




# Cyber Security and 5G-assisted Industrial Internet of Things using Novel Artificial Adaption based Evolutionary Algorithm

Shailendra Pratap Singh<sup>1</sup> · Giuseppe Piras<sup>2</sup> · Wattana Viriyasitavat<sup>3</sup> · Elham Kariri<sup>4</sup> · Kusum Yadav<sup>5</sup> · Gaurav Dhiman<sup>6,7,8,9,10</sup>  · S Vimal<sup>11</sup> · Surbhi B. Khan<sup>12</sup>

Accepted: 13 June 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

## Abstract

The Industrial Internet of Things (IIoT) evolved quickly at the start of the twenty-first century. Various services, such as quality of service (QoS) for smart cyber security management from the industrial domain, are complicated for us. It is challenging to select the optimal malicious nodes by taking into account QoS criteria, including information communication, and network coverage regions. Numerous constrained evolutionary optimization strategies are known to address these problems. This study proposes a broader definition of differential evolution (DE) that uses a quick adaptation strategy and an optimization-based design. It combines DE with a unique mutation approach to broaden the range of viable answers. This research also suggests a novel fitness function for energy harvesting in IIoT-based applications. Both on the IIoT-service architecture and in IIoT-based applications, the suggested method is assessed. The outcomes are then contrasted using state-of-the-art algorithms. It is discovered that the proposed approach produces better results in terms of cyber security of QoS, fitness cost, and detection of IIoT nodes from the IIoT service network.

**Keywords** Artificial intelligence algorithm · Optimization · Industrial internet of things · Quality of services · Security

## 1 Introduction

The Industrial Internet of Things (IIoT) is a subset of the Internet of Things (IoT), which mainly focuses on industrial applications. The IIoT significantly depends on smart devices to evaluate and gather data in real-time and to more effectively disseminate important information. Business choices may be made more swiftly and accurately with the help of IIoT. IIoT helps firms grow by enhancing the efficiency of their business operations and by assisting in their better understanding. Industrial services monitoring is always in use because of numerous IoT capabilities and equipment that must continually adhere to a patient's wellness limits. Due to the fundamental design of IIoT service frameworks, a variety of medical care devices have been developed using a variety of concepts and techniques, such as remote monitoring and air ambulances, which have been deployed in many countries to handle the rapidly growing demand for medical services during emergencies and hasten patient recovery.

The framework that is being presented consists of a few elements that are significant in terms of security. The system has a number of sensor hubs that are in charge of identifying and gathering malicious nodes, sending the information to a private or public cloud for storage and handling, and enabling qualified experts and the suggested method to detect malicious nodes information efficiently and continuously. The proposed architecture has been created with the flexibility of IPv6 transmission data in mind. The IIoT-nodes will receive messages in cases of emergency. Each sensor centre gathers and transmits the essential messages used by the GSM module that are linked to the suggested approach for the detection of malicious nodes.

For the purpose of producing data for the cloud, IIoT sensors continually monitor the whole industrial infrastructure. The sensors' lifespan is shortened by the energy consumption at a bit rate from the smart industrial framework. The lifespan of IoT sensors for IIoT must be extended by these sensors. These sensors are thus necessary for the optimisation strategies. The differential evolutionary algorithm (DE) was developed by Stron and Price [9–11] to effectively look for global optimisation in terms of continuous spaces. The initialization, mutation strategy, crossover strategy, and

✉ Gaurav Dhiman  
gdhiman0001@gmail.com

Extended author information available on the last page of the article

selection strategy phases of the DE algorithm work in that sequence. This approach contributes to the acceleration of the convergence process by providing a solution based on artificial adaptation vectors. A novel "Differential Evolution algorithm employing artificial adaptation vectors" (DEAAV) is suggested in this case. By using the suggested approach, merging solutions were transformed into locally optimum ones, the solution's diversity was preserved, and eventually the convergence rate rose. The recommended method has been used to assess the performance of sensor nodes in an IIoT application. There are several state-of-the-art evolutionary optimisation techniques with limits to handle such problems. This research suggests a new mutation operator that was developed through mutant vector adaptation. This article also suggests a novel fitness function for IIoT-based applications to maximise security and identify rogue nodes.

### 1.1 Problem statement

Highlights of problem description are as follows.

- The existing optimisation methods [3–7, 10–13] suffer from the mathematical model's growing computing cost. As a consequence of this problem getting worse, the diversity of the current algorithms is lost, and their rate of convergence increases.
- For the proper functioning of its sensor networks, IIoT [14–22] makes considerable use of sensors. The sensors have low security and data loss since they are using sensing services from the IIoT sensor network. As a consequence, IIoT-based wireless sensor networks (WSN) suffer data loss, which makes it challenging to identify fraudulent IIoT nodes [26–34].

### 1.2 Highlights of Author's Contribution are as follows

- It is suggested to use a DE algorithm variation called DEAAV (DE artificial adaptation-based algorithm).
- The DEAAV method enhances the search space convergence rate and maintains diversity.
- To evaluate our suggested approach to determine the optimal best value and identify malicious nodes, Addition we developed two novel fitness functions for IIoT-based scenario services.
- To evaluate our suggested approach, we developed three scenarios for IIoT-based smart industrial services. For the purpose of verifying the findings, the suggested method has been compared with traditional evolutionary algorithms.
- The proposed strategy minimises data loss during transmission and improves the process of detecting malicious nodes for the IIoT-smart framework.

### 1.3 Article organization

The rest of the paper is structured as follows: The related work on the DE algorithm and IoT is explained in Section 2, the proposed IIoT-based framework is explained in Section 3, the proposed artificial based operator is explained in Section 4, the experimental results and analysis are explained in Section 5 along with comparisons to existing DE variants, and the conclusion and future work of the presented study are presented in Section 6.

## 2 Related work

In [1], an original mutation mechanism is proposed for the initial selection method of the crossover in differential evolution. Combining DMDE and non-decomposition methods with DE variants may increase efficiency. Numerous combinations of optimisation problem cases have been utilised to assess the method's efficacy [2]. The results show that, in terms of processing speed, the suggested technique performs better than the other strategies that are currently in use. The researchers in [3] propose a neighbourhood mutation method based on mutation for adaptive differential evolution. Here, the mutation rate is accelerated by employing the typical number of mutations.

The researchers cited in [5] propose a mutation technique known as HABDE. Using fitness and geographical data, the HABDE technique dynamically splits into roles, each with its unique mutation. [9] proposes a novel PBDE-variant with an excellent self-adaptive strategy and homeostasis mutation method. The suggested approach [23] is compared to several DE iterations. The data analysis's findings indicate that, generally speaking, the recommended approach outperforms more established ones.

The researchers in [12] suggest a unique heuristic strategy for decreasing nonlinear & non-differentiable continuous space functions and show that the method picks up momentum more quickly than traditional methods.

The authors in [13] introduced an IoT-based quality of services (QoS) for data analysis. In order to maintain track of the smart applications, IoT devices are utilised. The recommended method for analysing IoT-based QoS data was shown to be effective in the experimental investigation. Researchers have not yet solved the issue of energy lifetime and service enhancement.

The authors of [14] provided a survey for the Internet of things based on energy efficiency, latency, life time, and security. The dynamic resource management strategy was recommended for the IoT services architecture by the authors of [15]. This concept offered a novel method for choosing how to distribute resources inside the IT architecture. The recommended requirements on research resource

management have shown to be fantastic for data gathered across numerous places.

The authors of [16] indicated that in order to increase data accessibility for a subsequent course of treatment as permanent history, the 5G physiologically inspired resource allocation be made accessible whenever the experts and the services framework require it. Such a vast volume of data must be handled and stored in a manner that ensures the security and secrecy required for the IIOT's resource information restriction [17]. Additionally, by identifying odd occurrences, this framework may notify the smart-based communication system. The authors of [18] proposed a method to offer scheduling services for an IoT by combining quality of service (QoS). The layered architecture is composed of the application, processor, perception, transport, and network layers.

The researchers [19] devised a multi-objective based PSO (MOPSO) technique for wireless sensor networks taking into account an energy efficiency parameter. The notion of cutting down on energy costs and maintenance times is also discussed. But when a wireless sensor network is tested, the energy consumption issue is still there. The IoT strategy was tried, however the energy consumption issue was not solved.

The authors [20] have provided a cyber-physical based survey to aid in the detection of assaults on different communication networks. The issue of human-to-human cyber-physical for services was solved by the vulnerability. However, as can be seen from the cyber physical, the problem of security usage has not yet been overcome.

This is how the agricultural farm is monitored with IoT devices. The recommended strategy for IoT-based farm data analysis was shown to be effective in the experimental study. Researchers have not yet developed a solution for the issue of enhancing service and prolonging the lifetime of energy [25].

The authors of [26] presented a Particle Swarm Optimisation (PSO) approach for wireless sensor networks with regard to the energy efficiency parameter. It also considers the issue of lowering energy costs and reaction times. However, when a wireless sensor network is considered, the energy consumption issue still exists.

For the purpose of detecting IoT network attacks, the authors [32] have proposed a minimal security solution. This attack challenge technique makes use of an IoT processor. The recommended method guarantees the security of a response as well as a scenario-aware request service. However, the issue with security use is still there, as observed in IoT networks. duration of energy usage and improvement of services.

Lightweight ECC security has been recommended by the authors [33, 35, 36] for detecting IoT network authentication. In this attack challenge strategy, the ECC is used. The

recommended method guarantees the security of a response as well as a scenario-aware request service [37, 38]. However, the issue with security use is still there, as observed in IoT networks [39, 40].

## 2.1 Advantages of the proposed approaches over existing systems

- The increased processing costs of the mathematical model adversely affects the current optimisation techniques [1–3, 6–10]. The suggested approach preserves variety while speeding up search space convergence [41–43].
- The proposed DE algorithm may be used in IIoT-smart industrial during testing and validation.
- The sensors have low data transmission costs and malicious nodes since they are detecting the IIoT sensor network's services. A new artificial mutation operator for the DE algorithm has been developed to address the problem [44–46].

## 2.2 Notation & abbreviation

This section is consists of abbreviations & notations and description of differential evolutionary algorithm. Description of notations and abbreviations is presented in Table 1.

**Table 1** Description of Notations and Abbreviations

Notation	Description
DE	Differential Evolution
NP	Population Size
G	Number of Generation
Cr	Crossover Rate
$\delta_1$	Scale factor of mutation operator
D	Dimensions
<i>FunEvs</i>	Function Evaluation
<i>DonorVector</i>	Mutant Vector
<i>MaxFunEvs</i>	Number of Function Evaluation
<i>TargetVector</i>	Original Vector
$G(X, Y)$	Geographical area of smart agriculture
X	Number of request for sensor nodes
Y	Number of request for sensor nodes
Scenarios 1	(200 × 200): Simple Transmissions
Scenarios 2	(200 × 200): Congestion Transmissions
Scenarios 3	(200 × 200): Mixed Transmissions
<i>B_id</i>	Identification service provider
<i>B_Type</i>	Types of services of smart agriculture
AVL	The service ability

### 3 Internet of Things based industrial framework for QoS

#### 3.1 Architecture of IIoT

IIoT: The perception layer is collected for further processing via connection technologies including Wi-Fi, Infrared, ZigBee, Bluetooth, 4G/5G, etc. The collected and processed data is then passed on to the stage of processing that comes next. By using an optimisation approach and taking IIoT goal functions into consideration, the decision layer is in charge of selecting the data sensor source. And, the bottom layer's pre-processed data must be handled and managed by the cloud in order to increase the quality of the service. Approaches for data optimisation or cloud computing are used at this tier. These optimisation methods, which raise the quality of the security services that are requested and provided by the application/business layer, might be based on one or more objective functions. Using data analytics technologies [47], this layer is also in charge of supplying data in the form of graphs, business models, charts, etc. for use in corporate decision-making.

#### 3.2 Framework of communication between IIoT wireless sensor networks

An security architecture for IIoT wireless sensor networks is provided in this section. The analysis method for determining data transmission loss and malicious nodes in a wireless sensor network is from one node (sensor) [48] to another. The sensor nodes in this model are represented by a non-directed acyclic graph  $G(Q, R)$  [4, 21, 22], where  $Q$  stands for the sensor nodes and  $R$  stands for the connected sensor nodes in the IIoT network design. According to the network model, the energy (battery of sensor nodes) is used to send data requests and data responses (graph). As illustrated in Fig. 1, the graph

shows a significant number of sensors dispersed throughout a static and dynamic environment-based IIoT infrastructure. Fig. 1 represents the three scenarios such that simple transmission of data depicts the locations of several sensors that are linked to others in Fig. 1(a), congestion data transmission depicts the locations of several sensors that are linked to others in Fig. 1(b), mixed data transmission depicts the locations of several sensors that are linked to others in Fig. 1(c). The following equation is explained by the framework [3–7, 22]:

**(I) Cluster Sensor node:** Cluster sensors are advanced sensing systems that consist of multiple individual sensors working together in a coordinated manner. These sensors are designed to provide enhanced capabilities and improved performance compared to standalone sensors by combining their outputs and processing the data collectively [49–51]. The concept of cluster sensors is often employed in various applications where increased sensing capabilities are required. Cluster sensors offer redundancy by using multiple sensors to measure the same parameter. This redundancy increases the reliability of the sensor system, as any faulty sensor can be identified and compensated for by other functioning sensors within the cluster. The use of multiple sensors in a cluster improves the overall robustness of the system. If one sensor is affected by environmental factors or external interference, the other sensors can provide additional data to compensate for the error and maintain the accuracy of the measurements [52, 53]. The following formula is used to calculate the first objective(fun1) in terms of distance nodes. Equation 1:

$$\text{Dist}(Q_i^t, R_j^t) = \sqrt{(Q_i - Q_j)^2 + (R_i - R_j)^2} \quad (1)$$

Where  $Q_i^t$  represents an information request and  $R_i^t$  represents an information response, and sensor cost is determined using  $\text{Dist}(Q_i^t, R_j^t)$ .

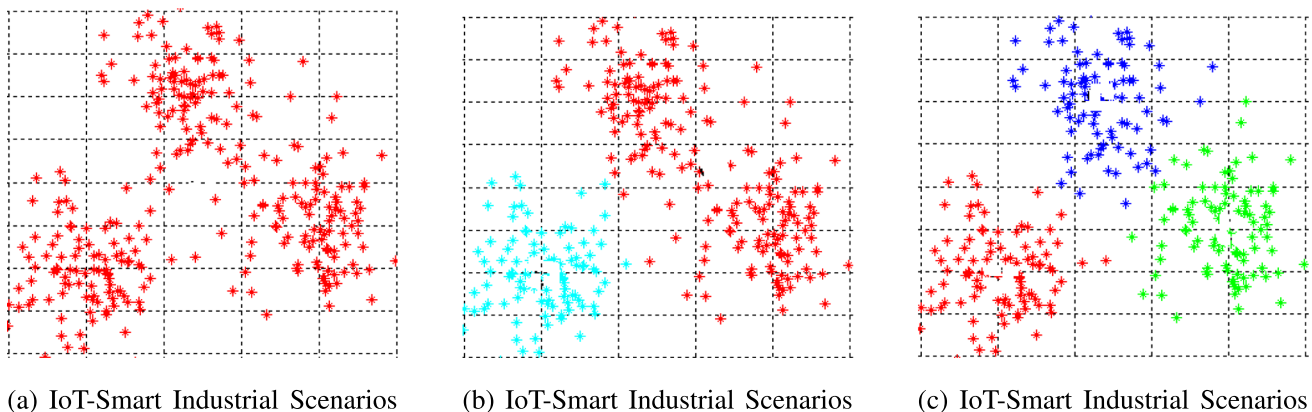


Fig. 1 Security Service of IoT-Smart Industrial Scenarios

### (II) Data transmission cost calculated on sensor nodes:

In terms of data communication per unit time nodes, the second goal (fun2) is computed using the formula Eq. 2:

$$SE_{i,j} = (EC_r + \text{Dist}(Q_i^t, R_j^t)^2) * RC_{i,j} \quad (2)$$

where,  $SE_{i,j}$  denoted of data communication per unit time between sensor node  $i$  and  $j$ ,  $RC_{i,j}$  denoted of rate of data communication between sensor node  $i$  and  $j$ ,  $EC_r$  denoted the consumed data energy transmitted and respond on sensor devices, and  $\text{Dist}(Q_i^t, R_j^t)$  denoted distance of sensor nodes in IIoT model.

### (III) Data transmission loss calculated on sensor nodes:

In the third objective(fun3) in terms of Spent time of sensor nodes is calculated by using the following formula Eq. 3:

$$SE_{i,j}^t = (SE_i + SE_j * \text{Dist}(Q_i^t, R_j^t)^2) * DS_{i,j} \quad (3)$$

Where,  $SE_{i,j}^t$  represent the spent time of transmit data between sensor node  $i$  and  $j$ ,  $DS_{i,j}$  denoted distance between sensors  $i$  and  $j$ ,  $\text{Dist}(Q_i^t, R_j^t)$  denoted distance of sensor nodes in IIoT model, and  $EC_i$  denoted the current energy of sensor device  $i$  and  $EC_j$  denoted the current energy of sensor device  $j$ .

## 3.3 Fitness function formulation

In this part, we analysed the optimal fitness function produced by secure fitness value as well as the proposed fitness function [54, 55]. We constructed the secure fitness function after first calculating the formulation of the fitness function.

### 3.3.1 Proposed the fitness function formulation

The fitness functions computed by Eqs. 1, 2, and 3 are non-contradictory in this section. As a result, using the sum of the weighted approach as given in Eq. 4, all of the objectives are turned into a single objective function.

$$fit_j = f_{v1} \times fun1 + f_{v2} \times fun2 + f_{v3} \times fun3 \quad (4)$$

Where  $fit_j$  denoted the proposed the fitness function. Furthermore, the weights for each of the objective functions are assigned using the values  $f_{v1}$ ,  $f_{v1}$ , and  $f_{v3}$ . For comparison with the IoT service framework model, the fitness function used genetic algorithms (GA), the Grey Wolf Optimization Algorithm (GWO), DE, and Particle Swarm Optimization (PSO) [56, 57].

### 3.3.2 Proposed the fitness function formulation

The functions formulation of detection of malicious nodes computed by original fitness function  $fit_i$ , which are given

by actual data from generated according to the IIoT as given in Eq. 5, all of the objectives are turned into a single objective function.

$$fit_i = \sum fit_i \quad (5)$$

The  $fit_i$  are assigned to each of the objective functions using the values of generated according to secure data transmission.

## 3.4 Function formulation: detection of malicious node

The functions formulation of detection of malicious nodes computed by original fitness function  $fit_i$ , which are given by actual data from generated according to the IIoT framework. We have proposed  $fit_j$  the sum of weighted approach as given in Eq. 6, all of the objectives are turned into a single objective function.

$$\text{MaliciousNodes} = \sum fit_i - \sum fit_j \quad (6)$$

The  $fit_i$  are assigned to each of the objective functions using the values of generated according to secure data transmission. Furthermore, the proposed fitness function  $fit_j$  by using in Eq. 4. For comparison of IIoT service framework model, the fitness function used Genetic Algorithm(GA), Grey Wolf Optimization Algorithm (GWO), DE, and Particle Swarm Optimization (PSO).

## 4 The proposed approach: differential evolution(De) algorithm using artificial adaption-based operators

The DE algorithm is a global optimization method that solves problems with and without constraints. However, to systematically incorporate advised artificial adaptation-based operators, the best population-based technique is used (AABO). This operator directs the solution toward a better solution while still remaining within the search space. In order to choose the best solution from the vast search space, the AABO operator supports the artificial adaptation technique. The mutation operator is used in this method to choose the best solution vector from the entire search space. The artificial adaptation vector is essential for increasing convergence speed while maintaining diversity. The choosing of the search location and the type of adaptability in the current environment determine the optimized solution. Our objective in this research is to improve the context for an artificial adaptive strategy. This is the rationale behind developing a workable global search space solution using autonomous



adaptation-based selection. The following is a step-by-step explanation of this selection strategy:

#### 4.1 Initialization

In this section, a random population is generated for the particular problem or application. This application considers randomly initialized population members with tuning parameter with respect to problem specification. This problem lies between the lower and upper bound values. This randomly generated population is used as base problem.

#### 4.2 Artificial Adaption-Based Operators(AABO)

In this sub section, designing and modifying the original mutation operator using DE algorithm. This updated operator improves the selection of best vector approach in standard DE algorithm. This research paper explores the concept of artificial adaption-based operators as a promising approach to enhance optimization algorithms. These operators aim to incorporate adaptive mechanisms inspired by natural phenomena, such as evolutionary processes and biological adaptation, into optimization frameworks. This process is represented by an expression in Eq. 7:

$$Aut = Aut_{randomvector} * (A_{i,d}^U - A_{i,d}^L) \quad (7)$$

Where,  $Aut$  denotes the feasible solution of current environment, and  $Aut_{randomvector}$  denotes the selected random best vector as per lower bound and upper bound constraint.

##### 4.2.1 Generation of New Donor Vector(DV)

Mutation operators play a crucial role in evolutionary algorithms by introducing diversity and enabling exploration of the search space. In recent years, the concept of donor vectors has emerged as an effective approach to enhance the mutation operator's performance. This research paper delves into the concept of donor vectors and their utilization in mutation operators for optimization algorithms. This vector provides the sufficient diversity from Eqs. 8, 9, and 10, we define the donor vector and the viable environment, respectively.

$$\vec{DV}_{i,G} = \vec{\alpha}_{r_1^i,G} + \delta_1 \cdot (\vec{\alpha}_{r_2^i,G} - \vec{\alpha}_{r_3^i,G}) \quad (8)$$

From Eq. 8, we used the standard DE optimization algorithm[1]. The proposed artificial adaption operator is responsible for generating new candidate solutions by perturbing the existing best pool populations. The mutation operator introduces diversity in the population, allowing exploration as well as exploitation of the search space. The proposed

mutation operator in DE is called “mutation to the best” in terms of generating donor vectors.

$$\vec{Av}_{i,G} = \vec{Aut}_{r_1^i,G} + \delta_1 \cdot (f\vec{v}_{1,r_2^i,G} - f\vec{v}_{2,r_3^i,G}) \quad (9)$$

$$\vec{Av}_{i,G} = \vec{Aut}_{r_1^i,G} + \delta_1 \cdot (f\vec{v}_{3,r_2^i,G} - f\vec{v}_{4,r_3^i,G}) \quad (10)$$

Where  $G$  stands for generation and  $\vec{Av}_{i,G}$  is a donor vector that employs the artificial adaptation vector for non-continuous search. The artificial adaptation-based vector, denoted as  $\vec{Aut}_{r_1^i,G}$ , is chosen based on the best artificial based fitness value. A mutant factor,  $\delta_1$  is a number chosen at artificial based random (AR) from according to the best pool such that  $AR(0,1)$ . This value improves the best possible search using the mutation operator's difference vector. The difference vector of the mutation strategy has represented by the following vectors:  $f\vec{v}_{1,r_2^i,G}$ ,  $f\vec{v}_{2,r_3^i,G}$ ,  $f\vec{v}_{3,r_2^i,G}$ , and  $f\vec{v}_{4,r_3^i,G}$ . Equations 9 and 10 mutation techniques combine to provide the donor vector enough variety and quicken convergence. After the mutation operator is applied, crossover and selection operations are typically used to produce the trial vector, which is compared against the original individual to determine if it should replace it in the population.

#### 4.3 Crossover strategy

The suggested method creates the trail vector using a conventional crossover operator. This operator's main focus is on parameter tinkering with regard to dynamically changed value. For estimation using the tuned trail vector, this value is between the ranges of (0, 1). This vector selects various values depending on the application.

#### 4.4 Selection strategy

Compare the fitness of the corresponding trial vector with the fitness of the original individual. If the fitness of the trial vector is better (lower in case of minimization problems or higher in case of maximization problems), replace the original individual with the trial vector in the next generation. If the fitness of the trial vector is worse, keep the original individual in the next generation. This selection strategy ensures that the best individuals (those with improved fitness) are always selected for the next generation. By doing so, the DE algorithm gradually converges towards better solutions over successive generations. The pseudo code of proposed algorithm is given in Algorithm 1.

The proposed Algorithm 1, is an amalgamation of DE and AABO. For validating the significance of results, the input parameters like dimension, control parameter, number of iterations and fitness functions are designed and adopted in line of meeting the stated objective.

**Algorithm 1** The proposed evolutionary algorithm**Result:** Write here the result

---

```

1 Input: (1)Control parameters of algorithm ;
2 (2) Search_space of D denoted for Dimension;
3 (3) Generate an initial population of candidate solutions. Each
  solution is represented as a vector of decision variables within
  the problem's search space;
4 (4)  $\delta_1 = \text{rand}/2$ , where rand value (0 to 1);
5 (5)  $Cr = \text{rand}(0,1)$ ;
6 (6) Population Size =  $100 \times D$ ;
7 (7) Fitness function design according to randomly adaption;
8 (8) Set  $i=0$ ,  $t=0$ .

```

---

```

9 Step 3;
10 while ( $t! = \text{Max}_T$ ) do
11   while ( $i! = n$ ) do
12     3.1 For each individual in the population, generate a
13       trial vector by applying the mutation operator;
14     3.2 The mutation operator perturbs the individual's
15       decision variables based on the best donor vector
16       (Eqs. 9 either 10);
17     3.3 The crossover combines the decision variables of
18       the trial vector with those of the target individual to
19       create a new candidate solution.;
20     3.4 Compare the fitness of each trial vector with the
21       fitness of its corresponding target individual. If the
22       trial vector's fitness is better, replace the target
23       individual with the trial vector in the next generation.;
24     3.5  $i=i+1$ ;
25   end while
26   3.10  $t=t+1$ ;
27 end while

```

---

**4.5 The proposed liot-evolutionary algorithm**

However, solutions to real-world application-based problems with evolutionary algorithms like DE, PSO, GWO, and GA Algorithm are bit complex. Here, an attempt has been made for designing an algorithm in simplified manner for an IoT application-based environment. Succeeding, the finest population-based methodology is adopted to systematically integrate recommended artificial adaption-based operators (AABO). This method includes the mutation operator for selecting the best solution vector from the global search space. The artificial adaption vector plays a vital role in escalating the convergence speed along with preserving the diversity. In this paper, our objective is to create a better environment for an artificial adaption-based selection of best optimum value of Quality of services in the WSN. This selection strategy step by step process is explained as follows as well as Algorithm 2:

- Set the population size, maximum number of generations, and other algorithm parameters. Initialize the communication and networking infrastructure for the IIoT system.
- Evaluate the fitness of each candidate solution based on the objectives and constraints of the IIoT problem. The

fitness evaluation may involve collecting data from IIoT devices, analyzing it, and quantifying the performance or quality metrics.

- Utilize the IIoT infrastructure to facilitate communication and information exchange among IIoT devices, sensors, and actuators. Exchange data, control signals, and feedback information to support collaborative optimization and coordination among devices.
- To evaluate our suggested approach to determine the optimal best value and identify malicious nodes, Addition we developed two novel fitness functions for IIoT-based scenario services.
- Check if the termination condition is met (e.g., maximum number of generations or satisfactory fitness level achieved). If the condition is met, proceed to the next step. Otherwise, go back to the Evolutionary Loop.
- Analyze the obtained solution to gain insights into the IIoT system's behavior, performance, or other relevant aspects such that minimises data loss during transmission and improves the process of detecting malicious nodes for the IIoT-smart framework.

**Algorithm 2** The proposed IIoT based evolutionary algorithm**Result:** Write here the result

---

```

1 Input: (1)  $fun_{obj}$ ,  $obj = 1, 2, \dots, n$ . Wireless Sensor Network
  based objective problem with  $obj$  is a objectives;
2 (2) Search_space of D ;
3 (3) Generate the request response data from scenarios 1, 2, and
  3 ;
4 (4) scenarios 1: Represent the data set of simple data set;
5 (5) scenarios 2: Represent the data set of insecure data set;
6 (6) scenarios 3: Represent the data set of mixed data set;
7 (7) Number of generation according to fitness functions of
  behaviour of data;
8 (8) Set  $i=0$ ,  $t=0$ .

```

---

```

9 Step 9;
10 while ( $t! = \text{Max}_T$ ) do
11   while ( $i! = n$ ) do
12     9.1 Generate the initial Population according to QoS
13       of WSN;
14     9.2 Apply mutation operator as mentioned the best
15       donor vector (Eqs. 9 either 10);
16     9.3 Apply Cr using the tuning parameter;
17     9.4 Apply selection best solutions according to
18       fitness;
19     9.5  $i=i+1$ ;
20   end while
21   9.6  $t=t+1$ ;
22 end while

```

---

Algorithm 2 is designed in view of applying the proposed approach for IIoT based WSN environment. it is been observed with set of experiments that objective of minimization in terms of energy consumption is achieved.

**Table 2** Control Parameters of Proposed Algorithm

Sr. No.	Parameter	Type
1	Donor vector	optimum value
2	Mutant vector [ $DV$ ]	best random vector( $fv$ ) of search space
3	Scale factor ( $\delta 1$ )	[0.12-2]
4	Crossover Rate (Cr)	[0.1-0.9]
5	Dimension(D)	3, 10, & 20
6	Function Evaluations	FunEvs
7	Search Space	[10,-10]
8	Population Size	25, 50, & 100

## 5 Result and analysis

In this section, the proposed approach is evaluated on an IIoT-based wireless sensor network for comparing the fitness function cost and find the malicious node. Furthermore, this approach also calculates the data transmission cost, and data transmission loss, as well as detection of malicious node according to generations.

### 5.1 Performance analysis with respect to IIoT based framework

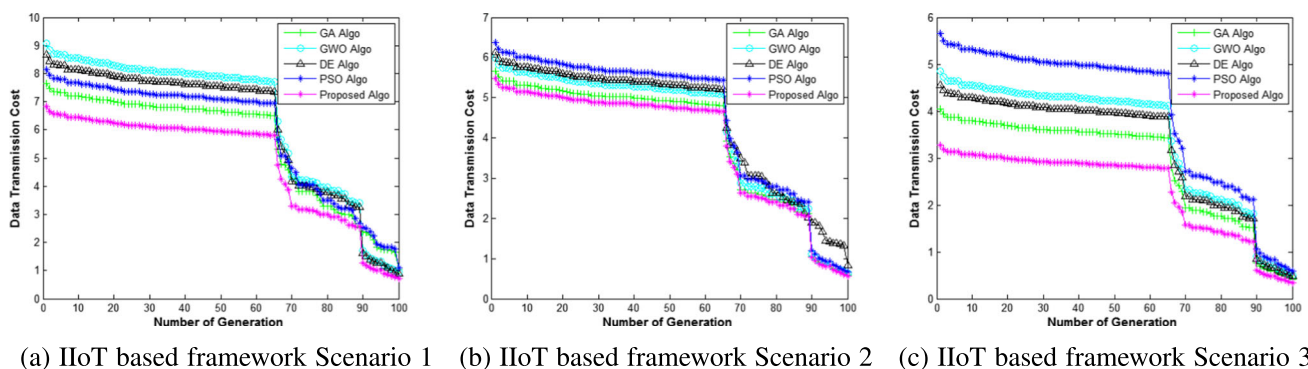
An Intel Core i7-8850H processor, 8 GB of RAM, and Windows 10 Pro 64 bit are used to achieve the research objective. We designed the minimization and maximization problem based on how it will actually be used. As a result, the suggested method is used in IIoT-based smart industry. Three scenarios from IIoT-based services are tested using this framework to validate our suggested methodology in this study. For an efficient service cost of WSN, we must optimise the various limitations. All of the criteria listed in Table 2 have been incorporated and fine-tuned for this research. Based on service demands and replies, a diverse range of services are

the focus of the IIoT concerns. The proposed method is used to three scenarios of IIoT services for fitness functions. The experimental findings of the suggested method are also contrasted with those of well-known algorithms like GA [33], GWO [34], PSO [25], and DE [2].

#### 5.1.1 Experimental setup of the IIoT based WSN framework

This subsection described the setup of an IoT framework ( $200 \times 200$ ) in Fig. 2, with 250 sensors distributed evenly, i.e., service requests, in this experimental configuration. In addition, based on request and response data from processes, people, and objects, we used 250 active sensors that are regarded as service providers. In a 25 by 25 matrix, we've chosen the experimental area. Scenario 1 in Fig. 1(a) is used to connect the smallest sensor nodes in an undirected network and provides a connection between objects (nodes). Scenario 2 in Fig. 1(b) is used to connect objects (nodes) in an undirected graph and provides the connection between them. In Fig. 1(c), scenario 3 is used to connect entire congested nodes and provides an undirected graph connection between objects (nodes). Additionally, the suggested approach generates a solution consisting of real values and array-encoded bits that specify the bits per second of the sensors. The three dimensions of prospective IoT service framework solutions were represented by the sensors.

The proposed algorithm is used to estimate the cost of service of the IIoT framework, such as data transmission cost, fitness cost, and malicious node cost. This framework is used by IIoT services, where we must optimise numerous restrictions for optimal malicious node prediction for diverse services. To keep the suggested algorithm's evolutionary process going, this study incorporates and tunes all of the control parameters listed in Tables 1 and 2. The proposed technique is tested using IoT with service. The suggested technique for comparing the fitness function from scenarios 1, 2, and 3 is tested on IIoT-based security.

**Fig. 2** Security Service of IIoT based framework Scenarios: Number of generations v/s Transmission Cost



## 5.2 Comparative analysis of data transmission cost from IIoT framework

In this section, the experimental results of the suggested method are compared with those obtained using well-known state-of-the-art algorithms like GA [33], GWO [34], PSO [25], and DE [2]. Applying each of these methods to scenarios 1, 2, and 3. In this subsection, the goal functions of various common algorithms are compared to the proposed method. As illustrated in Tables 3, 4, and 5, the suggested method analyses the rate of convergence and diversity such that data transmission costs from IIoT-based scenarios Fig. 2(a), (b), and (c) exhibit this method for various sensors in IIoT smart scenarios (1, 2, and 3). With well-distributed data transfer from an IIoT service framework, the suggested approach produces good results.

Illustration of Fig. 2: For the various scenarios depicted in Fig. 2(a), (b), and (c), the proposed algorithm achieves better maximizes in terms of data transmission (bits/seconds). According to the IIoT objective-based problem employed in Eq. 2, Fig. 2 illustrates the X-axis of the number of generations and the Y-axis of the data transmission cost. The proposed method is compared with well-known algorithms like GA [33], GWO [34], PSO [25], and DE [2], broadening the range of scenario-based services and accelerating their convergence.

## 5.3 Comparative analysis of data transmission lost from IIoT framework

In this part, the experimental outcomes of the proposed methodology are contrasted with those attained utilising well-known cutting-edge algorithms like GA [33], GWO [34], PSO [25], and DE [2]. Using each of these techniques for scenarios 1, 2, and 3. The aim functions of different popular algorithms are contrasted with the proposed methodology in this subsection. As illustrated in Tables 3, 4, and 5, the proposed method analyses the rate of convergence and diversity such that data transmission costs from IIoT-based scenarios Fig. 3(a), (b), and (c) exhibit this method for various sensors in IIoT smart scenarios (1, 2, and 3). With well-distributed data transfer from an IIoT service framework, the suggested approach produces good results. The proposed algorithm achieves better minimization in terms of data transmission (bits per second). According to the IIoT objective-based problem employed in Eq. 3, Fig. 3 illustrates the X-axis of the number of generations and the Y-axis of the data transmission lost. The proposed method is compared with well-known algorithms like GA [33], GWO [34], PSO [25], and DE [2], broadening the range of scenario-based services and accelerating their convergence.

## 5.4 IIoT framework of the fitness value (or cost) with standard evolutionary algorithms

The proposed algorithm achieves the minimum bit rate (i.e., transmission data loss and delay) and maximises the transmission data cost and coverage area of malicious nodes for the IIoT framework in fewer iterations, as shown in Tables 3, 4, and 5. This strategy, as illustrated in Fig. 4, maximizes fitness function usage for various sensors in IIoT scenarios. The proposed approach offers good results with a well-distributed delay fitness value from an IIoT service framework.

Figure 4 illustration: In terms of maximization fitness value from diverse IIoT scenarios 1, 2, and 3, the proposed algorithm produced a superior optimum value. This algorithm achieves various scenarios as shown in Figs. 4(a), (b), and 8(c). Figure 8, represents the X-axis of the number of generations and the Y-axis of the fitness value according to the IIoT framework objective-based problem used in Eq. 4. The proposed method broadens the range of scenario-based services and accelerates their convergence. Figure 4 represents the fitness function efficiency when tested on proposed and existing optimisation techniques. It has been observed that high efficiency was achieved in the proposed algorithm compared to other tested optimisation techniques.

## 5.5 Detection of malicious nodes from IIoT-service framework

In this paper, we propose a novel IIoT-Service framework for the detection of malicious nodes. The framework aims to enhance the security and reliability of IIoT systems by leveraging advanced detection techniques. By effectively identifying and isolating malicious nodes, the framework mitigates potential threats and ensures the proper functioning of IIoT networks. In the following sections, we present a comprehensive overview of the proposed framework, discuss the employed detection techniques, evaluate its performance through experiments, and provide insights into its potential impact on the field of IIoT security.

The proposed method of analysing the maximum coverage of malicious nodes from the IIoT framework from scenarios 1, 2, and 3 is described. The proposed algorithm chooses a superior optimum value for maximising the coverage rate from IIoT framework scenarios 1, 2, and 3, as shown in Fig. 5(a), (b), and (c). Figure 5, depicts a two-dimensional circle which denotes the different colours generated according to the data item that authenticates the data. But it is not complete authenticated data, which is mixed data. Therefore, it is necessary to find the malicious data or nodes, which represent the black circles. The proposed method produces

**Table 3** Data Loss of IIoT based framework Scenario 1

Sr No	No. of Generation	GA Algo		GWO Algo		DE Algo		PSO Algo		Proposed Algorithm	
		Best Mean Value	Worst Value	Best Mean Value	Worst Value	Best Mean Value	Worst Value	Best Mean Value	Worst Value	Best Mean Value	Worst Value
1	50	7.076682	10.47222	6.918012	9.36153	10.599156	12.407994	6.82281	9.488466	6.315066	8.441244
2	100	6.974994	10.32174	6.818604	9.22701	10.446852	12.229698	6.72477	9.352122	6.224322	8.319948
3	150	6.840748	10.12308	6.687368	9.04942	10.245784	11.994316	6.59534	9.172124	6.104524	8.159816
4	200	6.821347	10.09437	6.668402	9.023755	10.216726	11.960299	6.576635	9.146111	6.087211	8.136674
5	250	6.799047	10.06137	6.646602	8.994255	10.183326	11.921199	6.555135	9.116211	6.067311	8.110074
6	300	6.663017	9.86007	6.513622	8.814305	9.979586	11.682689	6.423985	8.933821	5.945921	7.947814
7	350	6.194494	9.16674	6.055604	8.19451	9.277852	10.861198	5.97227	8.305622	5.527822	7.388948
8	400	5.947187	8.80077	5.813842	7.867355	8.907446	10.427579	5.733835	7.974031	5.307131	7.093954
9	450	5.6900457	8.420247	5.5624662	7.5271905	8.5223106	9.9767169	5.4859185	7.6292541	5.0776641	6.7872294
10	500	5.493382	8.12922	5.370212	7.26703	8.227756	9.631894	5.29631	7.365566	4.902166	6.552644
11	550	5.281532	7.81572	5.163112	6.98678	7.910456	9.260444	5.09206	7.081516	4.713116	6.299944
12	600	5.052511	7.47681	4.939226	6.683815	7.567438	8.858887	4.871255	6.774443	4.508743	6.026762
13	650	4.845567	7.17057	4.736922	6.410055	7.257486	8.496039	4.671735	6.496971	4.324071	5.779914
14	700	4.658247	6.89337	4.553802	6.162255	6.976926	8.167599	4.491135	6.245811	4.156911	5.556474
15	750	4.407595	6.52245	4.30877	5.830675	6.60151	7.728115	4.249475	5.909735	3.933235	5.25749
16	800	4.044328	5.98488	3.953648	5.35012	6.057424	7.091176	3.89924	5.422664	3.609064	4.824176
17	850	3.610147	5.34237	3.529202	4.775755	5.407126	6.329899	3.480635	4.840511	3.221611	4.306274
18	900	2.9242213	4.327323	2.8586558	3.8683645	4.379754	5.1272221	2.8193165	3.9208169	2.6095069	3.4880846
19	950	2.3094326	3.417546	2.2576516	3.055079	3.4589708	4.0492742	2.226583	3.0965038	2.0608838	2.7547492
20	1000	2.002094	2.96274	1.957204	2.64851	2.998652	3.510398	1.93027	2.684422	1.786622	2.388148

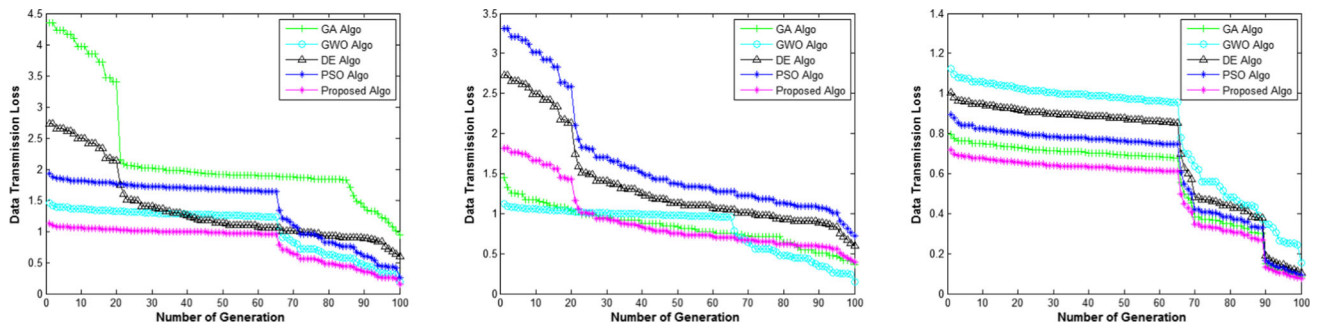
**Table 4** Data Loss of IIoT based framework Scenario 2

Sr No	No. of Generation	GA Algo		GWO Algo		DE Algo		PSO Algo		Proposed Algorithm	
		Best Mean Value	Worst Value	Best Mean Value	Worst Value	Best Mean Value	Worst Value	Best Mean Value	Worst Value	Best Mean Value	Worst Value
1	50	10.488582	15.52122	10.253412	13.87503	15.709356	18.390294	10.11231	14.063166	9.359766	12.511044
2	100	7.710894	11.41074	7.538004	10.20051	11.549052	13.519998	7.43427	10.338822	6.881022	9.197748
3	150	6.907648	10.22208	6.752768	9.13792	10.345984	12.111616	6.65984	9.261824	6.164224	8.239616
4	200	6.754447	9.99537	6.603002	8.935255	10.116526	11.842999	6.512135	9.056411	6.027511	8.056874
5	250	6.732147	9.96237	6.581202	8.905755	10.083126	11.803899	6.490635	9.026511	6.007611	8.030274
6	300	6.484617	9.59607	6.339222	8.578305	9.712386	11.369889	6.251985	8.694621	5.786721	7.735014
7	350	5.993794	8.86974	5.859404	7.92901	8.977252	10.509298	5.77877	8.036522	5.348722	7.149548
8	400	5.969487	8.83377	5.835642	7.896855	8.940846	10.466679	5.755335	8.003931	5.327031	7.120554
9	450	5.912845	8.74995	5.78027	7.821925	8.85601	10.367365	5.700725	7.927985	5.276485	7.05299
10	500	5.827882	8.62422	5.697212	7.70953	8.728756	10.218394	5.61881	7.814066	5.200666	6.951644
11	550	5.727532	8.47572	5.599112	7.57678	8.578456	10.042444	5.52206	7.679516	5.111116	6.831944
12	600	5.610011	8.30181	5.484226	7.421315	8.402438	9.836387	5.408755	7.521943	5.006243	6.691762
13	650	5.291567	7.83057	5.172922	7.000055	7.925486	9.278039	5.101735	7.094971	4.722071	6.311914
14	700	4.881247	7.22337	4.771802	6.457255	7.310926	8.558599	4.706135	6.544811	4.355911	5.822474
15	750	4.652895	6.88545	4.54857	6.155175	6.96891	8.158215	4.485975	6.238635	4.152135	5.55009
16	800	4.222728	6.24888	4.128048	5.58612	6.324624	7.403976	4.07124	5.661864	3.768264	5.036976
17	850	3.833147	5.67237	3.747202	5.070755	5.741126	6.720899	3.695635	5.139511	3.420611	4.572274
18	900	3.1472213	4.657323	3.0766558	4.1633645	4.7137754	5.5182221	3.0343165	4.2198169	2.8085069	3.7540846
19	950	2.4432326	3.615546	2.3884516	3.232079	3.6593708	4.2838742	2.355583	3.2759038	2.1802838	2.9143492
20	1000	2.225094	3.29274	2.175204	2.94351	3.332652	3.901398	2.14527	2.983422	1.985622	2.654148

**Table 5** Data Loss of IIoT based framework Scenario 3

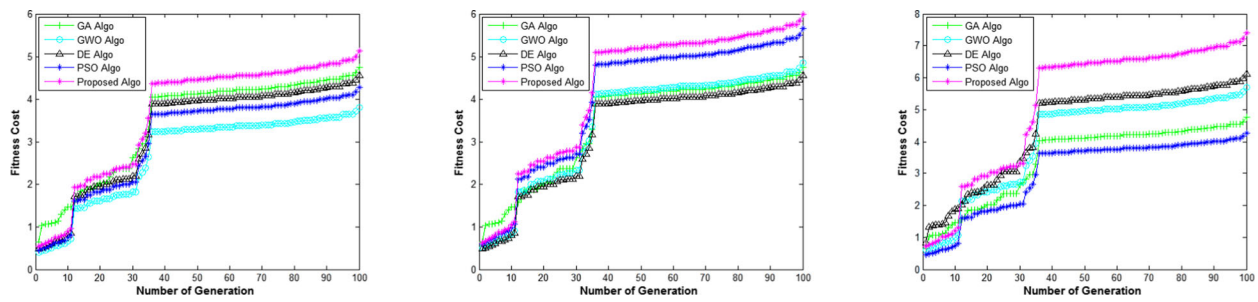
Sr No	No. of Generation	GA Algo		GWO Algo		DE Algo		PSO Algo		Proposed Algorithm	
		Best Value	Mean Value	Worst Value	Best Value	Mean Value	Worst Value	Best Value	Mean Value	Worst Value	Best Value
1	50	3.798582	5.62122	5.02503	5.689356	3.713412	5.02503	3.66231	6.660294	7.682334	3.389766
2	100	3.250894	4.81074	4.30051	4.869052	3.178004	4.30051	3.13427	5.699998	6.574678	2.901022
3	150	3.228148	4.77708	4.27042	4.834984	3.155768	4.27042	3.11234	5.660116	6.528676	2.880724
4	200	3.208747	4.74837	4.244755	4.805926	3.136802	4.244755	3.093635	5.626099	6.489439	2.863411
5	250	3.186447	4.71537	4.215255	4.772526	3.115002	4.215255	3.072135	5.586999	6.444339	2.843511
6	300	3.184217	4.71207	4.212305	4.769186	3.112822	4.212305	3.069985	5.583089	6.439829	2.841521
7	350	3.161694	4.67874	4.18251	4.735452	3.090804	4.18251	3.04827	5.543598	6.394278	2.821422
8	400	3.137387	4.64277	4.150355	4.699046	3.067042	4.150355	3.024835	5.500979	6.345119	2.799731
9	450	3.103045	4.59195	4.104925	4.64761	3.03347	4.104925	2.991725	5.440765	6.275665	2.769085
10	500	3.018082	4.46622	3.99253	4.520356	2.950412	3.99253	2.90981	5.291794	6.103834	2.693266
11	550	2.984632	4.41672	3.94828	4.470256	2.917712	3.94828	2.87756	5.233144	6.036184	2.663416
12	600	2.957203	4.37613	3.911995	4.429174	2.890898	3.911995	2.851115	5.185051	5.980711	2.638939
13	650	2.838567	4.20057	3.755055	4.251486	2.774922	3.755055	2.736735	4.977039	5.740779	2.533071
14	700	2.874247	4.25337	3.802255	4.304926	2.809802	3.802255	2.771135	5.039599	5.812939	2.564911
15	750	2.645895	3.91545	3.500175	3.96291	2.58657	3.500175	2.550975	4.639215	5.351115	2.361135
16	800	3.152328	4.66488	4.17012	4.721424	3.081648	4.17012	3.03924	5.527176	6.375336	2.813064
17	850	2.472847	3.65937	3.271255	3.703726	2.417402	3.271255	2.384135	4.335799	5.001139	2.206711
18	900	2.2552213	3.337323	2.2046558	3.377754	2.2046558	2.9833645	2.1743165	3.9542221	4.5610081	2.0125069
19	950	1.9972326	2.955546	1.9524516	2.9913708	1.9524516	2.642079	1.925583	3.5018742	4.0392462	1.7822838
20	1000	1.712194	2.53374	1.673804	2.564452	1.673804	2.26501	1.65077	3.002098	3.462778	1.527922
											2.042348





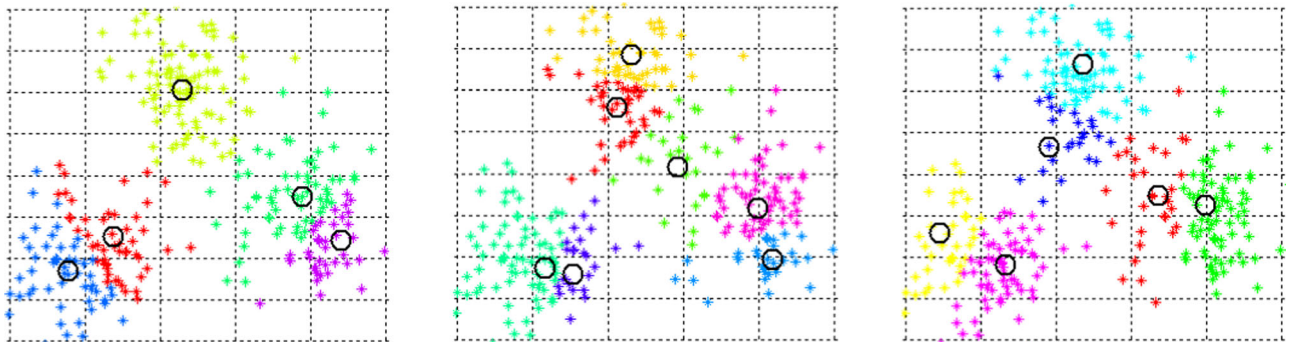
(a) IIoT based framework Scenario 1 (b) IIoT based framework Scenario 2 (c) IIoT based framework Scenario 3

**Fig. 3** Service security loss of IIoT based framework Scenarios: Number of generations v/s Transmission data loss



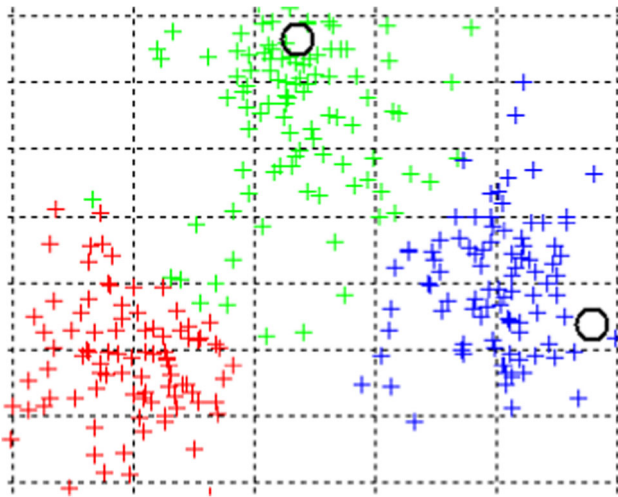
(a) IIoT based framework Scenario 1 (b) IIoT based framework Scenario 2 (c) IIoT based framework Scenario 3

**Fig. 4** IIoT based framework Scenarios: Number of generations v/s Fitness Cost



(a) IIoT based framework Scenario 1 (b) IIoT based framework Scenario 2 (c) IIoT based framework Scenario 3

**Fig. 5** Security Coverage Malicious Nodes of IIoT based framework Scenarios

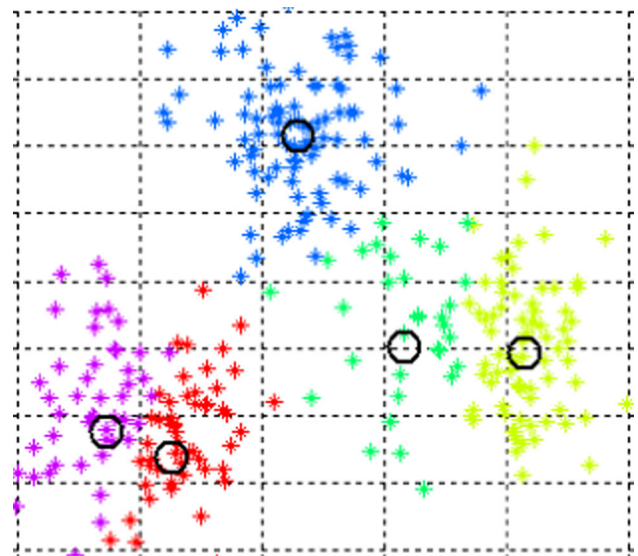


**Fig. 6** Genetic Algorithm: Detection of Malicious Nodes from the IIoT Framework

good results with well-distributed coverage for malicious nodes in IIoT service framework scenarios. In scenarios 1, 2, and 3, the proposed method detects five malicious nodes, five nodes, and six malicious nodes, respectively.

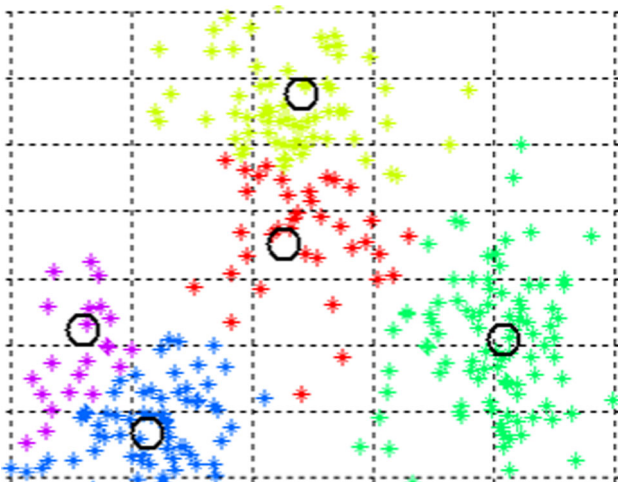
### 5.6 Detection of malicious nodes: the proposed algorithm comparing with other state-of-the-art algorithms

In this paper, we propose a novel algorithm for the detection of malicious nodes and compare its performance with other state-of-the-art algorithms. By analysing network traffic patterns, abnormal behaviour, and other relevant parameters, our algorithm can accurately differentiate between legitimate and malicious nodes. To evaluate the effectiveness of

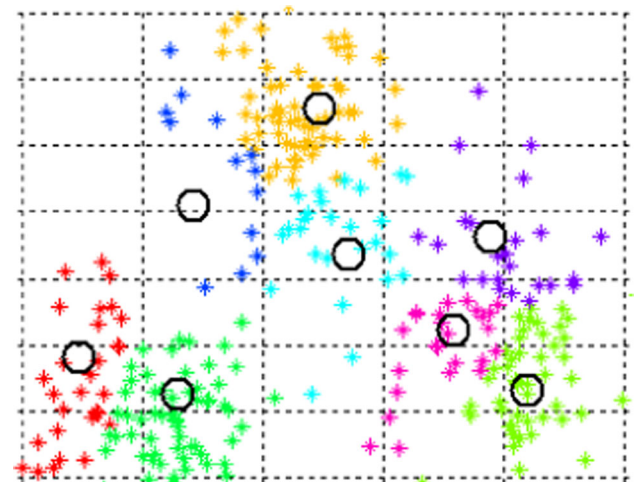


**Fig. 8** DE Algorithm: Detection of Malicious Nodes from the IIoT Framework

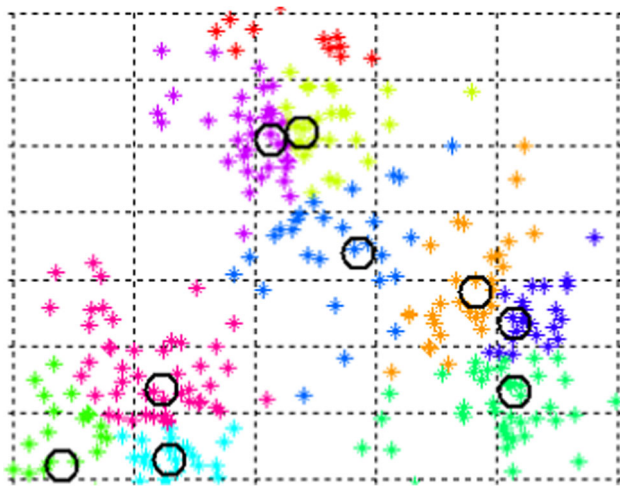
our proposed algorithm, we conduct comprehensive experiments using real-world datasets and compare its performance with several widely used algorithms in the field. The evaluation metrics include detection accuracy, false positive rate, false negative rate, and computational efficiency. The results demonstrate that our algorithm outperforms the existing state-of-the-art algorithms. Our proposed algorithm in detecting malicious nodes in scenario 3, depicted in Fig. 10. This algorithm finds the nine malicious nodes. Similarly, the GA algorithm finds the two malicious nodes depicted in Fig. 6; the GWO algorithm finds the five malicious nodes in given Fig. 7; the DE algorithm finds the five malicious nodes in given Fig. 8; and the PSO algorithm finds the eight malicious nodes in given Figs. 9 and 10. The proposed method is



**Fig. 7** GWO Algorithm: Detection of Malicious Nodes from the IIoT Framework



**Fig. 9** PSO Algorithm: Detection of Malicious Nodes from the IIoT Framework



**Fig. 10** The proposed Algorithm: Detection of Malicious Nodes from the IIoT Framework

compared with well-known algorithms like PSO [25], GA-III [33], WOA [28], and FFA [34], broadening the range of scenario-based services and accelerating their convergence.

## 6 Conclusion and future research direction

This article suggests using a differential evolutionary algorithm with artificial adaptation. It maintains diversity while quickening the global environment's or search space's convergence. As a result, IIoT-smart applications can use the proposed approach. A novel fitness function made up of data transmission cost, coverage rate, and data transmission loss is designed in the suggested technique in accordance with the IIoT-smart framework. The fitness function of the suggested algorithm is to guide the best optimum solutions for the IIoT-smart framework. The suggested approach for making the smart IIOT framework more effective and secure is to enhance the real-time monitoring systems of the scenarios in terms of the detection of malicious nodes. The suggested approach decreases the amount of data that is lost during transmission and makes it simpler for the IIoT-smart framework to identify malicious nodes in fewer iterations, as demonstrated in the result analysis section. The suggested approach can therefore be utilised in the future to address a range of NP-Complete issues.

**Author Contributions** Shailendra Pratap Singh wrote the paper, Gaurav Dhiman simulated the work, Wattana Viriyasitavat supervised the work, S. Vimal proof read the work, Ketan Kotecha supervised the work, Venkatesan Rajinikanth simulated the work.

## References

1. Rainer S, Kenneth P (1995) "Differential Evolution -A Simple and Efficient Adaptive Scheme for Global Optimization Over Continuous Spaces", International Computer Science Institute. Berkeley, CA, Berkeley
2. Nadimi-Shahraki MH, Zamani H (2022) "DMDE: Diversity-maintained multi-trial vector differential evolution algorithm for non-decomposition large-scale global optimization." *Expert Syst Appl* 198
3. Sheng M, Chen S, Liu W, Mao J, Liu X (2022) A differential evolution with adaptive neighborhood mutation and local search for multi-modal optimization. *Neurocomputing* 489:309–322
4. Fang SS, Chai ZY, Li YL (2021) Dynamic multi-objective evolutionary algorithm for IoT services. *Appl Intell* 51:1177–1200
5. Singh SP, Kumar A (2017) Homeostasis Mutation Based Differential Evolution Algorithm. *J Intell Fuzzy Syst* 32(5):3525–3537
6. Chen X, Du W, Qian F (2014) Multi-objective differential evolution with ranking-based mutation operator and its application in chemical process optimization. *Chemometr Intell Lab Syst* 136(2014):85–96
7. Wang P, Xue B, Liang J, Zhang M (2022) "Differential Evolution Based Feature Selection: A Niching-based Multi-objective Approach." *IEEE Trans Evol Comput*
8. Meng Z, Yang C (2022) Two-stage differential evolution with novel parameter control. *Inf Sci* 596:321–342
9. Singh SP, Kumar A (2017) Pareto Based Differential Evolution with Homeostasis Based Mutation. *J Intell Fuzzy Syst* 32(5):3245–3257
10. Hu Z, Su Q, Yang X, Xiong Z (2016) Not guaranteeing convergence of differential evolution on a class of multimodal functions. *Appl Soft Comput* 41:479–487
11. Pham QV, Mirjalili S, Kumar N, Alazab M, Hwang WJ (2020) "Whale Optimization Algorithm With Applications to Resource Allocation in Wireless Networks." *IEEE Trans Veh Technol*
12. Singh SP (2021) Improved based Differential Evolution Algorithm using New Environment Adaption Operator. *J Inst Eng India Ser B*. <https://doi.org/10.1007/s40031-021-00645-y>
13. Khanouche ME, Gadouche H, Farah Z (2020) Tari A "Flexible, "QoS-aware services composition for service computing environments". *Comput Netw* 166:106982
14. Chowdhury A, Raut SA (2018) A survey study on Internet of things resource management. *J Netw Comput Appl* 120:42–60
15. Wan J, Chen B, Imran M, Tao F, Li D, Liu C, Ahmad S (2018) Toward dynamic resources management for IoT-based manufacturing. *IEEE Commun Mag* 56(2):52–59
16. Wu D, Zhang Z, Wu S et al (2018) "Biologically inspired resource allocation for network slices in 5G-enabled internet of things." *IEEE Internet Things J* 6(6):9266–9279
17. Li G, Wu J, Li J, Wang K, Ye T (2018) Service popularity-based smart resources partitioning for fog computing-enabled industrial Internet of things. *IEEE Trans Ind Inform* 14(10):4702–4711
18. Qiu T, Zheng K, Han M et al (2017) A data-emergency-aware scheduling scheme for internet of things in smart cities. *IEEE Transactions on Industrial Informatics* 14(5):2042–2051
19. El-Shorbagy MA, Elhoseny M, Hassanien AE et al (2019) A novel PSO algorithm for dynamic wireless sensor network multiobjective optimization problem. *Trans Emerg Telecommun Technol* 30(11):3523
20. Tan S, Guerrero JM, Xie P, Han R, Vasquez JC (2020) Brief Survey on Attack Detection Methods for Cyber-Physical Systems. *IEEE Syst J* 14(4):5329–5339. <https://doi.org/10.1109/JSYST.2020.2991258>
21. Saravanan M, Madheswaran M (2014) A Hybrid Optimized Weighted Minimum Spanning Tree for the Shortest Intrapath Selection in Wireless Sensor Network. *Math Probl Eng* 2014:1–8
22. Langley DJ, van Doorn J, Ng ICL, Stieglitz S, Lazovik A, Boonstra A (2021) The Internet of Everything: Smart things and their impact on business models. *J Bus Res* 122:853–863




23. Singh SP, Singh, VP, Mehta AK (2018) 'Differential evolution using homeostasis adaption based mutation operator and its application for software cost estimation'. *J King Saud Uni-Comput Inf Sci*
24. Paul S, Ding F, Utkarsh K, Liu W, O'Malley MJ, Barnett J, (2022) On Vulnerability and Resilience of Cyber-Physical Power Systems: A Review. *IEEE Syst J* 16(2):2367–2378. <https://doi.org/10.1109/JSYST.2021.3123904>
25. Khalid QS, Azim S, Abas M, Babar AR, Ahmad I (2021) Modified particle swarm algorithm for scheduling agricultural products. *Eng Sci Technol Int J* 24(3):818–828
26. Quy VK, Hau NV, Anh DV, Quy NM, Ban NT, Lanza S, Randazzo G, Muzirafuti A (2022) "IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges." *Appl Sci*
27. Huang M, Zhai Q, Chen Y, Feng S, Shu F (2021) Multi-Objective Whale Optimization Algorithm for Computation Offloading Optimization in Mobile Edge Computing. *Sensor* 21:2628
28. El-Shorbagy MA, El-Refaey AM (2022) A hybrid genetic-firefly algorithm for engineering design problems. *J Comput Des Eng* 9(2):706–730
29. Rikalovic A, Suzic N, Bajic B, Piuri V (2022) Industry 4.0 Implementation Challenges and Opportunities: A Technological Perspective. *IEEE Syst J* 16(2):2797–2810. <https://doi.org/10.1109/JSYST.2021.3101673>
30. Agyekum KOBO, Xia Q, Sifah EB, Cobblah CNA, Xia H, Gao J (2022) A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. *IEEE Systems Journal* 16(1):1685–1696. <https://doi.org/10.1109/JSYST.2021.3076759>
31. Kumar R, Swarnkar M, Singal G, Kumar N (2022) IoT Network Traffic Classification Using Machine Learning Algorithms: An Experimental Analysis. *IEEE Internet Things J* 9(2):989–1008. <https://doi.org/10.1109/JIOT.2021.3121517>
32. Aman MN, Javaid U, Sikdar B (2022) IoT-Proctor: A Secure and Lightweight Device Patching Framework for Mitigating Malware Spread in IoT Networks. *IEEE Syst J* 16(3):3468–3479. <https://doi.org/10.1109/JSYST.2021.3070404>
33. Hammi B, Fayad A, Khatoun R, Zeadally S, Begriche Y (2020) A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT). *IEEE Syst J* 14(3):3440–3450. <https://doi.org/10.1109/JSYST.2020.2970167>
34. Kamalova A, Navruzov S, Qian D, Lee SG (2019) "Multi-Robot Exploration Based on Multi-Objective Grey Wolf Optimizer." *Appl Sci* 9(14). <https://doi.org/10.3390/app9142931>
35. Abdellatif H, Khalil-Hani M, Shaikh-Husin N, Ayat SO (2022) Accurate and compact convolutional neural network based on stochastic computing. *Neurocomputing* 471:31–47
36. Shen D, Saab SS (2021) Noisy output based direct learning tracking control with markov nonuniform trial lengths using adaptive gains. *IEEE Trans Autom Control*
37. Sayour MH, Kozhaya SE (2022) Saab SS (2022) Autonomous Robotic Manipulation: Real-Time. Deep-Learning Approach for Grasping of Unknown Object. *J Robot*
38. Shen D, Huo N, Saab SS (2021) A Probabilistically Quantized Learning Control Framework for Networked Linear Systems. *IEEE Trans Neural Netw Learn Syst*
39. Saab SS, Jaafar RH (2021) A proportional-derivative-double derivative controller for robot manipulators. *Int J Control* 94(5):1273–1285
40. Saab SS, Shen D, Orabi M, Kors D, Jaafar RH (2021) Iterative learning control: practical implementation and automation. *IEEE Trans Ind Electron* 69(2):1858–1866
41. Hammoud A, Otrouk H, Mourad A, Dziong Z (2022) On demand fog federations for horizontal federated learning in IoV. *IEEE Trans Netw Serv Manag*
42. Helwan A, Ma'aitah MKS, Uzelaltinbulat S, Altobal MZ, Darwish M (2021) Gaze Prediction Based on Convolutional Neural Network. In *International Conference on Emerging Technologies and Intelligent Systems* (pp. 215–224). Springer, Cham
43. Gerges F, Shih F, Azar D (2021) Automated Diagnosis of Acne and Rosacea using Convolution Neural Networks. In *2021 4th International Conference on Artificial Intelligence and Pattern Recognition* (pp. 607–613)
44. Abbas N, Nasser Y, Shehab M, Sharafeddine S (2021) Attack-Specific Feature Selection for Anomaly Detection in Software-Defined Networks. In *2021 3rd IEEE Middle East and North Africa COMMUNICATIONS Conference (MENACOMM)* (pp. 142–146). IEEE
45. Tarhini A, Harfouche A, De Marco M (2022) Artificial intelligence-based digital transformation for sustainable societies: The prevailing effect of COVID-19 crises. *Pac Asia J Assoc Inf Syst* 14(2):1
46. Tarhini A, Danach K, Harfouche A (2020) Swarm intelligence-based hyper-heuristic for the vehicle routing problem with prioritized customers. *Ann Oper Res* 1–22
47. Hammoud A, Otrouk H, Mourad A, Dziong Z (2021) Stable federated fog formation: An evolutionary game theoretical approach. *Future Gener Comput Syst* 124:21–32
48. Sorkhoh I, Assi C, Ebrahimi D, Sharafeddine S (2021) Optimizing Information Freshness for MEC-Enabled Cooperative Autonomous Driving. *IEEE Trans Intell Transp Syst*
49. Chamra A, Harmanani H (2020) A smart green house control and management system using iot. In *17th International Conference on Information Technology-New Generations (ITNG 2020)* (pp. 641–646). Springer, Cham
50. Zouein PP, Kattan S (2022) An improved construction approach using ant colony optimization for solving the dynamic facility layout problem. *J Oper Res Soc* 73(7):1517–1531
51. Sami H, Mourad A, Otrouk H, Bentahar J (2021) Demand-driven deep reinforcement learning for scalable fog and service placement. *IEEE Trans Serv Comput* 15(5):2671–2684
52. Arnaout JP, ElKhouri C, Karayaz G (2020) Solving the multiple level warehouse layout problem using ant colony optimization. *Oper Res* 20:473–490
53. Haddad BM, Dodge SF, Karam LJ, Patel NS, Braun MW (2020) Locally adaptive statistical background modeling with deep learning-based false positive rejection for defect detection in semiconductor units. *IEEE Trans Semicond Manuf* 33(3):357–372
54. Samir M, Assi C, Sharafeddine S, Ebrahimi D, Ghayeb A (2020) Age of information aware trajectory planning of UAVs in intelligent transportation systems: A deep learning approach. *IEEE Trans Veh Technol* 69(11):12382–12395
55. Mourad A, Tout H, Wahab OA, Otrouk H, Dbouk T (2020) Ad hoc vehicular fog enabling cooperative low-latency intrusion detection. *IEEE Internet Things J* 8(2):829–843
56. AbdulRahman S, Tout H, Mourad A, Talhi C (2020) FedMCCS: Multicriteria client selection model for optimal IoT federated learning. *IEEE Internet Things J* 8(6):4723–4735
57. AbdulRahman S, Tout H, Ould-Slimane H, Mourad A, Talhi C, Guizani M (2020) A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet Things J* 8(7):5476–5497

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



## Authors and Affiliations

Shailendra Pratap Singh<sup>1</sup> · Giuseppe Piras<sup>2</sup> · Wattana Viriyasitavat<sup>3</sup> · Elham Kariri<sup>4</sup> · Kusum Yadav<sup>5</sup> · Gaurav Dhiman<sup>6,7,8,9,10</sup>  · S Vimal<sup>11</sup> · Surbhi B. Khan<sup>12</sup>

Shailendra Pratap Singh  
shail2007singh@gmail.com

Giuseppe Piras  
giuseppe.Piras@uniroma1.it

Wattana Viriyasitavat  
hardgolf@gmail.com

Elham Kariri  
e.kariri@psau.edu.sa

Kusum Yadav  
kusumasyadav0@gmail.com

S Vimal  
svimalphd@gmail.com

Surbhi B. Khan  
s.khan138@salford.ac.uk

<sup>1</sup> SCSE, Bennett University, Greater Noida, India

<sup>2</sup> Ministero dell'Istruzione, dell'Università e della Ricerca, Italia, Sapienza University of Rome, Rome, Italy

<sup>3</sup> Department of Statistics, Chulalongkorn Business School, Faculty of Commerce and Accountancy, Bangkok, Thailand

<sup>4</sup> College of Computer Science and Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

<sup>5</sup> College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia

<sup>6</sup> Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon

<sup>7</sup> University Centre for Research and Development, Department of Computer Science and Engineering, Chandigarh University, Gharuan, 140413 Mohali, India

<sup>8</sup> Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248002, India

<sup>9</sup> Division of Research and Development, Lovely Professional University, Phagwara, India

<sup>10</sup> Department of Computer Science, Government Bikram College of Commerce, Patiala, India

<sup>11</sup> Department of Artificial Intelligence and Data Science, Ramco Institute of Technology, Rajapalayam, Tamilnadu, India

<sup>12</sup> School of Science Engineering and Environment, University of Salford, Salford, UK