Intelligent Multimedia Processing & Communication Systems Journal

IMPCSJ

J IMPCS (2025) 19: 67-78
DOI 10.71856/IMPCS.2025.1209464

Research Paper

An Optimized Intrusion Detection System Framework for Internet of Things Networks: Integrating Arctic Puffin Optimization and RNN

Mohammad Arefi[1], Parisa Rahmani[2*], Zoleikha Jahanbakhsh Naghadeh[3], Mahdieh Rahmani[4]

1. Department of Computer Engineering, ST.C., Islamic Azad University, Tehran, Iran.
2. Department of Computer Engineering, Par.C., Islamic Azad University, Tehran, Iran. **Corresponding Author*, Prahmani@pardisiau.ac.ir
3. Department of Computer Engineering, ST.C., Islamic Azad University, Tehran, Iran.
4. Department of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran.

Article Info

Article history:
Received: 16 Jan 2025
Accepted: 27 Feb 2025
DOR:

Keywords:
Intrusion Detection System,
IoT,
Machine Learning Algorithm,
Metaheuristic Algorithms
Network Security.

ABSTRACT

Over the past few years, significant research has been conducted on the Internet of Things (IoT), with a major challenge being network security and penetration. Security solutions require careful planning and vigilance to safeguard system security and privacy. In this paper, we propose a new hybrid Intrusion Detection System (IDS) based on machine learning and metaheuristic algorithms called IDS-RNNAPO, which has 3 stages: (1) Pre-Processing, (2) Feature Selection, and (3) Attack Detection. In the pre-processing stage, including Cleaning, Visualization, Feature Engineering, and Vectorization. Intrusion Detection Systems (IDS) form a transitional security component of networks that monitor malicious activities within networks. In the feature selection stage, Arctic puffin Optimization (APO) is used, In the attack detection stage, a modified Random Neural Network (RNN) is used, the proposed method is evaluated using the DS2OS dataset. The results have shown that The proposed approach in these experiments through a multiple learning model resulted in an improvement in accuracy to 99.62%.

I. Introduction

The Internet of Things (IoT) is a network composed of devices equipped with specialized sensors for detecting and monitoring areas, and transmitting collected data to end users. The IoT is widely used in many scenarios, such as COVID-19, healthcare, environmental monitoring, smart buildings, and more. According to Gartner, the global IoT market was reported to comprise nearly 6 billion devices in 2020. McKinsey estimates that by 2025, IoT will be worth around 11 trillion dollars. Additionally, the rise of 6G wireless communications and mobile edge computing can support the expansion of IoT devices **[1]**. Figure 1 shows how the detection process works in IDS. The merging of sensors and wireless communication has facilitated the expansion of the Internet of Things. Wireless sensor nodes play a crucial role in the structure of IoT networks**[2]**.

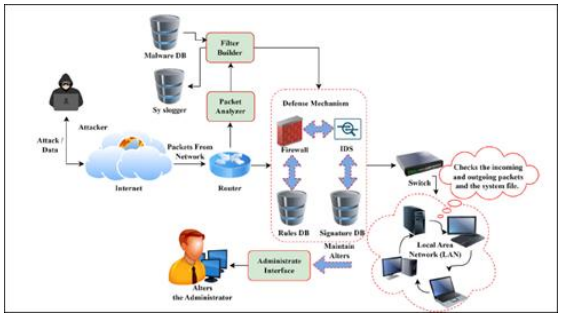

Fig **1:** The process of detecting attacks in IDS **[2]**

Enhancing network efficiency and defending against attacks are crucial challenges in IoT networks. The efficiency of the entire system can be compromised as these attacks can damage or weaken the transmitted packets **[3,4]**. To achieve complete security in the IoT network in today's world, in addition to attack prevention equipment, systems called Intrusion Detection Systems (IDS) are required to detect intrusions if an intruder bypasses security equipment and enters the network, recognize it, and think of a solution to deal with it, addressing these issues requires very scalable solutions **[5]**. An Intrusion Detection System is a cybersecurity approach that watches and analyzes network traffic to prevent and identify potential malicious attacks. A cyberattack is infiltrating the Internet of Things, as depicted in Figure 2. Therefore, effectively dealing with cyber threats has become a primary focus **[6]**.

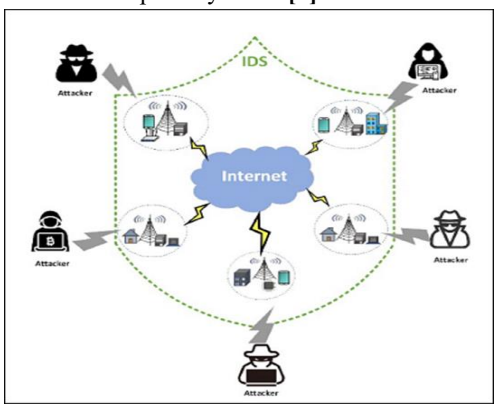

Fig 2: illustrates various scenarios of Internet of Things Cyber Attacks **[6]**

Designing an efficient network intrusion detection model is a crucial step in ensuring data security. Correspondingly, designing an efficient network intrusion detection model requires understanding the architecture of IoT systems. The IoT system is made up of various components like IoT devices, computation servers, Internet devices, and wireless devices. IDS is a technology that ensures security by continuously scanning network and host traffic for any suspicious activity, that may breach security policies and jeopardize data confidentiality as well as integrity. Feature engineering plays a crucial role in extracting relevant network information for Machine Learning (ML) based Intrusion Detection Systems (IDSs) **[7, 18]**. A metaheuristic optimization algorithm called Arctic Puffin Optimization (APO) **[8]** and a Random Neural Network (RNN)-based attack detection method for IoT networks (IoT-RNNAPO) are proposed in this paper to address the aforementioned issues. The proposed model utilizes the Arctic Puffin Optimization to enhance the architecture and hyperparameters of the random neural network. The paper's innovations can be summarized in the following way:

1. *In this paper, a hybrid algorithm is proposed that has improved the search capability of algorithms while also increasing computational speed and accuracy.*
2. *The random neural network was upgraded and enhanced using Arctic puffin optimization. In this study, this process aims to reduce training time and improve the model's robustness.*
3. *To address early convergence in a local minimum of the squared error function that adjusts the weights of the standard random neural network, this paper proposes utilizing Arctic puffin optimization to approach the minimum of the error square function.*

The paper continues with the following structure: Section 2 offers a review of pertinent research. In Section 3, you will find Arctic puffin optimization. Section 4 proposes the algorithm and methodology; Section 5 demonstrates the implementation and evaluation of the proposed model; Finally, in Section 6, we present the conclusion and future work.

II. Related Work

This section focuses on research conducted in the field of developing attack detection systems in IoT applications, one based on traditional machine learning algorithms and the other based on deep learning techniques, as well as meta-heuristic algorithms. This study aims to provide a comprehensive perspective for researchers and practitioners in this field by comparing the main principles, advantages, and limitations of these three approaches. In the field of attack detection, Machine Learning (ML) has been widely used, and its effectiveness has been proven. Support Vector Machine (SVM), Naive Bayes, Decision Tree (DT), Random Forest (RF), and Artificial Neural

Network (ANN) are commonly used in attack detection systems **[19, 20]**.

A. Machine Learning based attack detection methods

ET-DCANET, a highly efficient hierarchical intrusion detection model, was introduced by Xin Yang et al **[9]**. In this model, the extreme random tree algorithm was utilized to meticulously choose the optimal feature subset. Subsequently, the dilated convolution and dual attention mechanism (channel attention and spatial attention) were introduced, along with a plan to transition from overall learning to detailed learning by decreasing the expansion rate of cavity convolution. It was discovered that this model has an accuracy of 99.85%. ARINDAM SAKAR et al **[10]** proposed intrusion detection system within a Block Chain framework that leverages federated learning (FL) and an Artificial Neural Network (ANN)-based key exchange mechanism. The proposal by SATHISH Kumar et al **[11]** outlines a homomorphic encryption scheme that utilizes the privacy chain, the weight of evidence, and the information value of the statistical transformation method. This scheme is designed to safeguard the user's private and sensitive information. The proposed STHE algorithm ensures that perturbing numerical and categorical values from multiple datasets does not impact data utility. In another research, **[12]** Created design and computation to support fine-tuned static allocation scheduling for distributed computing space with dynamic distribution of virtual machines. The design coordinated delicate continuous assignment planning calculations, particularly expert hub and virtual machine hub plans. In **[13]**, a new DOS attack detection system was introduced, which was equipped with the previously developed MCA technique and EMD-L1. The technique used previously helps extract the correlations between individual pairs of two distinct features within each network traffic record and detects more accurate characterization for network traffic behaviors. The recent technique facilitates our system to be able to effectively distinguish both known and unknown DOS attacks from authorized network traffic. In **[14]**, the authors offered a system that recommended the right crops for the region and the right fertilizers for the crops to farmers based on soil measurements, all based on past years' yield history. This agricultural yield forecast and fertilizer recommendation would employ machine learning methods. The random forest algorithm and the K-means clustering algorithm proved to be successful in predicting crop suitability and recommending FERTILISER. The dataset for the Salem region contains a number of factors that are used for this purpose. Elsewhere **[15]** conducted a study on a water quality monitoring system to make water quality predictions with a machine learning system. The aim of this study was to create a water quality prediction model using an Artificial Neural Network (ANN) and time-series analysis. The specific data and investigation goals will determine the chosen prediction model. in another research, **[16]** proposed framework for advancing an explicit sprayer arrangement. The created gadget aimed to reduce the use of pesticides by spraying individual targets explicitly and by setting the separation of spray items based on the target. A sharp mechanical structure for spraying pesticides in cultivation field for controlling the robot by the use of a remote choice rather than manual completion of yields shower tests, would reduce the prompt prologue to pesticides and the human body, while also decreasing pesticide harm to people and improving age adequacy. In **[17]**, the authors tried to diagnose heart disease through Support Vector Machine (SVM) and Genetic Algorithm (GA) as a data analysis approach. AI methodologies were utilized during this work to influence crude data providing novel insights into coronary artery disease. In their proposal, ANITTHA GOVINDARAM and JEGATHEESAN A **[21]** presented FLBC-IDS, a technique that utilizes HFL, HYPERLEDGER BLOCKCHAIN, and EFFICIENT Net for effective intrusion detection in IoT environments. HFL empowers the FLBC-IDS model to enable secure and privacy-preserving model training on a wide range of IoT devices, leading to decentralized data privacy and optimized resource utilization. presented an accuracy of 98.89%, recall of 98.044%, F1-score of 98.29%, and precision of 98.44%. They created a model in **[22]** that combines federated learning with distributed computing resources and Blockchain decentralized features to introduce an intrusion detection framework called IOV-BCFL. It was capable of distributed intrusion detection and reliable logging with privacy protection. Elsewhere, **[23]** introduced a model called MP-GUARD, a novel framework which used software-defined networking (SDN), machine learning (ML), and multi-controller architecture to address intrusion detection challenges. MP-GUARD tackles multi-pronged intrusion attacks in IoT networks by offering real-time intrusion detection, collaborative traffic monitoring and multi-layered attack mitigation. This model achieved exceptional performance with 99.32% accuracy, 99.24% F1 score, and 0.49% false positive rate. In a different study, **[24]** proposed a client selection method using clustering to identify malicious clients by analyzing their run time. This was paired with a trigger-set-based encryption system for client authentication, achieving a model accuracy of 99.8%. In **[25]**, researchers studied the use of feature reduction, feature selection, and machine learning models to detect attacked traffic in IoT industrial networks. They explored the combination of PSO and PCA with MARS or GAM machine learning models.

B. Deep Learning based attack detection methods

In recent years, with the rapid development of deep learning technologies, advanced deep learning algorithms have found widespread applications in the field of attack detection. Such as DNN, CNN, RNN, and Deep Convolutional GAN. Wang et al **[26]** introduced a network intrusion detection model based on

Deep Learning (DL). This model sought to boost detection accuracy through feature extraction from spatial and temporal aspects of network traffic data. The aim of the model was to amplify the minority class samples, handle data imbalance, and enhance the accuracy of network intrusion detection. The model achieved an accuracy of 97.47%. elsewhere in their work. G. SATHISH Kumar et al **[27]** introduced a statistical differential privacy-deep neural network (DNN - SDP) algorithm to protect sensitive personal data. The input layer of the neural network received both numerical and categorical human-specific data. The statistical methods weight of evidence and information value was applied in the hidden layer along with the random weight (w_i) to obtain the initial perturbed data. This initially perturbed data were taken by Laplace computation based differential privacy mechanism as the input and provided the final perturbed data. DNN-SDP algorithm provided 97.4% accuracy. In **[28]**, the main goal was to develop suitable models and algorithms for data augmentation, feature extraction, and classification. The proposed TB-MFCC multi-fuse feature consisted of data amplification and feature extraction. In the proposed signal augmentation, each audio signal used noise injection, stretching, shifting, and pitching separately, where this process increased the number of instances in the dataset. The proposed augmentation reduced the overfitting problem in the network. The suggested Pooled MULTIFUSE Feature Augmentation (PMFA) with MCNN & A-BILSTM enhanced the accuracy to 98.66 %. Elsewhere, in **[29]** a new model and lightweight forecasting model was proposed using time series data from the KAGGLE website. The obtained dataset was then processed with the help of deep learning techniques. The Long Short-Term Memory (LSTM) algorithm was used to produce better results with higher accuracy when compared with other deep learning methodologies. In **[30]**, A model for the class imbalance problem was addressed using Generative Adversarial Networks (GANs). Accordingly, an equal number of train and test images was considered for better accuracy. The prediction accuracy was enhanced by Multi piled Deep Convolutional Generative Adversarial Network (DCGAN). In **[31]** An automatic number plate recognition (ALPR) system provided the vehicle's license plate (LP). The computer vision area considered the ALPR system as a solved problem. The algorithm applied in the proposed methodology was Convolution Neural Network (CNN). In **[32]**, was model used to increase cognitive efficiency in Artificial General Intelligence (AGI), thereby improving agent image classification and object localization. This system, which used RNN and CNN, would enable any user to do creative work using the system model. The system model took in the sample input and produced the output based on the input given. P.R. KANNA and P. SANTHI **[33]** presented an efficient hybrid IDS model built using Map Reduce-based optimized Black Widow short-term convolutional-long-term memory (BWO-CONV-LSTM) network. This model was used for intrusion detection in online systems. The first stage of this IDS model involved the feature selection by the Artificial Bee Colony (ABC) algorithm. The second stage was the hybrid deep learning classifier model of BWO-CONV-LSTM on a Map Reduce framework for intrusion detection from the system traffic data. P Rajesh KANNA and P SANTHI **[34]** proposed a high-accuracy intrusion detection model using an integrated Optimized CNN (OCNN) model and hierarchical multiscale LSTM (HMLSTM) to effectively extract and learn SPATIO-temporal features. The proposed intrusion detection model performed pre-processing plus feature extraction through network training and network testing together with final classification. The approach in **[35]** utilized deep learning technology to detect leaf diseases through the Recurrent Neural Network (RNN) algorithm. About 53,000 images of infected and healthy leaves, showcasing fruits and vegetables such as apple, orange, strawberry, and more, make up the dataset. The neural network was trained to increase accuracy in predicting efficient outputs. In another study, **[36]** discussed a new intrusion detection system that approached big data management. Intrusion detection was done by a hybrid model, fusing the long short term memory and optimizing Convolutional Neural Network (CNN). Then, the optimization-assisted training algorithm called Elephant Adapted Cat Swarm Optimization (EA-CSO) was proposed which would tune the optimal weights of CNN to enhance the performance of detection. In **[37]** A quadratic static method was used to find the correlation between features, enhancing the dimensionality reduction in the dataset, where deep over-optimization and genetic hyper-learning model (DHO-GML) were applied to efficiently perform the classification by selecting the optimized model. The proposed model produced an accuracy above 99%.

C. Meta-Heuristic-based attack detection methods

Due to Reducing computational overhead and Increasing classification accuracy, metaheuristic algorithms have received more attention in recent years and have also been used in attack detection systems. Such as PSO, GA, ACO, GOA. A. SUBRAMANIAM et al **[38]** Intrusion Detection System using Hybrid Evolutionary Lion and Balancing Composite Motion Optimization Algorithm espoused feature selection with Ensemble Classifier (IDS-IOT Hybrid ELOA-BCMOA-Ensemble-DT-LSVM-RF-XGBOOST) propose for Securing IoT Network. Accuracy of this model was achieved 94.47%. In **[39]**, a new light intrusion detection system was designed in two phases using swarm intelligence based technique. In the first step, the basic features were selected using the particle swarm optimization algorithm considering the unbalanced data set. The ant colony optimization algorithm was used in the second phase to extract information-rich and unrelated features. In addition, genetic algorithm was employed to fine-tune each detection

model. The accuracy of the model was 97.87%. In **[40]**, an advanced local search grasshopper algorithm was proposed based on recurrent federated network (RFN-ELG). Datasets such as UNSW-NB15 and MQTT-IoT-IDS2020 dataset were used to determine IIoT performance through two different phases, i.e. data preprocessing phase as well as attack detection phase.

III. Preliminary Concept

The main goal of this paper is to find optimal values for the weights of a Random Neural Network using the APO metaheuristic algorithm; for this reason, basic concepts such as the APO optimization algorithm are discussed in this section. A set of metaheuristic algorithms is actually a swarm intelligence algorithm. Swarm intelligence algorithms are a type of artificial intelligence method that is based on group behaviors in decentralized, self-organizing systems. These systems are **typically** composed of a population of simple agents that interact locally with **one another** and their environment. Algorithms are a type of artificial intelligence method based on group behaviors in decentralized, self-organizing systems. The Arctic puffin is a rare and small bird native to the Arctic. They typically live in the oceans, and these birds usually **form** groups or flocks, **often** with **well-developed** fishing skills. Arctic puffins are **mighty** hunters, catching at least ten small fish per dive. Before diving, they use coordinated feeding behaviors, working together to increase their hunting efficiency.

In this section, inspired by the survival behaviors of the Arctic Puffin, the APO algorithm is proposed. The mathematical model of APO consists of three main stages: population initialization, the aerial flight stage (exploration), and the underwater foraging stage (exploitation). Additionally, it involves the transition between these two strategies, induced by the behavioral transformation factor B of the puffin.

Initial population: Each Arctic Puffin represents a potential solution participating in the optimization. **The following Equation describes the generation process of initializing the population**:

$$\overrightarrow{X_i^t} = rand * (ub - lb) + lb\ , i = 1,2,3, \dots, N \quad (1)$$

Where $\overrightarrow{X_i^t}$ represents the position of the i th Arctic Puffin; $rand$ generates a random number between 0 and 1; ub and lb represent the upper and lower bounds, N is the number of individuals in the population.

Aerial flight stage (Exploration): Arctic puffins rely on unique flight and foraging strategies to navigate their challenging existence. In their daily lives, they must flexibly adapt between the ocean and the air. The **strategy above** is shown in Figure 3.

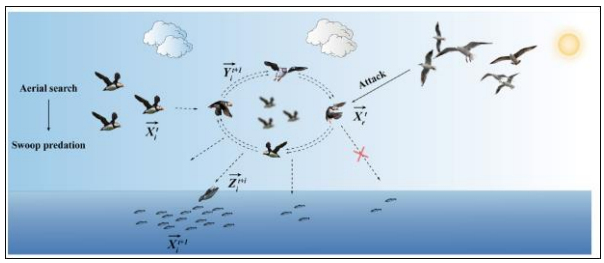

Fig 3: Flight stage of Arctic Puffins **[8]**

Arctic puffins typically participate in coordinated flight in groups, a collaborative action that increases flight efficiency and joint hunting opportunities. In favorable conditions, or when predators are scarce and fish populations are abundant, they skillfully accelerate towards the **water's surface** to better capture their prey. Below are the position updating Equations associated with this **strategy**.

$$\overrightarrow{Y_i^{t+1}} = \overrightarrow{X_i^t} + rand * \left(\overrightarrow{X_i^t} - \overrightarrow{X_r^t}\right) * L(D) + R \quad (2)$$

$$R = round\left(0.5 * (0.05 + rand)\right) * \alpha \quad (3)$$

$$\alpha \sim Normal\ (0,1) \quad (4)$$

where r is a random integer between 1 and $N - 1$, excluding i; $\overrightarrow{X_i^t}$ represents the current i th candidate solution in the population; $\overrightarrow{X_r^t}$ is a candidate solution randomly selected from the current population, with $\overrightarrow{X_i^t} \neq \overrightarrow{X_r^t}$; $L(D)$ denotes a random number D is the dimension; α is a random number which follows the standard normal distribution.

Underwater foraging stage (Exploitation): Survival strategy in the Arctic involves two **essential** aspects: air flight and underwater search. Figure 4 shows the underwater search phase in the Arctic Puffins that stay on the sea surface, observe the behavior of other members to identify diving hotspots or food sources. Equation 5 describes the position update.

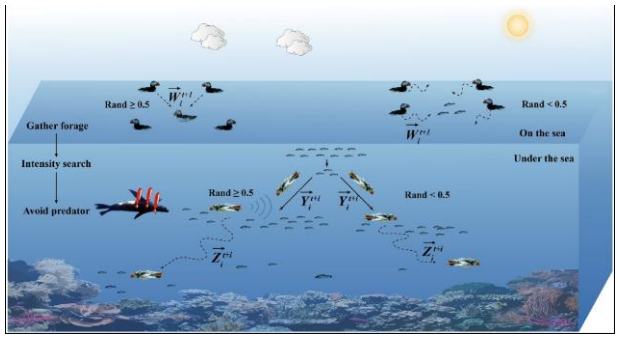

Fig 4: Underwater foraging stage of Arctic Puffins **[8]**

$$\overrightarrow{W_i^{t+1}} = \begin{cases} \overrightarrow{X_{r1}^t} + F * L(D) * \left(\overrightarrow{X_{r2}^t} - \overrightarrow{X_{r3}^t}\right) & rand \geq 0.5 \\ \overrightarrow{X_{r1}^t} + F * \left(\overrightarrow{X_{r2}^t} - \overrightarrow{X_{r3}^t}\right) & rand < 0.5 \end{cases} \quad (5)$$

where F represents the cooperative factor, adjusting the predation behavior of Arctic puffins. We consider $F = 0.5$ in this paper. variables $r1, r2, r3$ are random numbers between 1 and $N - 1$. $\overrightarrow{X_{r1}^t}$ $\overrightarrow{X_{r2}^t}$ $\overrightarrow{X_{r3}^t}$ are candidate solutions randomly selected from the current population, and $r1 \neq r2 \neq r3$, $\overrightarrow{X_{r2}^t} \neq \overrightarrow{X_{r3}^t}$. In the APO **algorithm's** parameter F is designed as a synergistic factor, inspired by the collaboration and team predation exhibited by Arctic puffins in their foraging behavior.

As predation progresses, Arctic puffins may sense a depletion or exhaustion of food resources in their current foraging area after a **specific** period. To continue meeting their nutritional needs, they must alter their underwater positions to search for more fish or other underwater food sources. The position update Equation for this stage is as follows:

$$\overrightarrow{Y_i^{t+1}} = \overrightarrow{W_i^{t+1}} * (1 + f) \quad (6)$$

$$f = 0.1 * (rand - 1) * \frac{(T-t)}{T} \quad (7)$$

where T represents the total number of iterations, and t denotes the current iteration count. $rand$ is a random number that introduces some randomness to f.

In the Arctic Puffin algorithm, a behavioral conversion factor, B, is designed to make a smooth transition from global search to local exploitation. This factor is defined as:

$$B = 2 * \log\left(\frac{1}{rand}\right) * \left(1 - \frac{t}{T}\right) \quad (8)$$

Where $rand$ is a random number between (0, 1) and t and T are the current iteration number and the maximum iteration number, respectively. B plays **a vital** role in adjusting the rate of global search and local exploitation in this algorithm, so that in the early stages of the algorithm, it allocates **a larger** amount for global search. In the later stages, it allocates **a greater** amount for local exploitation. This mechanism **enables** the algorithm to **transition** from extensive search to a deeper and local search at different iteration stages, which helps improve the **algorithm's efficiency** in finding optimal solutions.

IV. Poposed Method for Detecting Attacks in IoT

Network intrusion detection benefits from the superior performance of hybrid models. The limitation of single CNN or RNN models is the singular feature extraction dimension, resulting in relatively worse classification outcomes. model has become popular because of its ability to be applied to different tasks. however, we know that Random Neural Network is a suitable solution for attack detection in Internet of Things networks. Meanwhile, adjusting the weights of random neural networks is directly related to their classification accuracy. Also, by adjusting the internal parameters of neural networks, they reach high accuracy in classification. So in our proposed framework, the internal parameters and architecture of the random neural network are adjusted using meta-innovative algorithms to enhance its classification performance and accuracy. Indeed, adjusting the weights and architecture of the neural network aims to improve the classification accuracy.

A. Dataset Description

An open-source dataset named DS2OS was obtained from KAGGLE **[41]**. This is one of the new generations of IoT datasets for evaluating the fidelity and efficiency of different cybersecurity applications based on machine/deep learning algorithms. The dataset consists of 357952 samples and 13 features. It has 347935 normal data values and 10017 anomalous data values, with 8 classes. Two features ``Value" and ``Accessed Node Type" have 2500 and 148 missing values, respectively. Indeed, in this paper, the dataset consists of 260,000 samples with eleven features (Source Address, Source Type, Source Location, Destination Address, Destination Type, Destination Location, Accessed Node Address, Accessed Node Type, Operation, Value, Timestamp). The dataset is split into 70% for training and 30% for testing the model. Figure (5) shows the IoT network intrusion detection model of metaheuristic optimization algorithm and RNN in flow chart.

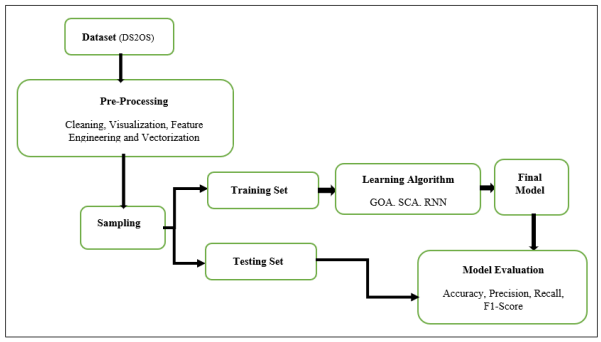

Fig 5: The IoT network intrusion detection model uses metaheuristic optimization algorithms and RNN in its structural flow chart

B. Input Features

In this paper, the DS2OS dataset consists of 260,000 samples with eleven features (Source Address, Source Type, Source Location, Destination Address, Destination Type, Destination Location, Accessed Node Address, Accessed Node Type, Operation, Value, Timestamp). The dataset is divided into 70% for training and 30% for testing the model. These input features are named X1, X2, to X11. The dataset is split into a training set and test set, with a ratio of 80% and 20%, respectively. Eleven features were used as input for the RNN.

C. Random neural network architecture

In this section, we briefly explain the architecture of the random neural network. The technique for attack detection in IoT systems, such as the ANN and the Random Neural Network (RNN) is also inspired by the human brain. RNN contains 1 input layer, 8 hidden layers, and 1 output layer. The input layer assigns weights plus biasness values and forwards these data to hidden layers for further processing. Learning is very important in hidden layers as it plays a critical role in predicting the output from real features. Hidden layers transfer this information to the output layer for suitable output generation. After learning, the trained model is used to predict attacks by using a test set.

D. Adjusting the architecture of the Lightweight random neural network by using the Arctic Puffin Optimization

We know that a neural network is a black box, but by using the optimized parameters and architecture of the random neural network modeled in this paper, we can increase the speed and accuracy of executing the attack detection process in the network. An important factor that affects the learning process of a neural network is the number of neurons in the hidden layers. If the number of neurons is too high, it can cause overfitting, and if the number of neurons is too low, it can cause underfitting. The correct determination of the number of neurons is very important for designing neural networks. In problems where we do not know the search space completely, using metaheuristic algorithms is efficient and useful. Stochastic optimization algorithm are often population-based, such as the Arctic Puffin Optimization. The steps for implementing the algorithm are as follows:

1. A search agent is a vector with a specified number of cells (the number of non-zero cells in the array is equivalent to the hidden layers of the network), where the number inside each array indicates the number of neurons in that hidden layer. as shown in Figure (6), and the Arctic Puffins position are updated using Equation (5). The goal of optimization in this phase is to minimize the number of layers of the neural network as well as the number of neurons corresponding to each layer, in order to reduce the complexity of calculations and the amount of memory consumed.

The number of neurons in the first hidden layer	The number of neurons in the second hidden layer	...	The number of neurons in the n hidden layer

Fig **6:** Vector of a search agent

2. Using the Arctic Puffin Optimization, the best search agent is obtained.

3. The fitness function is the classification accuracy; using Equation (8), the fitness function of each search agent is determined.

$$\text{Accuracy} = \frac{T_{Pos}+T_{Neg}}{T_{Pos}+T_{Neg}+F_{Pos}+F_{Neg}} \quad (8)$$

Where T_{Neg} is The number of records whose actual class is negative and the classification algorithm correctly identifies them as negative. T_{Pos} denotes the number of records whose actual class is positive and the classification algorithm correctly identifies them as positive. F_{Pos} shows the number of records whose actual class is negative but the classification algorithm incorrectly identifies them as positive. Finally, F_{Neg} reflects the number of records whose actual class is positive but the classification algorithm incorrectly identifies them as negative.

4. A search agent is a vector with a specified number of cells, where the number inside each array represents the number of each weight, Figure (7) shows the Structure of a search agent.

Number of weight number 1	Number of weight number 2	...	Number of weight number n_{th}

Fig **7:**Structure of a search agent

5. Using the Arctic Puffin Optimization, the best search agent is obtained.

6. Each search agent can estimate the weights of the network according to the fitness function. As mentioned, the fitness function is the classification accuracy, which is obtained using Equation (8).

V. Results of Evaluations

In this section, the software and hardware implementation of the proposed scheme are described in detail. We make a comprehensive evaluation of our proposed scheme in comparison with the new common schemes through simulation. After detailing the simulation settings, protocol comparisons, and metric evaluations, the simulation results are presented along with their analysis. The performance evaluation was conducted using the MATLAB R2024b software. These tests were performed on a 12-core central processing unit with 16 GB of RAM, (ASUS TUF GAMING F15).

A. Metrics for Evaluation

The Confusion Matrix (CM) **[42]** was used to assess, analyze, and confirm the proposed detection technique. Various factors are taken into account when assessing the proposed model. In the following, performance parameters that are used to evaluate the proposed algorithm are briefly explained. We evaluated the suggested model by considering various performance metrics

like accuracy, precision, recall, F1–score, and false alarm rate (FAR). The details of the Confusion matrix are clearly shown in Figure (8).

TN: *The number of records whose actual class is negative and the classification algorithm correctly identifies them as negative.*
TP: *The number of records whose actual class is positive and the classification algorithm correctly identifies them as positive.*
FP: *The number of records whose actual class is negative but the classification algorithm incorrectly identifies them as positive.*
FN: *The number of records whose actual class is positive but the classification algorithm incorrectly identifies them as negative.*

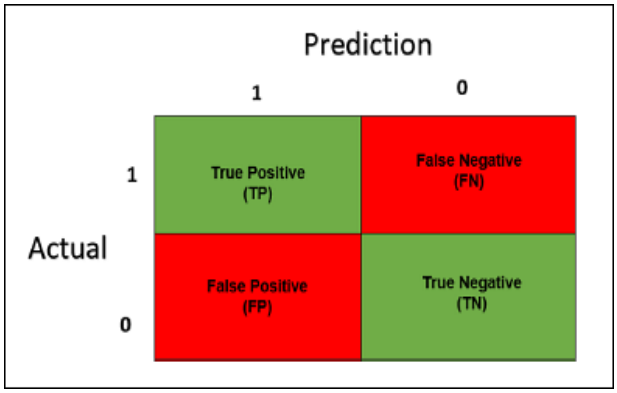

Fig 8: Confusion matrix **[16]**

1. Accuracy
Accuracy is mathematically described as the ratio between accurate positive and negative results to complete the results of the machine learning model.

$$\text{Accuracy} = \frac{T_{Pos}+T_{Neg}}{T_{Pos}+T_{Neg}+F_{Pos}+F_{Neg}} \quad (9)$$

2. Precision
It is a ratio between truly predicted positive results to true and false-positive results and is mathematically described.

$$\text{Precision} = \frac{T_{Pos}}{T_{Pos}+F_{Pos}} \quad (10)$$

3. Recall *(Detection Rate)*
It describes the relationship between true positive predictions to true positive and false negative predictions.

$$\text{Recall} = \frac{T_{Pos}}{T_{Pos}+F_{Neg}} \quad (11)$$

4. F1 SCORE
This is a weighted average of precision and recall. The F1 score maintains the balance between precision and recall by considering positive and negative results.

$$\text{F1} - \text{score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision}+\text{Recall}} \quad (12)$$

5. False Alarm Rate (FAR)
False alarm rate means the false rate of the detection system. Indeed, malicious behaviors are detected as normal behaviors. Thus, a lower false alarm rate is more desirable.

$$\text{FAR} = \frac{F_{Pos}}{T_{Pos}+F_{Pos}} \quad (13)$$

B. Datasets
Due to the constant advancements in network intrusion detection technology, there is now a larger selection of publicly accessible network intrusion detection datasets that are diverse and tailored to specific contexts, serving as valuable resources for research **[43]**. In addition to the DS2OS dataset **[41]**, two other datasets, CIC-IDS2018 **[44]** and CIC-IoT2023 **[45]**, were chosen to test the performance of the proposed framework for network intrusion detection in this study. To achieve better detection results, further processing is required. In the Cross Validation (CV) method, the training dataset is divided into several parts. Training, testing, and validation data are then obtained by averaging the data to get a more accurate answer. The calculation of the dataset's imbalance ratio is as follows:

$$\text{imbalance} - \text{ratio} = \frac{N_{min}}{N_{max}} \quad (14)$$

Where N_{min} is the number of the minority class samples, and N_{max} denotes the number of the majority class samples, a scalar object has been created using the MinMax class Then, the minimum and maximum values have been found for each feature, and then all data has been converted based on the minimum and maximum values in the range of 0 and 1. This method is obtained using the following equation.

$$Z = \frac{X-\min(x)}{\max(x)-\min(x)} \quad (15)$$

Here Z is normalized data, X is original data, min(X) is the minimum data of the feature, max(x) is the maximum data of the feature, Figure (9) clearly reveal the comparison between the new methods and the proposed model (IDS-RNNAPO) on DS2OS dataset in terms of accuracy rate.

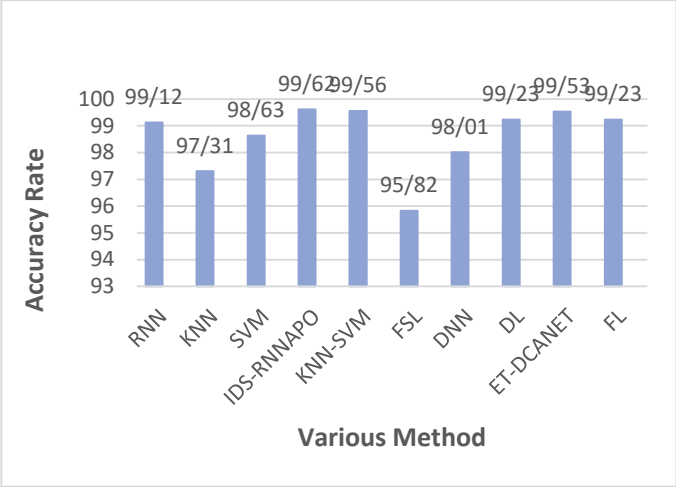

Fig **9:**Comparison of the tested methods and the proposed model on DS2OS dataset

Figure (10) graphically indicates the difference between various methods on DS2OS dataset based on the recall (detection rate).

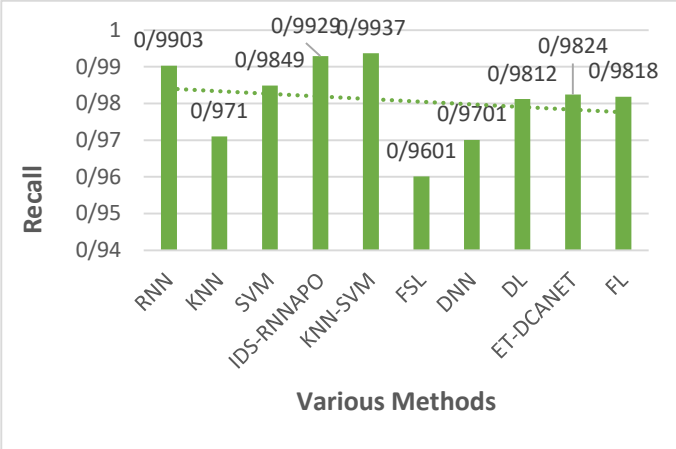

Fig 10: Comparison of the tested methods and the proposed model on DS2OS dataset

Figure (11) demonstrates the variation between different methods and the proposed model on DS2OS.Considering that the lower the FAR, the better the performance of the model.

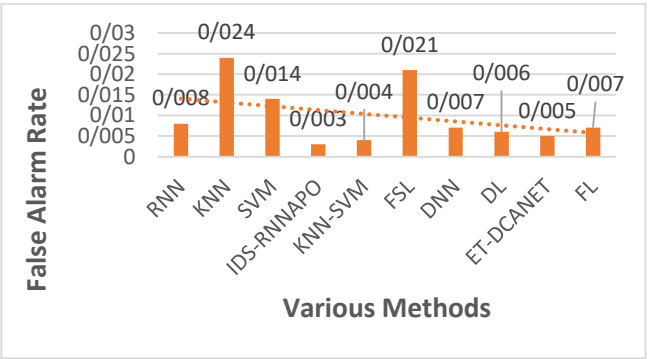

Fig **11:** Comparison of the tested methods and the proposed model on DS2OS dataset

Figure (12) graphically illustrates the difference between various methods on CIC-IDS2018 dataset based on the recall (detection rate).

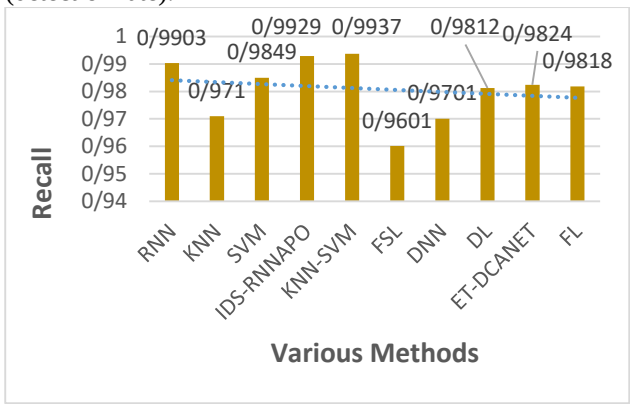

Fig 12: Comparison of the Tested Methods and the Proposed Model on CIC-IDS2018 Dataset

Figure 13 graphically indicates the difference between various methods on CIC-IoT2023 dataset based on the recall (detection rate).

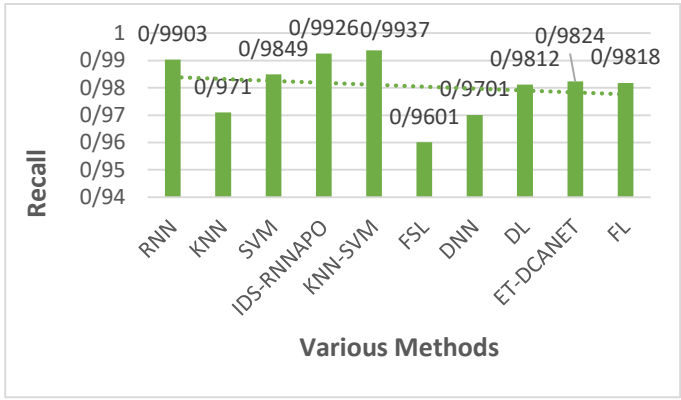

Fig **13:**Comparison of the tested methods and the proposed model on CIC-IoT2023 dataset

Figure (14) graphically displays the difference between various methods on CIC-IoT2023 dataset based on the false alarm rate (FAR).

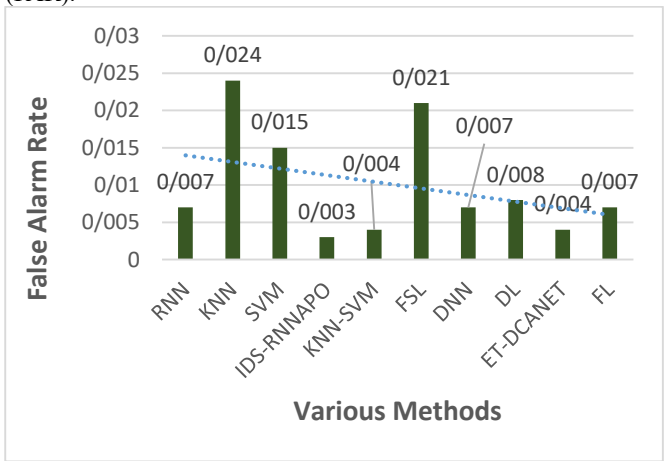

Fig **14:**Comparison of the tested methods and the proposed model on CIC-IoT2023 dataset

Figure (15) graphically shows the difference between various methods on CIC-IDS2018 dataset based on the false alarm rate (FAR).

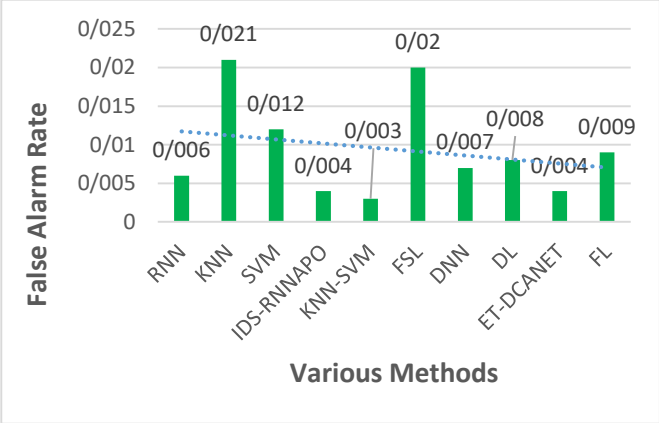

Fig **15:**Comparison of the tested methods and the proposed model on CIC-IDS2018 dataset

Limitations

Simulation results showed that the proposed approach has several advantages over other methods; however, it also has some limitations. Evolutionary intelligence algorithms such as APO **require** time to discover the best solution in the search space. Parameters may also need to be tuned in different application environments to maintain the **model's optimal** performance. **Additionally**, the continuous communication between IoT devices **during** model **training** in the proposed framework can **result in excessive** communication overhead. However, our model can save computational resources by **utilizing** metaheuristic algorithms, although these algorithms may take longer to reach the global optimum, especially with large IoT datasets, **which** can also affect the energy consumption of network nodes. If IoT devices lack computational power, the training time for algorithms can **be significantly increased**. APO can only solve single-objective problems involving continuous variables. **Additionally**, the proposed framework requires **constant** communication between IoT devices **during** model training, **which can lead to excessive** communication overhead. Data collected from different devices exhibit diverse qualitative characteristics. **Achieving** model generalizability and scalability across diverse IoT datasets. The deployment of the proposed model in a live test environment is uncertain.

VI. Conclusion and Future Works

A proper intrusion detection system's effectiveness depends directly on the choice and effectiveness of the classification method. Tweaking parameters, such as network weights, can enhance a neural network's performance. A method for detecting attacks in IoT networks is outlined in this paper, utilizing evolutionary intelligence and random neural networks. By utilizing Arctic puffin optimization the proposed model upgraded the architecture and internal parameters of the random neural network. The effectiveness of the proposed model was confirmed on dataset (DS2OS) with an accuracy rate of **99.62%,** recall value of **0.9929,** and false alarm rate of **0.003**. future work will focus on optimizing the model with various metaheuristic optimization algorithms in vehicular networks, also Edge computing provides IoT services at the edge of the network. The proposed approach increases the efficiency and scalability of IoT devices. Fog computing addresses the problems of cloud-based architectures such as latency and location awareness. Fog is a decentralized platform, which can make it ideal for several IoT applications. The proposed model can be considered for future implementation in fog domain security for Internet of Things applications.

REFERENCES

[1] Chao Chen, Li-Chun Wang, CHIH-Min Yu, (2022), **"**D2CRP: A Novel Distributed 2-Hop Cluster Routing Protocol for Wireless Sensor Networks" *IEEE INTERNET OF THINGS JOURNAL*, DOI: 10.1109/JIOT.2022.3148106

[2] MAHDIEH MAAZAAHI, SOODEH HOSSEINI. (2025) "MACHINE LEARNING AND METAHEURISTIC OPTIMIZATION ALGORITHMS FOR FEATURE SELECTION AND BOTNET ATTACK DETECTION" *KNOWLEDGE AND INFORMATION SYSTEMS,* HTTPS://DOI.ORG/10.1007/S10115-024-02322-0

[3] SANGREZ KHAN A, AHMAD NASEEM ALVI A, MUHAMMAD AWAIS JAVED, YASSER D. AL-OTAIBI, ALI KASHIF BASHIR, (2021), "AN EFFICIENT MEDIUM ACCESS CONTROL PROTOCOL FOR RF ENERGY HARVESTING BASED IOT DEVICES"*COMPUTERCOMMUNICATIONS*, HTTPS://DOI.ORG/10.1016/J.COMCOM.2021.02.011.

[4] SAMIRA RAJABI, SAMANE ASGARI, SHAHRAM JAMALI, REZA FOTOHI, (2024), "AN INTRUSION DETECTION SYSTEM USING THE ARTIFICIAL NEURAL NETWORK-BASED APPROACH AND FIREFLY ALGORITHM" *WIRELESS PERSONAL COMMUNICATIONS,* HTTPS://DOI.ORG/10.1007/S11277-024-11505-5

[5] SHAHID LATIF, ZHUO ZOU, ZEBA IDREES, JAWAD AHMAD, (2020), "Novel Attack Detection Scheme for the Industrial Internet of Things using a Lightweight Random Neural Network" *IEEE Access* Digital Object Identifier 10.1109/ACCESS.2020.2994079

[6] ZHENDONG WANG, XIN YANG, ZHIYUAN ZENG, DAOJING HE, SAMMY CHAN, (2024), "A HIERARCHICAL HYBRID INTRUSION DETECTION MODEL FOR INDUSTRIAL INTERNET OF THINGS" *PEER-TO-PEER NETWORKING AND APPLICATIONS,* HTTPS://DOI.ORG/10.1007/S12083-024-01749-0

[7] SAYEDA SUAIBA ANWAR, ASADUZZMAN, IQBAL H. SARKER, (2024), "A DIFFERENTIAL PRIVACY AIDED DEEPFED INTRUSION DETECTION SYSTEM FOR IOT APPLICATIONS" *SECURITY PRIVACY,* HTTPS://DOI.ORG/10.1002/SPY2.445

[8] WEN-CHUAN WANG, WEI-CAN TIAN, DONG-MEI XU , HONG-FEI ZANG., (2024), "ARCTIC PUFFIN OPTIMIZATION: A BIO-INSPIRED METAHEURISTIC ALGORITHM FOR SOLVING ENGINEERING DESIGN OPTIMIZATION" *ADVANCES IN ENGINEERING SOFTWARE,* HTTPS://DOI.ORG/10.1016/J.ADVENGSOFT.2024.103694

[9] ZHENDONG WANG, XIN YANG, ZHIYUAN ZENG, DAOJING HE, SAMMY CHAN, (2024), "A HIERARCHICAL HYBRID INTRUSION DETECTION MODEL FOR INDUSTRIAL INTERNET OF THINGS" *PEER-TO-PEER NETWORKING AND APPLICATIONS,* HTTPS://DOI.ORG/10.1007/S12083-024-01749-0

[10] CHONGZHOU ZHONG, ARINDAM SARKAR, SARBAJIT MANNA, MOHAMMAD ZUBAIR KHAN, ABDULFATTAH NOORWALI, ASHISH DAS, KOYEL CHAKRABORTY, (2024), "FEDERATED LEARNING-GUIDED INTRUSION DETECTION AND NEURAL KEY EXCHANGE FOR SAFEGUARDING PATIENT DATA ON THE INTERNET OF MEDICAL THINGS" *INTERNATIONAL JOURNAL OF MACHINE LEARNING AND CYBERNETICS,* HTTPS://DOI.ORG/10.1007/S13042-024-02269-2

[11] G. SATHISH KUMAR, K. PREMALATHA, G. UMA MAHESHWARI, P. RAJESH KANNA. (2023), "NO MORE PRIVACY CONCERN: A PRIVACY-CHAIN BASED HOMOMORPHIC ENCRYPTION SCHEME AND STATISTICAL METHOD FOR PRIVACY PRESERVATION OF USER'S PRIVATE AND SENSITIVE DATA" *EXPERT SYSTEMS WITH APPLICATIONS,* HTTPS://DOI.ORG/10.1016/J.ESWA.2023.121071

[12] P. Rajesh KANNA, G. RAJESHKUMAR, S. SRIRAM, S. SADESH, C. VINU, LOGANATHAN Mani, (2023), "Effective Scheduling of Real-Time Task in Virtual Cloud Environment Using Adaptive Job Scoring Algorithm" *Proceedings of International Conference on Advanced Communications and Machine Intelligence, Studies in Autonomic, Data-driven and Industrial Computing,* https://doi.org/10.1007/978-981-99-2768-5_30

[13] P. RAJESH KANNA, K. SINDHANAISELVAN, M.K. VIJAYMEENA, (2017), "A Defensive Mechanism based on PCA to Defend Denial-of-Service Attack" *International Journal of Security and Its Application,* http://dx.doi.org/10.14257/ijsia.2017.11.1.07

[14] DR GAYATHIRI B, BRINDHA P, KARTHIKA I, SARANYAE, DR RAJESHKUMAR G, DR Rajesh KANNA P, (2023), "Machine Learning based Crop Suitability Prediction and FERTILISER Recommendation System" *Proceedings of the Fourth International Conference on Electronics and Sustainable Communication Systems,* 10.1109/ICESC57686.2023.10193542

[15] SRIRAM S, S SANTHIYA, RAJESHKUMAR G, S. GAYATHRI, K. VIJAYA, Rajesh KANNA P, (2023), "Predict the Quality of Freshwater using Support Vector Machines" *Proceedings of the Second International Conference on Applied Artificial Intelligence and Computing,* 10.1109/ICAAIC56838.2023.10140956

[16] P.RAJESH KANNA, R.VIKRAM, (2020), "Agricultural Robot – A pesticide spraying device" *International Journal of Future Generation Communication and Networking,* https://www.researchgate.net/publication/340827655

[17] A.PANDIARAJ, Dr. S. Lakshmana Prakash, P. Rajesh KANNA, (2021), "EFFECTIVE HEART DISEASE PREDICTION USING HYBRIDMACHINE LEARNING" *Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks,* 10.1109/ICICV50876.2021.9388635

[18] Unveiling the Power of Sklearn AutoML: Revolutionizing Machine Learning – mosescore.eu. https://mosescore.eu/scikit/sklearn-automl/

[19] Analysis of Various Machine Learning / Deep Learning Performance of Advanced Persistent Threat Attack | AIJR Books. https://books.aijr.org/index.php/press/catalog/book/120/chapter/1341

[20] Sugiana, A., Cahyadi, W., & Yusran, Y. (2024). Current-Signal-Based Fault Diagnosis of Railway Point Machines Using Machine Learning. Applied Sciences, 14(1), 267.

[21] NANNAN XIE, CHUANXUE Zhang, QIZHAO Yuan, Jing Kong, XIAOQIANG Di, (2024), "IOV-BCFL: An intrusion detection method for IOV based on BLOCKCHAIN and federated learning" *Ad Hoc Networks,* https://doi.org/10.1016/j.adhoc.2024.103590

[22] Ameer El-Sayed, WAEL Said, Amr TOLBA, Yasser ALGINAHI, Ahmed A. TOONY, (2024), "MP-GUARD: A novel multi-pronged intrusion detection and mitigation framework for scalable SD-IOT networks using cooperative monitoring, ensemble learning, and new P4-extracted feature set" *Computers and Electrical Engineering,* https://doi.org/10.1016/j.compeleceng.2024.109484

[23] ANITTHA GOVINDARAM, JEGATHEESAN A, (2024), "FLBC-IDS: a federated learning and BLOCKCHAIN-based intrusion detection system for secure IOT environments" *Multimedia Tools and Applications,* https://doi.org/10.1007/s11042-024-19777-6

[24] R. Alexander, K. Pradeep Mohan Kumar, (2024), "FWICSS-Federated Watermarked Ideal Client Selection Strategy for Internet of Things (IOT) Intrusion Detection System" *Wireless Personal Communications,* https://doi.org/10.1007/s11277-024-11477-6

[25] Ravi SHEKHAR Tiwari, D. Lakshmi, TAPAN Kumar Das, ASIS Kumar TRIPATHY, KUAN-CHING Li, (2024), "A lightweight optimized intrusion detection system using machine learning for edge-based IIoT security" *Telecommunication Systems,* https://doi.org/10.1007/s11235-024-01200-y

[26] XIAO WANG, LIE DAI, GUANG YANG, (2024), "A NETWORK INTRUSION DETECTION SYSTEM BASED ON DEEP LEARNING IN THE

IOT" THE JOURNAL OF SUPERCOMPUTING, HTTPS://DOI.ORG/10.1007/s11227-024-06345-w

[27] G. SATHISH KUMAR, K. PREMALATHA, G. UMA MAHESHWARI, P. RAJESH KANNA, G. VIJAYA, M. NIYAASHINI, (2024), "DIFFERENTIAL PRIVACY SCHEME USING LAPLACE MECHANISM AND STATISTICAL METHOD COMPUTATION IN DEEP NEURAL NETWORK FOR PRIVACY PRESERVATION" *ENGINEERING APPLICATIONS OF ARTIFICIAL INTELLIGENCE*, HTTPS://DOI.ORG/10.1016/J.ENGAPPAI.2023.107399

[28] T.M. NITHYA, P. DHIVYA, S.N. SANGEETHAA, P. Rajesh KANNA, (2024), "TB-MFCC MULTIFUSE feature for emergency vehicle sound classification using MULTISTACKED CNN – Attention BILSTM" *Biomedical Signal Processing and Control*, https://doi.org/10.1016/j.bspc.2023.105688

[29] T.M. NITHYA, P. DHIVYA, S.N. SANGEETHAA, P. Rajesh KANNA, (2024), "TB-MFCC MULTIFUSE feature for emergency vehicle sound classification using MULTISTACKED CNN – Attention BILSTM" *Biomedical Signal Processing and Control*, https://doi.org/10.1016/j.bspc.2023.105688

[30] KARTHIKA S, T Priyanka, J. INDIRAPRIVADHARSHINI, DR S SADESH, RAJESHKUMAR G, Rajesh KANNA P, (2023), "Prediction of Weather Forecasting with Long Short-Term Memory using Deep Learning" *Proceedings of the Fourth International Conference on Smart Electronics and Communication (ICOSEC)*, 10.1109/ICOSEC58147.2023.10276273

[31] E. MYTHILI, DR.S. VANITHAMANI, DR Rajesh KANNA, DR RAJESHKUMAR G, K GAYATHRI, R. HARSHA, (2023), "AMLPDS: An Automatic Multi-Regional License Plate Detection System based on EASYOCR and CNN Algorithm" *Proceedings of the Second International Conference on Edge Computing and Applications (ICECAA 2023)*, 10.1109/ICECAA58104.2023.10212354

[32] A. PANDIARAJ, S. Lakshmana Prakash, R. Gopal, P. Rajesh KANNA, (2022), "Generating Art and Music Using Deep Neural Networks" *Artificial Intelligent Techniques for Wireless Communication and Networking*, https://doi.org/10.1002/9781119821809.ch7

[33] P. Rajesh KANNA, P. SANTHI, (2022), "Hybrid Intrusion Detection using Map Reduce based Black Widow Optimized Convolutional Long Short-Term Memory Neural Networks" *Expert Systems with Applications*, https://doi.org/10.1016/j.eswa.2022.116545

[34] P Rajesh KANNA, P SANTHI, (2021), "Unified Deep Learning approach for Efficient Intrusion Detection System using Integrated Spatial–Temporal Features" *Knowledge-Based Systems*, https://doi.org/10.1016/j.knosys.2021.107132

[35] HARSHA R, KARTHIKA S, MOHANA PRIYA D, DR Rajesh KANNAP, DR RAJESHKUMAR G, MYTHILIE, (2023), "FOLLA Disease Detection using In-Depth Learning" *Proceedings of the Second International Conference on Applied Artificial Intelligence and Computing*, 10.1109/ICAAIC56838.2023.10141305

[36] L. MADHURIDEVI, N. V. S. SREE RATHNA Lakshmi, (2024), "Metaheuristic assisted hybrid deep classifiers for intrusion detection: a big data perspective" *Wireless Networks*, https://doi.org/10.1007/s11276-024-03815-0

[37] P. DHIVYA, P. Rajesh KANNA, K. DEEPA, S. SANTHIYA, (2023), "Square Static – Deep Hyper Optimization and Genetic Meta-Learning Approach for Disease Classification" *IETE JOURNAL OF RESEARCH*, https://doi.org/10.1080/03772063.2023.2206367

[38] ANUVELAVAN SUBRAMANIAM, SURESHKUMAR CHELLADURAI, Stanly Kumar ANDE, SATHIYANDRAKUMAR Srinivasan, (2024), "Securing IOT network with hybrid evolutionary lion intrusion detection system: a composite motion optimization algorithm for feature selection and ensemble classification" *JOURNAL OF EXPERIMENTAL & THEORETICAL ARTIFICIAL INTELLIGENCE*, https://doi.org/10.1080/0952813X.2024.2342858

[39] ARPITA Srivastava, DITIPRIVA Sinha, (2024), "PSO-ACO-based bi-phase lightweight intrusion detection system combined with GA optimized ensemble classifiers" *Cluster Computing*, https://doi.org/10.1007/s10586-024-04673-3

[40] MADINI O, ALASSAFI, (2024), "Securing IIOT operations with recurrent federated network-based enhanced local search grasshopper" *Neural Computing and Applications*, https://doi.org/10.1007/s00521-024-10129-x

[41] M.-O. PAHL and F.-X. AUBET, (2018), "Ds2Os Traffic Traces IoT Traffic Traces Gathered in a The Ds2Os IoT Environment" [Online]. Available: https://www.kaggle.com/francoisxa/ds2ostraffictraces

[42] CHONGZHOU ZHONG, ARINDAM SARKAR, SARBAJIT MANNA, Mohammad ZUBAIR Khan, ABDULFATTAH NOORWALI, Ashish Das, KOYEL Chakraborty, (2024), "Federated learning-guided intrusion detection and neural key exchange for safeguarding patient data on the internet of medical things" *International Journal of Machine Learning and Cybernetics*, https://doi.org/10.1007/s13042-024-02269-2

[43] Xiao Wang, Lie Dai, GUANG Yang, (2024), "A network intrusion detection system based on deep learning in the IoT" *The Journal of Supercomputing*, https://doi.org/10.1007/s11227-024-06345-w

[44] SHARAFALDIN. I, HABIBI LASHKARI. A, GHORBANI. AA (2018) "Toward generating a new intrusion detection dataset and intrusion traffic characterization" In: *Proceedings of the 4th International Conference on Information Systems Security and Privacy - ICISSP, INSTICC* SCITE Press, pp 108–116, https:// DOI. org/ 10. 5220/ 00066 39801 080116

[45] NETO ECP, DADKHAH S, Ferreira R et al (2023) CICIOT 2023: "a real-time dataset and benchmark for large-scale attacks in IOT environment" *Sensors* https:// DOI. org/ 10. 3390/ s2313 5941