Received: November 3, 2024. Revised: December 4, 2024.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Network Intrusion Detection System in Internet of Things Using Chaotic Elite Guidance Learning Strategy-based Lotus Effect Optimization Algorithm

Sowmya Karanam Syamarao[1] Amith Shekhar Chandrashekhar[2]* Anupkumar Manohara Bongale[3] Deepak Sudhakar Dharrao[4]

[1]*Department of Information Science and Engineering, B.M.S. College of Engineering, Bengaluru, India*
[2]*Department of Computer Science and Engineering, B N M Institute of Technology, Bengaluru, India*
[3]*Department of Artificial Intelligence and Machine Learning, Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune, India*
[4]*Department of Computer Science and Engineering, Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune, India*
* Corresponding author's Email: amith_shekhar@bnmit.in

Abstract: Intrusion Detection Systems (IDS) are vital for Internet of Things (IoT) network security that is used to detect and prevent harmful actions like malicious attacks. The network intrusion data are combined into several typical examples because of its dynamic nature that results in a lack of instances to train the models and increase the false detection rate. To overcome these limitations, a Chaotic Elite Guidance learning strategy-based Lotus Effect Optimization algorithm (CEG-LEO) and Bi-directional Long Short-Term Memory (Bi-LSTM) with categorical cross-entropy loss function is proposed for network intrusion detection in an IoT environment. The proposed CEG learning strategy with the LEO algorithm is used to select significant features based on the best fitness solution obtained by the pollination activity of the lotus flower. The proposed Bi-LSTM model is employed to detect and classify multiple intrusive attacks accurately by extracting temporal information from the selected attacks features which are in sequence order of network traffic events. The experimental results of proposed methods utilized in network intrusion detection in IoT achieved accuracy of 99.34 % and 99.37% for CICIDS-2018 and CICIDS-2019 datasets which is higher when compared to existing detection approaches like Rat Swarm Hunter Prey Optimization based Deep Maxout Network (RSHPO-DMN).

Keywords: Bi-directional long short-term memory, Chaotic elite guidance learning strategy, Internet of things, Intrusion detection systems, Lotus effect optimization algorithm.

1. Introduction

Recently the attention to the Internet of Things (IoT) has increased due to its global operations, way of communication, connectivity, and intelligent decisions that suggest activities from several devices. An Intrusion Detection System (IDS) is a specific model that is used to interpret and analyze the network as well as the host behaviour in an IoT environment [1-3]. The network traffic data in IoT is obtained from several places which includes routers, network packet analysis and statistics, firewalls, local system logs, server log files, access calls, and other sources [4]. An IDS distinguish the patterns of network traffic, behavior or activity found from the obtained data and monitor those patterns for detection of whether a signature and recent behavior are virtually the same or not. Nowadays, IoT networks become more vulnerable to security attacks such as cyber-attacks and other anomalies due to the diversity of devices and several key factors [5, 6]. These malicious attacks occur in several manners and especially target anomalous properties that affect one or more IoT devices that are utilized as "platforms" or "resources" for the attack, namely data leakage, Man middle attack, Distributed Denial-of-Service, and spoofing [6]. Thus, the security of IoT devices

against these attacks is increased significantly to safeguard the data. The objective of the IDS is to identify possible events where the IDS can detect whether a system has been successfully broken by a hacker utilizing system vulnerabilities [7].

In the early stages, the IDS is developed based on traditional machine learning algorithms, and the detection or classification of a that single approach is estimated frequently. Therefore, the machine learning model utilized for detection should provide accurate results which are highly constrained [8-10]. For network IDSs, machine learning models like K-nearest neighbor (KNN), Random Forest (RF), Decision tree (DT), Support vector machine (SVM), and so on are utilized to detect the attacks in existing research. Since the above-mentioned machine learning algorithms are straightforward and consume more time to learn they impact on detection of intrusive and malicious attacks which results in a risk of losing sensitive information. While deep learning techniques perform well in the detection and classification process, they have a substantial computational cost and a high training period which affect the detection system's accuracy [13]. Additionally, optimization algorithms such as Particle Swarm Optimization (PSO), Swarm Bipolar Algorithm (SBA) [14], Genetic Algorithm (GA), Swarm Space Hopping Algorithm (SSHA) [15], etc. are used in feature selection process to enhance the intrusion detection performance. However, the traditional rule-based IDSs based on deep learning algorithms are inadequate for detecting complex intrusive attacks in IoT systems since they are dynamic and heterogeneous nature. These traditional methods still face difficulties in dealing with the physical and functional diversity of IoT environment [16, 17]. To overcome these limitations, a Chaotic Elite Guidance learning strategy-based Lotus Effect Optimization algorithm (CEG-LEO) and Bi-directional Long Short-Term Memory (Bi-LSTM) with categorical cross entropy loss function is proposed for network intrusion detection in IoT network. The major contributions of this research are:

- Preprocessing techniques like one-hot encoding and normalization are used to convert categorical data into a numerical format and then normalize or rescale the values into a specific range that enhances the detection process.
- To adapt the dynamic network and select optimal features, the proposed CEG learning strategy is incorporated with LEO optimization to select features which have attack patterns effectively though the network changes.
- The proposed Bi-LSTM associated with categorical cross entropy data is employed to detect multiple attacks accurately by extracting temporal information from the selected attack features which are in sequence order of network traffic events.

This research paper is structured as follows: Section 2 discusses the literature survey. Section 3 describes the proposed methodology. Section 4 illustrates the results and discussion. The conclusion of this research paper is given in Section 5.

2. Literature review

Gunupudi Sai Chaitanya Kumar [18] developed a Deep Residual Convolutional Neural Network (DRCNN) for network intrusion detection. The developed DRCNN model was utilized to enhance network security by intrusion detection with the help of the Improved Gazelle Optimization Algorithm (IGOA) for fine-tuning hyperparameters of the network. The main advantage of the developed DRCNN model with IGOA was that effectively categorizes the several attack types in the network that accelerates feature learning to enhance detection performance. However, the developed DRCNN model has the limitations of overfitting and data sparsity affecting the detection performance that led to increase inaccurate detection of attacks.

Parameshwari [19] explored a Rat Swarm Hunter Prey Optimization based Deep Maxout Network (RSHPO-DMN) network intrusion detection model. The explored DMN model was incorporated with the RSHPO algorithm for tuning hyperparameters that are utilized to detect various threats in the network. An advantage of the explored RSHPO-DMN was the extracted features that were converted into feature maps. The DMN model was fine-tuned by the proposed RSHPO algorithm which helps to tune parameters effectively, which enhanced the intrusion detection performance. However, the explored RSHPO-DMN model has limitations that fail to learn to adopt the evolving nature of network traffic in IoT environment that affects the detection performance of certain attacks.

Yesi Novaria Kunang [20] presented an IDS that depends on auto-encoder models with unsupervised feature extraction. The presented auto encoder-based detection model involves two different sets of models, in the first case models like deep auto encoder, LSTM auto encoder and convolutional encoder were combined and used to detect the malicious attacks. In the second case, stacked auto encoder and deep belief network methods were used for detecting of attacks in the intrusive detection system. The advantage of

the presented detection system which utilises a feature extraction model that addresses data diversity effectively. However, the presented model has the drawback of adopting the dynamic nature of the IoT environment and failing to detect certain attacks.

Jalai Saikam and Koteshwararao CH [21] designed a Squeeze and Excitation based Deep Residual Network-152 (SE-ResNet-152) with hybrid optimization algorithms for network IDS. The developed ensemble approach was an integration of a deep learning model with improved spotted hyena optimization and honey badger algorithm used to improve intrusion detection performance in IoT networks. The main advantage of the developed SE-ResNet-152 model was that it improved the feature selection process by selecting optimal features. However, the developed model has limitations that fail to learn and adopt the evolving nature of network traffic in IoT environments that affect the detection performance of certain attacks.

Ahmed ABD EL-Baset Donkol [22] represented an intrusion detection model based on particle swarm optimization and a hybrid model Enhanced LSTM-Recurrent Neural Network (ELSTM-RNN). The represented ELSTM-RNN model was employed to improve the network security by detecting the malicious effectively. The main advantage of the represented intrusion detection model was that a like-point particle swarm optimization was utilized to address the gradient clipping issue in LSTM to enhance the classification performance. However, the represented ELSTM-RNN model has a drawback in adopting the dynamic nature of the IoT environment and the redundant features affect the accurate multiple attack detection.

3. Methodology

The proposed framework for network intrusion detection in IoT includes four phases: Dataset, preprocessing, feature selection and classification. Fig. 1. Illustrates the block diagram for proposed network intrusion detection in IoT. Firstly, the data about attacks in IoT are acquired from the two benchmark datasets and then pre-processed to normalize all features for further processing. After that, important features with significant information about malicious attacks are selected by the proposed optimization algorithm. Finally, the intrusive attacks in IoT networks are identified and classified by the proposed Bi-LSTM approach.

3.1 Dataset

In this research, CICIDS-2018 and CICIDS-2019 are two benchmark datasets used for network IDS in IoT.

3.1.1. CICIDS-2018 dataset

This dataset is an open-source dataset that is widely used for intrusion detection in IoT networks [23]. The raw network traffic data are frequently updated after being collected from various states. Thus, IDS 2018 provides 80 statistical features from both forward and reverse mode, which includes volume, byte quality and the packet's length.

3.1.2. CICIDS-2019 dataset

In this dataset, various DDoS attacks and other malicious attack related data are collected from the TCP/UDP-based network protocols. The dataset includes 80 feature-based traffic data. The dataset was collected in two ways: training and testing analyses. This CICIDS-2019 dataset [24] consists of data about attack types such as MSSQL, SNMP, DNS, WebDDos, SYN, LDAP, Net BIOS, UDP-Lag, and NTP.

3.1.3. NSL-KDD dataset

The NSL-KDD dataset [25] is the publicly available dataset which is most widely used in network intrusion detection.

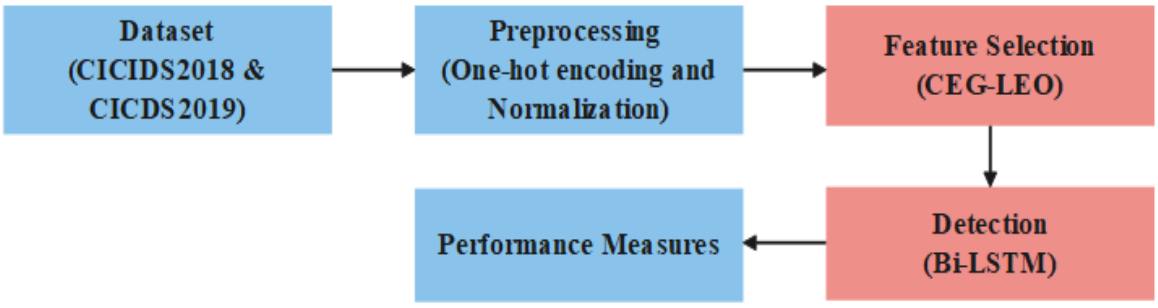


Figure. 1 Block Diagram for proposed network IDS in IoT

The dataset is processed and transformed into 42 digital features, 4 symbol features and 38 dimensional features. Each feature in the dataset is labelled as normal and attack. The attack labelled features are further classified into four attack categories such as Denial of Service (DoS), Probe, R2L, and U2R attacks.

3.1.4. UNSW NB-15 dataset

The UNSW NB-15 dataset [26] is an open-source dataset which involves 2.54 million network packets and 9 various attack types. This dataset is one of the extensively used datasets in network intrusion detection in IoT. The UNSW-NB 15 consists of 87.35% of ordinary traffic and 12.65% of attack traffic in the overall dataset. These acquired features and data about different attacks are fed to the preprocessing stage.

3.2 Preprocessing

The acquired raw data are fed as input to the preprocessing phase to convert them into useful formats for effective IDS. To enhance these data, the preprocessing techniques such as one-hot encoding, and normalisation utilized in this research are explained as follows:

3.2.1. One-hot encoding

Initially, the raw data or features are fed as input to the one-hot encoding method which converts categorical or symbolic-based features into numerical features. This encoding technique is the most widely-used preprocessing method in IDS which deals with the ordinal properties of the attribute-based data. The ordinal properties of acquired data indicate a number representing the place of something in sequence order. These properties are transformed into binary vectors, where the unit has values of 1 and others have 0. A unit with numerous 1' values represents possible features that match the similar feature category. This one-hot encoding helps in enhancing the detection accuracy of the method which converts the data into numerical format and even the data for all forms. When utilizing this encoding process in an intrusion detection system, a new column is generated for all possible classes makes the model learn the relationship between each category and helps to enhance the accuracy of the detection results.

3.2.2. Normalization

The encoded features are further fed to this normalization technique which is used to match the wide range of encoded data properties [27]. By permitting the suggested categorization method that rapidly selects an optimal option. In this research, the Min-Max normalization method is utilized to scale the numerical values of features. The minimum and maximum values of attributes which are represented by min and max among the values of 0 and 1 are the normalized range values. The mathematical representation of this min-max normalization technique is represented in Eq. (1):

$$z' = \frac{z - z_{min}}{z_{max} - z_{min}} \quad (1)$$

Where, z denotes initial point; z' represents normalized value. min and max refers to minimum and maximum values. These preprocessed features are forwarded to proposed feature selection stage.

3.3 Proposed feature selection

The pre-processed features are fed as input to the proposed feature selection method based on the LEO algorithm with the CEG learning strategy. The proposed LEO algorithm is used to select the most important features which is vital to classify multiple classifications of various attacks effectively. This proposed model selects features by a repellent mechanism that eliminates redundant features by carrying away the dirt in the leaves of the lotus. Selecting the optimal set of features helps to distinguish between attacks and enhance the classification process. Generally, LEO is a nature-inspired algorithm that leaves self-cleaning and super hyperbolic features of a lotus flower [28]. The proposed LEO algorithm majorly involves exploration and exploitation phases which are explained as follows:

- Exploration phase: This phase refers to actions of insects like dragonflies and seed-spreading activities are used for selecting optimal features for in-network intrusion detection.
- Exploitation phase: The optimization algorithm exploitation is also known as the extraction phase where the flower buds (lotus) are grouped around a core that inspires the local search strategies.

3.3.1. Exploration phase

The dragonfly provides leaf pollination which is referred to as global search in the LEO strategy that involves, food behaviour and enemy behaviour of the dragonfly to determine the best optimal features. For searching for food and escaping from enemies, the position of the dragonfly is updated which is mathematically formulated as represented in Eq. (2):

$$T_j^u = \sum_{k=1}^{O}\left(Y_j^u - Y_k^u\right) \quad (2)$$

Where, k represents index; u denotes present iteration; Y_j indicates current position of dragonfly; O refers to the number of individuals. The food-searching activities and escaping strategy of dragonflies is illustrated in Eq. (3) and Eq. (4):

$$G_j^u = Y_+^u - Y_j^u \quad (3)$$

$$Q_j^u = Y_-^u - Y_j^u \quad (4)$$

Where, G_j^u and Q_j^u denotes food search and escaping strategies of dragonfly; Y_+^u and Y_-^u represents positions of food and enemy; The food search activity is used to determine the best fitness solution whereas, the escaping from the enemy strategy is utilized for the worst fitness solution. The location of the lotus is estimated by the Eq. (5):

$$Y_j^{(u+1)} = Y_j^u + LEVY(z) \times Y_j^u \quad (5)$$

Where, $Y_j^{(u+1)}$ represents location vector; z denotes dimension; The term $LEVY$ is evaluated by Eq. (6):

$$LEVY(y) = 0.01 \times \left(\frac{S_1 \times \vartheta}{|S_2|^{\frac{1}{\theta}}}\right) \quad (6)$$

Where, S_1 and S_2 denotes random values; θ indicates constant values.

3.3.2. Exploitation Phase

In this phase, the pollination activity which also referred to as a local search where a coefficient is used to specify the size of every flowering area. The size determined by the coefficient from the growing area is around the best-found flower in this type of pollination activity, which is measured by Eq. (7):

$$Y_j^{(u+1)} = Y_j^u + S\left(Y_j^u - h^*\right) \quad (7)$$

Where, $Y_j^{(u+1)}$ represent position of pollens; h^* indicates best position; S denotes area growth. The area growth of the flower is estimated by the Eq. (8):

$$S = 2q^{-\left(\frac{4u}{M}\right)^2} \quad (8)$$

Where, M denotes iteration count; S represents balancing terms between the exploration and exploitation phases. The capacity of the area is calculated by Eq. (9):

$$i_j^u = \frac{\left(\left|g_j^u - g_{MAX}\right|\right) \times Cns}{\left(|g_{MIN} - g_{MAX}|\right)} \quad (9)$$

Where, i_j^u indicates capacity; g_j^u represents size; g_{MIN} and g_{MAX} denotes minimum and maximum fitness size. The velocity of a drop and moving drop in lotus leaves is evaluated by Eq. (10), (11) and (12):

$$W_j^{(u+1)} = r \times W_j^u \quad (10)$$

$$W_j^{(u+1)} = W_j^u + rnd\left(Y_{DEp}^u - Y_j^u\right) \quad (11)$$

$$Y_j^{(u+1)} = Y_j^u + W_j^{(u+1)} \quad (12)$$

Where, $W_j^{(u+1)}$ represents present velocity; Y_{DEp}^u indicates present location; rnd denotes random values. However, IoT networks are comprised of a diverse range of devices with various communication protocols, power capabilities, and security requirements. This heterogeneity makes difficult the feature selection process, as different types of devices require different feature sets for optimal intrusion detection. To address this problem, a CEG-learning strategy is proposed and incorporated with the LEO algorithm.

3.3.2.1 CEG learning strategy

In the CEG strategy, during each pollen's evolution at the current phase, the identified best solutions are stored, with the global best position holding the current optimal solution and the personal best position archiving the most favourable location. To enhance the population's performance and development in an evolution process, an arbitrary and ergodic chaotic sequence is presented based on the global and personal best position to understand the refined search near favourable position region. In the beginning stage, it is essential to create the model for utilizing the information completely about itself for large-scale exploration, and in the future search phase, it is necessary to acquire more data near the best pollen. After that, if a new pollen is performed better than an actual pollen, then new individual pollen is exchanged to enhance exploration. To enhance the pollen that has poor performance in the population, this CEG technique is proposed effectively in this

section which is mathematically expressed in Eq. (13) and (14):

$$z_{l+1} = z_l.\eta.(1 - z_l) \quad (13)$$

$$X_{i3j}^t = \begin{cases} G_j^t = step.(2.z_l - 1), if\left(r_5 < \frac{F_{es}}{F_{es_{max}}}\right) \\ P_{i3j}^t \quad , else \end{cases} \quad (14)$$

Where, z_l represents chaos value at l^{th} denotes control degree of chaos; η indicates random number; $step$ and r_5 also denotes random values; F_{es} and $F_{es_{max}}$ refers to current functional evaluation and total evaluation function; P_{i3j}^t represents personal best position. These chosen features are passed to proposed classification model.

3.4 Proposed Bi-LSTM Classification

The selected optimal features are fed as input to the proposed Bi-LSTM model to detect and categorize intrusive attacks in IoT networks. The sequential order of IoT network packets or connections contains several important patterns. For example, in a brute-force attack, when multiple failed login attempts happen over a short period, network traffic in IoT occurs as a sequence of events. Thus, Bi-LSTM is used to learn such temporal sequences, to model effectively for network intrusion detection in IoT.

The Bi-LSTM model is a kind of recurrent neural network and an improved version of LSTM models. In this research, the Bi-LSTM framework is used to detect and classify the various intrusive attacks in the IoT environment which effectively classify the attacks by integrating outputs of two various RNN layers. In Bi-LSTM, one layer analyzes data sequence from right to left whereas the other layer processes it from left to right. The main objective of choosing the Bi-LSTM method for detection is that it is permitted to process the long-term sequences effectively by utilizing data in both directions [29]. The Bi-LSTM model consists of 3 main gates which are input, output, and forget gates which are represented in Eq. (15) to (19):

$$f_t = \sigma\left(W_f x_t + Uh_{t-1} + b_f\right) \quad (15)$$

$$i_t = \sigma(W_i x_t + Uh_{t-1} + b_i) \quad (16)$$

$$o_t = \sigma(W_o x_t + Uh_{t-1} + b_o) \quad (17)$$

$$c_t = f_t * C_{t-1} + \sigma(W_c x_t + Uh_{t-1} + b_c) \quad (18)$$

$$h_t = o_t * \sigma_c\,(c_t) \quad (19)$$

Where, f_t, i_t, o_t, c_t and h_t represents forget, input, output gates, current state and output obtained from throughout the network; In network intrusion detection to classify multiple types of attacks such as DoS, DDoS, Botnet, Brute Force, etc., a loss function like Categorical Cross-Entropy (CCE) that ensures learning process of Bi-LSTM model to distinguish not only between normal and malicious traffic but also for different types of attacks. The mathematical representation of the categorical cross-entropy loss function is expressed in Eq. (20):

$$CCE(p,q) = -\sum_{i \in C} y_i log p_i(x) \quad (20)$$

Where, CCE denotes categorical cross entropy loss function; x, y_i and y_i represents input sample, target and probability distribution values. C indicates category domain with equivalent number of n classes. Some of the intrusive attacks only become deceptive when specific traffic features are considered together. The proposed CEG-LEO identifies these crucial features efficiently by differentiating between the best solution and the worst solution. The selected optimal features are fed as input to the Bi-LSTM model with CCE loss function, which prevents the incorrect classifications of attacks and enhances the detection and classification of multiple malicious attacks precisely. This enhanced the Bi-LSTM model to make more accurate classification results of attacks that reduced false positives and false negatives that improved overall security of the IoT network.

4. Results and discussion

Experimental results of the proposed CEG-Bi-LSTM model employed for character animation generation and human pose recognition are depicted in this section. The CEG-Bi-LSTM method is simulated in the Python 3.9 software tool with system configuration of Windows 10 OS, i5 processor, and 16 GB RAM. The performance metrics used for the experimental evaluation of the proposed method are Accuracy, precision, Recall and F1-score. A mathematical representation of performance metrics is given in Eq. (21) to (24):

$$Accuracy = \frac{TP+FN}{TP+TN+FP+FN} \times 100 \quad (21)$$

$$Precision = \frac{TP}{TP+FP} \times 100 \quad (22)$$

Table 1. Performance of feature selection using CICIDS-2018

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
PSO	97.26	96.49	95.78	96.13
SSHA	97.48	97.15	96.89	97.01
GWO	97.59	96.37	95.43	95.89
SBA	96.88	95.72	94.95	95.33
LEO	98.33	97.96	97.26	97.60
Proposed method CEG-LEO	99.34	99.28	99.32	99.30

Table 2. Performance of feature selection using CICIDS-2019

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
PSO	96.58	95.46	94.32	94.88
SSHA	96.93	96.37	95.91	96.13
GWO	97.86	96.59	95.47	96.02
SBA	97.49	96.84	95.25	96.03
LEO	98.27	97.36	96.67	97.01
Proposed method CEG-LEO	99.37	99.26	99.14	99.19

$$Recall = \frac{TP}{TP+FN} \times 100 \quad (23)$$

$$F1 - score = 2 \times \frac{recall \times precision}{recall + precision} \quad (24)$$

Were, TP- True Positive, FP-False Positive, TN-True Negative, FN-False Negative.

4.1 Quantitative and qualitative analysis

The performance analysis of proposed feature selection and classification method utilizing CICIDS-2018 dataset is evaluated by four different performance measures such as accuracy, precision, recall and F1-score. Performance evaluation of proposed feature selection methods according to the dataset is represented in Tables 1 and 2. Similarly, the performance of the proposed Bi-LSTM with the corresponding datasets is illustrated in Tables 3 and 4. The performance of the LEO algorithm-based feature selection in the CICIDS-2018 dataset is represented in Table 1. The proposed feature selection method is analyzed with existing optimization methods like Particle Swarm Optimization (PSO), Swarm Space Hopping Algorithm (SSHA), Grey Wolf Optimization (GWO), Swarm Bipolar Algorithm (SBA), and LEO algorithms. The proposed CEG-LEO algorithm in feature selection for network intrusion detection in IoT achieved accuracy of 99.34 %, precision of 99.28%, recall of 99.32% and F1-score of 99.30% respectively.

The performance of the PLEO algorithm-based feature selection in the CICIDS-2019 dataset is represented in Table 2. The proposed feature selection method is analyzed with existing optimization methods such as PSO, SSHA, GWO, SBA and LEO algorithms. The proposed CEG-LEO algorithm in feature selection for network intrusion detection in IoT accuracy of 99.37 %, precision of 99.26%, recall of 99.14 % and F1-score of 99.19 % respectively.

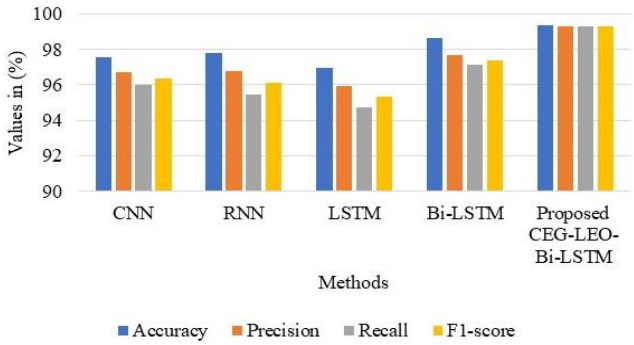


Figure. 2 Performance of Classification methods using CICIDS-2018

The effectiveness of the proposed classification approach in the CICIDS-2018 dataset is represented in Fig. 2. The proposed classification method is analyzed with existing classification approaches such as Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), LSTM, and Bi-LSTM. The proposed Bi-LSTM-based classification for network intrusion detection in IoT achieved the accuracy of 99.34 %, precision of 99.28%, recall of 99.32% and F1-score of 99.30% respectively.

The performance of proposed Bi-LSTM based classification model in the CICIDS-2019 dataset is represented in Fig. 3. The proposed classification

method is analyzed with existing classification methods such as CNN, RNN, LSTM, and Bi-LSTM. The proposed Bi-LSTM based classification for network intrusion detection in IoT achieved the accuracy of 99.37 %, precision of 99.26%, recall of 99.14 % and F1-score of 99.19 % respectively.

The performance analysis of the proposed CEG-LEO and Bi-LSTM model based on confusion matrix and ROC curve utilizing various standard datasets are represented from Fig. 4 and 5. The confusion matrix of proposed CEG-LEO and Bi-LSTM method used to detect and classify multiple attacks utilizing four standard datasets are represented in Fig. 4 (a), (b), (c) and (d) respectively. The combination of CEG-LEO and Bi-LSTM model reduced the false positive rate by selecting optimal features and learn the temporal dependencies from features in all datasets that results in efficient multi-classification of attacks in IoT network.

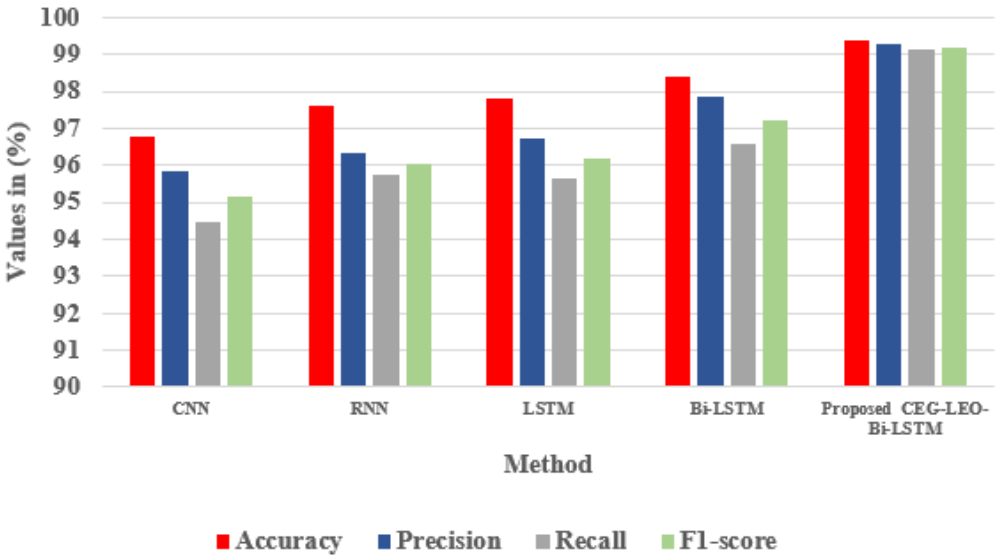
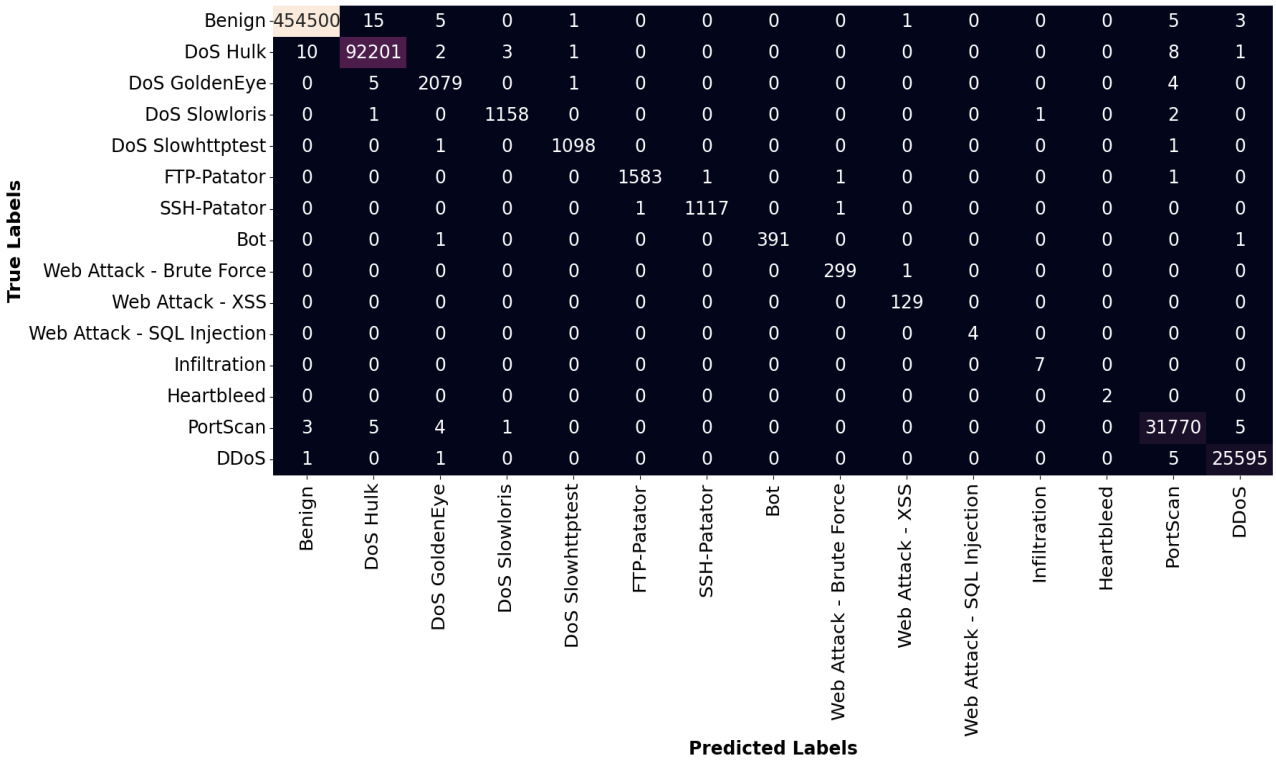
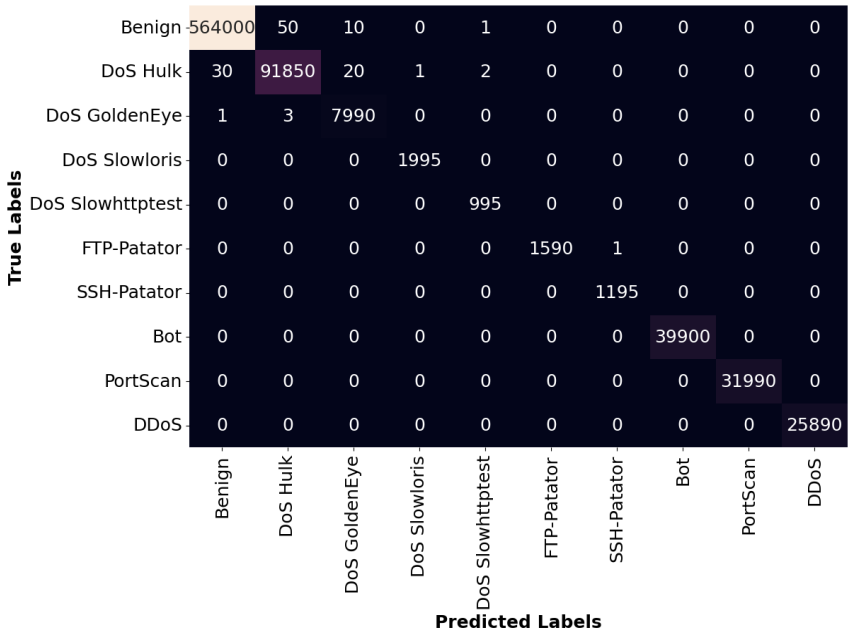


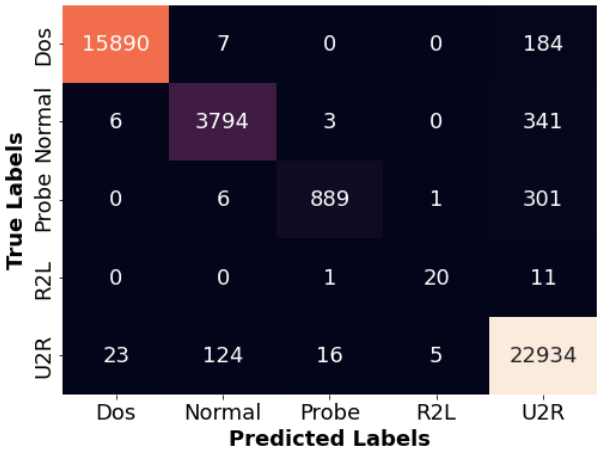
Figure. 3 Performance of Classification methods using CICIDS-2019



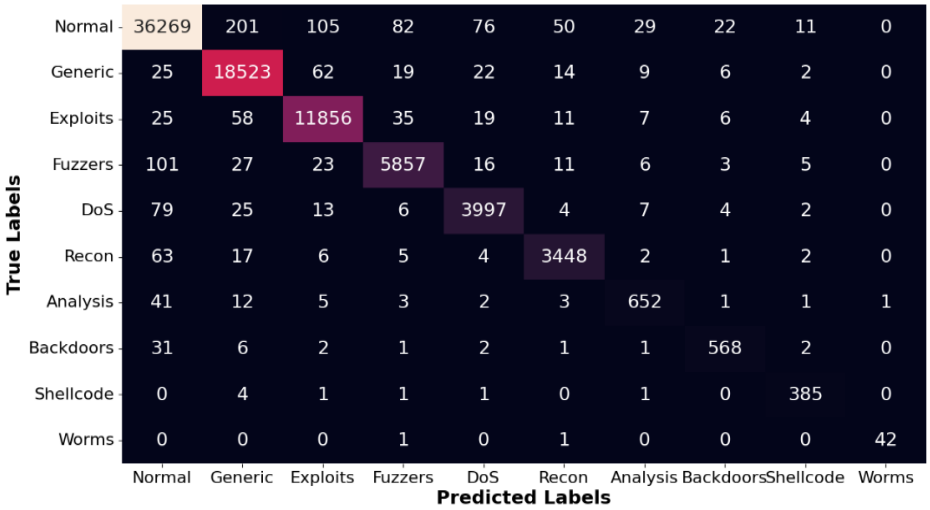
(a)



(b)



(c)



(d)

Figure. 4: (a), (b), (c), and (d) represents the Confusion matrix for proposed method in CICIDS-2018, CICIDS-2019, NSL-KDD and UNSW NB-15 datasets

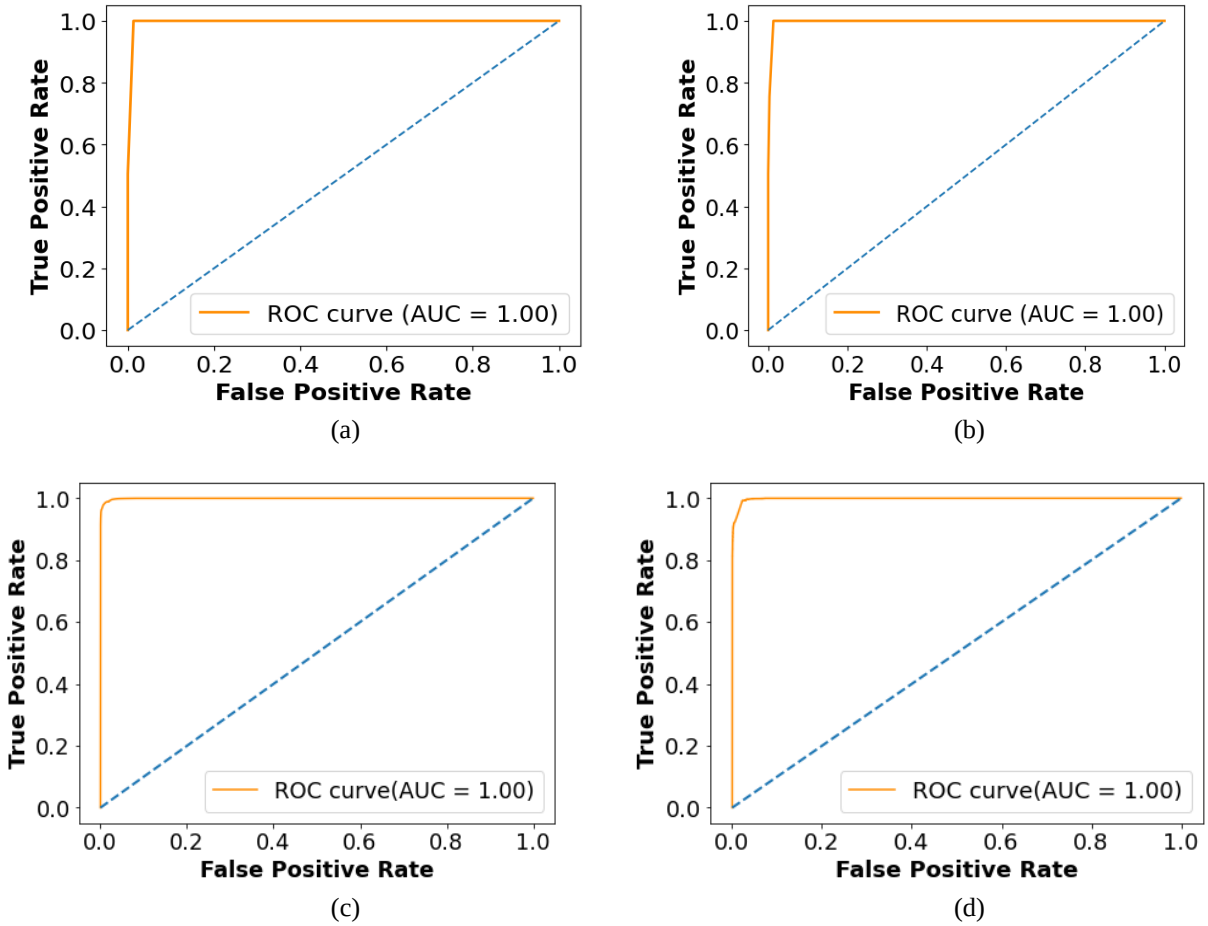


Figure. 5: (a), (b), (c), and (d) represents the ROC curve for proposed method in CICIDS-2018, CICIDS-2019, NSL-KDD and UNSW NB-15 datasets

The ROC curve of proposed CEG-LEO and Bi-LSTM method used to detect and classify multiple attacks utilizing four standard datasets are represented in Fig. 5 (a), (b), (c) and (d) respectively. From the Fig. 4 (a), (b), (c) and (d) it is clear that proposed CEG strategy enhanced the performance of LEO algorithm by selecting significant features which helps to select optimal features that assist the Bi-LSTM model detect the known and new modern attacks in IoT environment effectively.

4.2 Comparative analysis

The comparative analysis of the proposed method in feature selection and classification method utilizing CICIDS-2018, CICIDS-2019, NSL-KDD, and UNSW NB-15 datasets is assessed by different performance metrics like accuracy, precision, recall and F1-score. The comparison of proposed network intrusion detection method according to the different datasets are represented from Table 3 to 6. The comparative analysis of the proposed CICIDS-2018 dataset is illustrated in Table 3. Existing detection and classification methods such as DRCNN-IGOA [18], RSHPO-DMN [19], LSTM-AE [20] and SE-ResNet-152 [21] are the existing methods utilized for network intrusion detection for comparative analysis. The proposed method used for network intrusion detection in IoT achieved accuracy of 99.34 %, precision of 99.28%, recall of 99.32% and F1-score of 99.30% respectively.

Table 3. Performance of Classification methods using CICIDS-2018

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
RSHPO-DMN [19]	83.57	89.87	92.57	91.20
LSTM-DAE [20]	99.07	99.16	99.07	99.10
SE-ResNet-152 [21]	99.26	99.21	99.27	99.06
Proposed method CEG-LEO and Bi-LSTM	99.34	99.28	99.32	99.30

Table 4. Performance of Classification methods using CICIDS-2019

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
DRCNN-IGOA [18]	99.12	98.89	99.06	99.32
Proposed method CEG-LEO and Bi-LSTM	99.37	99.26	99.14	99.43

Table 5. Performance of Classification methods using NSL-KDD

Methods	Accuracy	Precision	Recall	F1-score
RSHPO-DMN [19]	0.908	0.935	0.965	0.95
Proposed method CEG-LEO and Bi-LSTM	0.970	0.969	0.968	0.968

Table 6. Performance of Classification methods using UNSW-NB15

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
DRCNN-IGOA [18]	99.06	N/A	N/A	N/A
SE-ResNet-152 [21]	99.43	99.57	99.17	99.16
Proposed method CEG-LEO and Bi-LSTM	99.54	99.60	99.46	99.52

The comparative analysis of CEG-LEO and Bi-LSTM method with existing detection algorithms utilizing the CICIDS-2019 dataset is represented in Table 4. The existing detection method like DRCNN-IGOA [18] is considered for comparative analysis with the proposed method. The of CEG-LEO and Bi-LSTM method used for network intrusion detection in IoT achieved accuracy of 99.37 %, precision of 99.26%, recall of 99.14 % and F1-score of 99.19 % respectively.

The comparative analysis of the CEG-LEO and Bi-LSTM method with existing detection algorithms utilizing the NSL-KDD dataset is represented in Table 5. The existing detection method like RSHPO-DMN [19] is considered for comparative analysis with the proposed method. The CEG-LEO and Bi-LSTM method used for network intrusion detection in IoT achieved accuracy of 0.97, precision of 0.969, recall of 0.968 and F1-score of 0.968 respectively.

The comparative analysis of the of CEG-LEO and Bi-LSTM method with existing detection algorithms utilizing the UNSW-NB15 dataset is represented in Table 6. The existing detection method like DRCNN-IGOA [18] and SE-ResNet-152 [21] is considered for comparative analysis with the proposed method. The CEG-LEO and Bi-LSTM method used for network intrusion detection in IoT achieved accuracy of 99.54 %, precision of 99.60 %, recall of 99.46 % and F1-score of 99.52 % respectively.

4.3 Discussion

The proposed CEG-LEO and Bi-LSTM model achieved better performance in network IDS in an IoT environment. The existing approaches have some limitations in detecting attacks such as the developed DRCNN [18] model has the limitations of overfitting and data sparsity affecting the detection performance which leads to increased inaccurate detection of attacks. An explored RSHPO-DMN [19] and LSTM-DAE [20] model failed to adopt the evolving and dynamic nature IoT environment that affects the detection performance for certain attacks. To overcome these limitations, a CEG-LEO and Bi-LSTM with categorical cross-entropy loss function are proposed for network intrusion detection in IoT networks. The proposed CEG learning strategy with the LEO optimization algorithm is proposed to select the most relevant features based on the best fitness solution obtained by the pollination activity of the lotus flower. The Bi-LSTM method is employed for the detection and classification of multiple attacks with the help of the CCE loss function accurately by extracting temporal information from the selected attack features which are in sequence order of network traffic events.

5. Conclusion

The CEG-LEO and Bi-LSTM with CCE loss function are proposed for network intrusion detection in IoT networks. The proposed CEG learning strategy with the LEO optimization algorithm is employed to select significant features based on the best fitness solution obtained by the pollination activity of the lotus flower. The Bi-LSTM model acquires the temporal information like a sequence of network traffic events obtained from the selected feature, helps in differentiating between malicious attacks and normal data to detect and classify the various types of malicious and intrusive attacks efficiently. The acquired raw data are pre-processed by a one-hot encoding and normalization process that enhances the data by converting categorical data into numerical data and rescaling numerical values into a specific range. The experimental results of proposed

method utilized in network intrusion detection in IoT achieved accuracy of 99.34 %, 99.37%, 99.54 % and 0.970 for CICIDS-2018, CICIDS-2019, UNSW-NB 15 and NSL-KDD datasets which is higher when compared to existing approaches such as RSHPO-DMN, DRCNN, and LSTM-DAE. In future, advanced deep learning models with metaheuristic optimization algorithms will be implemented to enhance network intrusion detection in an IoT environment.

Notation

Notations	Description
z	Initial point
z'	Normalized value
min and max	Minimum and maximum values
k	Index;
u	Present iteration
Y_j	Current position of dragonfly
O	Number of individuals
G_j^u and Q_j^u	Food search and escaping strategies of dragonfly
Y_+^u and Y_-^u	Positions of food and enemy
$Y_j^{(u+1)}$	Location vector
z	Dimension
S_1 and S_2	Random values
θ	Constant values
$Y_j^{(u+1)}$	Position of pollens
h^*	Best position
S	Area growth
M	Iteration count
S	Balancing terms between the exploration and exploitation phases
i_j^u	Capacity
g_j^u	Size
g_{MIN} and g_{MAX}	Minimum and maximum fitness size
$W_j^{(u+1)}$	Present velocity
Y_{DEp}^u	Present location
rnd	Random values
z_l	Chaos value at l^{th} denotes control degree of chaos
η	Random number
$step$ and r_5	Random values
F_{es} and $F_{es_{max}}$	Current functional evaluation and total evaluation function
P_{i3j}^t	Personal best position
f_t, i_t, o_t, c_t and h_t	Forget, input, output gates, current state and output obtained from throughout the network
CCE	Categorical cross entropy loss function
x, y_i and y_i	Input sample, target and probability distribution values
C	Category domain with equivalent number of n classes.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 3rd and 4th author. The supervision and project administration, have been done by 1st and 2nd author.

References

[1] H. Nguyen, and R. Kashef, "TS-IDS: Traffic-aware self-supervised learning for IoT Network Intrusion Detection", *Knowledge-Based Systems*, Vol. 279, p.110966, 2023.

[2] S. Roy, J. Li, B.J. Choi, and Y. Bai, "A lightweight supervised intrusion detection mechanism for IoT networks", *Future Generation Computer Systems*, Vol. 127, pp. 276-285, 2022.

[3] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, "Feature extraction for machine learning-based intrusion detection in IoT networks", *Digital Communications and Networks*, Vol. 10, No. 10, pp. 205-216, 2022.

[4] B. Madhu, M.V.G. Chari, R. Vankdothu, A.K. Silivery, and V. Aerranagula, "Intrusion detection models for IOT networks via deep learning approaches", *Measurement: Sensors*, Vol. 25, p. 100641, 2023.

[5] Y. Wang, J. Wang, and H. Jin, "Network intrusion detection method based on improved CNN in internet of things environment", *Mobile Information Systems*, Vol. 2022, No. 1, p. 3850582, 2022.

[6] H. Zhang, B. Zhang, L. Huang, Z. Zhang, and H. Huang, "An efficient two-stage network intrusion detection system in the Internet of Things", *Information*, Vol. 14, No. 2, p. 77, 2023.

[7] A. Abbas, M.A. Khan, S. Latif, M. Ajaz, A.A. Shah, and J. Ahmad, "A new ensemble-based intrusion detection system for internet of things", *Arabian Journal for Science and Engineering*, Vol. 47, pp. 1805-1819, 2022.

[8] B. Jothi, and M. Pushpalatha, "WILS-TRS—A novel optimized deep learning based intrusion

detection framework for IoT networks", *Personal and Ubiquitous Computing*, Vol. 27, No. 3, pp. 1285-1301, 2023.
[9] R. Gangula, and V, M.M., "Network intrusion detection system for Internet of Things based on enhanced flower pollination algorithm and ensemble classifier", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 21, p. e7103, 2022.
[10] C.U. Om Kumar, S. Marappan, B. Murugeshan, and P.M.R. Beaulah, "Intrusion detection model for IoT using recurrent kernel convolutional neural network", *Wireless Personal Communications*, Vol. 129 No. 2, pp. 783-812, 2023.
[11] R. Kumar, A. Malik, and V. Ranga, "An intellectual intrusion detection system using Hybrid Hunger Games Search and Remora Optimization Algorithm for IoT wireless networks", *Knowledge-Based Systems*, Vol. 256, p. 109762, 2022.
[12] A. Basati, and M.M. Faghih, "PDAE: Efficient network intrusion detection in IoT using parallel deep auto-encoders", *Information Sciences*, Vol. 598, pp. 57-74, 2022.
[13] S. Jain, P.M. Pawar, and R. Muthalagu, "Hybrid intelligent intrusion detection system for internet of things", *Telematics and Informatics Reports*, Vol. 8, p. 100030, 2022.
[14] P.D. Kusuma, and A. Dinimaharawati, "Swarm Bipolar Algorithm: A Metaheuristic Based on Polarization of Two Equal Size Sub Swarms", *International Journal of Intelligent Engineering & Systems*, Vol. 17, No, 2, pp. 377-389, 2024, doi: 10.22266/ijies2024.0430.31.
[15] P.D. Kusuma, and M. Kallista, "Swarm Space Hopping Algorithm: A Swarm-based Stochastic Optimizer Enriched with Half Space Hopping Search", *International Journal of Intelligent Engineering & Systems*, Vol. 17, No. 2, pp. 670-682, 2024, doi: 10.22266/ijies2024.0430.54.
[16] S. Bacha, A. Aljuhani, K.B. Abdellafou, O. Taouali, N. Liouane, and M. Alazab, "Anomaly-based intrusion detection system in IoT using kernel extreme learning machine", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 15, No. 1, pp. 231-242, 2024.
[17] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, "Anomaly-based intrusion detection system for IoT application", *Discover Internet of things*, Vol. 3, No. 1, p. 5, 2023.
[18] G.S.C. Kumar, R.K. Kumar, K.P.V. Kumar, N.R. Sai, and M. Brahmaiah, "Deep residual convolutional neural network: an efficient technique for intrusion detection system", *Expert Systems with Applications*, Vol. 238, p. 121912, 2024.
[19] A. Parameswari, R. Ganeshan, V. Ragavi, and M. Shereesha, "Hybrid rat swarm hunter prey optimization trained deep learning for network intrusion detection using CNN features", *Computers & Security*, Vol. 139, p. 103656, 2024.
[20] Y.N. Kunang, S. Nurmaini, D. Stiawan, and B.Y. Suprapto, "An end-to-end intrusion detection system with IoT dataset using deep learning with unsupervised feature extraction", *International Journal of Information Security*, Vol. 23, pp. 1619-1648, 2024.
[21] J. Saikam, and K. Ch, "An ensemble approach-based intrusion detection system utilizing ISHO-HBA and SE-ResNet152", *International Journal of Information Security*, Vol. 23, No. 2, pp. 1037-1054, 2024.
[22] A.A.E.B. Donkol, A.G. Hafez, A.I. Hussein, and M.M. Mabrook, "Optimization of intrusion detection using likely point PSO and enhanced LSTM-RNN hybrid technique in communication networks", *IEEE Access*, Vol. 11, pp.9469-9482, 2023.
[23] CICIDS-2018 Dataset: https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv/data (Accessed on October 2024)
[24] CICIDS-2019 Dataset: https://www.kaggle.com/datasets/tarundhamor/cicids-2019-dataset (Accessed on October 2024)
[25] NSL-KDD dataset : https://ieee-dataport.org/documents/nsl-kdd-0 (Accessed on November 2024)
[26] UNSW-NB15 dataset: https://research.unsw.edu.au/projects/unsw-nb15-dataset (Accessed on November 2024)
[27] J. Saikam, and K. Ch, "EESNN: hybrid deep learning empowered spatial-temporal features for network intrusion detection system", *IEEE Access*, Vol. 12, pp. 15930-15945, 2024.
[28] E. Dalirinia, M. Jalali, M. Yaghoobi, and H. Tabatabaee, "Lotus effect optimization algorithm (LEA): a lotus nature-inspired algorithm for engineering design optimization", *The Journal of Supercomputing*, Vol. 80, No. 1, pp. 761-799, 2024.
[29] Q. Zhang, R. Wang, Y. Qi, and F. Wen, "A watershed water quality prediction model based on attention mechanism and Bi-LSTM", *Environmental Science and Pollution Research*, Vol. 29, No. 50, pp. 75664-75680, 2022.