section emphasized papers that utilized homomorphic encryption techniques. Numerous attempts were made to encrypt the data in such a way that it maintained integrity and confidentiality. The solutions proved to be useful as they helped in reducing time and increasing throughput and enhancing the security in the cloud environment. The next section focused on the utilization of the Particle Swarm Optimization technique for the purpose of data encryption. Numerous pieces of research were performed to find the best optimal encryption of the image or data with the help of the PSO algorithm. Considerable pieces of evidence were acquired that proved PSO to be a valuable technique in encryption. The last section focused on data encryption with the help of the ALO technique. Numerous attempts were made to utilize the ALO algorithm for the purpose of providing security. Moreover, ALO proved to be a better alternative as compared to existing methods as it depicted to have a good succession rate. Moreover, there have been several attempts at combining two algorithms to make them more effective. However, no attempts have been made so far by combining Particle Swarm Optimization with the ALO algorithm. Furthermore, the research conducted by me typically focuses on generating an optimal encryption key for encrypting data with the combination of two meta-heuristic algorithms called PSO and ALO. The proposed encryption technique will be compared to existing homomorphic technique in terms of execution time and resource utilization to demonstrate its effectiveness.

Author	Year	Description	Findings
Halder & Newe	2022	SmartCrypt was developed for efficient storage and sharing of encrypted data. (SHE) encryption was used to attain end-to-end encryption. A real-time dataset was utilized for testing the proposed approach.	Query time was reduced by almost 17%. Throughput was increased by 9%. Encryption was scaled up by 20%.
Kocabas & Soyata	2020	A method for medical cloud computing was developed to resolve the issues of CSP privacy. The suggested approach made it possible to compute sensitive patient data without reviewing it.	Functional implementation was performed on a real-time application using an existing open-source library. The analysis confirmed that such operations could be performed homomorphically ensuring confidentiality and security.
Zeng & Wang	2021	A hyperchaotic approach for image encryption was proposed. The hash function was utilized in the encryption of plaintext images. Additionally Particle Swarm Optimization (PSO) and Cellular Automata (CA) in combination to obtain the best outcomes.	Simulations and analysis showed that the proposed encryption system for images has a high level of immunity with respect to statistical attacks as well as plaintext attacks.
Paramarathi Rao	2022	AROA-based BMCG method for secure data transmission was developed in this research. MECC Encryption is also used in the privacy-preserving phase during implementation.	AROA-based BMCG achieved 94% accuracy. Data loss was around 6% in the proposed technique.

3 Methodology

The research proposed in this paper mainly focuses on the enhancement of the generation of the key which reduces the execution time required and the utilization of resources required to encrypt the data to improve the existing Homomorphic Encryption technique. The primary goal of the research is to generate a key used to encrypt the data using the proposed encryption scheme which is a combination of PSO and ALO algorithm techniques. This will eventually help in reducing encryption and decryption time between the cloud service provider and the user. The results will be compared based on the Execution time required for encryption, the Number of buffers (Memory), and the Convergence Curve. The methods, procedures, and methodology that will be applied in our study are summarized in this section.

3.1 Particle Swarm Optimization (PSO) and its limitations

Particle Swarm Optimization (PSO) algorithm is a nature-inspired algorithm that constantly seeks the optimal output within the available search space. The reason why PSO is distinct from numerous optimization strategies is that PSO only requires the fitness method or function and is not dependent on a pattern or any specific type of objective function (Rini et al. (2011)). The algorithm is also known as population-dependent algorithm as it highly depends on the size of the population. It is comparable with the pre-existing genetic algorithm in this respect. Moreover, PSO tends to have a faster convergence rate.

Moreover, the particle swarm optimization algorithm in combination with the ALO algorithm generates the optimal value that will serve as the encryption key from input

data that is used for encryption. The PSO consists of particles that are a collection of discrete components which traverse around a search space in sequential steps. The updated velocity of each and every particle is calculated by the program after evaluation. Re-evaluation of code is performed with every position of a particle. The process of key generation is an iterative process. The PSO algorithm/technique is widely used to generate solutions with respect to continuous optimization problems without any prior data. This usually leads to numerous challenges with respect to the generation of keys for encryption. Moreover, in some scenarios, the PSO algorithm/technique gets trapped in the local optimum (pbest) and is not able to update the global optimum value (gbest). Hence, to overcome this limitation of the PSO algorithm, a modification/hybridization of PSO with another algorithm was needed which will tend to achieve a much more effective resolution from the given search space.

3.2 Modification of PSO with Ant-Lion Algorithm

The antlion and ant interactions in the trap are simulated by the ALO algorithm. Antlions are permitted to hunt ants and improve their fitness using traps, whereas, ants are expected to move across the search space to replicate such interactions. Since ants move stochastically in nature in search of food, their movement is simulated using a random walk. Prabhu et al. (2022)

$$X_i^t = \frac{(X_i^t - a_i) \times (d_i - c_i)}{(d_i^t - a_i)} + c_i \quad (1)$$

The above equation stated by Mirjalili (2015) provides a value that is then used to calculate the updated value of the position in the PSO algorithm. Where a is the minimum of random walk of i -th variable, c is the minimum of i -th variable at t -th iteration, and d indicates the maximum of i -th variable at t -th iteration. ALO technique ensures that the search space will be explored by selecting various antlions at random and making ants perform a random walk around them. Additionally, it is ensured that the search space is exploited by adaptively shrinking bounds created by antlions traps. Moreover, we can resolve the challenge of local optima stagnation faced in Particle Swarm Optimization with the implementation of the random walks of ants concept. Moreover, the Ant-Lion algorithm is a population-centric algorithm so the intensity of the ant's movement relatively reduces over the course of each iteration, thus guaranteeing the convergence of the ALO algorithm. Every ant undergoes a random walk calculation, and each dimension fosters population diversity. Additionally, during optimization, Antlions go to the location of the best ants, saving promising search spaces. This process continues until the maximum number of iterations is achieved. Every time a new iteration is performed, the finest antlion is saved and compared to the best antlion previously acquired.

3.3 Pseudo-code of the proposed Algorithm

The suggested Modified PSO algorithm helps us in achieving the best optimal key that can be utilized for the encryption of data. The pseudo-code designed for the explanation of the proposed research is shown in figure 1. Initially, parameters such as w -weight inertia, c_1 & c_2 - acceleration coefficients, p -probability variable, and V_{max} - maximum velocity required by Particle Swarm Optimization and Ant-Lion Optimization technique

```

1  Input parameters : c1 & c2 - Acceleration coefficients,
2  w - Inertia weight, p - probability, Max_iteration,
3  n - population size, fitness - Fitness function
4
5  Output Data - Optimal key for encryption
6
7  set pbest = inf // initialise local optimal as infinite
8  set gbest = inf // initialise global optimal as infinite
9
10 for each particle
11   Initialize particle // generate random population
12 Endfor
13
14 Do
15   For each particle
16     Calculate Fitness value //using fitness function
17     if Fitness(new) > pbest(current)
18       update pbest(current) = fitness(new)
19     endif
20     if pbest(new) > gbest(current)
21       then set gbest(current) = pbest(new)
22     endif
23   EndFor
24   update w = wMax-1*((wMax-wMin)/Max_iteration) //weight inertia
25   For "i" and in population size
26     calculate Velocity based on Vmax
27   EndFor
28   Calculate s \ \ Binary transfer function
29   if p>rand
30     create a random walk and normalize it
31     update the position
32   endif
33 While maximum iteration or minimum error criteria is not attained.

```

Figure 1: Pseudo-code of proposed Algorithm

are defined. Further, the random population is initialized and the fitness function is calculated, also the local and global optimums are calculated. Also, a function in Binary PSO known as the transfer function is triggered. Lastly, if the pre-defined probability value is compared with random and a decision is made whether to initiate the Random-Walk concept. Finally, the best key for encryption is generated and various factors such as Execution time, convergence curve, and Resource utilization are recorded. Salah Farrag et al. (2015)

3.4 Proposed architecture

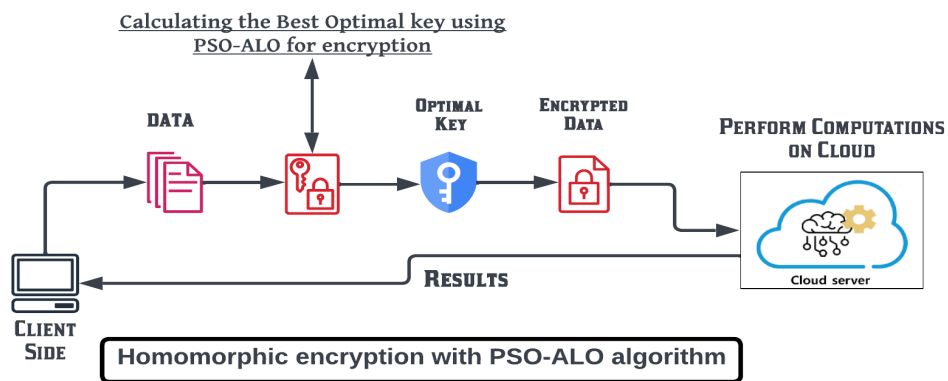


Figure 2: Proposed architecture

The encryption of data is one of the vital aspects while maintaining data integrity and confidentiality. The architecture starts with the user selecting data that needs to be encrypted as shown in figure 2. Generally, this data is encrypted using a homomorphic encryption technique. However, there tend to be drawbacks such as key generation and

its management in the existing standard homomorphic encryption technique which makes it an unfavorable option for carrying out encryption. So as per our proposed research, we calculate the best optimal key that can be utilized for the encryption of client data with the help of a combination of two meta-heuristic algorithms known as PSO & ALO, also the concept of Binary PSO is applied. Additionally, the concept of RandomWalkOfAnts Mirjalili (2015) is initialized to generate the best key. In other words, the application of the PSO-ALO algorithm supports the process of generating an optimal key. This optimal key is then used to encrypt the data where computations can be performed in the cloud environment.

3.5 Evaluation Parameters

The necessary parameters for evaluating the algorithms and comparing them to an already-in-use homomorphic encryption method were established during the development of this research. The primary goals of the research are to create the optimal key for encryption, estimate the amount of time needed for execution (fitness), and assess resource utilization. When it comes to optimization-based key generation methods, the convergence curve is probably a significant element. This is taken into consideration when comparing the suggested research with the earlier literature. Moreover, the effectiveness of the algorithm can be evaluated easily by selection of specific performance measurement factors. Below are the three different parameters which are used for evaluation.

- **Execution Time:** This denotes the total time utilized for the encryption of the image. The execution time will reduce considerably in the proposed algorithm as the keys will be generated using the PSO-ALO value.
- **Resource utilization:** This parameter states the exploitation of resources performed by the technique which is utilized during execution. The number of buffers i.e memory allocated to each image for encryption is calculated.
- **Convergence curve:** This parameter represents the overall iterations required by the method to arrive at an ideal result. To ascertain how quickly the ideal solution will be found in our situation, the convergence curve of the modified PSO algorithm will be assessed.

4 Design Specification

The existing Homomorphic encryption has multiple drawbacks which need to be addressed. The process of generation of an optimal key is one of the vital issues that is faced within the homomorphic encryption technique. It is essential to overcome these drawbacks or loopholes to preserve and maintain the confidentiality of data. To enhance the process of key generation which helps in faster encryption, we created a modified algorithm that improves on the one developed by Khan et al. (2019) in which they enhanced the encryption process using PSO. The research proposal combines the ALO algorithm with the standard PSO which helps us in obtaining a better key that decreases the execution time and resource utilization, whereas the previous research focused on utilizing the PSO algorithm on the basis of factors like time and resource information.

Figure 3 depicts the flow of the proposed MPSO algorithm. The initial step is defining the numerous parameters such as population, weight, and maximum iterations which will

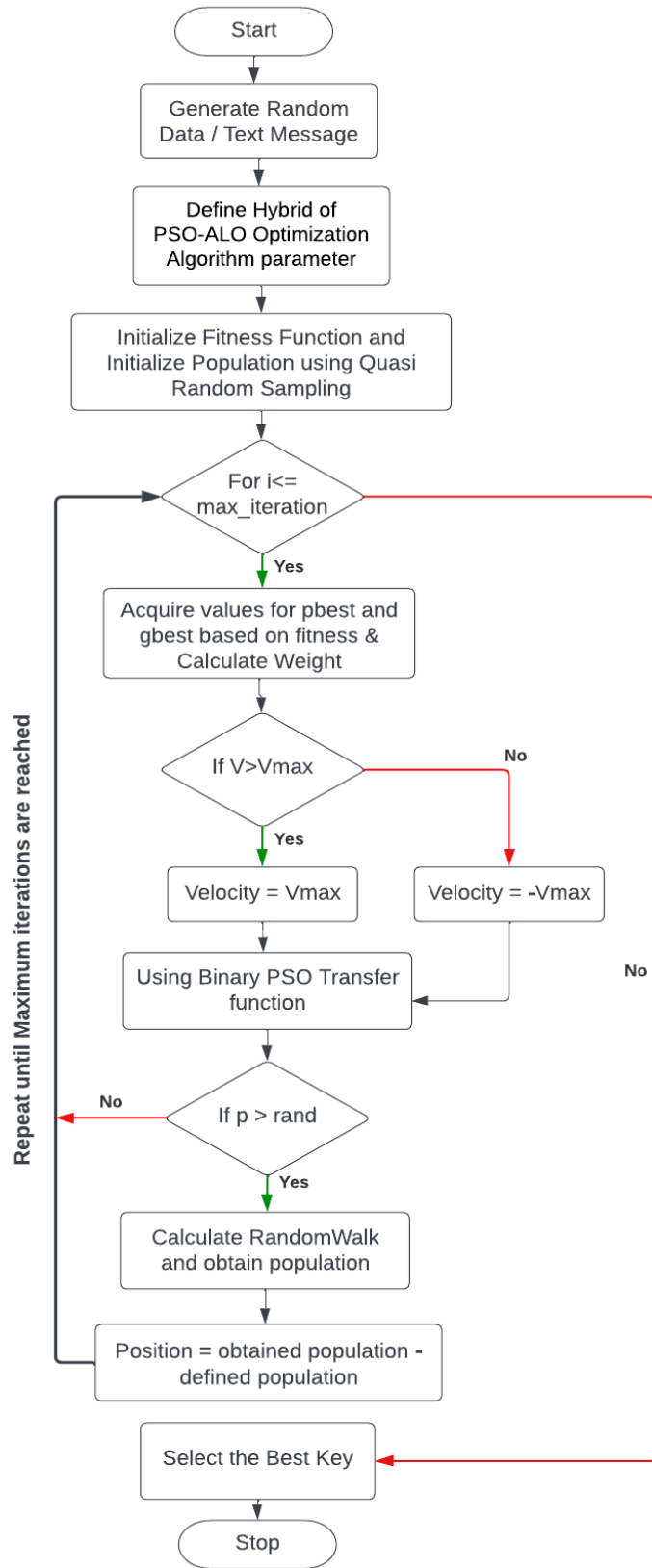


Figure 3: Flowchart of Proposed Algorithm

be utilized by the standard PSO and ALO algorithm. Then the population is initialized with the help of Quasi Random Sampling and fitness function which is the Objective function is initialized as well, Objective function used to find the best position. For loop is initiated which keeps on running until it reaches the maximum number of iterations. On the execution of the loop, a fitness value is generated which helps in obtaining the pbest(Local optimum) and gbest(Global optimum) values respectively. It also calculates the weight inertia which is then utilized in finding the value for velocity. Thereafter, the velocity is compared with Vmax and is replaced if it is greater whereas in other cases velocity is updated depending on the value of Vmax. The value of "S" a transfer function is obtained with the help of the Binary PSO transfer function. Thereafter, if the probability variable "p" which we had defined is greater than the random value generated by Matlab then we would proceed to calculate RandomWalkOfAnts and obtain the population. Furthermore, the final position is calculated by obtaining the difference between obtained population and the defined population, this updated position is then passed onto the objective function. This complete process keeps on running unless the maximum number of iterations is reached or until minimum error criteria are not attained.

5 Implementation

Matlab tool was utilized in the implementation of the proposed research. The decision was made keeping in mind the cost constraints that might incur when implementing such live scenarios on a cloud computing architecture. The utilization of Matlab helps in testing various algorithms such as the Ant-Lion Optimization algorithm, Particle Swarm Optimization, and lots more. Moreover, simulation helps in the detection of errors that can be avoided during the live deployment of the implementation. The simulation was performed on a 64-bit Windows platform computer which had AMD Ryzen 7 as the core processor and 8 cores. Furthermore, C programming language was used in Matlab to simulate the proposed scenario of the research.

5.1 Evaluation Tool

Matlab is a type of software program that may be used to perform complicated operations like technical computation, graphics, and animation as well as simple numerical calculations like addition and subtraction. The C programming language is compatible with Matlab. It offers a user-friendly interface with a wide range of built-in features. Depending on the software version, these features change. The fundamental block in Matlab is the matrix. This platform also comes with built-in capabilities for image processing, signal processing, communication, control mechanisms, and NN (neural networks). MATLAB, which enables high graphics, can be used to model the network. Moreover, complex programming tasks which are implemented using C programming language which typically utilizes vector or matrix compositions can be executed more quickly. Mathworks (2018)

Utilization of a simulation tool like MATLAB helps in the implementation of various ideas and methods before a full-scale live deployment as seen in figure 4. The advantage of using an advanced coding interface is that concerns related to low-level programming languages like resource utilization and parameter class are looked after and the users can emphasize on how the algorithm should operate. After successful testing of its operational capabilities, the encryption technique can be enhanced for more effectiveness

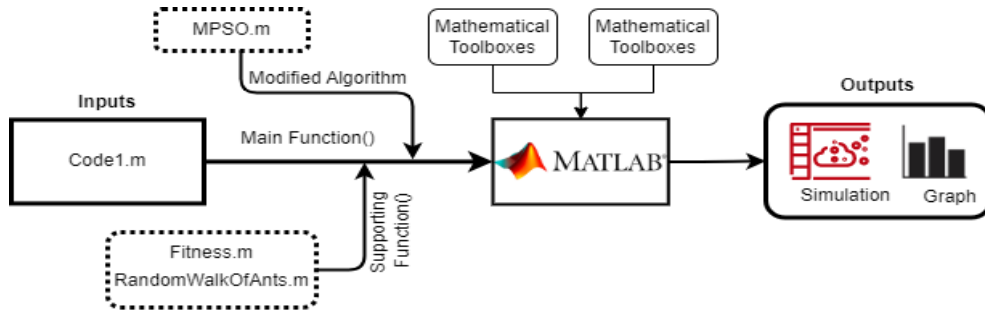


Figure 4: Architecture of proposed technique in MATLAB

and dependability. MATLAB helps in the detection and resolution of various problems with the help of different tools within the system. Using a variety of data structures and arithmetic operations we can make sure the method consistently operates on predefined CPUs. We have also utilized various in-built toolboxes within MATLAB for the purpose of implementation of our proposed research. CIMMSEducation (2020)

5.2 Formulation of the required Objective Function

An objective function is executed in the background by the Particle Swarm Optimization algorithm to calculate the fitness of a specific task. Moreover, this objective function is considered to be an important component of the newly proposed Modified PSO algorithm. The explanation of how the optimization algorithm calculates the fitness function, which is a feature of the algorithm is done by implementing a Matlab function and storing it in a file named 'fitness.m' 5.

```

Editor - C:\Users\Adwait\Desktop\Thesis\Adwait_Thesis\Adawait\fitness.m*
Code1.m  fitness.m*  HYPPO.m  RandomWalksOfAnts.m  +
1  function fit=fitnessfunc(pop)
2
3  fq=0;
4  for i=1:length(pop)-1
5      df=abs(pop(i)-pop(i+1));
6      if df==1
7          fq=fq+1;
8      end
9  end
10
11  fit=1/(fq+entropy(pop));

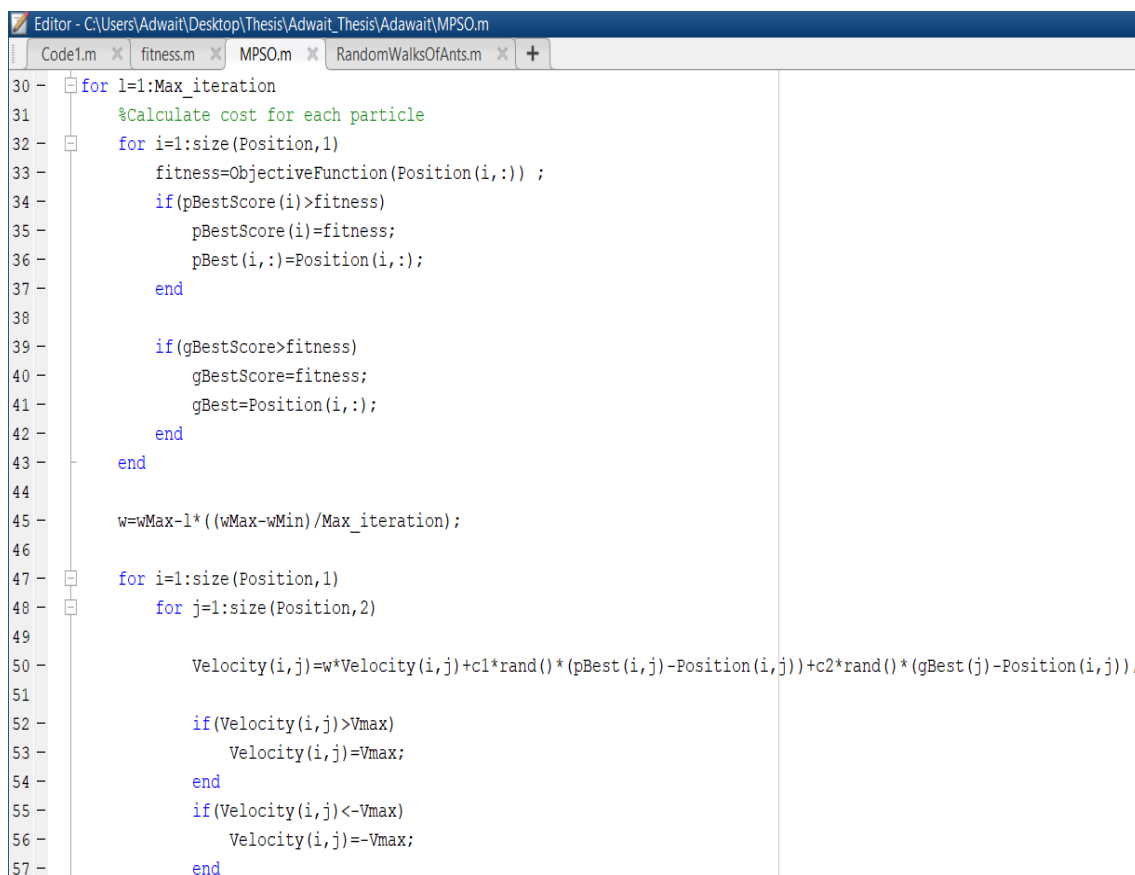
```

Figure 5: Fitness function

The above function is then used in the 'Code1.m' file in order to calculate the objective function 5. Furthermore, to simplify the calling of this function in the code, a function handle is generated using '@' symbol reserved for function handling in Matlab is created by us. Moreover, we have calculated the frequency and entropy of the key using the fitness function. Here entropy produces a random number which helps in producing the key in the fitness function.

5.3 Generation of key & Binary transfer function concept

The ‘MPSO.m’ file would contain an objective function which is defined below in figure 6 along with various parameters such as w-weight inertia, c1 & c2- acceleration coefficients to generate a key for encryption. We have also defined a probability variable within the file which will update the values obtained using the ALO technique. The PSO algorithm keeps on exploring the search space to find a better ”Global Optimum value” until it completes its maximum iteration. The Local Optimal(pbest) and Global Optimal(gbest) values are updated and compared after each iteration to find the best values. The effectiveness of PSO’s algorithm is achieved by running a PSO equation in the loop. This eventually helps us in obtaining the updated values of the velocity of the particles.



```
Editor - C:\Users\Adwait\Desktop\Thesis\Adwait_Thesis\Adawait\MPSO.m
Code1.m x fitness.m x MPSO.m x RandomWalksOfAnts.m x +
30 - for l=1:Max_iteration
31 -     %Calculate cost for each particle
32 -     for i=1:size(Position,1)
33 -         fitness=ObjectiveFunction(Position(i,:)) ;
34 -         if(pBestScore(i)>fitness)
35 -             pBestScore(i)=fitness;
36 -             pBest(i,:)=Position(i,:);
37 -         end
38 -
39 -         if(gBestScore>fitness)
40 -             gBestScore=fitness;
41 -             gBest=Position(i,:);
42 -         end
43 -     end
44 -
45 -     w=wMax-1*((wMax-wMin)/Max_iteration);
46 -
47 -     for i=1:size(Position,1)
48 -         for j=1:size(Position,2)
49 -
50 -             Velocity(i,j)=w*Velocity(i,j)+c1*rand()* (pBest(i,j)-Position(i,j))+c2*rand()* (gBest(j)-Position(i,j));
51 -
52 -             if(Velocity(i,j)>Vmax)
53 -                 Velocity(i,j)=Vmax;
54 -             end
55 -             if(Velocity(i,j)<=-Vmax)
56 -                 Velocity(i,j)=-Vmax;
57 -             end
```

Figure 6: MPSO

Furthermore, we compare the population size with the random value threshold and generate a key. Moreover, here we will compare the positions of 0’s and 1’s to finalize the generated key by utilizing the binary PSO concept of the transfer function as shown in figure 7. Lastly, the RandomWalkOfAnts concept is initiated if the pre-defined value of the probability variable is greater than the random value generated in Matlab. The RandomWalkOfAnts helps us in obtaining an updated value of the population which will be later utilized to get the updated position.

```

Editor - C:\Users\Adwait\Desktop\Thesis\Adwait_Thesis\Adawait\MPSO.m*
Code1.m x fitness.m x MPSO.m* x RandomWalksOfAnts.m x +
59
60         s=1/(1+exp(-2*Velocity(i,j))); %S1 transfer function
61
62         if rand<s % Equation (4) and (8)
63             Position(i,j)=1;
64         else
65             Position(i,j)=0;
66         end
67
68     end
69
70 end
71
72 if p>rand
73     AntAlpha=RandomWalksOfAnts(noV,Max_iteration,0, 1,gBest,1);
74     Position=AntAlpha(1:noP,:);
75 end
76 ConvergenceCurve(1)=gBestScore;
77 end
78

```

Figure 7: Binary PSO Transfer Function & RandomWalkOfAnts Concept

5.4 Calculating the RandomWalkOfAnts ALO

Calculating the RandomWalkOfAnts is an important factor as the proposed research is a combination of PSO and ALO algorithms. The RWs or RandomWalkOfAnts factor is derived using min-max normalization as shown in figure 8. Hence, to prove the functionality of this we have developed a function called "RandomWalkOfAnts.m" and saved it in a '.m' file for the purpose of code re-useability.

```

Editor - C:\Users\Adwait\Desktop\Thesis\Adwait_Thesis\Adawait\RandomWalksOfAnts.m*
Code1.m x fitness.m x MPSO.m x RandomWalksOfAnts.m* x +
46 % vectors
47 for i=1:Dim
48     X = [0 cumsum(2*(rand(titeration,1)>0.5)-1)'];
49     % [a b] ---> [c d]
50     a=min(X);
51     b=max(X);
52     c=LB(i);
53     d=UB(i);
54
55     X_norm=(X-a).*(d-c)./(b-a)+c;
56     RWs(:,i)=X_norm;
57 end

```

Figure 8: The RandomWalkOfAnts Function and calculation of the final population

Moreover, we also calculate the final population value using the formula of RandomWalkOfAnts and return the obtained value to the MPSO file. Furthermore, this final population value will help us in determining the position value. Lastly, this will help us in obtaining the objective function which will provide an exploration to us with each passing iteration, hence increasing the possibility of generating the best solution.

6 Evaluation

This section conducts a thorough evaluation of the proposed Modified Particle Swarm Optimization algorithm. The implementation of the proposed algorithm is done using Matlab and simulation is carried out to achieve results. Various factors such as Execution time, Convergence curve, and Resource utilization are utilized to compare the proposed optimization algorithm. The suggested key optimization approach is based on optimization methods such as particle swarm optimization (PSO) and the Ant-Lion optimization (ALO) algorithm, and it is then compared to the existing homomorphic encryption technique.

The results obtained are on the basis of the best key which was derived with the help of an objective function. By utilizing Matlab we have simulated the proposed scenario with respect to execution time and resource utilization. We have implemented the usage of graphical representation as it is easy to represent the effectiveness of the proposed encryption technique. Moreover, the proposed algorithm is compared with the existing algorithm technique to showcase the enhancement of the proposed encryption technique. Three experiments/cases were taken into consideration to examine the dynamic outcomes, varying the number of photos passed for encryption while holding the other variables constant.

6.1 Experiment 1 / Case Study 1

First, in experiment 1, I will test the PSO-ALO method that has been proposed and then state if the proposed algorithm works better. This will be done by comparing and analyzing the algorithm's performance, we'll take into account things like resource usage and encryption execution time.

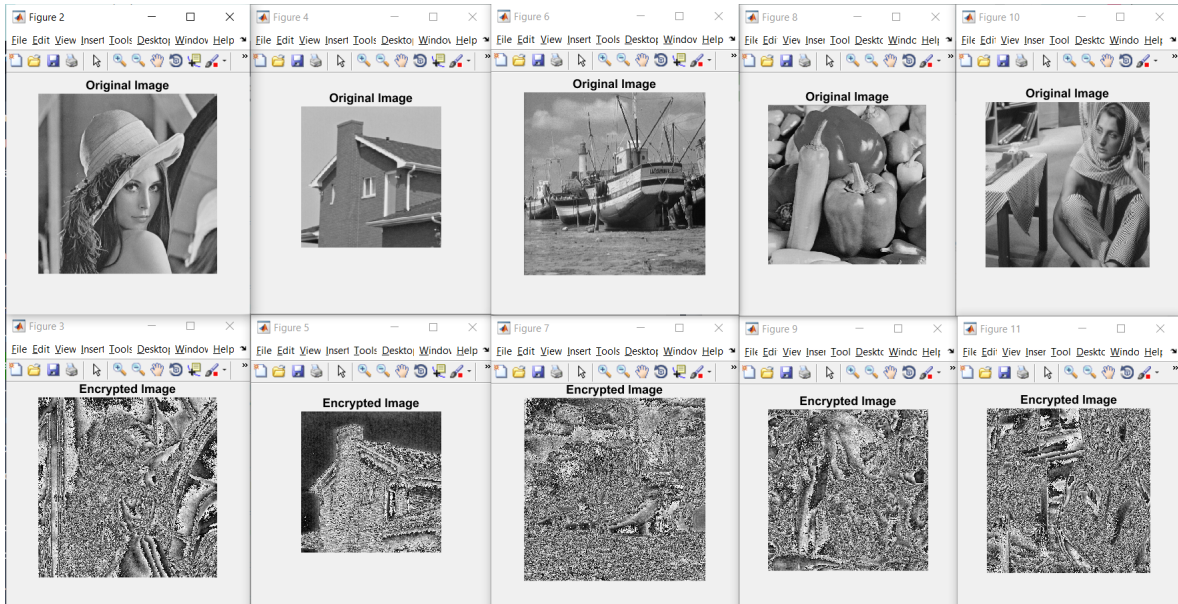


Figure 9: Original and Encrypted images after encryption

The results are also thoroughly compared to a Homomorphic encryption method that is already in use. With respect to case 1, we will pass 5 images for encryption. The outcomes of the test are shown in the figures 10, 11, and 12.

The results of the execution time needed to encrypt five images are shown in figure 10. We can see from the results that we were effective in reducing the amount of time required for encryption. It is observed that encryption of 1st image was done within 0.2 to 0.3 seconds whereas, all of the 5 images were encrypted within 1 second. Also, on the comparison, the suggested technique also takes extremely less execution time when compared to the existing homomorphic technique.

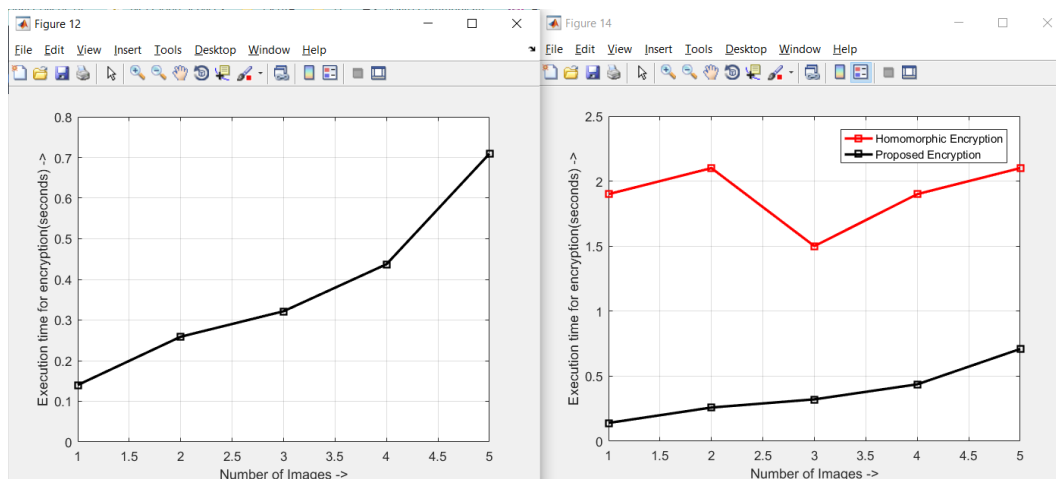


Figure 10: Execution time comparison for 5 images

The number of buffers(memory) required to encrypt 5 images is shown in figure 11. Also, in comparison, the proposed technique required a considerably lesser amount of memory(buffer) for the encryption of images as compared to the standard technique.

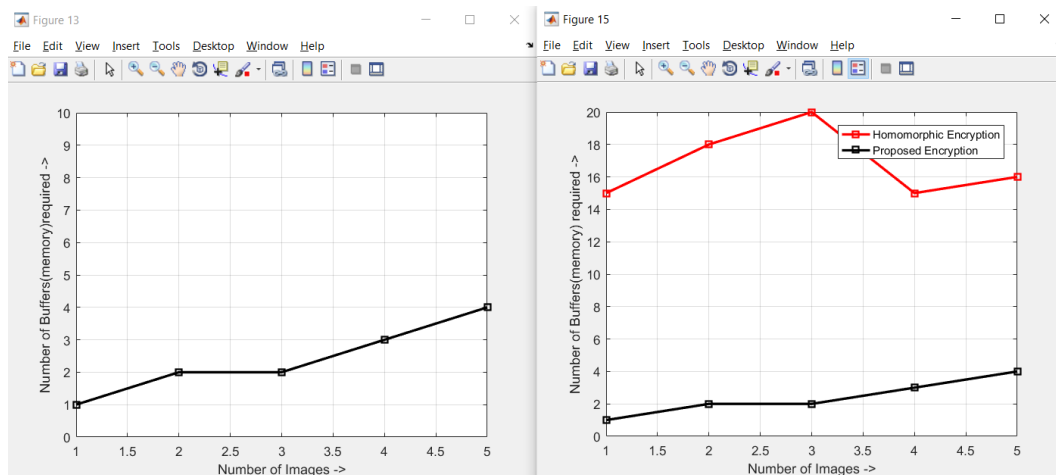


Figure 11: Resource utilization comparison for 5 images

Additionally, as shown in figure 12, the best optimal solution was discovered after 13 iterations. The algorithm's capacity to finish the optimization process and identify the best possible solution for encryption is defined by the convergence curve. In simple terms, it details the precise number of iterations at which the given algorithm discovered an ideal answer.

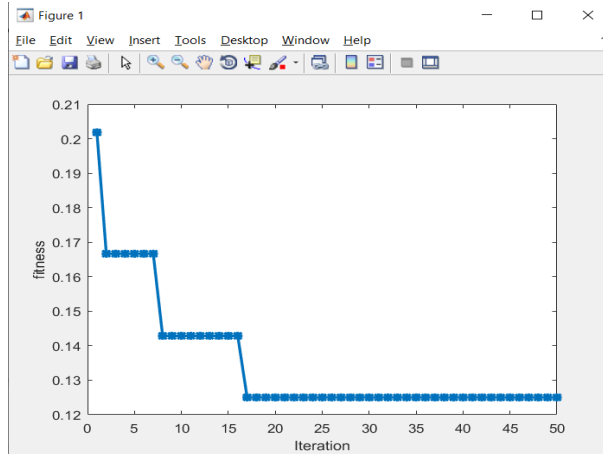


Figure 12: Convergence curve of PSO-ALO for encryption of 5 images

6.2 Experiment 2 / Case Study 2

Here in experiment number 2, we changed the number of images that will undergo encryption through the proposed technique. Resource usage and the amount of time needed to execute the encryption will be taken into consideration when analyzing the results of this experiment.

The obtained results are also thoroughly compared to a Homomorphic encryption method that is already in use. With respect to case 2, we will pass 8 images for encryption. The outcomes of the test are shown in the figures 13, 14, and 15.

Here as seen in experiment 1, the result of the encrypted image with the original image isn't displayed to avoid repetition.

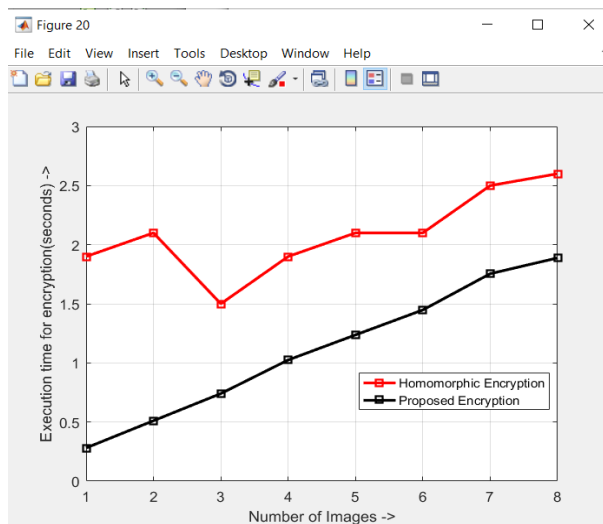


Figure 13: Execution time comparison for encryption of 8 images

Figure 13 shows the execution time required for the encryption of 8 images using the proposed encryption technique. The results depict that the execution time required for the encryption of 8 images is comparatively less as compared to the existing technique.

Here, figure 14 states the resource utilization required for the encryption of 8 images. On analysis, it is observed that resource utilization in the proposed encryption technique

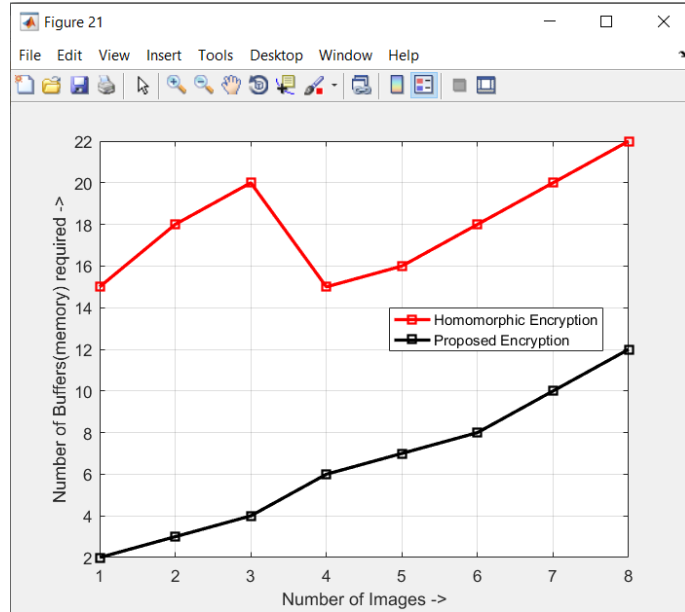


Figure 14: Resource utilization comparison for encryption of 8 images

is lesser than in the existing technique. Moreover, an optimal solution was found on the 8th iteration as seen in figure 15.

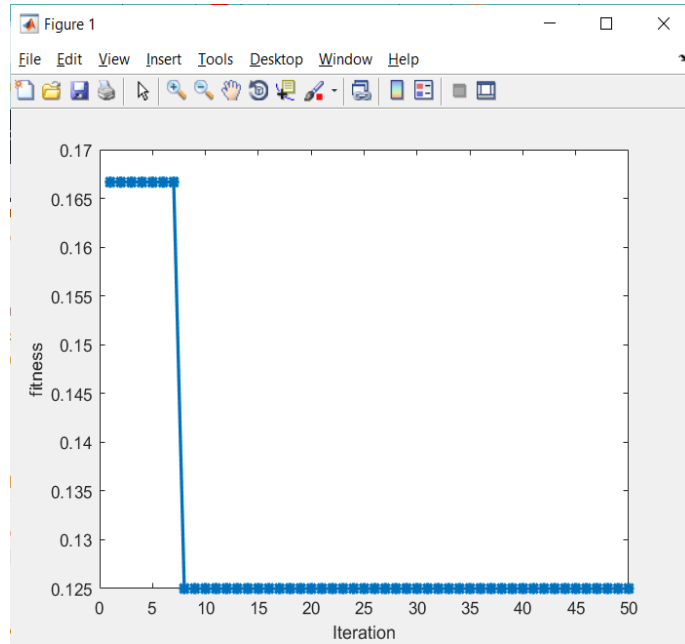


Figure 15: Convergence curve of PSO-ALO for encryption of 8 images

6.3 Experiment 3 / Case Study 3

Now here in experiment 3, we tested the proposed technique by increasing the number of images that need to be encrypted to 15. In scenario 3, we will pass 10 images for encryption. The outcomes of the test performed are shown in the figures 16.

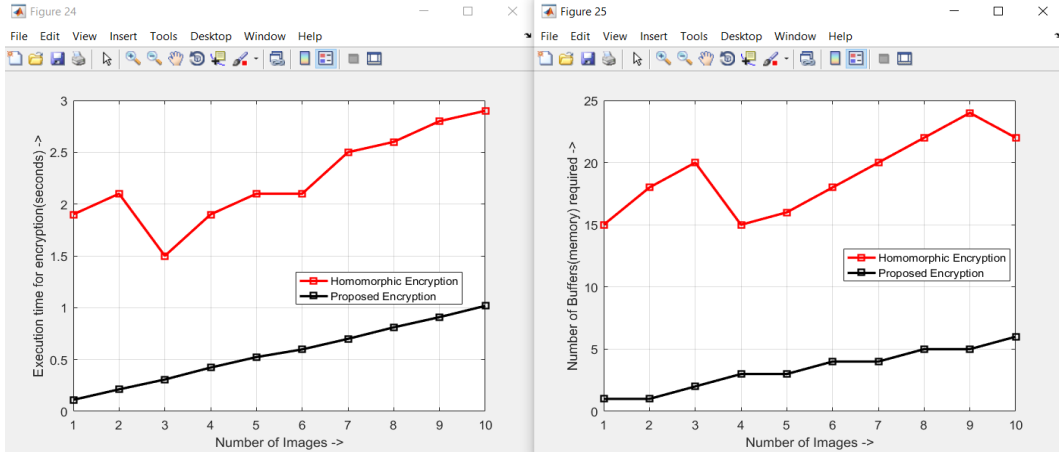


Figure 16: Execution time and Resource utilization comparison for encryption of 10 images

The execution time required for the encryption of 10 images as well as the number of buffers (memory) required (Resource utilization) for the encryption of images is obtained in figure 16. Moreover, these parameters are compared with the existing algorithm to analyze how effective the proposed algorithm is in comparison to the standard homomorphic technique.

6.4 Discussion

On the basis of the results obtained from the above graphs, it can be claimed that the proposed homomorphic encryption in cloud computing is more effective at better key generation and faster encryption based on a fitness function. Moreover, the proposed research also states that utilization of the proposed encryption technique would help in faster encryption of data in the cloud environment. Also, the obtained outcomes state that factors such as time required for the execution of encryption as well as utilization of the resources will be reduced drastically as compared to previously existing homomorphic encryption technique. Furthermore, the modified PSO algorithm will emphasize on the creation of the best key for encryption to overcome the problems of key generation and its management faced in the existing encryption techniques.

Furthermore, as the world becomes more conscious of green computing and energy efficiency, increasing the usage of resources may result in an increase in the consumption of energy. In a real-time setting, the suggested algorithm will succeed in producing better outcomes.

7 Conclusion and Future Work

A significant barrier to cloud computing as the globe develops is the threat posed by data and its exploitation. Many encryption techniques are utilized to overcome these challenges, Homomorphic encryption is one such encryption technique. Nevertheless, there is various issue faced in homomorphic encryption one of which deals with the generation of the optimal key which will be utilized for the purpose of data encryption. However, in order to resolve this problem, we carried out research to speed up the encryption process and use decreased resource utilization for each image. We proposed combining two

meta-heuristic algorithms with a modified approach to develop the best optimal key for data encryption. In terms of encryption using the optimal key, the proposed research successfully reduced the execution time by a considerable margin as compared to the standard homomorphic encryption technique, for example, the execution time required for the encryption of 5 images in the proposed research was 0.8 seconds whereas the existing homomorphic technique required about 2.1 seconds for the same. Moreover, the suggested approach also achieved the aim of reducing resource usage for encryption by decreasing the number of buffers required for each image. Through the simulation outputs created by Matlab, the results are clear and can be independently confirmed.

Additionally, with respect to limitations and future work, the suggested algorithm is designed to perform better and faster encryption with the help generated optimal key. Also, my future work includes working more on measuring the security aspects of the encryption process using the PSO-ALO Algorithm.

References

- Ahmad, M., Alam, M. Z., Umayya, Z., Khan, S. & Ahmad, F. (2018), ‘An image encryption approach using particle swarm optimization and chaotic map’, *International Journal of Information Technology* **10**(3), 247–255.
- Ahmad, M., Khaja, I. A., Baz, A., Alhakami, H. & Alhakami, W. (2020), ‘Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications’, *IEEE Access* **8**, 116132–116147.
- Alabdulatif, A., Khalil, I. & Yi, X. (2020), ‘Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption’, *Journal of Parallel and Distributed Computing* **137**, 192–204.
- Alam, T. (2020), ‘Cloud computing and its role in the information technology’, *IAIC Transactions on Sustainable Digital Innovation (ITSIDI)* **1**(2), 108–115.
- Atayero, A. A. & Feyisetan, O. (2011), ‘Security issues in cloud computing: The potentials of homomorphic encryption’, *Journal of emerging Trends in computing and Information Sciences* **2**(10), 546–552.
- Chen, B. & Zheng, X. (2022), ‘Implementing linear regression with homomorphic encryption’, *Procedia Computer Science* **202**, 324–329.
- CIMMSEducation (2020), ‘Introduction to matlab and its workfolow’.
URL: <https://cimss.ssec.wisc.edu/wxwise/class/aos340/spr00/whatismatlab.htm>
- Elhoseny, M., Shankar, K., Lakshmanaprabu, S., Maseleno, A. & Arunkumar, N. (2020), ‘Hybrid optimization with cryptography encryption for medical image security in internet of things’, *Neural computing and applications* **32**(15), 10979–10993.
- Halder, S. & Newe, T. (2022), ‘Enabling secure time-series data sharing via homomorphic encryption in cloud-assisted iiot’, *Future Generation Computer Systems* **133**, 351–363.
- Kakkottakath Valappil Thekkepuryil, J., Suseelan, D. P. & Keerikkattil, P. M. (2021), ‘An effective meta-heuristic based multi-objective hybrid optimization method for workflow scheduling in cloud computing environment’, *Cluster Computing* **24**(3), 2367–2384.

- Khan, L. S., Hazzazi, M. M., Khan, M. & Jamal, S. S. (2021), ‘A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes’, *Chinese Journal of Physics* **72**, 558–574.
URL: <https://www.sciencedirect.com/science/article/pii/S0577907321000952>
- Khan, S. A., Aggarwal, R. K. & Kulkarni, S. (2019), ‘Enhanced homomorphic encryption scheme with pso for encryption of cloud data’, pp. 395–400.
- Kocabas, O. & Soyata, T. (2020), ‘Towards privacy-preserving medical cloud computing using homomorphic encryption’, pp. 93–125.
- Mathworks (2018), ‘Algorithm development and simulink solutions’.
URL: <https://www.mathworks.com/solutions/algorithm-development.html>
- Mirjalili, S. (2015), ‘The ant lion optimizer’, *Advances in engineering software* **83**, 80–98.
- Mirjalili, S. (2021), ‘The ant lion optimizer’, *Advances in Engineering Software* **83**, 80–98.
URL: <https://www.sciencedirect.com/science/article/pii/S0965997815000113>
- Paramarthy, N. & Rao, N. N. (2022), ‘A data obfuscation method using ant-lion-rider optimization for privacy preservation in the cloud’, *Int. J. Distributed Syst. Technol.* **13**, 1–21.
- Prabhu, G. J., Perumal, B. & Jarin, T. (2022), ‘A composite medical image optimization scheme using honey encryption and antlion algorithms for secured diagnostic systems’, *International Journal of Pattern Recognition and Artificial Intelligence* p. 2240004.
- Rini, D. P., Shamsuddin, S. M. & Yuhaniz, S. S. (2011), ‘Particle swarm optimization: technique, system and challenges’, *International journal of computer applications* **14**(1), 19–26.
- Salah Farrag, A. A., Mahmoud, S. A. & El-Horbaty, E. S. M. (2015), Intelligent cloud algorithms for load balancing problems: A survey, in ‘2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)’, pp. 210–216.
- Shankar, K. & Lakshmanaprabu, S. (2021), ‘Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm’, *International Journal of Engineering & Technology* **7**(9), 22–27.
- Zeng, J. & Wang, C. (2021), ‘A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata’, *Security and Communication Networks* **2021**.