International Journal of
Circuit, Computing and Networking

E-ISSN: 2707-5931
P-ISSN: 2707-5923
IJCCN 2022; 3(2): 27-43
Received: 09-05-2022
Accepted: 09-06-2022

KH Vani
Assistant Professor,
Department of Computing,
Coimbatore Institute of
technology, Coimbatore, Tamil
Nadu, India

Dr. P Balamurugan
Assistant Professor,
Department of Computer
science, Government arts
college (Autonomous),
Coimbatore, Tamil Nadu,
India

Bio inspired based multi-objective data-privacy-preservation-technique (MO-DPPT) system model for cloud datas

Riyanto Efendi and Rofiul Wahyudi

DOI: https://doi.org/10.33545/27075923.2022.v3.i2a.47

Abstract

The significance of data security in the cloud system has boosted the increasing quantity of sensitive and personal data being harvested by data controllers. As the cloud has more outsourced, unsecured sensitive data for public access, the data security for the cloud sectors is very important. The majority of state-of-the-art strategies fail to manage optimal privacy in implementing data privacy preservation model. To ensure data privacy preservation, most of the traditional techniques can perform the transformation on the actual data. These traditional methods are utilized limitedly, as they are pretty memory intensive and complicated. Hence, to defeat this dispute, this paper tries to develop a novel approach named Multi-Objective Data-Privacy-Preservation-Technique (MO-DPPT) that can look after the data privacy issues. The two main phases of the data privacy preservation model consist of the data sanitization and restoration process. Here, the optimal key generation is based on the proposed sanitization process and it is done by a novel meta-heuristic algorithm namely the Muddy Soil Fish Optimization Algorithm (MSFOA). The optimal key generation is achieved by developing the multi-objective function that focuses on the parameters of hiding ratio (HR) rate, Preservation Ratio (PR) rate, False Rule (FR) generation rate, and Degree of Modification (DM). Moreover, the proposed MSFOA algorithm has confirmed improved execution through statistical analysis, analysis on KPA and CPA attacks, and computational time analysis over the conventional algorithms. Finally, the proposed MSFOA based MO-DPPT system model using is compared with the existing traditional algorithms namely PSO, GWO, JA, SSO, JA-SSO, and the performance analysis of the proposed MSFOA based MO-DPPT system model has proven the superior efficiency in improving cloud security.

Keywords: Degree of Modification (DM), False Rule (FR), Muddy Soil Fish Optimization Algorithm (MSFOA), Multi-Objective Data-Privacy-Preservation-Technique (MO-DPPT), Preservation Ratio (PR)

Introduction

In various fields of interest such as education, medical, and business [1], a substantial quantity of support to the global environment is provided by the cloud computing sector. Data Security is the most important part of the services that are obtainable around the globe. It has a key role in a cloud network environment. In cloud data security, various kinds of security risks such as key management and encryption, security applications, audit scheduling, physical and user access control, and access and identity management are discussed in [2] and [3]. By employing various encryption algorithms, the encryption of data is done recently in which the actual data is modified into a novel form named ciphertext. Only the permitted users can access this ciphertext. A separate key is utilized on the encrypted data using an algorithm and the data is decrypted to get back the original data which can be accessed only by the permitted user [4]. Data storage security and data processing security are the two important aspects of the privacy maintenance model in cloud environments. When the data center stores the data, there is an issue of ensuring user data confidentiality, which is tackled by Data storage security. Similarly in a virtualized cloud platform, the issue of preserving user confidentiality during runtime is taken care of by Data processing security. In the cloud sector, many approaches are presented to improve the efficiency of the data privacy preservation model. In 2018, to enhance the effectiveness of data privacy in the cloud sector, the privacy-aware access control method, relying upon Attribute Fuzzy Grouping named PriGuarder is proposed by Xie *et al.* [5].

Corresponding Author:
KH Vani
Assistant professor,
Department of Computing,
Coimbatore institute of
technology, Coimbatore, Tamil
Nadu, India

These two important traditional methods are relying upon either the perturbation or cryptography approach. For achieving data protection, the authors Belguith *et al*., [7] and Li *et al*., [4] have proposed a perturbation-based method, which changes the data with noise.

For situating the model privacy and usability, the modification is to be done with cautious calibration to enhance the stability. When the original text is processed, the data privacy of features is managed with threats in data security. Jiang *et al*., [8] has proposed a cryptography-based technique, which is based on the FHE, is being promoted as a guaranteeing solution. Because of this, the encrypted data along with the public keys can be uploaded to the cloud service provider and SMC in the direction of resulting the encrypted intermediary outcomes as discussed in [9] and [10]. As the user record does not consist of any hidden keys, it can not be used by data services providers [11]. As data privacy requires support through CSPs, it is yet to be considered more difficult than data security. Depending on the cloud environment, the CSPs can make use of and analyze the large volume of private data. The processing of sensitive data in the cloud may be considered very simple if the CSP is taken as trustworthy as per [4] and [12]. Although the data subjects don't allow the controller to transmit the data by the trustworthy members, their private or healthcare data have faith in the data controller in many various cases. On the contrary, unlike the controllers, the CSP may be under authority. Many public CSPs offer their services without any charge, to develop the chances for legitimating the users' data. To conquer the above-discussed issues and to re-establish the user's control, many solutions are introduced recently. In addition. they also aimed for the data protection outsourced to the cloud [13]. The sensitive data are required to be masked and these secured values are stored in the cloud environment. Only the permitted user who is having the recovered data from the cloud environment can unmask these secured values. Because of high data security, if the user requires to use both the data storage and the computational power of the cloud, then it is very difficult. It may be arranged compatible with the outsourced computations on masked data on cloud premises as in [14] and [15]. Hence it is necessary to develop an enhanced security model for cloud security.

In cloud security, the ultimate aim of the proposed method is similar to the existing previous techniques. Security of integrity, availability, and confidentiality are concentrated here. The modified sanitization process takes care of the optimal key generation. This research paper presents an algorithm namely MSFOA to generate the optimal key and subsequently, the sanitized data is reinstated effectively by the authorized user. Finally, the proposed MO-DPPT model using MSFOA is evaluated over the conventional algorithms such as PSO, GWO, JA, SSO, JA-SSO, and the resultant outcome is analyzed

The significant contribution of this paper is given below.

- To present the enhanced Multi-objective Data-Privacy-Preservation Technique (MO-DPPT) model for cloud data security
- To generate an optimal key generation using the Muddy Soil Fish Optimization Algorithm (MSFOA) approach
- To analyze the parameters of hiding ratio, preservation ratio, false rules generation ratio, and degree of modification, of improved MSFOA based MO-DPPT system model

This paper is structured as follows: Section 2 explains the Literature review. Section 3 analyses the modeling of MSFOA based MO-DPPT system design. Section 4 describes the implementation of the proposed MSFOA algorithm. Section 5 discusses the simulation results of the proposed model, and finally, Section 6 concludes the paper.

Literature Survey

Based on the distributed ensemble strategies, two scattered data privacy-preserving methods are presented by Li *et al*. in 2016 [16]. Studying the data distribution and summarizing the smart strategy more precisely are the significant effects of the incorporated method.

Based on the powerful differential privacy concept, in 2018, a Differential Privacy Preservation Multiple Cores DBSCAN Clustering (DP-MCDBSCAN) [17] method is proposed by Ni *et al*. In addition, to manipulate the data privacy leakage dispute for the user data network within the data mining protocol, and to enhance the competency in the data clustering along with the addition of Laplace noise, a novel algorithm named DBSCAN is also proposed by the same author. When compared with the traditional methods, the proposed one has proven the improved precision, competency, and privacy preservation result via the simulation outcomes.

In 2020, Danish Ahamad *et al*., [18] has developed the multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. By utilizing advancements of artificial intelligent techniques, a new Privacy preservation model for the cloud environment is proposed in this paper. The existing two well-executed algorithms namely Shark Smell Optimization (SSO) Algorithm and Jaya Algorithm (JA) are integrated and formed a novel hybrid Jaya-based Shark Smell Optimization (J-SSO) Algorithm. This hybrid algorithm is taken care of optimal key generation. The simulation outcomes validated the effectiveness of the proposed model over the existing models in improving cloud security.

To meet the complete expected security constraints for data storage in the cloud environment, a perfect public auditing method in fog-to-cloud-based IoT situations is presented by Tian *et al*. [19]. According to the bilinear mapping strategy, to convert the tags, a tag-transformation method is developed. During the proof generation phase, these tags are generated by mobile sinks to the ones formed using the fog nodes. Even though it can not effectively defend the privacy of identity, during the verification stage, it reduces computation and communication costs. To validate the integrity of IoT data from many generators, a zero-knowledge proof technique is also developed by which it achieves data-privacy preservation with a high precision rate.

By properly selecting a count of safety attributes and relieving some of the tasks judiciously to fog nodes, a protected Fog-based advent of IIoT is proposed by Sengupta *et al*. [20]. By decreasing the trust and load on the cloud environment and resource-constrained devices, these attributes safeguard the system. Scalability, agility, efficiency, and decentralization are the key advantages of this method. As the latency and cost are reduced, the capacity of fog computing becomes more popular and the resultant security is superior also. The cost of computation and bandwidth are more, which are the demerits of the method. It is mandatory to encrypt the data individually for all users, as the same data is utilized by many users.

A new hybrid combination of the BS-WOA algorithm is proposed by Thanga Revathi *et al.* [21] to find the confidential key by using the fitness function in such a way that, the privacy and the usefulness of the data are kept as much as feasible. It uses the only minimum count of parameters and the lack of local optima in resolving clustering issues are the significant benefits. Despite that, if more users use the data pool, it is very tough to keep the privacy of the database.

Jyothi Mandala (2019) [22] has proposed the Particle Swarm Velocity Aided GWO (PSV-GWO) technique for Privacy Preservation of Data. The main strategy in this proposed model uses an improved sanitization process in which, the original data given by the users is concealed. A novel PSV-GWO algorithm is proposed to create the optimal key during the sanitization process. At first, the sanitized data is retrieved by the permitter user safely in addition. In the end, the proposed model is compared with the conventional algorithms namely Particle Swarm Optimization (PSO), Genetic Algorithm (GA), Differential Evolution (DE), Crow Search Optimization (CSA), and Adaptive Awareness Probability-based CSA (AAP-CSA) and the simulation results are analyzed.

A Genetically Modified GlowWorm (GMGW) swarm optimization-based privacy preservation in cloud computing for the healthcare sector is proposed by Annie Alphonsa and Amudhavalli [23]. A hybrid algorithm is utilized in both data sanitization and data restoration processes. The application hosting, consumption cost, delivery, and content storage are the key advantages. For complex issues, it fascinates into local minimum specifically and can converge prematurely. The performance of this proposed hybrid system model is compared with other traditional methods in terms of sanitization and restoration effectiveness, statistical analysis, key sensitivity analysis, and convergence analysis. The superiority is verified by the simulation outcomes.

A novel Opposition Intensity-Based Cuckoo Search Algorithm (OI-CSA) is proposed by Shailaja and Guru Rao [24] for Data Privacy Preservation. There are two important stages known as sanitization and restoration are involved in the proposed PPDM strategy. At first, the connection rules are filtered out from the database. The optimal key extraction has a significant role in both the sanitization and restoration methods. This is achieved efficiently by using an adapted form of CSA namely OI-CSA. In this research work, hiding failure rate, information preservation rate, false rule generation, and degree of modification are the key research issues considered. Minimization of these parameters is achieved using modified sanitization and restoration processes. Improved runtime and scalability are the added advantages, but the effect of usage in web mining is not taken into account. In 2020, Kavitha and Malathi [25] proposed a new energy management technique for microgrid systems using a muddy soil fish optimization algorithm. This algorithm focuses on minimizing the cost of production and energy utilization together along with system limitations compared to the meta-heuristic algorithms. The excellent execution of the proposed MSFOA technique is validated by the simulation outcomes in terms of convergence speed and accuracy of result with remarkably least implementation period. Mohana Prabha and Vidhya Saraswathi [26] have proposed the SKMA-SC strategy, in which the main disadvantage is it is unable to improve the level of secrecy and data integrity for various methods in the cloud. Load balancing of various auditors can not be tackled by the Public auditing scheme proposed by Tian *et al.*, [19]. In 2019, Kwabena *et al.*, [27] have proposed Multi-scheme FHE which can not be utilized for practical purposes. Li *et al.*, [4] have presented the Security-based trust assessment method which is unable to develop the functioning model and is unfit for the practical environment. By keeping all these points in mind, to overcome these issues, a novel MSFOA based MO-DPPT system model is proposed. Finally, they compared their technique with existing techniques in terms of running time which results in a remarkable improvement

Proposed MSFOA based MO-DPPT model developed for the cloud data security using suggested objectives

Developed architectural view of MSFOA based MO-DPPT model

In recent research issues, data security in cloud computing is a significant condition is to recognize. When the safety measures are not provided perfectly for data transmission and operations, the data will be under more threat. There is a possibility of having more threats for data processing, as the stored data in cloud computing are accessed by a set of users. To meet the challenges of security limitations in cloud data, proper effective safety measures are needed to be developed. There is a feasibility of data mishandling if many organization networks are using the same sources. It is mandatory to safeguard the data and its archives which involve process, transit, or storage, to keep away from the risks.

A novel MSFOA based MO-DPPT system model is developed for cloud data, to overcome the above-discussed shortcomings present in the data privacy preservation schemes in the research papers. Figure 1 illustrates the architectural structure of the proposed MSFOA based MO-DPPT system model for cloud data security.

Data sanitization and data restoration are the two important processes involved in the proposed MSFOA based MO-DPPT system model. The method of concealing sensitive data in a cloud environment is referred to as data sanitization.

This method aims to stop leaking to unpermitted points. Subsequently, according to optimal to key generation, the proposed sanitization process is carried out using a meta-heuristic algorithm called MSFOA. By taking into account the multi-objective function which uses parameters such as information preservation ratio, hiding ratio, and degree of modification, the optimal key generation process is standardized. The proposed MSFOA can efficiently execute the data sanitization and data restoration for cloud data security, by utilizing this multi-objective function. Similarly, the process of extracting sensitive data using the unique key that is used for the data sanitation process is referred to as data restoration.

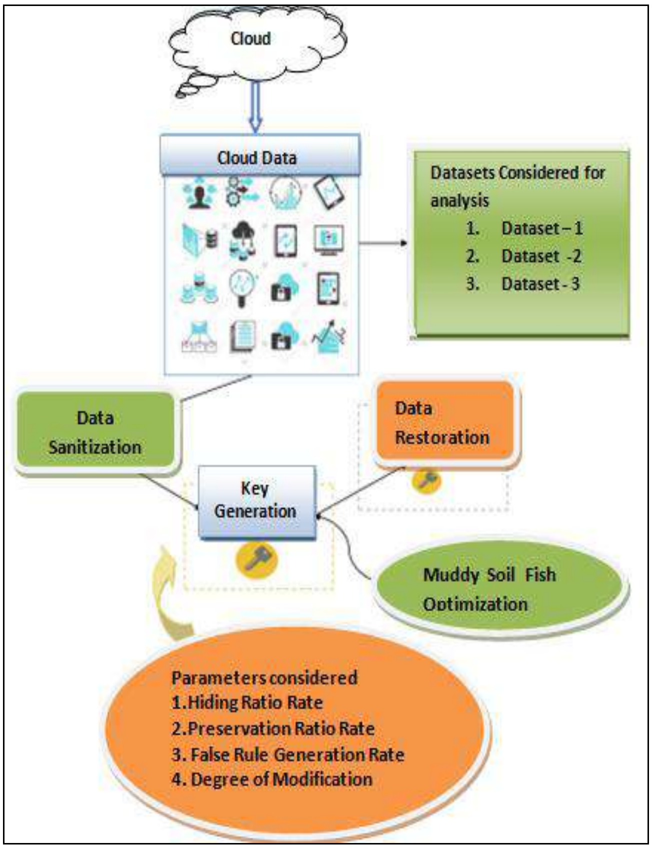

Fig 1: Data sanitization and restoration using an optimal key generation.

Dataset Description

The proposed MSOFOA based MO-DPPT system model for the cloud data is validated by collecting three different datasets in the Sports sector that are described below. Table 1 shows the three datasets that are taken into account.

Table 1: Dataset Description

Data Sets	Name of the datasets
Data Set 1	Chess dataset
Data Set 2	Cricket dataset
Data Set 3	Badminton dataset

Objective Function with suggested parameters

To achieve the objective function F for data preservation in the cloud environment, the MSFOA based MO-DPPT model is proposed and represented in Equation (1).

$$\text{Min F} = \max\left(\mathrm{HR_S}, \mathrm{PR_S}, \mathrm{FR_S}, \mathrm{DM_S}\right) \tag{1}$$

The four suggested objectives of $\mathrm{HR_S}$, $\mathrm{PR_S}$, $\mathrm{FR_S}$, and $\mathrm{DM_S}$ are used in Equation (1), which can be calculated as below. Here, the standardized HR rate is denoted by $\mathrm{HR_S}$ in equation (2), in which the worst HR among all loops is represented by max(HR).

$$\mathrm{HR_S} = \frac{\mathrm{HR}}{\max(\mathrm{HR})\,\forall\,\mathrm{loops}} \tag{2}$$

Now, the standardized PR rate is denoted by $\mathrm{PR_S}$ in equation (3), in which the worst PR among all loops is represented by max (PR).

$$\mathrm{PR_S} = \frac{\mathrm{PR}}{\max(\mathrm{PR})\,\forall\,\mathrm{loops}} \tag{3}$$

At this time, the standardized FR rate is denoted by $\mathrm{FR_S}$ in equation (4), in which the worst FR among all loops is represented by max (FR).

$$\mathrm{FR_S} = \frac{\mathrm{FR}}{\max(\mathrm{FR})\,\forall\,\mathrm{loops}} \tag{4}$$

At this time, the standardized DM is denoted by $\mathrm{DM_S}$ in equation (5), in which the worst DM among all loops is represented by max (DM).

$$\mathrm{DM_S} = \frac{\mathrm{DM}}{\max(\mathrm{DM})\,\forall\,\mathrm{loops}} \tag{5}$$

The actual database is denoted by $\mathrm{D_O}$ and the sanitized data based is denoted by $\mathrm{D_S}$.

Hiding Ratio (HR) rate

The HR rate donated by HR is defined as the rate of sensitive items that are correctly hidden in $\mathrm{D_S}$. The index of the value to be hidden is computed by using this. The association rules generated before the sanitization process are denoted by B and similarly, the association rules generated derived from $\mathrm{D_S}$. The sensitive rules are denoted by SRs.

$$\mathrm{HR} = \frac{\mathrm{abs}\,(B' \cap \mathrm{SRs})}{\mathrm{abs}\,(\,\mathrm{SRs})} \tag{6}$$

In Equation (6), the total number of data indexes that have to be hidden is termed $\mathrm{abs}\,(\,\mathrm{SRs})$ and $\mathrm{abs}\,(B' \cap \mathrm{SRs})$ as the length of the non-zero indexes. the mathematical formula for hiding ratio is equated in Equation (6) and the HR rate should be maximized for the best performance.

Preservation Ratio (PR) rate

Preservation Ratio (PR) rate is defined as the rate of non-sensitive rules not hidden in $\mathrm{D_S}$ and denoted by PR. The PR rate is the reciprocal of information loss, which is given in Equation (7).

$$\mathrm{PR} = 1 - \frac{abs\,(B \cap B')}{abs\,(\,B)} \tag{7}$$

The PR rate should be maximized for the proposed cloud security model.

False Rule (FR) generation rate

False Rule (FR) generation rate is defined as the rate of artificial rules produced in $\mathrm{D_S}$ and denoted by FR. Equation (8) illustrates the computation of the FR rate.

$$\mathrm{FR} = \frac{abs\,(B \cap B')}{abs\,(\,B')} \tag{8}$$

The FR rate should be maximized for the proposed cloud security model.

Degree of modification (DM)

The degree of modification (DM) is described as the degree of modification that happened between the original dataset $\mathrm{D_O}$ and sanitized data set $\mathrm{D_S}$ that is measured by finding the Euclidean distance ($\mathrm{E_d}$)among $\mathrm{D_O}$ and $\mathrm{D_S}$. The degree of modification is mathematically formulated in Equation (9).

$$\mathrm{DM} = \mathrm{E_d}(\mathrm{D_O}, \mathrm{D_S}) \tag{9}$$

Sanitization Process

During the sanitization phase, the binarization process of $\mathrm{D_O}$ and the obtained binarized key matrix $\mathrm{M_2}$ is computed. The acquired binarized key matrix is then subjected to the rule hiding method. In this process, between both the binarized forms of the resultant matrix $\mathrm{M_2}$ and original database $\mathrm{D_O}$, an XOR operation is done. Subsequently, with this result, the addition of one is done to derive the sanitized database $\mathrm{D_S}$. This is clearly illustrated in Equation (10).

$$\mathrm{D_S} = (M_2\ XOR\ \mathrm{D_O}) + 1 \qquad (10)$$

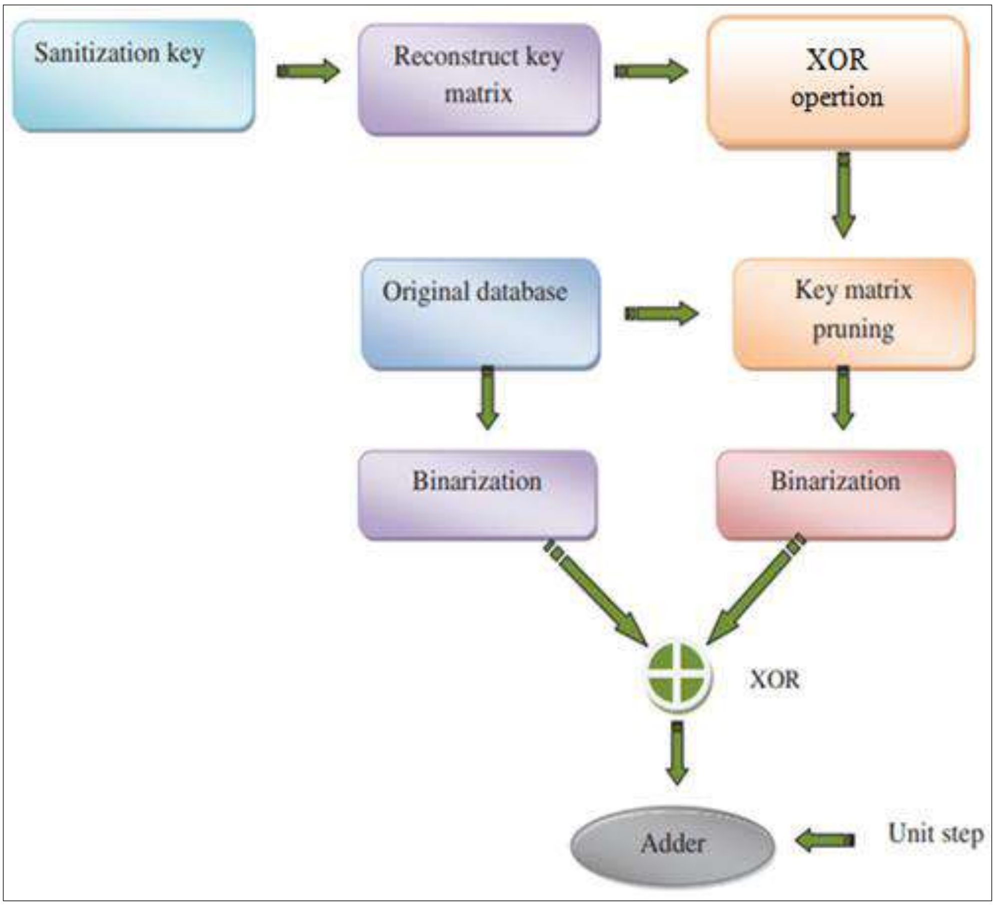

Fig 2: Structural design of sanitization process for the MSFOA based MO-DPPT system model.

Here, the sanitized data $\mathrm{D_S}$ reaches SRs and association rules tracking sanitization B′. Similarly, the corresponding associated rules before the sanitization B is filtered out by $\mathrm{D_O}$ for achieving the above discussed objective parameters. Figure 2 demonstrates the structural design of the sanitization process for the MO-DPPT system model.

Usually, before transferring to the cloud, the sensitive rules are concealed in the sanitization process. This further increases the protection of data for future applications and leads to enhancement in the operation of cloud data security environment without the threat of cyber-attacks.

Proposed Optimal Key Generation

In both the data sanitization and restoration process, the key extraction has a significant part in the proposed cloud data security model. The optimization is taken care of by the MSFOA algorithm. As a foremost step, by performing the XOR function, the key is transformed into a new form for key generation and this step is referred to as solution transformation. In this process, the XOR function is used to modify the reconstructed matrix M_2. By substituting in Equation (11), $\mathrm{M_{OK}}$ is derived from $\mathrm{M_2}$. The size of the array is calculated as $\sqrt{N''}$ X $\mathrm{TL_{peak}}$. In Equation (11), the key array $\mathrm{M_{OK}}$ is illustrated with an example for the key = {6,7,8}.

$$\mathrm{M_{OK}} = \begin{bmatrix} 6 & 6 & 6 \\ 7 & 7 & 7 \\ 8 & 8 & 8 \end{bmatrix}_{\left[\sqrt{N''}\ \mathrm{X}\ \mathrm{TL_{peak}}\right]} \qquad (11)$$

Here, N and N'' represents the number of transactions and the nearby roundoff exact square value of N respectively, and finally the $\mathrm{TL_{peak}}$ represents the peak value of transaction length. By implementing row-wise- replication using Equation (11), the restructured key matrix $\mathrm{M_{OK}}$ is generated. Finally by performing the XOR function, the key matrix $\mathrm{Key_{OK}}$ is created which is represented in Equation (12).

$$\mathrm{Key_{OK}} = \mathrm{M_{OK}} \oplus \mathrm{M_{OK}} \quad (12)$$

In Equation (12), the XOR function is denoted by the symbol $\oplus$, and similarly the dimension of the array $\mathrm{Key_{OK}}$ is taken as $\sqrt{\mathrm{N''}}$ X $\mathrm{TL_{peak}}$. Using the MSFOA algorithm, the generation of the optimal key is a significant achievement for the proposed MO-DPPT cloud data security model.

Restoration Process

By utilizing the same key that is generated using the proposed MSFOA, the actual data is extracted during restoration. Equation (13) depicts these steps, in which the restored data is denoted by $\widehat{D}_{RS}$. Both the sanitized data D_S and the key generated matrix M_2 are binarized in the restoration process. From the unit step, the binarized Sd from the binarization block is minimized. Now, one is deducted from the sanitized data D_S, which is in the binary form, and with this result XOR operation is performed with key matrix M_2. The resultant matrix is stored in a restored database, that denoted by $\widehat{D}_{RS}$. By making use of the updated data from the MSFOA technique and Equations (1), (10), and (11), the sanitizing key M_2, is restructured. By using Equation (13), there is a possibility of achieving lossless restoration, in which $\widehat{D}_{RS}$indicates the restored data.

$$\widehat{D}_{RS} = (D_S - 1) \oplus M_2 \tag{13}$$

Figure 3 demonstrates the Restoration Process of the Proposed MSFOA based MO-DPPT system model.

Optimal Solution Key Encoding

The proposed MSFOA algorithm is used for the optimization of keys to sanitize and restore the data. Based on the size of the data or the number of transactions, the length of the key is changed. The number of keys ranging from key M^1 to key M^M is optimized using MSFOA, and the optimal key is recognized. Figure 4 shows the optimal solution key encoding process. Here, the key length is assigned as $\sqrt{N''}$. The bounding limit is given from 1 to 2^6-1. The key vectors are optimized using the MSFOA algorithm for generating the best solution.

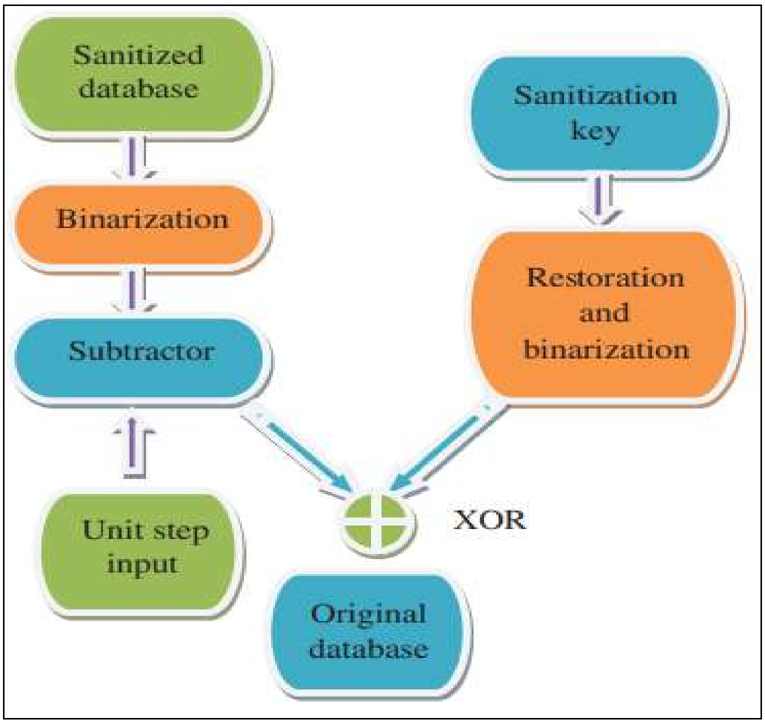

Fig 3: Structural design of Restoration Process for the Proposed MSFOA based MO-DPPT system model

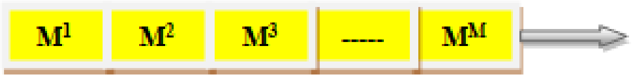

Fig 4: Keys for Encoding

Description of MSFOA Algorithm

In the proposed MSFOA based MO-DPPT system model for cloud data security, the presented MSFOA algorithm is used to create the optimal key. For resolving real-time optimization issues, this MSFOA algorithm offers improved efficiency. Also, it offers an excellent method of parameters transformation and improved searching capability at the beginning of the searching process itself. Moreover, this algorithm takes the least period for computing the optimal value and is very easy to resolve issues in multi-objective optimization challenges. Hence, it can be concluded that this combination of MO-DPPT using MSFOA offers improved execution than other meta-heuristic traditional algorithms.

Current updated technological changes motivate importance on evolutionary algorithms recently. These are particularly named meta-heuristic algorithms, which are derived based on biological development and they have more thrust with artificial intelligence. To resolve the global optimization issues, these algorithms offer the best solutions. Because of their flexible and adjustable attribute, these population-based algorithms can resolve multi-objective issues efficiently and provides expected results. Moreover, to achieve the objective function along with system model limitations, these algorithms will not have any constraints. Most of all, the combination of dispersed concepts along with efficient calculation in the discussed MSFOA algorithm aims to regulate the cost when compared with a centralized methodology.

The proposed MSFOA based MO-DPPT system model has outstanding advantages, which are listed below.

1. Possibility of easier calculation among all individual fishes because of widespread exploring capability
2. Feasibility of least computation cost because of the absence of centralized control drives
3. The capability of improving the convergence because of the fast transfer of local information among individuals
4. Viability of dynamic learning ability because of distributed memory storage

Based on the swarming fundamentals or the cooperative/communal reaction of fishes living in turbid water or muddy water, the searching (food) correlation is done in the presented MSFOA. Because of the own and neighborhoods effort of all individual single fish, they have an impact on the surroundings. The presented MSFOA method is presented to resolve the data privacy preservation techniques in the cloud environment. Based on the communal attitude model of fishes specifically living in the dull water or muddy ponds, this MSFOA has been developed. The more quantity of food accessibility is pointed out by the existence of a large count of fishes in a definite field. Figure 5 depicts the arresting attitude of muddy soil fishes toward food searching strategy.

By using an abnormal combination model of fishes, the proposed MO-DPPT using MSFOA is stimulated. Subsequently while foraging for possible prey (food), it undergoes the expansion and contraction process. Steps in the food searching process are illustrated in Figure 6.

By imitating the performance of fishes during many different phases such as searching, finding, and eating phase, the above discussed MSFOA method is concentrated on the global solution. While applying efficient techniques of food searching [28], muddy soil fishes utilize these three important conditions. The wonderful sensing capability [29] of fishes would facilitate to situate the food easily and earlier, irrespective of the visualization impairment of fishes in dull or unclear habitats.

By demonstrating the possible results over the design area, the basic attributes are considered in the discussed MSFOA, in which all individual fishes are assumed as a virtual entity and have their data and set of actions at K-dimensional position. The mass/weight of the fish is represented as a collective result of the success of the search and it is considered as the significant element that drives towards the ideal solution. is the mass of the fish. The objective function of minimization is the related factor of the thickness of food, which is derived from evolutionary techniques. In addition, the collected food in the specified area is also related to the objective function of minimization. There are important four types of functions namely solitary, foraging, impulsive-cooperative, and non-impulsive cooperative elements are achieved by MSFOA via foraging and movement.

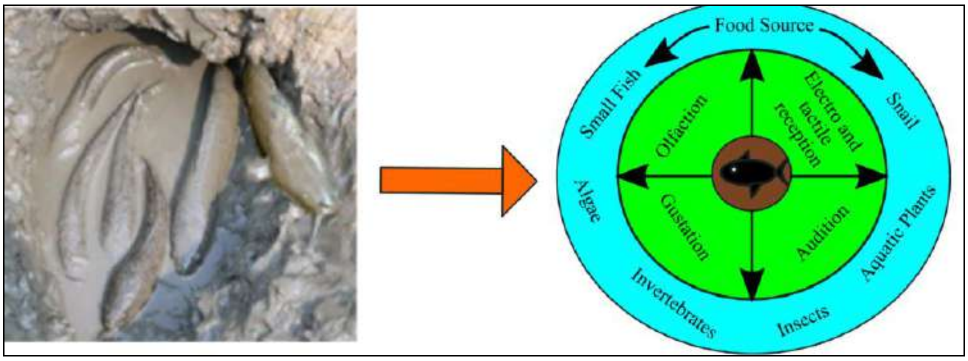

Fig 5: Food searching mechanism of MSFOA

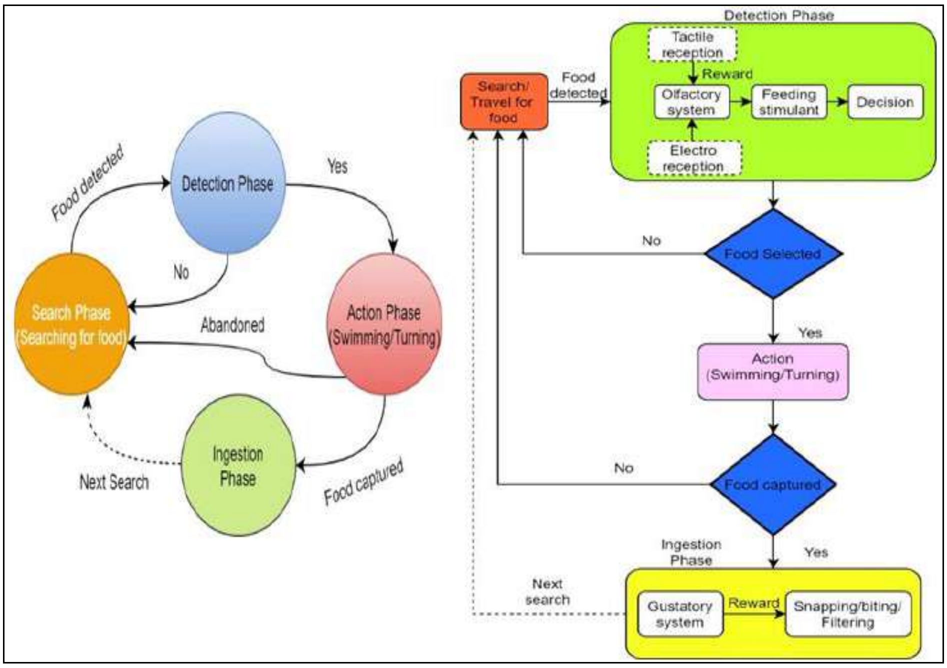

Fig 6: Steps involved in food searching process of Muddy Soil Fish Optimization

Solitary movement operator

The local search operation is performed arbitrarily by all individual fishes that live in the muddy water. Using the solitary operator, the capable solution is searched possibly in the constrained region. According to the current and previous progress of fish, the solitary operator is computed [30].

$$\delta_n(i+1) = \delta_n(i) + \alpha * \varsigma, \quad \alpha \in [-1, 1] \tag{14}$$

In Equation (14), the updated and current positions of fish are represented as $\delta_n(\mathrm{i}+1)$ and $\delta_n(\mathrm{i})$ correspondingly. In addition, using the uniform distribution element, the arbitrary number α is generated within the range from -1 to +1 and the step size is denoted by ς. Here, when the fitness function at a nearby position is higher than the current location (i.e) f($\delta_n(\mathrm{i}+1)$) > f ($\delta_n(\mathrm{i})$), then only all individual fishes are permitted to move towards the optimal position.

Otherwise, the updated and current positions reach the same values and that specified condition is stated as $\delta_n(i+1) = \delta_n(i)$ or $\Delta\delta_n = 0$. The difference between fitness values is computed using Equations (15) and similarly, the difference between displacement factors is computed using Equations (16). But this is possible only when the fish has solitary movement.

$$\Delta \mathrm{f_n} = \mathrm{f}\left(\delta_n(\mathrm{i}+1)\right) - \mathrm{f}\left(\delta_n(\mathrm{i})\right) \tag{15}$$

$$\Delta\delta_n = \delta_n(\mathrm{i}+1) - \delta_n(\mathrm{i}) \tag{16}$$

The magnitude of step size ς is reduced, when there is an enhancement in searching capability in further loops, and Equation (17) is used to determine the same.

$$\varsigma(\mathrm{i}+1) = \varsigma(\mathrm{t}) - \left[\frac{\varsigma_{\mathrm{b}} - \varsigma_{e}}{Maximum\ No.Loops}\right] \tag{17}$$

In this Equation (17), ς_{b} represents the step size length at the beginning and ς_{e} represents the step size length at the end, but the constraint here is the beginning step size length should be more than the end steps size length.

Foraging operator

The weight update technique of all individual fishes is associated with the foraging operator in a complex manner. While analyzing the movement of the current loops, according to the success rate, it is computed. The possibility of achieving the optimum region in the constrained area is maximized when the weight of fish rises. Using the foraging agent, the weight function is computed [30] as per Equation(18).

$$\mathrm{M_n}\,(\mathrm{i}+1) = \mathrm{M_n}\,(\mathrm{i}) + \left[\frac{\Delta \mathrm{f_n}}{\max\,(|\Delta \mathrm{f_n}|}\right] \tag{18}$$

In Equation (31), the mass of fish at updated and current positions are denoted by $\mathrm{M_n}\,(\mathrm{i}+1)$ and $\mathrm{M_n}\,(\mathrm{i})$ correspondingly. If the specified fish 'n' stays in the same position and does change its location, then the variations in the objective function Δf_n termed as the fitness function for updated and current positions, are assumed as zero. To ensure the improved convergence for reaching the optimum location in the considered area, using the mass scale (M_s), some unconventional attempts are made to evaluate the fitness function.

1. The approximate born mass of all individual fishes is to be $\frac{\mathrm{M_s}}{2}$
2. Mass scale Ms of the fish mass is limited within [1, Ms].

Impulsive cooperative movement operator

The presented movement structure/design is exposed by the cooperative operator. Along with the solitary movement of fish, this becomes successful and f_n reaches non-zero values. In Equation (19) using the variation in the fitness function ($\Delta \mathrm{f_n}$) of fishes, the mean weighted displacement factor $\mathrm{D} \in \mathrm{R}$ is computed, only by considering superior fitness functions of the fishes during the solitary movement [31].

$$\vec{D}(t) = \frac{\sum_{\mathrm{n}=1}^{N} \Delta\delta_{\mathrm{n}}\, \Delta \mathrm{f_n}}{\sum_{\mathrm{n}=1}^{N} \Delta \mathrm{f_n}} \tag{19}$$

In Equation (19), the variation between the updated and current locations of fishes present in the cluster is represented by $\overrightarrow{\Delta\delta_n}$ and similarly, the maximum quantity of a group is represented by N. Then using Equation (20), the current positions of all individual fishes are determined. $\overrightarrow{\Delta\delta_n}$

$$\overrightarrow{\delta_n}(i+1) = \overrightarrow{\delta_n}(i) + \vec{D}(i) \tag{20}$$

4.4 Nonimpulsive cooperative movement operator

During the search process, to tackle the search and search potential of the swarm, the non-impulsive cooperative movement operator is used. The efficient operation of the searching technique is indicated by the rise in the total weight of the swarm. The searching ability in the overall area of the considered region is decreased by increasing the swarm size. By applying the idea of centroid C via its expansion and compression technique, the size of the swarm is inhibited. According to the current locations of all individual fishes, the centroid G is determined and the Equation (21) represents its corresponding weight.

$$\vec{C}(i) = \frac{\sum_{\mathrm{n}=1}^{N} \overrightarrow{\delta_{\mathrm{n}}}\ \mathrm{M_n}(\mathrm{i})}{\sum_{\mathrm{n}=1}^{N} \mathrm{M_n}(i)} \tag{21}$$

Using Equation (22), the current position of all individual fishes is updated, when there is a rise in swarm size during current looping operations. Alternately, when there is a drop in swarm size during current looping operations, using Equation (23), the current position of all individual fishes is updated.

$$\overrightarrow{\delta_n}(i+1) = \overrightarrow{\delta_n}(i) - \alpha\,(0{,}1) * \varsigma_m \left[\frac{\overrightarrow{\delta_n}(i) - \vec{C}(i)}{d(\overrightarrow{\delta_n}(i), \overrightarrow{C}(i))}\right] \tag{22}$$

$$\overrightarrow{\delta_n}(i+1) = \overrightarrow{\delta_n}(i) + \alpha\,(0{,}1)\, X\, \varsigma_m \left[\frac{\overrightarrow{\delta_n}(i) - \vec{C}(i)}{d(\overrightarrow{\delta_n}(i), \overrightarrow{C}(i))}\right] \tag{23}$$

Euclidian distance is nothing but the separation distance between the centroid C and dynamic position of fish. To control the movement towards/from the centroid is denoted by the term predefined step length ςm and it is assumed as 0.5. The step size ς is doubled by ςm. The flowchart of the proposed MSFOA based MO-DPPT is illustrated in Figure 7.

The steps involved in the optimization method of MSFOA are described below.

Step1: The significant input information like the population count, control variables, increment step length, number of loops are assigned

Step2: The population of muddy soil fish is initialized arbitrarily to achieve the possible solution.

Step3: The computation of the fitness function is carried out.

Step4: A solitary movement operator is incorporated based on Equations (14) to (17).

Step5.1: Using Equation (18), the foraging operation is done. During verification, if the current position is more than the previous position, the control goes to step 6. If not, the subsequent step is executed.

Step5.2: Using Equations (19) and (20), the impulsive cooperative movement is performed and in addition, using equation (21) centroid location is used. Now again, it is evaluated that the current position is more than the previous position. If it is true, control goes to step 6. Otherwise, the control goes to the next immediate step.

Step 5.3: Using Equations (22) and (23), the non-impulsive cooperative movement is implemented

Step 6: Using Equation (17), the current optimum position and the maximum step size are updated.

Step 7: The steps from 4 to 5 are executed until the loop count achieves the maximum value.

Step 8: The current optimum position is given as output and exit.

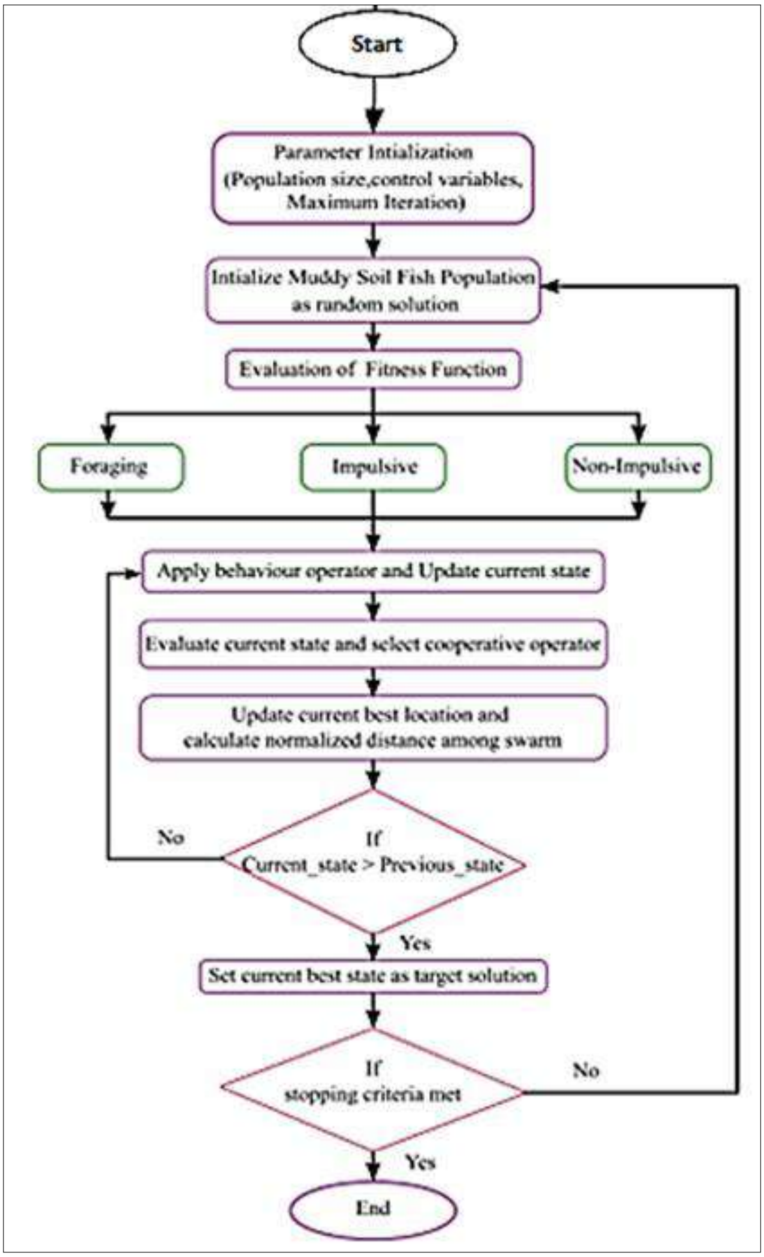
Start
Parameter Intialization
(Population size,control variables,
Maximum Iteration)
Intialize Muddy Soil Fish Population
as random solution
Evaluation of Fitness Function
Foraging
Impulsive
Non-Impulsive
Apply behaviour operator and Update current state
Evaluate current state and select cooperative operator
Update current best location and
calculate normalized distance among swarm
No
If
Current_state > Previous_state
Yes
Set current best state as target solution
If
stopping criteria met
No
Yes
End

Fig 7: Flow chart of proposed MSFOA

Results and Discussion

The proposed MSFOA based MO-DPPT system model for cloud security is implemented in MATLAB / Simulink platform and the analysis is carried out extensively for various security measures. Even though there are many tools available, MATLAB has more key merits such as easy debugging, simple computation coding, and the possibility of widespread data analysis. MATLAB has an excellent platform for the rapid development of many technologies to give absolute results, to achieve cloud data security through modern data preservation techniques. The population size is taken as 10 and the maximum number of loops is taken as 100 to complete the analysis. Table 2 shows the three different datasets that are collected for the analysis. For comparative analysis, the traditional optimization algorithms namely PSO [32], GWO [33], JA [34], SSO [35], and J-SSO [18] are considered.

By considering hiding ratio rate, Preservation Ratio rate, False Rule generation rate, and Degree of Modification parameters as suggested objective parameters, a multi-objective function is derived and optimal key generation is achieved. Other than the key parameter analysis, the performance of the proposed MSFOA based MO-DPPT system model is compared over the conventional models based on statistical analysis, analysis on KPA and CPA attacks, and computational time taken in addition.

5.1. Analysis of the Hiding Ratio (HR)

The HR rate should be maximized for the best performance of the proposed MSFOA based MO-DPPT system model. For three different datasets of 1, 2, and 3, the analysis of the Hiding Ratio (HR) is done by utilizing many optimization algorithms. The results are shown in the form of graphs as Hiding Ratio Vs Nos. of loops and the same is given from Figures 8 to 10. For all the datasets, the improved HR rate of the proposed MSFOA algorithm is computed and evaluated against traditional algorithms for many loops.

For the 100th loop, MSFOA is 69% enhanced than PSO, 19% enhanced than GWO, 39% enhanced than JA, 44% enhanced than SSO, and 14% enhanced than J-SSO for dataset-1. Then, for the 100th loop, MSFOA is 50% improved than PSO, 37% improved than GWO, 38% improved than JA, 27% improved than SSO, and 10% improved than J-SSO for dataset 2. Finally, for the 100th loop, MSFOA is 59% superior to PSO, 46% superior to GWO, 42% superior to JA, 36% superior to SSO, and 19% superior to J-SSO for dataset-3. Hence, it is concluded that the MSFOA based MO-DPPT system model gives better results than the traditional systems in terms of the hiding ratio for securing cloud data.

From the illustrated simulation results from Figures 8 to 10, it is concluded that for all the datasets the proposed MSFOA algorithm has outperformed traditional algorithms regarding the preservation of data in cloud sector.

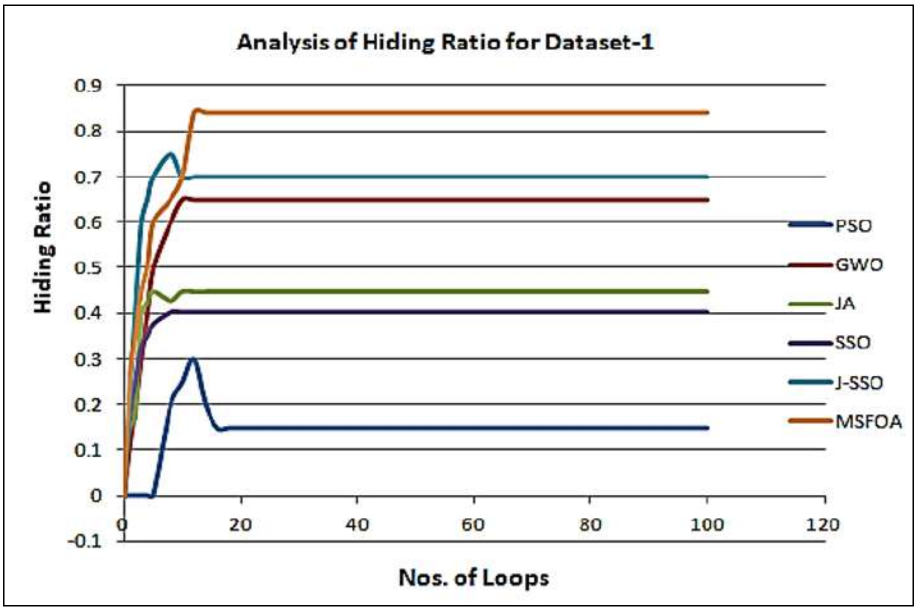

Fig 8: Analysis of HR for Dataset-1

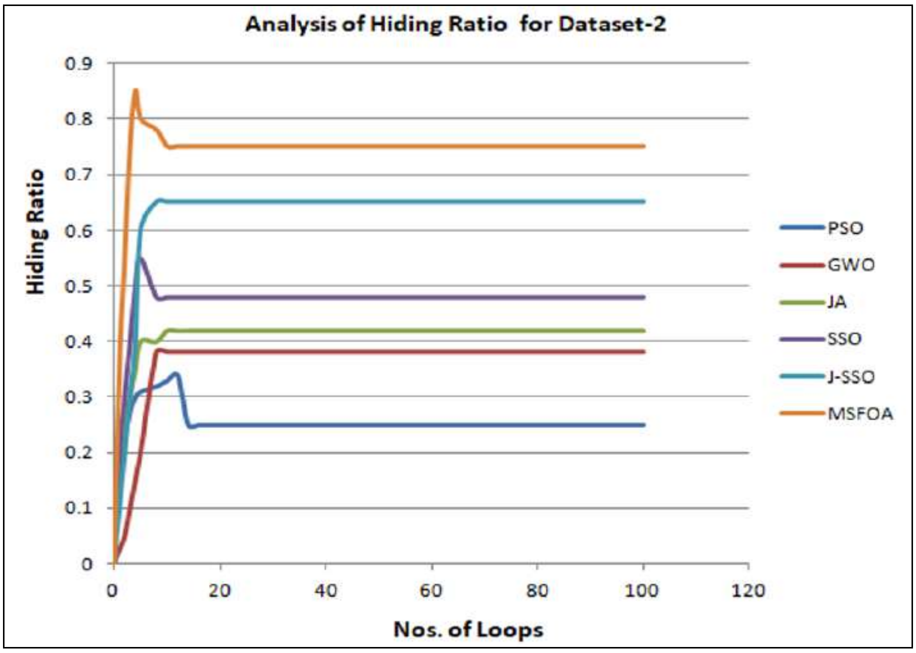

Fig 9: Analysis of HR for Dataset-2

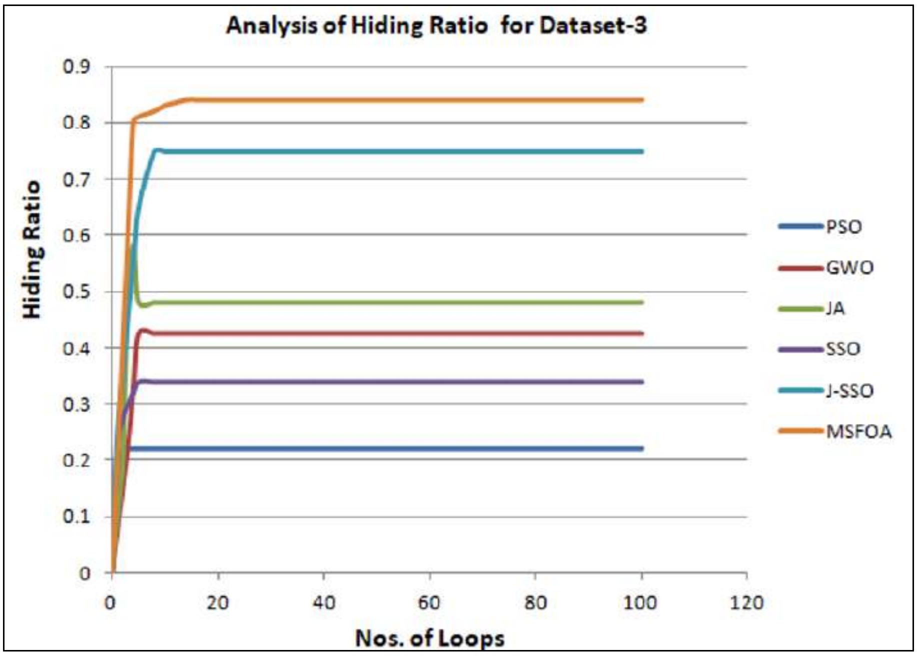

Fig 10: Analysis of HR for Dataset-3

5.2. Analysis of the Preservation Ratio (PR)

For three different datasets of 1, 2, and 3, the analysis of Preservation Ratio (PR) is carried out by making use of many existing traditional optimization algorithms. The results are shown in the form of graphs as preservation ratio Vs Nos. of loops and they are given from Figures 11 to 13. For all the datasets, the improved PR rate of the proposed MSFOA algorithm is computed and evaluated against traditional algorithms for many iterations.

When compared with the conventional algorithms, the presented MSFOA algorithm provides superior results for all the iterations from 0 to 100. For the 100th loop, MSFOA is 72% enhanced than PSO, 7% enhanced than GWO, 40% enhanced than JA, 42% enhanced than SSO, and 2% enhanced than J-SSO for dataset-1. Then, for the 100th loop, MSFOA is 10% improved than PSO, 73% improved than GWO, 38% improved than JA, 20% improved than SSO, and 8% improved than J-SSO for dataset 2. Finally, for the 100th loop, MSFOA is 12% superior to PSO, 75% superior to GWO, 40% superior to JA, 22% superior to SSO, and 10% superior to J-SSO for dataset-3. Hence, it is concluded that the MSFOA based MO-DPPT system model gives better results than the traditional systems in terms of the degree of modification for securing cloud data. From the illustrated simulation results from Figures 11 to 13, it is concluded that for all the datasets the proposed MSFOA algorithm has outperformed traditional algorithms regarding the preservation of cloud data.

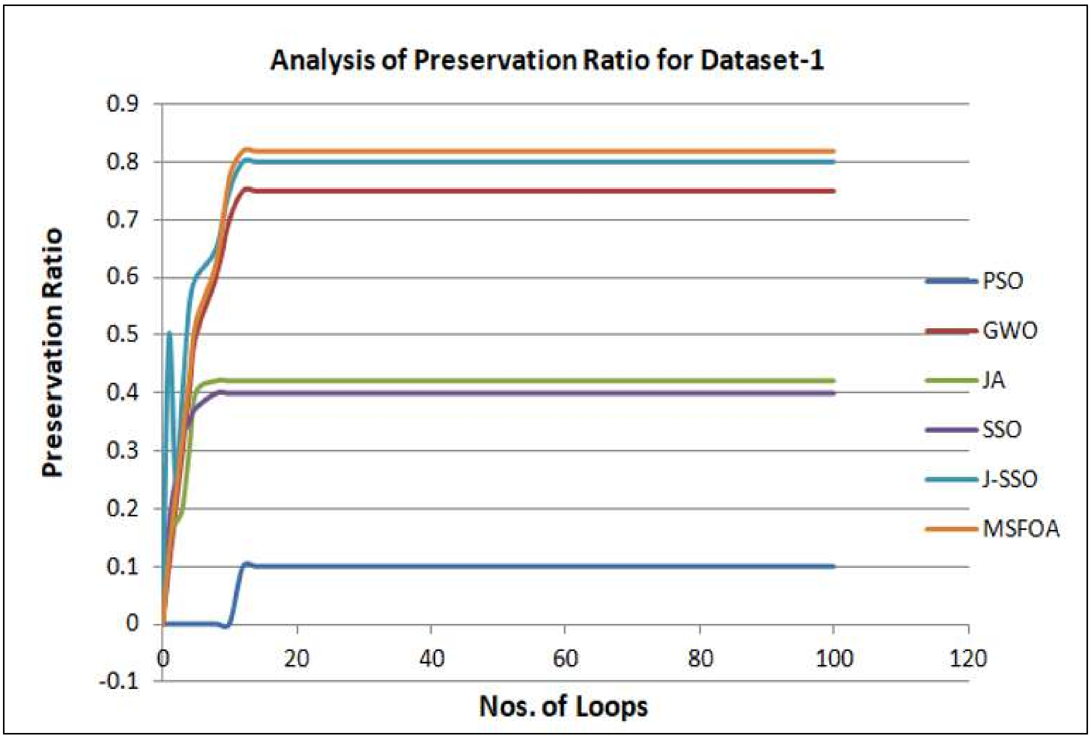

Fig 11: Analysis of PR for Dataset-1

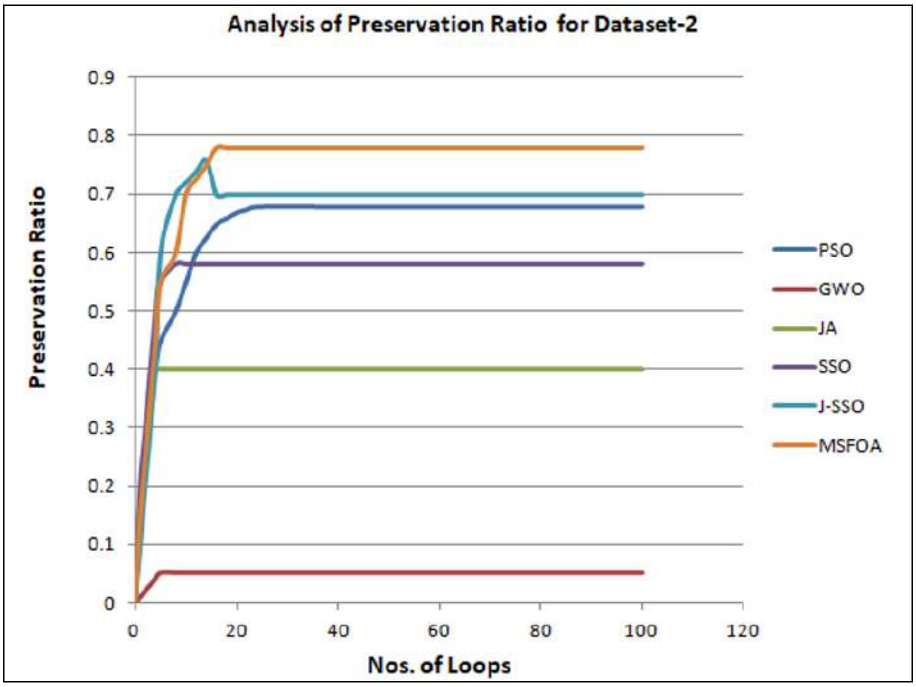

Fig 12: Analysis of PR for Dataset-2

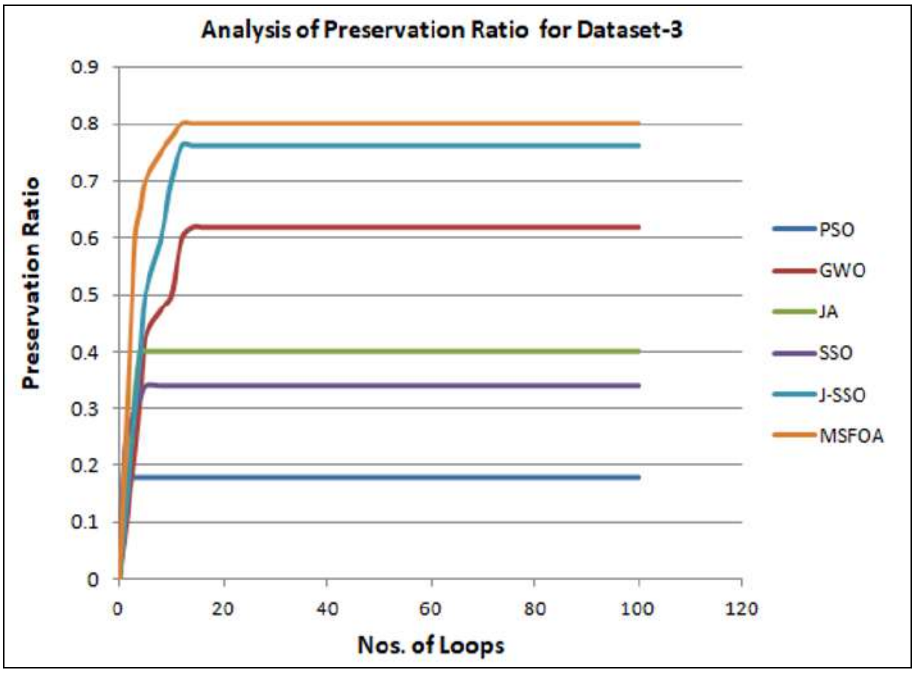

Fig 13: Analysis of PR for Dataset-3

Analysis of Failure Ratio or False Rule (FR) generation rate: Failure Ratio or False Rule (FR) generation rate is described as the rate of artificial rules produced in D_S and it must be maximized for the proposed cloud security model. For three different datasets of 1, 2, and 3, the analysis False Rule (FR) generation rate is done by making use of various optimization algorithms. The results are shown in the form of graphs as False Rule generation rate Vs Nos. of loops and they are given from Figures 14 to 16. For all the datasets, the improved FR rate of the proposed MSFOA algorithm is computed and evaluated against traditional algorithms for many loops. When compared with the traditional algorithms, the presented MSFOA algorithm provides superior results for all the loops from 0 to 100. For the 100th loop, MSFOA is 67% enhanced than PSO, 37% enhanced than GWO, 27% enhanced than JA, 14% enhanced than SSO, and 3% enhanced than J-SSO for dataset-1. Then, for the 100th loop, MSFOA is 49% improved than PSO, 37% improved than GWO, 30% improved than JA, 19% improved than SSO, and 3% improved than J-SSO for dataset 2. Finally, for the 100th loop, MSFOA is 57% superior to PSO, 45% superior to GWO, 38% superior to JA, 27% superior to SSO, and 11% superior to J-SSO for dataset-3. Hence, it is concluded that the MSFOA based MO-DPPT system model gives better results than the traditional systems in terms of the degree of modification for securing cloud data. From the illustrated simulation results from Figures 14 to 16, it is concluded that for all the datasets the proposed MSFOA algorithm has outperformed traditional algorithms regarding the preservation of cloud data.

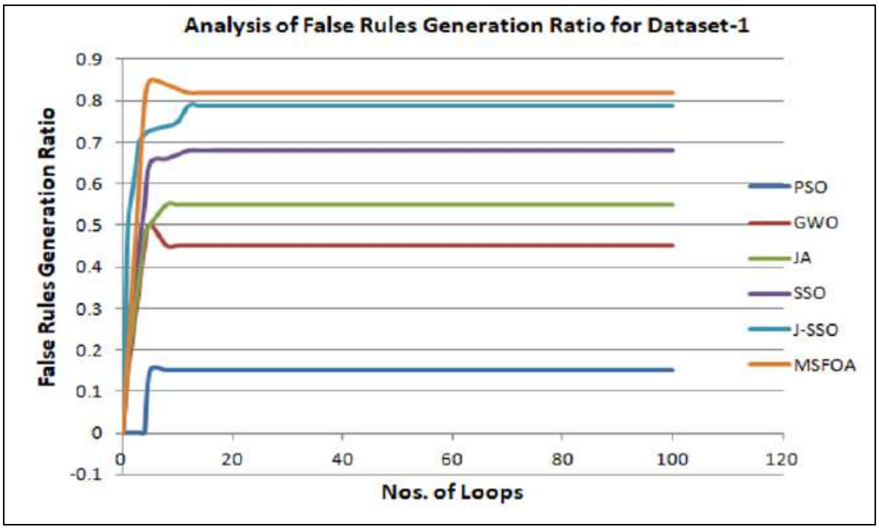

Fig 14: Analysis of FR for Dataset-1

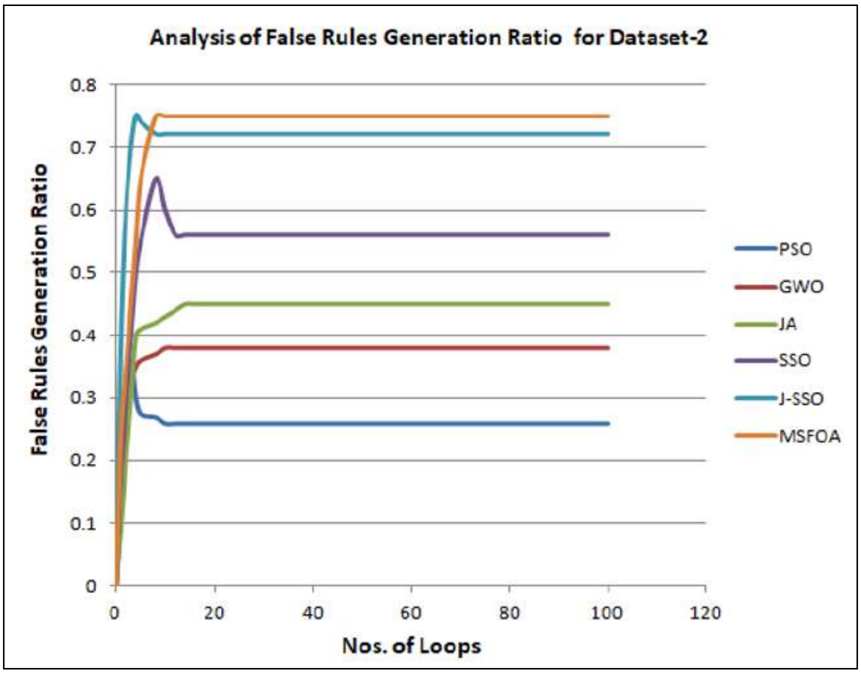

Fig 15: Analysis of FR for Dataset-2

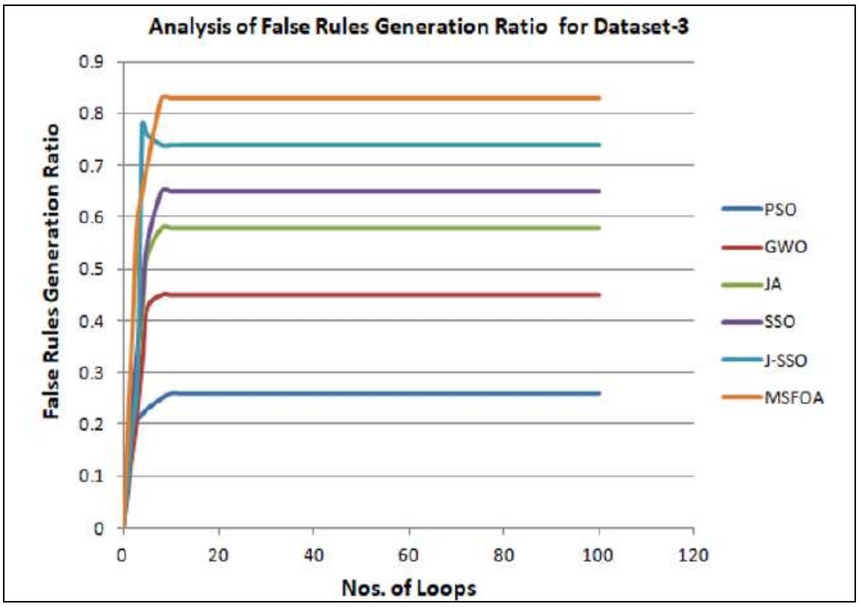

Fig 16: Analysis of FR for Dataset-3

Analysis of the Degree of Modification (DM)

For three different datasets of 1, 2, and 3, the analysis of the degree of modification (DM) is carried out by making use of various optimization algorithms. The results are shown in the form of graphs as distance Vs Nos. of loops and the same is given from Figures 8 to 10. As discussed above, the Euclidean distance(Ed) between the original data (DO) and sanitized data (DS) is considered as the DM. Zero data loss during the sanitization process is guaranteed, by achieving a minimum DM value.

When compared with the conventional algorithms, the presented MSFOA algorithm results in a very minimum distance for all the iterations from 0 to 100. For the 100th loop, MSFOA is 83% improved than PSO, 82% improved than GWO, 81% improved than JA, 76% improved than SSO, and 25% improved than J-SSO for dataset 1. Then, for the 100th loop, MSFOA is 75% enhanced than PSO, 85% enhanced than GWO, 86% enhanced than JA, 80% enhanced than SSO, and 33% enhanced than J-SSO for dataset-2. Finally, for the 100th loop, MSFOA is 90% superior to PSO, 46% superior to GWO, 86% superior to JA, 83% superior to SSO, and 30% superior to J-SSO for dataset-3. Hence, it is concluded that the MSFOA based MO-DPPT system model gives better results than the traditional systems in terms of the degree of modification for securing cloud data.

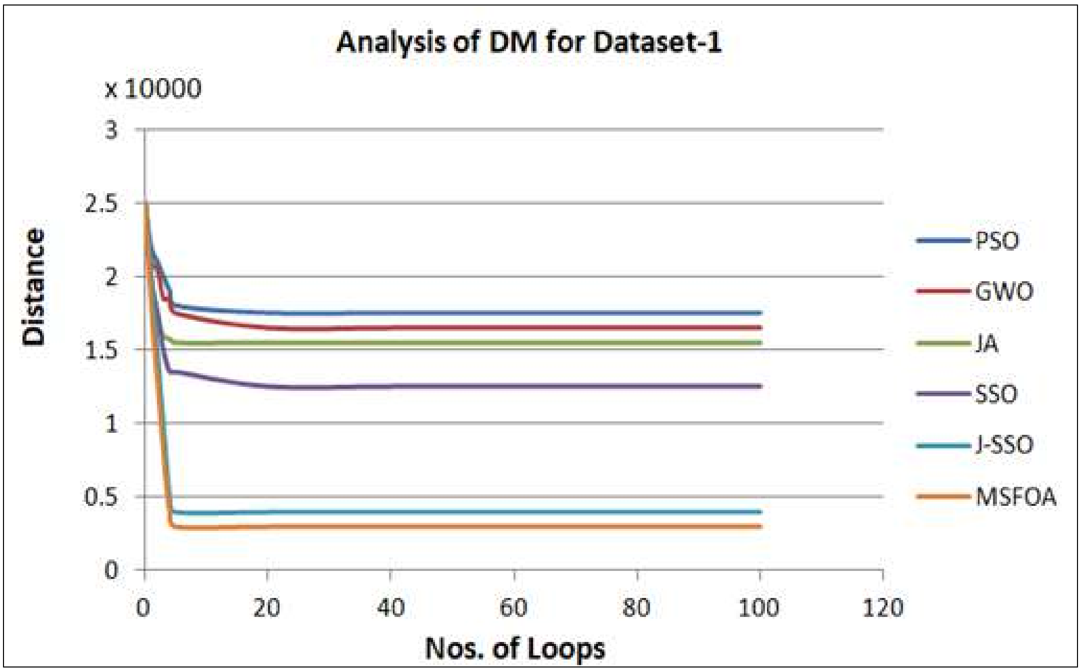

Fig 17: Analysis of DM for Dataset-1

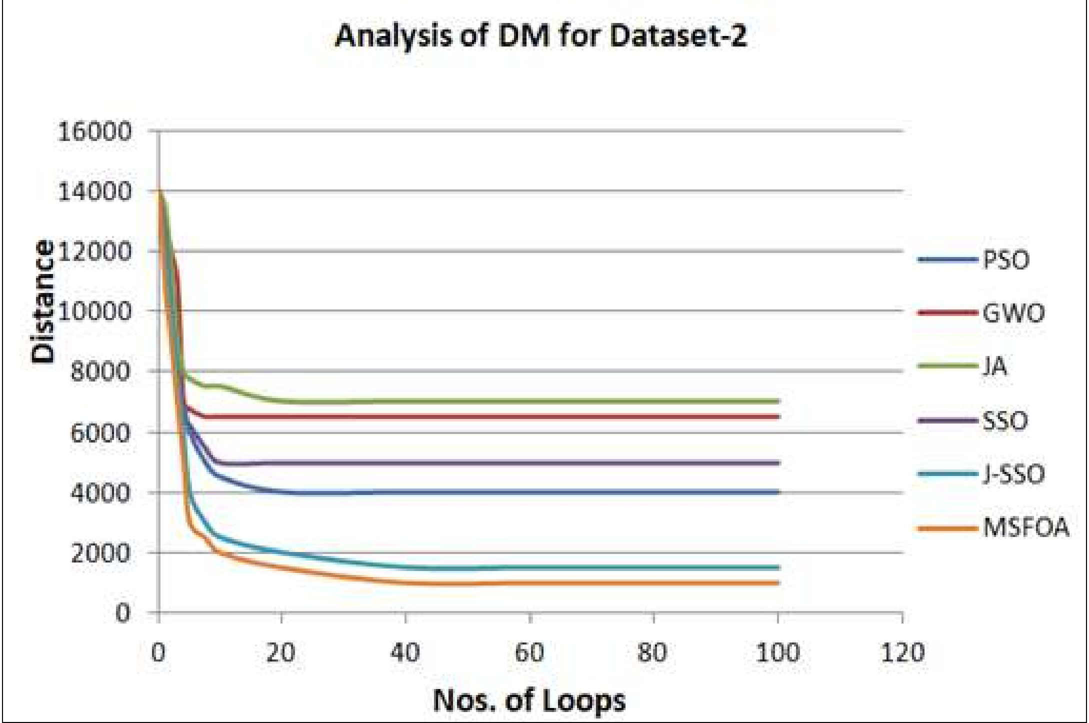

Fig 18: Analysis of DM for Dataset-2

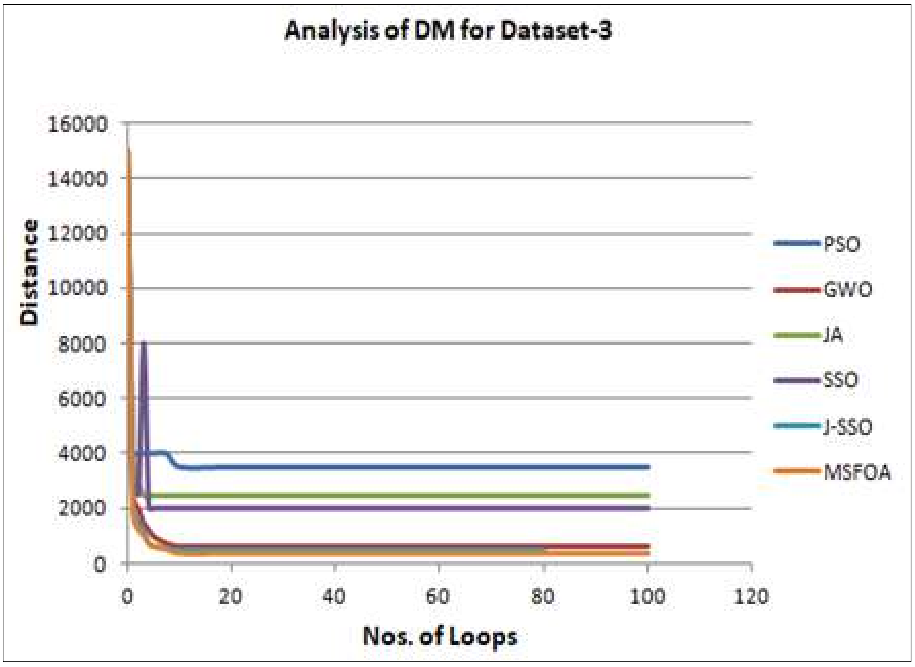

Fig 19: Analysis of DM for Dataset-3

Analysis of KPA and CPA attacks

Chosen Plaintext Attack (CPA) is defined as an attack model for crypt-analysis which presumes that the attacker can obtain the cipher-texts for arbitrary plain texts. Similarly, the term Known Plaintext Attack (KPA) is described as a model designed to attack in cryptanalysis in which, the attacker has permission to both the plaintext as well as the encrypted version of it. Table 2 shows the impact of data security against KPA and CPA attacks on different algorithms for three different datasets. When a CPA attack occurs, the association between the actual and restored data is carried out. In the same manner, the association between the actual and restored data is done, when the KPA attack occurs. From the results of this analysis, the correspondence between the actual and restored data achieves the least value, during these two attacks. Finally, it is concluded that the presented algorithm has proven the improved efficiency against the KPA and CPA attacks than the traditional algorithms for cloud data security.

Table 2: Effect on KPA and CPA attacks for various datasets in the cloud

Algorithms	Data Set 1	Data Set 2	Data Set 3
Effect on KPA attacks			
PSO (Bonyadi and Michalewicz, 2016) [32]	0.99998	0.99997	0.99998
GWO(Nirmala Sreedharan *et al*., 2018)	0.99992	0.99996	0.99997
JA (Venkata Rao, 2016)	0.99999	0.99998	0.99996
SSO (Abedinia *et al*., 2014)	0.99997	0.99996	0.99998
J-SSO (Danish Ahamad, 2020)	0.99996	0.99759	0.99498
Presented MSFOA	0.99995	0.99655	0.99425
Effect on CPA attacks			
PSO (Bonyadi and Michalewicz, 2016) [32]	0.99999	0.99999	0.99998
GWO(Nirmala Sreedharan *et al*., 2018)	0.99995	0.99996	0.99995
JA (Venkata Rao, 2016)	0.99989	0.99998	0.99999
SSO (Abedinia *et al*., 2014) [35]	0.99998	0.99975	0.99996
J-SSO (Danish Ahamad, 2020)	0.99797	0.99896	0.99995
Presented MSFOA	0.99658	0.99792	0.99459

Statistical analysis

The meta-heuristic algorithms can give only non-precise results, as they are stochastic. It is mandatory to execute each algorithm 5 times in terms of various measures like best performance, worst performance, mean, median, standard deviation, because of the stochastic nature of the algorithms. The efficiency of the MSFOA based MO-DPPT system model is to be analyzed and compared against other traditional algorithms of PSO, GWO, JA, SSO, J-SSO. The best way of confirming the competency of the algorithms is by conducting statistical analysis on the acquired outcomes. For Dataset-1, statistical analysis of MSFOA based MO-DPPT system model is carried out and evaluated against other traditional models. The same is demonstrated in Table-3, Table-4, and Table-5.

As an illustration for dataset-2, a detailed statistical analysis of MSFOA is illustrated. The best of the MSFOA is 52%, 72%, 77%, 77%, and 13% better than PSO, GWO, JA, SSO, and J-SSO respectively. The worst of MSFOA is 50%, 51%, 54%, 55%, and 13% better than PSO, GWO, JA, SSO, and J-SSO respectively. The mean of MSFOA is 50%, 63%, 66%, 66%, and 13% better than PSO, GWO, JA, SSO, and J-SSO respectively. The median of MSFOA is 58%, 71%, 72%, 70%, and 10% respectively. Finally the standard deviation of MSFOA is 64%, 36%, 10%, 6%, and 32% respectively.

Similar detailed statistical analysis is carried out on dataset-1 and dataset-3 also. The outcomes prove that the proposed MSFOA has shown enhanced performance than the conventional algorithms.

Table 3: Statistical analysis on Dataset -1 for proposed cloud data security

	PSO [32]	GWO [33]	JA [34]	SSO [35]	J-SSO [18]	Presented MSFOA
Best	12.917	15.237	9.7998	11.608	2.5918	2.2345
Worst	15.632	15.736	17.284	19.22	8.4012	7.568
Mean	14.47	15.339	15.088	17.187	4.3883	4.125
Median	15.237	15.237	16.000	18.447	3.6427	3.256
Standard Deviation	1.2488	0.2223	3.0637	3.1811	2.2985	1.958

Table 1: Statistical analysis on Dataset -2 for proposed cloud data security

	PSO [32]	GWO [33]	JA [34]	SSO [35]	J-SSO [18]	Presented MSFOA
Best	0.94072	4.4578	5.3572	5.4146	1.4369	1.2568
Worst	6.4628	6.6864	7.0371	7.1643	3.7535	3.2487
Mean	4.2533	5.7156	6.3388	6.2782	2.4564	2.135
Median	4.4961	6.4628	6.7868	6.2809	2.0879	1.869
Standard Deviation	2.024	1.1343	0.80731	0.77601	1.0656	0.7256

Table 2: Statistical analysis on Dataset - 3 for proposed cloud data security

	PSO [32]	GWO [33]	JA [34]]	SSO [35]	J-SSO [18]	Presented MSFOA
Best	1.1022	0.55068	0.61149	1.5107	0.52962	0.4925
Worst	3.7543	0.57555	2.6038	2.3195	0.57451	0.5268
Mean	2.1525	0.56557	1.2709	1.9279	0.5518	0.5157
Median	1.7947	0.56442	0.8682	1.9932	0.55068	0.5325
Standard Deviation	1.1131	0.009693	0.80661	0.37934	0.01591	0.1252

Analysis of computational time

The computational time of the proposed and existing methods is analyzed and listed in Table 5. The computational time of the proposed MSFOA is 11.33% better than PSO, 20.65% better than GWO, 20.72% better than JA, 21.22% better than SSO, 2.02% better than BS-WOA, 5.17% better than PSV-GWO, 5.31% better than GMGW, 6.33% better than OI-CSA, and 2.49% better than J-SSO respectively. Even though the computational time of the proposed method is lesser than one of the existing methods, the performance in securing the cloud data seems to be better when compared to all the existing methods

Table 3: Computational time of the MSFOA and existing methods for cloud data security

Methods	Computational time (sec)	% Of improvement
PSO [32]	142.38	11.33
GWO [33]	159.11	20.65
JA [34]	159.24	20.72
SSO [35]	160.26	21.22
J-SSO [18]	129.47	2.49
Presented MSFOA	126.25	-

Conclusion

The paper has presented a Muddy Soil Fish Optimization Algorithm (MSFOA) approach based on a Multi-objective Data-Privacy-Preservation-Technique (MO-DPPT) based system model for cloud security. The proposed MSFOA based MO-DPPT system model has been implemented specifically for data security in the cloud sector. The two significant steps namely data sanitization and restoration along with optimal key generation are included in the proposed model. By deriving a multi-objective function with the parameters of the hiding ratio rate, Preservation Ratio rate, False Rule generation rate, and Degree of Modification, the generation of the optimal key is optimized using the proposed MSFOA algorithm.

The key extraction strategy has a significant part and is chosen optimally by utilizing MSFOA, The proposed system model is evaluated against the traditional systems of PSO, GWO, JA, SSO, and J-SSO, and the optimal results are achieved for the proposed scheme. While considering the state-of-the-art meta-heuristic algorithms for solving the privacy preservation problem in handling numerous data, the conventional algorithms offer poor in maintaining the privacy of every database. Therefore, the proposed MSFOA based MO-DPPT system model has shown better performance through analysis on KPA and CPA attacks, statistical analysis, and computational time analysis over the conventional algorithms. In Summary, the improvement of the adopted MSFOA based MO-DPPT system model has been verified effectively and the simulation outcomes prove that the implemented system model has superior functionality to the traditional systems.

Future work: In the future, a key management strategy is to be taken into account to secure the keys.

Declaration of statement

The authors declare that they have no conflict of interest.

References

1. Alabdulatif A, Kumarage H, Khalil I, Yi X. Privacy-preserving anomaly detection in the cloud with lightweight homomorphic encryption. J. Comput. Syst. Sci. 2017;90:28-45.
2. Tysowski PK, Anwarul Hasan M. Hybrid attribute- and re-encryption-based key management for secure and

scalable mobile applications in clouds. IEEE Trans. Cloud Comput. 2013;1(2):172–186.

3. Chun-TaLi DH, Chun-ChengWang. Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Comput. Methods Prog Biomed. Elsevier. 2018;157:191-203.
4. Li P, *et al*. Multi-key privacy-preserving deep learning in cloud computing. Future Generation. Comput. Syst. 2017;74:76-85.
5. Xie X, Yuan T, Zhou X, Cheng X. ‘‘Research on trust model in a container- based cloud service”, CMC: Computers, Materials & Continua. 2018;56(2):273-283.
6. Su M, Zhang L, Wu Y, Chen K, Li K. Systematic data placement optimization in multi-cloud storage for complex requirements. IEEE Trans. Comput. 2016;65(6):1964–1977.
7. Belguith S, Kaaniche N, Laurent M, Jemai A, Attia R. ‘‘PHOABE: securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT”. Comput. Netw. 2018;133:141-156.
8. Jiang T, Chen X, Ma J. Public integrity auditing for shared dynamic cloud data with group user revocation. IEEE Trans. Comput. 2016;65(8):2363–2373.
9. Gao CZ, Cheng Q, Li X, Xia SB. Cloud-assisted privacypreserving prolematching scheme under multiple keys in mobile social network. Cluster Comput, 2018, 1-9
10. Mo S, Liu T, Zeng Q, *et al*. Research on central control cloud power grid system based on cloud energy storage and cloud power generation technology. Sichuan Electric Power Technol. 2018;41(4):28–31.
11. Liu J, Zhang N, Kang C. Research framework and basic model of cloud energy storage in electric power system. Chin. J. Electr. Eng. 2017;37(12):3361-3663.
12. Stergiou C, Psannis KE, Kim BG, Gupta B. Secure integration of iot and cloud computing. Future Generat. Comput. Syst. 2018;78:964-975.
13. Behl A. ‘Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation, World Congress on Information and Communication Technologies, 2011, 217-222.
14. Ali M, Khan SU, Vasilakos AV. Security in cloud computing: opportunities and challenges. Inf. Sci. 2015;305:357-383.
15. Choi M, Lee C. Information security management as a bridge in cloud systems from private to public organizations. Sustainability. 2015;7(9):12032-12051.
16. Li Y, Bai C, Chandan Reddy K. A distributed ensemble approach for mining healthcare data under privacy constraints, Information Sciences. 2016;330:245-259.
17. Ni L, Li C, Wang X, Jiang H, Yu J. DP-Mcdbscan: Differential Privacy Preserving Multi-Core Dbscan Clustering for Network User Data, IEEE Access. 2018;6:21053-21063.
18. Ahamad D, Hameed SA, Akhtar M. A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. Journal of King Saud University-Computer and Information Sciences, 2020.
19. Tian H, Nan F, Chang CC, Huang Y, Jing LU, Yongqian DU. Privacypreserving public auditing for secure data storage in fog-to-cloud computing. J. Netw. Comput. Appl. 2019;127:59-69.
20. Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit. A Secure Fog Based Architecture for Industrial Internet of Things and Industry 4.0, IEEE Transactions on Industrial Informatics, 2020, 1-9.
21. Thanga Revathi S, Ramaraj N, Chithra S. Brain storm-based whale optimization algorithm for privacy-protected data publishing in cloud computing. Cluster Comput. 2019;22(2):3521-3530.
22. Jyothi Mandala, Chandra Sekhara Rao MVP. Particle Swarm Velocity Aided GWO for Privacy Preservation of Data, Journal of Cyber Security and Mobility. 2019;8(4):439-446.
23. Annie Alphonsa MM, Amudhavalli P. Genetically modified glowworm swarm optimization based privacy preservation in cloud computing for healthcare sector. Evol. Intel. 2018;11(1):101-116.
24. Shailaja GK, Guru Rao CV. Opposition Intensity-Based Cuckoo Search Algorithm for Data Privacy Preservation”, Journal of Intelligent Systems. 2019;29(1):1441-1452.
25. Veluchamy K, Veluchamy M. A new energy management technique for microgrid system using muddy soil fish optimization algorithm. International Journal of Energy Research. 2021;45(10):14824-14844.
26. Mohana Prabha KT, Vidhya Saraswathi P. Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography for privacy preserved data access in cloud computing, Computer Communications. May 2020;158:85-94.
27. Owusu-Agyemang Kwabena, Zhen Qin, Tianming Zhuang, Zhiguang Qin. MSCryptoNet: Multi-Scheme Privacy-Preserving Deep Learning in Cloud Computing, IEEE Access. February 2019;7:29344-29354.
28. Olsén KH, Sukovich N, Backman J, Lundh T. Chemical foraging stimulation in the omnivorous species crucian carp, Carassius carassius (Linnaeus 1758). Aquac Rep. 2018;12:36-42. https://doi.org/10.1016/j.aqrep.2018.09.003.
29. Ohara WM, Costa IDD, Fonseca ML. Behaviour, feeding habits and ecology of the blind catfish Phreatobius sanguijuela (Ostariophysi: Siluriformes). J Fish Biol. 2016;89(2):1285-1301. https://doi.org/10.1111/jfb.13037
30. Neto FBL, Albuquerque IMC, Filho JBM. Weight-based fish school search algorithm for many-objective optimization. arxiv170804745 cs. 2019, 1-12. http://arxiv.org/abs/1708.04745.
31. Bastos-Filho CJA, Monteiro RP, Verçosa LFV. Improving the performance of the fish school search algorithm. Int J Swarm Intell Res. 2018;9(4):21-46. https://doi.org/10.4018/IJSIR.2018100102
32. Bonyadi MR, Michalewicz Z. Impacts of coefficients on movement patterns in the particle swarm optimization algorithm. IEEE Transactions on Evolutionary Computation. 2016;21(3):378-390.
33. Sreedharan NPN, Ganesan B, Raveendran R, Sarala P, Dennis B. Grey Wolf optimisation-based feature selection and classification for facial emotion recognition. IET Biometrics. 2018;7(5):490-499.
34. Rao RV, Rai DP, Ramkumar J, Balic J. A new multi-objective Jaya algorithm for optimization of modern machining processes. Advances in Production Engineering & Management. 2016;11(4):271.
35. Abedinia O, Amjady N, Ghasemi A. A new metaheuristic algorithm based on shark smell optimization. Complexity. 2016;21(5):97-116.