AIMS Mathematics, 11(2): 5062–5091.
DOI: 10.3934/math.2026207
Received: 05 December 2025
Revised: 28 January 2026
Accepted: 04 February 2026
Published: 27 February 2026

https://www.aimspress.com/journal/Math

Research article

Echo whale optimization-based incentive learning: A bidirectional long short-term memory model for intrusion detection in wireless networks

Afnan M. Alhassan* and Nouf I. Altmami

Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra 11961, Saudi Arabia

*** Correspondence:** Email: aalhassan@su.edu.sa.

Abstract: Intrusion detection distinguishes unauthorized system access by monitoring network activities, where identifiable patterns and behaviors are difficult to recognize due to factors such as false positives and negatives. The inability to work on large and complex networks, poor generalizability, high computation time, and the adoption of new threats that emerge over time are major concerns. Therefore, we established a model for handling the aforementioned challenges using the Echo whale optimization-incentive learning-based Bidirectional Long Short-Term Memory (EWO-IL-BiLSTM) model, which was proposed to improve the accuracy of intrusion detection. The EWO algorithm was incorporated to effectively tune the best parameters of the BiLSTM model to improve detection accuracy while increasing convergence speed and reducing false errors. Through incentive learning integration, the system demonstrated an award mechanism during training, which effectively captures the temporal dependencies in the network data and prompts the BiLSTM classifier to reach the best results. This research demonstrated that the benefits of the EWO and the Incentive Learning mechanism-based BiLSTM are a major advancement that improves the accurate intrusion detection, thereby promoting the network security and robustness in the ever-changing cyber-threat environments. The evaluation findings indicated that the proposed EWO-IL-BiLSTM model demonstrated superior performance with a high accuracy of 97.06%, F1-Score of 96.78%, precision of 97.59%, and recall of 95.98% at 80% training using the WSN-BFSF dataset.

Keywords: Echo whale optimization; incentive learning based BiLSTM; WSN; SMOTE; KNN imputation
Mathematics Subject Classification: 68M18, 68M25, 68T05, 68T07, 90C59

1. Introduction

Wireless sensor networks (WSNs) are described as less-infrastructure, being distributed, and used to monitor dynamic environments by placing multiple sensors [1]. Advances in technology, such as fog computing, have enhanced the capabilities of WSNs [2]. The Fog node is essential for enabling

mobility support, geo-distribution, locational awareness, and low latency in IoT applications [3]. Even though authentication protocols and secure routing protocols using cryptographic keys are in place to ensure secure data transmission [4], WSNs are susceptible to a range of threats, including passive attacks [5]. Various attacks targeting WSNs can undermine the network's operability, as conventional security measures do not offer sufficient protection [6]. Potential attacks on WSNs include routing attacks, Sybil attacks, and denial of service (DoS) attacks [7]. Intrusion Detection Systems (IDS) are implemented in WSNs to detect any suspicious and malicious behaviors exhibited by network nodes [8]. Cluster-based WSNs aim to lessen the performance strain by reducing the overall computation and energy consumption of nodes [9]. As WSNs become more prevalent in everyday life, ensuring the dependable performance of network nodes is essential for network security [10]. IDS-based systems are highly effective at pinpointing unusual actions by internal nodes, thereby shielding the network from malicious attacks [11]. IDS agents observe and analyze abnormal node behaviors over a specified time period before taking appropriate actions [12].

Compared to traditional wired networks, the cases of WSN are intricate and varied, which encounter several distinct issues and obstacles. To begin with, each sensor node has limited computing power and storage capacity, along with weak communication capabilities with other nodes [13]. Furthermore, the sensor nodes are frequently dispersed across large areas or challenging physical surroundings, which complicates maintenance duties related to energy provision [14]. In addition, the network has a constantly changing and unpredictable structure, further complicating matters [15]. Consequently, focused research is crucial to fulfill the real-time, energy-saving, and dependable operational needs of WSNs. Operating as a data-focused network, WSN gathers, retains, sends, and analyzes valuable information, intensifying its security implications [16]. Due to the constraints and attributes of WSNs, data is at risk of being compromised, stolen, or tampered with. Thus, finding effective ways to protect network security against attacks is a crucial area of research [17]. Dependence only on passive defenses like firewalls and access control is inadequate for stopping all network attacks. Intrusion detection is a proactive security solution that can monitor system activities to detect and counter intrusions, including internal and external attacks, as well as operational errors [18]. Wired network intrusion detection technology, which is established, includes misuse-based and anomaly-based detection methods. Misuse detection relies on predefined intrusion patterns to identify attacks, while anomaly detection looks for deviations from normal network behavior [19].

Although misuse detection is effective against known attack methods, it is not reliable for dealing with unknown attacks. To address the constant evolution of attacks, one potential solution is the implementation of anomaly detection. This method is based on the idea that cyber-attacks are not commonly seen compared to regular network activities [20]. By analyzing network behavior in comparison to standard patterns, it is possible to identify potential intrusions. While anomaly detection is effective in identifying unknown attacks, it requires a large amount of historical data for training. Researchers have looked into using artificial neural networks, machine learning, evolutionary computing, and other approaches for intrusion detection in WSN [8,10]. However, the unique characteristics and limitations of WSNs, such as small network size, limited computing power, storage capacity, energy resources, communication bandwidth, and networking modes, make it difficult to apply traditional intrusion detection system structures directly [14]. AI technology usually requires a lot of computing power and consumes a significant amount of running time, storage resources, and energy. Therefore, it is crucial to customize the WSN intrusion detection model to suit specific application scenarios and user requirements while maintaining a balance between security, energy usage, real-time capabilities, and other objectives.

This research innovatively contributes to the intrusion detection area through the utilization of effective preprocessing and feature extraction methods. Moreover, the Synthetic Minority Over-Sampling Technique (SMOTE) technique handles the data imbalance problem that smooths the intrusion detection process and reduces overfitting. The proposed model integrates EWO and Incentive Learning within a BiLSTM framework to enhance the detection accuracy and reduce complexity and false errors. Moreover, the introduction of Incentive Learning delivers a systematic means for rewarding model enhancement during the training period. The major contributions are as follows:

- **Echo whale optimization:** The integration of EWO in optimizing the parameters of BiLSTM makes the model more effective in extracting complex temporal dependencies, which enhances the convergence rate and reduces complexity. The merging of features of echolocation and collective intelligence is encompassed in the new EWO. Nevertheless, EWO would aim to incorporate the concepts of echolocation and strong team cooperation in order to improve its problem-solving strategies.
- **EWO-based IL-BiLSTM:** The incorporation of incentive learning utilizes the reward mechanism, with the BiLSTM model effectively extracting significant features, resulting in accurate intrusion detection with superior performance. It is more adaptable to network dynamics, enabling them to improve the decision-making ability of the model by capturing important temporal information. The benefits of these EWO algorithms and the IL based BiLSTM model is that they detect intrusions accurately and reduce computational complexity.

The research is well-organized, with Section 2 dedicated to the literature, discussing the methods and obstacles, and current efforts. In Section 3, we give a detailed description of the system model of WSN. The intrusion detection model's methodology, which incorporates the EWO-IL-BiLSTM model working, is elaborately discussed in Section 4. In Section 5, we explore the results achieved through the implementation of the EWO-IL-BiLSTM approach. Finally, in Section 6, a thorough analysis of the study's findings is presented.

2. Literature review

Gautam M. Borkar et al. [2] introduced a clustering method known as the adaptive chicken swarm optimization algorithm for selecting cluster heads (CH). This adaptive approach led to significant reductions in time consumption, as well as improvements in network lifetime and scalability. However, challenges related to computing power were encountered by this model. Jeng-Shyang Pan et al. [3] introduced a streamlined intelligent intrusion detection model for WSN that enhanced classification accuracy and decreased false alarms, effectively detecting different types of attacks, even unknown ones. However, storage space complexities remained a challenge for this model.

Mukaram Safaldin et al. [4] developed a more efficient intrusion detection system that combines a modified binary grey wolf optimizer with a support vector machine. This system aims to improve accuracy and detection rate, as well as reduce processing time in WSN settings by decreasing the occurrence of false alarms. However, this model may encounter significant security issues. Shuai Jiang et al. [5] introduced a Light GBM algorithm for detecting various network attacks, which led to improved accuracy and recall rates, decreased calculation time, and enhanced overall model performance. Nonetheless, this model experienced challenges with overfitting.

Safa Otoum et al. [6] introduced an ensemble classifier method for intrusion detection that outperformed models in terms of accuracy and detection. However, the model experienced a high number of false alarms, posing a significant challenge. In a study by Wenjie Zhang et al. [7], a hierarchical intrusion detection model was proposed for WSNs, which sorted nodes based on their

functions. This approach not only improved detection accuracy and reduced detection time but also proved to be suitable for WSNs with limited resources. Nonetheless, the model was impacted by high network energy consumption.

Gowdhaman and Dhanapal [8] created a system for detecting intrusions that relies on deep neural networks, which perform better than standard machine learning algorithms in identifying attacks with precision. The system excels in detecting attacks effectively and has a low rate of false alarms. Nevertheless, the model faces several computational obstacles. Singh et al. [9] emphasized the importance of quick detection and prevention of intrusions by utilizing machine learning with the Gaussian Process Regression (GPR) model. This approach achieved greater accuracy than other established methods but also faced computational hurdles.

Shaikh Afnan Birahim et al. [21] proposed an ensemble machine learning approach that incorporates random forest and K-Nearest Neighbors (KNN) models to enhance the intrusion detection performance. The integration of Particle Swarm Optimization (PSO) enhances the convergence rate and reduces errors. Moreover, the SMOTE-Tomek technique is used to handle the class imbalance issues. Although the model has high transparency and interpretability, it struggles with poor generalizability with limited resources. Abhilash Singh et al. [22] developed a fast intrusion detection and prevention model based on a fully connected feed-forward Artificial Neural Network (ANN) using the Gaussian and uniform sensor distribution methods. Hence, the model attained minimum computational complexity. However, the model failed to reduce false errors, which affected the model's performance.

2.1. Challenges

- The main security challenge in WSNs arises from the transmission of packets between sensor nodes in the network, along with data mining [2].
- Detecting suspicious behavior is made difficult by the irrelevant features and noises present in network traffic data, leading to a higher consumption of resources and a lower detection rate [3].
- Reducing false alarms in WSN intrusion detection systems is difficult because the increasing network traffic poses a challenge in conducting real-time data analysis for intrusion detection [4].
- Furthermore, intrusion detection methods in WSNs encounter difficulties like low detection accuracy, heightened computational workload, and a high number of false alarms. These challenges arise from limitations in sensor node capabilities, unnecessary duplication, and the close relationship between network information [5].
- Typically, a WSN consists of numerous small, inexpensive sensor nodes deployed in a specific area to collect data. The primary concern is ensuring the secure transmission of data packets [10].

2.2. Motivation

The intrusion detection models experience difficulties that deal with issues of handling the continuously changing attack patterns, balancing bad and good classification, scalability problems, the complexity of modern attacks, and the utilization of resources. Researchers deal with the challenges of intrusion detection model development by enhancing its accuracy using advanced algorithms. Hence, the proposed model is developed to overcome these limitations by utilizing advanced preprocessing, feature extraction, and data balancing techniques. Moreover, the incentive learning based BiLSTM

model is constructed by integrating the EWO algorithm to increase intrusion detection accuracy while reducing complexity.

3. System model

The structure of the WSN simulation includes an environment model that resembles the sensor networks in the real world. Often, this involves specifying the number of sensor nodes and their location, the communication protocols they use, and the kind of data they collect. The WSN is made up of a specific number of nodes. These nodes successfully transmit sensed data to the sink node B_h. The transmission pattern for each node is based on a consistent distribution, ensuring that data is spread using the strongest radio signal within the S_T and S_R dimensions in meters. Each node forms a cluster represented as D_T, with each cluster having an identical Cluster Head (CH) designated as U_D^T. CH-oriented routing is a recently developed approach for transferring data from multiple nodes to the Base Station (BS). The major benefits of this method are an enhanced lifespan and smooth flow of data within the system. However, WSNs are exposed to unauthorized access and intrusions; hence, an intrusion detection model is developed to detect these threats, which enhances the lifetime and reliability of data flow between nodes and sensors. Figure 1 shows the architecture of the WSN system model.

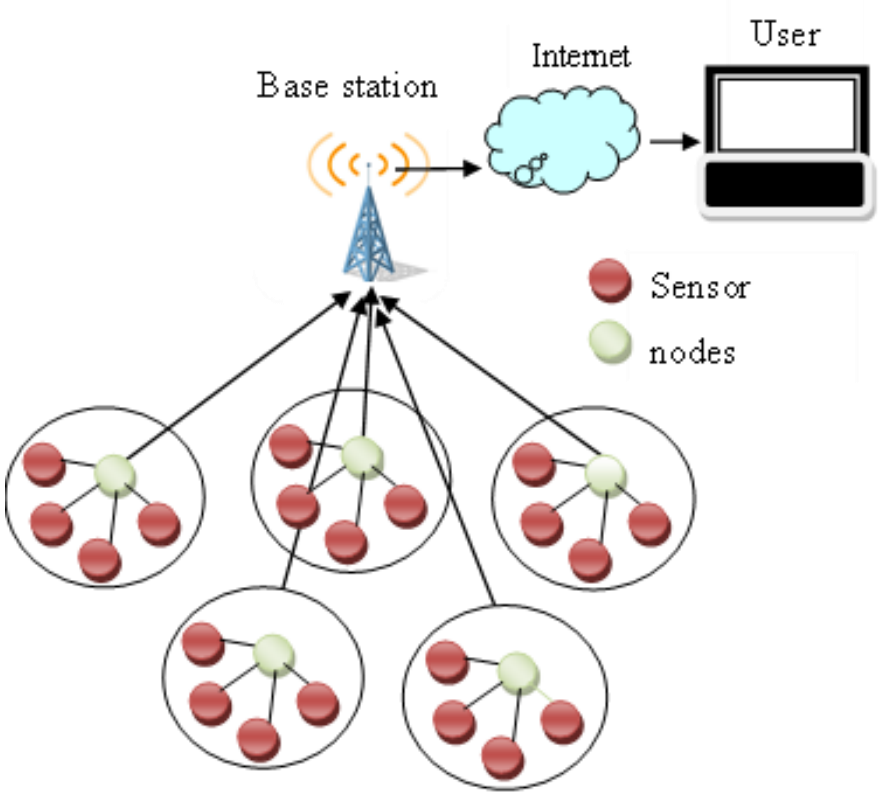


Figure 1. Architecture of the WSN system model.

4. Proposed methodology for intrusion detection using an incentive learning-Bidirectional LSTM model for intrusion detection

Our key goal of the research is the development of an effective intrusion detection system for WSNs. The traditional intrusion detection models struggle with high energy consumption, computation

complexity, overfitting, security issues, and false errors. Hence, the proposed model is developed using an incentive learning-based bidirectional LSTM model to overcome the limitations while attaining effective performance. At the beginning of our work, WSN simulations are collected from the datasets and processed with multiple preprocessing techniques. In this case, there can be a KNN imputation step for the missing values handling, normalization of the data to scale it, and the logarithmic transformation to achieve a proper data distribution. Eventually, the obtained data goes through a data balancing using the SMOTE technique, which is the method of synthetic minority oversampling, to balance the dataset with respect to classes. Subsequently, the balanced data is forwarded into an Optimized Incentive Learning-based Bidirectional Long Short-Term Memory (BiLSTM) model to complete the training phase. The incentive learning helps the model enhance the detection performance with a rewarding method. Specifically, if the accuracy is higher than 80%, a reward of 0.5 will be awarded, while if the accuracy is below this limit, the loss function will be increased by 0.5 to motivate further improvement in the model's performance. To achieve better performance, the model incorporates five BiLSTM models to extract significant features that help detect intrusion accurately. Moreover, the EWO algorithm is integrated with the proposed model, which fine-tunes the parameter weights of the BiLSTM model to obtain an optimal solution while reducing loss. Hence, the final output is generated through a dense layer, which produces the detected intrusions with multiple classes. Therefore, the benefits of these advanced techniques improve the model's performance and reduce complexity issues. This intrusion detection system has an exceptional level of accuracy and is capable of precisely pinpointing and classifying the intrusion events, thus enhancing the network security and reliability. Figure 2 explains the working flow of the EWO-IL-BiLSTM model for intrusion detection.

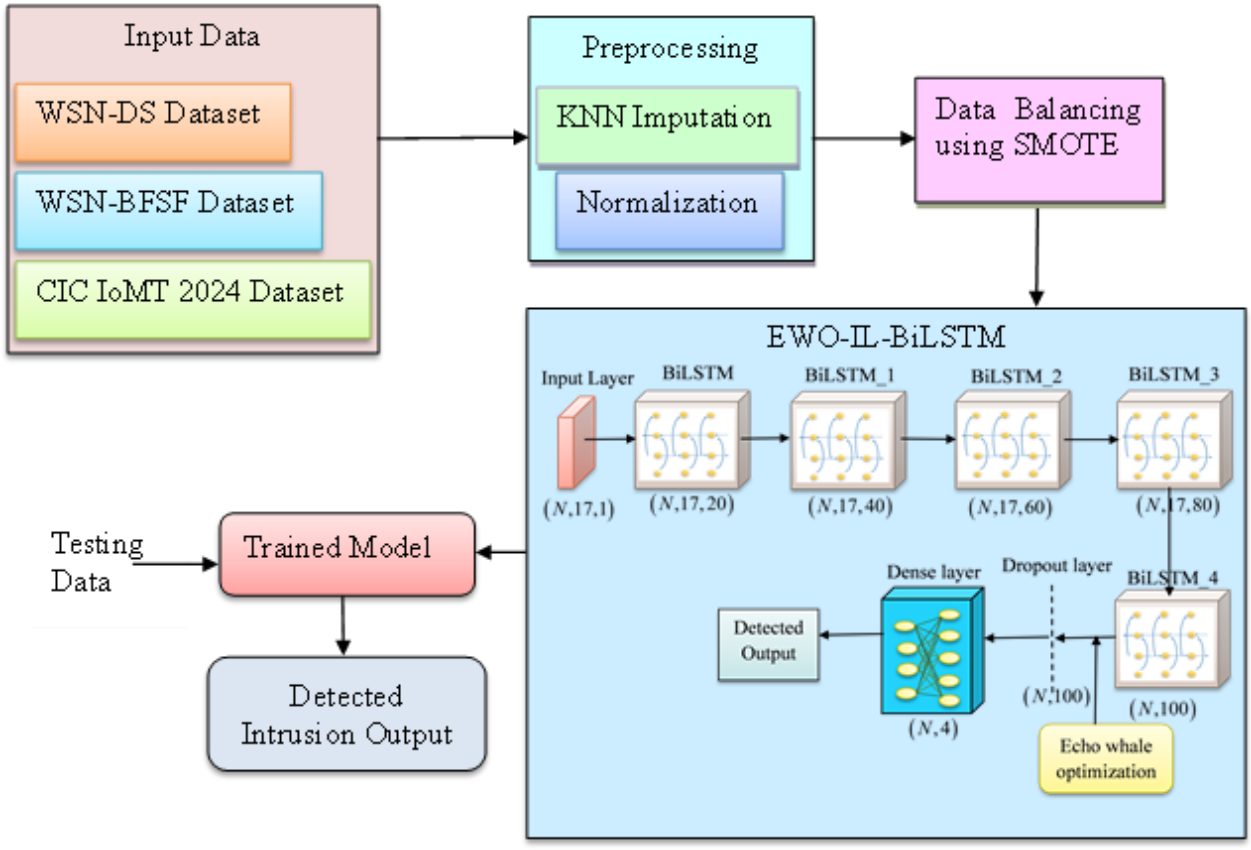


Figure 2. Architecture of the proposed EWO-IL-BiLSTM model for intrusion detection.

4.1. Input

Data is generated by simulating activities within the WSNs, including the movement of nodes, data transmission, and response to intrusion attempts. Such simulated events generate a dataset containing the ways WSNs operate under various situations. Then, the dataset is saved in the CSV file and used for further analysis. The input data utilized for detecting intrusions is derived from the WSN-DS dataset [23], WSN-BFSF dataset [24], and CIC IoMT 2024 dataset [25], and is expressed using the mathematical notation outlined below:

$$H = \sum_{n=1}^{t} H_m. \tag{1}$$

Here, H_m represents the database.

4.2. Pre-processing

Initially, the raw data collected from the dataset is processed and transformed into location-based data through the use of configuration data. This process involves eliminating unnecessary data as the target changes locations. Furthermore, the dataset contains gaps in the data. To address this, the KNN imputation technique is utilized to manage missing data effectively.

i) KNN Imputation. The presence of missing values in a dataset is a common problem in data analytics. One way to address this issue is to use advanced techniques to accurately predict the missing values with the help of a suitable data mining tool. Among various methods used for predicting missing values in datasets, the KNN imputation method has been identified as an effective approach. In this method, missing values are estimated by selecting k samples that closely resemble the sample being analyzed. The similarity between samples is determined by a distance function. To illustrate, imagine a dataset with missing values.

Separate the dataset into two groups: One called H_T, consisting of samples from the RSS matrix with at least one missing row, and the other called L_T, consisting of samples with complete data. Each RSS vector in H_T is divided into two parts: The missing portion and the observed portion. Compute the distance between the missing segments.

The dataset $i_p = \{i_{1p}, i_{2p}, \ldots\ldots i_{qp}\}$ has some missing values, while $i_L = \{i_{1L}, i_{2L}, \ldots\ldots i_{qL}\}$ represents the dataset with all values present. The distance between the data points is determined by a specific metric.

$$T_{Lp} = \left[\sum_{n=1}^{q} \left(i_{Lj} - i_{pj} \right)^2 \right]^{1/2}. \tag{2}$$

Here, T_{Lp} favors the Euclidean distance between i_L and i_p over other factors. The value of a variable j in a set i_L is represented by i_{jn}. The difference in distance is determined by the similarity factor D_{Lp}.

$$D_{Lp} = 1/T_{Lp}. \tag{3}$$

The calculated weight of the k sample vector is represented as F_{Lp}.

$$F_{Lp} = \frac{D_{Lp}}{\sum_{L=1}^{c} D_{Lp}}. \tag{4}$$

Here, F_{Lp} represents the weight of the sample i_L in comparison to the sample i_p. To estimate missing values for the specified attributes, the k-nearest neighbors (k closest sample vectors) are utilized in a weighted manner.

$$i_{pl} = \sum_{p=1}^{k} F_{Lp} i_{Ll}, (l = 1,.....q). \tag{5}$$

Here, i_{pl} represents the estimated missing values of variable l within the provided sample i_p. This concept is extended to all other variables when dealing with a multivariable situation. However, in our scenario, we consider only the single variable of a received signal strength.

ii) Normalization. In the intrusion detection dataset, there are nominal and non-normalized features. For those who rely on statistical features for learning, data normalization is an important initial step. Data normalization involves adjusting the values of each attribute to fit within a defined range to prevent one attribute from having a disproportionate influence. There are two major types of feature-based data normalization: Linear and non-linear methods and Logarithmic transformation to distribute the data.

Logarithmic means: Logarithmic transformation is applied to get a more symmetric distribution among data and underweight the effect of outliers. Moreover, a skew in sensor data might be more frequent in intrusion detection systems, where some readings or features can be represented by a few high or low data points. A logarithmic transformation is a suitable tool that eliminates the issues with the distribution of values because it compresses the dynamic range, especially for data points that have bigger magnitudes. By taking the logarithm of the data, the range of values is compressed, and extreme values are brought closer to the mean. This helps stabilize the variance of the data, making it more consistent and reducing the influence of outliers.

$$y_j^{'} = \log_{10}(y_j), \qquad j = 0,....., n-1. \tag{6}$$

4.3. Data balancing using SMOTE

Many learning algorithms are designed assuming equal distribution of class data or no significant variations in class probabilities. However, real-world data often has imbalanced class distributions, with one class being represented by only a few instances while the other has more. Research has shown that there can be as much as a 1% representation of the minority class and 99% or higher of the majority class. In such cases, classifiers generated by learning algorithms tend to prioritize the majority class, resulting in low error rates overall but ineffective performance when it comes to accurately predicting the rare instances in the minority class. Various concepts expand upon an algorithmic method to address class disparities by modifying algorithms and techniques to account for the distinct characteristics of biased outcomes. These principles encompass cost-sensitive training, one-class classification, and classifier ensembles. The objective of cost-sensitive learning is to reduce the costs associated with misclassification. Hence, the SMOTE method is utilized to balance the input data.

SMOTE: The SMOTE is a technique for over-sampling minority data by generating synthetic examples. The main idea is to create new instances of minority classes by interpolating between examples. Specifically, SMOTE randomly selects a group F_k and its neighbors, and generates a new example by using an equation involving the closest neighbor F_k.

$$F_{new} = F_k + (F_k - F_k)\delta. \tag{7}$$

In a randomly selected interval $(0,1)$, where δ is fixed, SMOTE can expand the minority class's area by creating synthetic instances that extend further into the space of the dominant class, enabling the closest neighbor to potentially be from a different class than F_k. An illustration of the SMOTE method is provided in Figure 3, where the sample y_k from the minority class serves as the foundation for generating new synthetic data points. By focusing on a selected distance metric, multiple nearest neighbors of the same class (points F_{k_1} to F_{k_4}) are chosen, and simultaneous interpolation is utilized to create new samples t_1 to t_4.

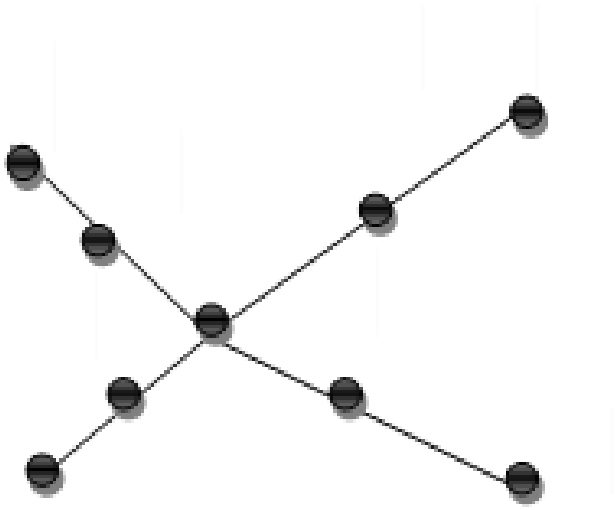


Figure 3. An illustration of how the SMOTE algorithm creates synthetic data points.

4.4. Working with optimized incentive learning based BiLSTM

After the completion of handling the class imbalance problem, the obtained input data with dimension $(N,17,1)$ is forwarded to the optimized incentive learning based BiLSTM model. The proposed model adopts IL techniques into the structure of BiLSTM networks, which will be helpful for better detection and classification of intrusions. During training, the model's performance accuracy is continually checked, and rewards are assigned based on its performance. When the output exceeds a predetermined threshold, a lower reward is given, while a higher reward is given if the output falls below the threshold, thus encouraging a higher performance. This stimulates a dynamically self-adaptive process and furnishes a means for harnessing BiLSTM capabilities of bidirectional processing to the forefront to detect intrusion attempts that have long-term dependencies that may be seen in sequential data. The proposed EWO-IL-BiLSTM model employs five BiLSTM models with a dense layer to extract important features that influence the intrusion detection. The input data is extracted through multiple BiLSTMs and generates the output with dimensions $(N,17,20)$, $(N,17,40)$, $(N,17,60)$, and $(N,17,80)$, and the BiLSTM_4 produces the output with dimension $(N,100)$. Moreover, the EWO algorithm is integrated in this layer to adjust the parameters to obtain a high detection performance and enhance the convergence rate while minimizing false errors. The data is then applied to a dense layer, where the detected output is generated with a dimension $(N,4)$. Therefore, the combinations of the incentive learning approach, BiLSTM, and EWO employed in the model make it more durable and responsive while increasing its ability to accurately work out and

categorize intrusion incidents, which strengthens network security. Figure 4 explains the architecture of the EWO-IL-BiLSTM model for intrusion detection.

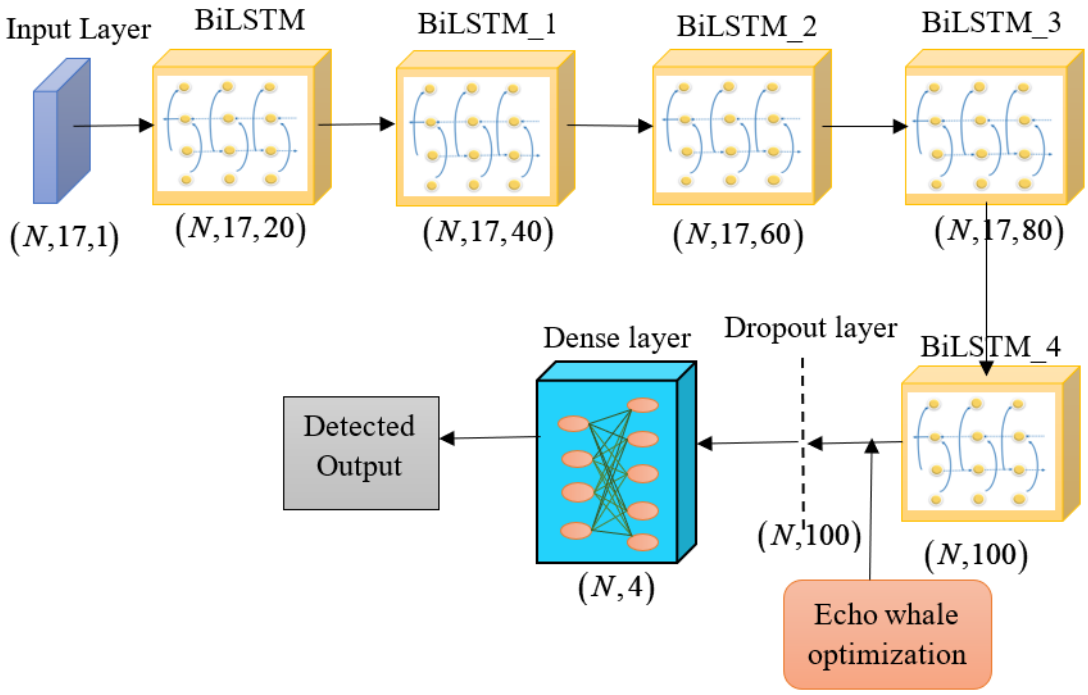


Figure 4. Architecture of the proposed EWO-IL-BiLSTM model.

i) BiLSTM

The BiLSTM model processes input sequences in forward and backward directions through multiple hidden layers. In contrast, BiLSTM links all hidden layers to one output layer.

The BiLSTM network determines the output sequences of the forward $\vec{f}(t)$ and backward $\overleftarrow{f}(t)$ hidden layers, as well as the output layer, by iterating through the forward layer from $t=1$ to t_u and the backward hidden layer from $t=t_u$ to 1. The final values are updated using the equations provided:

$$\vec{f}(t)=F\left(W_{i}^{\rightarrow}T_t+U_{i}^{\rightarrow}f_{i}^{\rightarrow}(t-1)+b_{i}^{\rightarrow}\right), \tag{8}$$

$$\overleftarrow{f}(t)=F\left(W_{i}^{\leftarrow}T_t+U_{i}^{\leftarrow}f_{i}^{\leftarrow}(t-1)+b_{i}^{\leftarrow}\right), \tag{9}$$

$$x(t)=V_{i}^{\rightarrow}f_{i}^{\rightarrow}+V_{i}^{\leftarrow}f_{i}^{\leftarrow}(t)+b_x. \tag{10}$$

In this scenario, the weight matrix for the forward hidden layer is labeled as $W_{i}^{\rightarrow}$, the input at time step t is denoted as T_t, $U_{i}^{\rightarrow}$ represents the weight matrix for the connections from the previous forward hidden state to the current one, $f(t-1)$ is used to represent the previous forward state, $b_{i}^{\rightarrow}$ is the term for the bias in the forward layer, and the activation function is represented as σ. Similarly, for the backward hidden layer, the weight matrix is labeled as $W_{i}^{\leftarrow}$, $U_{i}^{\leftarrow}$ represents the weight

matrix for connections from the previous backward hidden state to the current one, $f(t-1)$ is the previous backward state, and $b\overleftarrow{}_i$ is the bias term for the backward layer.

The final result vector $x(t)$ is computed as

$$x(t) = \sigma_x\left(\vec{f}, \overleftarrow{f}\right). \tag{11}$$

The outcome at time step t is identified as $x(t)$, the collective function is denoted as σ_x, and the result of the forward hidden layer is labeled as $\vec{f}$, while the output of the backward hidden layer is referred to as $\overleftarrow{f}$. The σ_x function blends the output sequences of the neurons within the hidden layers.

ii) Integration of incentive learning

Incentive learning is a technique used to obtain important features using reward learning and tunes the model parameters based on reward feedback, which is incorporated into the BiLSTM model to enhance the decision-making ability. Hence, the reward learning with the BiLSTM model for intrusion detection is linked with a new loss function, including a reward term, which is expressed as

$$Loss = -\frac{1}{n}\sum_{j=1}^{n}\left[x_j \log\left(\hat{x}_j\right) + (1-x_j)\log\left(1-\hat{x}_j\right)\right] + \alpha J. \tag{12}$$

Here, the total loss is denoted as $Loss$, the number of total samples is denoted as n, the sample j true label is denoted as x_j, for sample j, the probability predicted is denoted as $\hat{x}_j$, the incentive term weighting factor is denoted as α, and the reward obtained based on the performance of the model is J.

The reward value J can be related to pre-set accuracy channels in this regard. If the accuracy exceeds a threshold, a lower reward can be assigned, and if it falls below, a higher reward can be assigned. By adjusting the loss function with incentive learning, the model is incentivized to not only minimize classification loss of Mean Squared Error (MSE), but also maximize rewards based on its performance. This enables the model to strive toward greater accuracy anytime it updates, increasing its capacity to correctly identify and classify intruder events in terms of an intrusion detection system architecture that incorporates a BiLSTM neural network.

4.5. Echo whale optimization

The nature-based algorithms tune the detection models for better performance. The traditional algorithms struggled with certain limitations such as poor convergence, local optimal solutions, and high false errors. Hence, the EWO algorithm is developed to overcome these limitations and enhance the performance of the proposed model while maintaining minimum loss. EWO aims to design a novel optimization framework utilizing the unique capacities of whales [26] and dolphins [27] by joining key features of these species. Through a convergence of the echolocation behaviors of dolphins with the food detection techniques of whales, EWO creates a holistic approach that includes the precision and coordination of dolphin pods, characterized by the strategic behavior of whales. This mixed-up nature increases the autonomy and ability of the algorithm to search for solutions as well as execute them very smoothly compared to other methods, boosting its capability to search in complex search spaces and, consequently, returning the best solutions for many problem situations.

4.5.1. Inspiration

The EWO algorithm harnesses the collective intelligence of two remarkable marine creatures: Dolphins and whales. Dolphins, renowned for their intelligence and social behavior, excel in utilizing echolocation to encircle and capture prey effectively, often living in cohesive groups to enhance their hunting success. Moreover, their method of hunting differs from those of whales and, being highly intelligent mammals, dolphins take advantage of sophisticated techniques such as food isolation through bubble-netting and food shrinking to successfully catch food. The developments of EWO are most probably inspired by the great behaviors of these wonderful creatures and how they function in their natural habitat. Dolphins are credited with their smartness, squad interactions, and information transmission skills that include echolocation to explore their space and discover food. Whales, on the contrary, have gained worldwide fame due to the highly advanced social activities that they undertake, including bubble net feeding, which is a process where they work together to isolate and eat fish. By using concepts of echolocation behavior to explore or encircle prey for exploitation, EWO not only reflects the intelligence and cooperation of the dolphins and whales as we know, but also demonstrates the interaction of dolphins and whales vocally.

The EWO algorithm is mathematically formulated in the following section.

i) Initialization

Initialization is the process of generating a random initial solution from the search space, and a random population solution is mathematically termed as

$$X_t = X_{rand} + C_t(u - l). \tag{13}$$

Here, u and l denote the upper and the lower bounds, and C_t denotes the communicative factor at the t^{th} iteration.

ii) Fitness evaluation

In this optimization, the multi-objective fitness function is utilized to achieve an optimal solution. The multi-objective fitness function is the ensemble of precision, accuracy, and recall metrics in intrusion detection. Accuracy examines the overall correctness; precision assesses the ability of the model to minimize the false positives, and recall evaluates the capability of the model to capture the critical things. Merging these metrics with an averaging measure enables us to avoid the tendencies of bias in the assessment by considering correct classification types and an error category. This fitness evaluation maximizes the precision, accuracy, and recall to get a good model that succeeds in multitasking, with low accuracy errors, and clear decisions in different scenarios of applications.

$$Fitness(X_t) = \max\left(\frac{accuracy + precision + recall}{3}\left(X^{t+1}\right)\right). \tag{14}$$

iii) Solution update

Case 1) Scanning phase: $if\ |E_l| < |A_E|$.

The scanning phase involves cetaceans measuring the sound reception amount that food sources probably emit compared to the average amount of sound reception by predators. It uses sound scanning to detect the presence of any prey as it operates on a radar or echolocation system.

E_l denotes the sound reception level using echolocation by the food and A_E denotes the average level of sound reception by the predator. Moreover, $A_E \cong 0.5$ shows that the sound received from the food to the cetacean is less than the average level of sound reception. Thus, the position of the cetacean is mathematically explained as

$$X^{t+1} = 0.5\left[X_{rand} - AD\right] + 0.5\left[X_g + W_t\right], \tag{15}$$

$$A = 2\vec{a}.r - \vec{a}\ ,\ r = \frac{1}{a}\ ,\ C = 2r\quad ;\ a \in (2 \to 0).$$

Here, the cetacean's new position is denoted as $X^{t+!}$, A is represented as a coefficient vector, a is represented as a minimal factor, r represented as a reciprocal factor, C is denoted as a quantity factor with a random number (0,1), X_g denotes the global best solution, and w_t denotes the direction attribute of sound at t.

$$D = \left|CX_{rand} - X_{prey}\right|. \tag{16}$$

Here, D represents the distance factor, X_{prey} denotes the prey's position, and X_{rand} denotes the random position of the solution.

Case 2) Manipulation phase: $if\ |E_l| \geq |A_E| \& |E_l| \leq |T_s|$.

In response to detecting enough predators in the vicinity of food, the whale begins to reduce its internal amount of water to optimize the flow and inner energy while maintaining a high possibility of hunting. By fusing information exchange with the shrinkage mechanism, the cetacean improves its feeding strategy, which enables it to efficiently use the food sources nearby and spare energy outflow. This phase of manipulation showcases the adaptive skills and social interactions of cetaceans, showing how they adjust their behavior strategically to enhance their hunting success based on environmental signals.

Here, T_s denotes the safety threshold level for sound signal reception. This condition shows that the cetacean receives an equal amount of average level sound reception signal, showing that there is a sufficient amount of food nearby. Thus, the cetacean uses the shrinking mechanism along with information exchanging characteristics, so we get

$$X^{t+1} = \frac{1}{2}\left[D_1 e^{bl}.\cos(2\pi rlk) + X_g^t\right] + \frac{1}{2}\left[Xp + w_t\right], \tag{17}$$

$$D_1 = \left|X_g^t - X_{prey}^t\right|.$$

Here, b denotes the logarithmic spiral term shape, l represents the size of the food $\varepsilon[-1,1]$, r bubble factor, D_1 represents the distance factor, k denotes the time matrix (time required to reach the prey by the predator), X_p denotes the personal best, and w_t denotes the direction attribute of sound.

Case 3) Absconding phase: $if\ |E_l| > |A_E|$ and $|E_l| \geq T_s$.

During the escape phase, the cetacean promptly reacts to perceived dangers to the group's safety by using evasive tactics and notifying other members. This phase illustrates the cetacean's keen awareness of its environment and its ability to organize group responses to threats, underscoring the significance of collective defense mechanisms in guaranteeing the pod's survival.

T_s denotes the safety threshold level for sound signal reception. This condition shows if the received sound signal indicates danger is coming (any intruders or threats) to the pod (group) and so on. The solution alerts all members by sending an alert signal and escaping from the threat.

$$X^{t+1} = 0.5\left[X_g^t - AD\right] + 05\left[X^t(0.5) + \left(X^{t-1} - X^{t-2}\right)1.359\right]. \tag{18}$$

Here, the group's global best solution is denoted as X_g^t, the current position is denoted as X_t, and previous positions are denoted as X_{t-1}, X_{t-2}.

iv) Termination phase

Finally, the optimization terminates the iterative process upon reaching the optimal solution with the condition $t < t_{\max}$. Otherwise, the solution is re-evaluated to obtain the optimal solution. Hence, the global solution is declared, resulting in improved intrusion detection performance. Figure 5 shows the flowchart of the proposed Echo whale optimization.

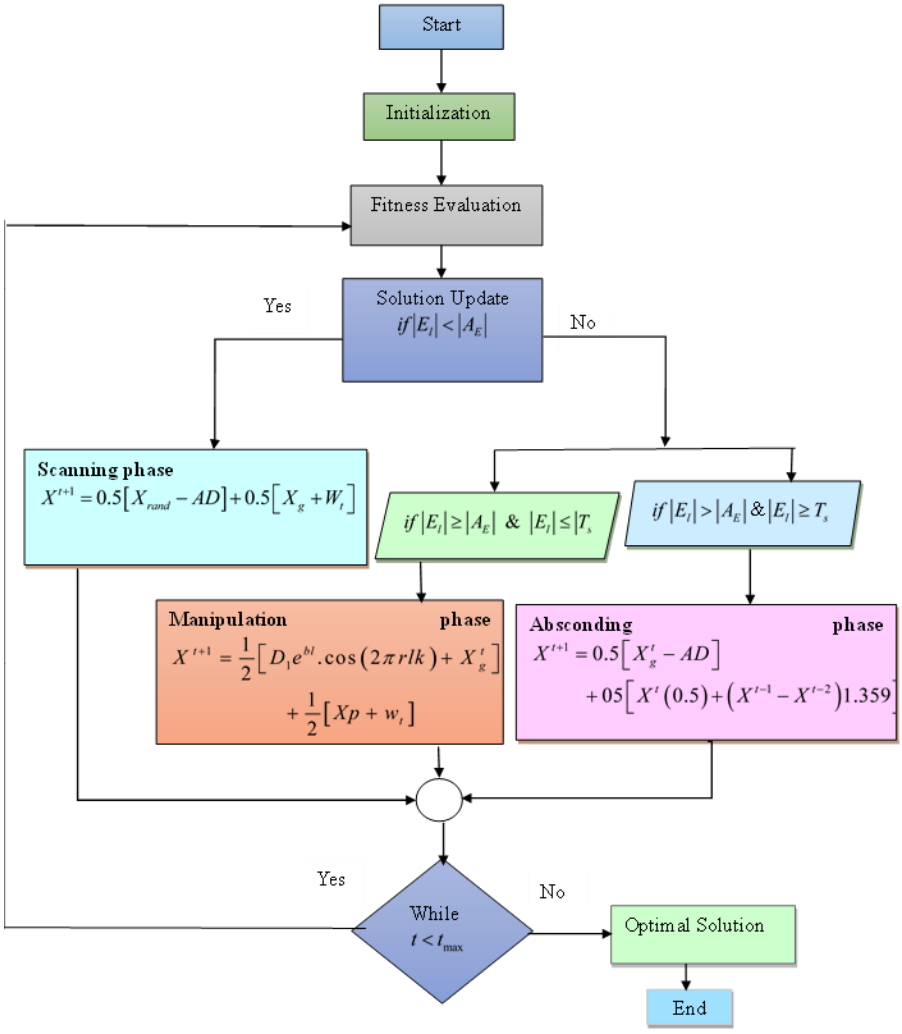


Figure 5. Flowchart for proposed Echo whale optimization.

5. Result and discussion

Our purpose of this research is to develop an intrusion detection system utilizing EWO- IL-BiLSTM. The effectiveness of the model is evaluated by comparing it to other models in terms of performance.

5.1. Experimental setup

An intrusion detection task is performed by a Python program on a computer operating on a Windows 11 system with 16GB of RAM and 128GB of ROM with the Python 3.8 programming

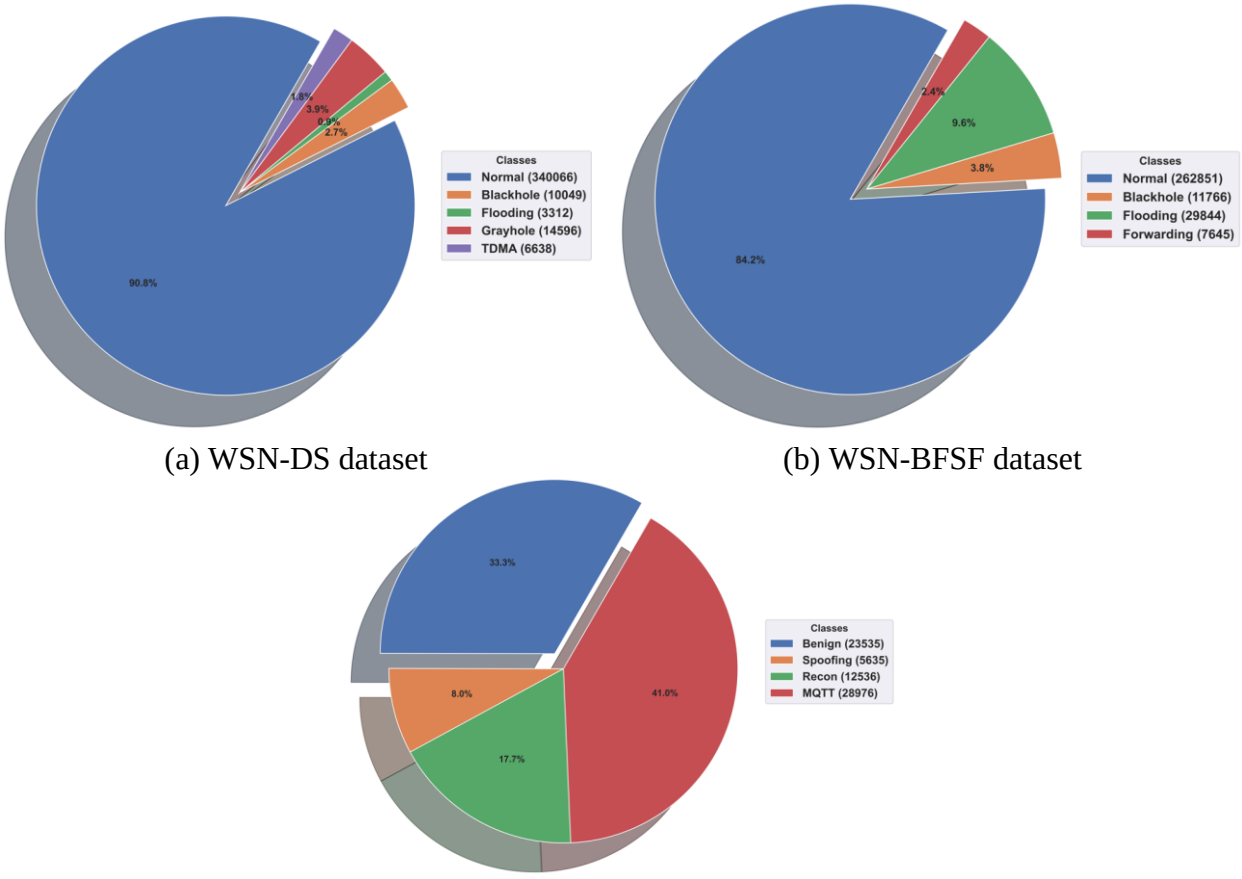
language. The initial parameter settings of the proposed framework involve a batch size of 32, a learning rate of 0.001, a dropout rate of 0.2, a ReLU activation function, loss function "MSE", Metrics 'Accuracy', number of BiLSTM layers 5, population size of 50, and default optimizer Adam. In this research, the proposed model utilizes input data in a certain train-test split ratio, such as 40:60, 50:50, 60:40, 70:30, and 80:20. Here, the proposed model obtains the highest performance using an 80% training and 20% testing split and a 10-fold cross-validation for the multiple datasets.

5.2. Dataset description

i) WSN-DS Dataset [23]: The WSN-DS dataset is designed to detect intrusions in WSNs, which comprises 19 characteristics and 374,661 entries that illustrate various forms of Denial of Service (DoS) attacks, such as Black hole, gray hole, Flooding, and Scheduling attacks.

ii) WSN-BFSF Dataset [24]: The WSNBFSF dataset includes Black Hole, Flooding, and Selective Forwarding attacks, all known as forms of DDoS attacks. By conducting necessary pre-processing, a dataset containing 16 attributes and 312,106 instances is extracted from the original dataset.

iii) CIC IoMT 2024 Dataset [25]: This dataset includes DDoS, DoS, Recon, MQTT, and spoofing attacks, which are collected from the security of healthcare devices connected to the Internet of Medical Things (IoMT). The dataset comprises 18 cyberattacks related to 40 IoMT devices in healthcare, such as Wi-Fi, MQTT, and Bluetooth. In this research, a total of 70,682 instances are extracted from the dataset. The datasets visualization is presented in Figure 6.



(a) WSN-DS dataset

(b) WSN-BFSF dataset

(c) CIC IoMT 2024 dataset

Figure 6. Dataset visualization.

5.3. Comparative methods

An assessment is carried out to showcase the achievements of the EWO-IL-BiLSTM model, comparing it with other techniques such as Ensemble Model [21], Feed-forward ANN [22], CNN [28], CNN-LSTM [29], IL-BiLSTM [30], WOA-IL-BiLSTM [26], DEO-IL-BiLSTM [27], DNN [31], and SMOTE-TomekLink [32].

5.3.1. Comparative analysis based on TP for the WSN-DS dataset

The proposed EWO-IL-BiLSTM model is evaluated with other models based on multiple training percentages using the WSN-DS Dataset, which is illustrated in Figure 7. At 80% training, the proposed model obtains a high detection accuracy of 96.89%, which is 9.86% greater than the DNN model. Similarly, the proposed model achieves a F1-Score of 96.88%, which is 10.06% higher than the DNN model. The proposed model attains a high precision of 97.37% and outperforms the DNN model with 9.5% improvement rate. Moreover, the recall value of 96.4% is obtained by the proposed model with 11.71% improvement over the DNN model. Specifically, the integration of the EWO algorithm enhances the convergence rate of the proposed EWO-IL-BiLSTM model for intrusion detection.

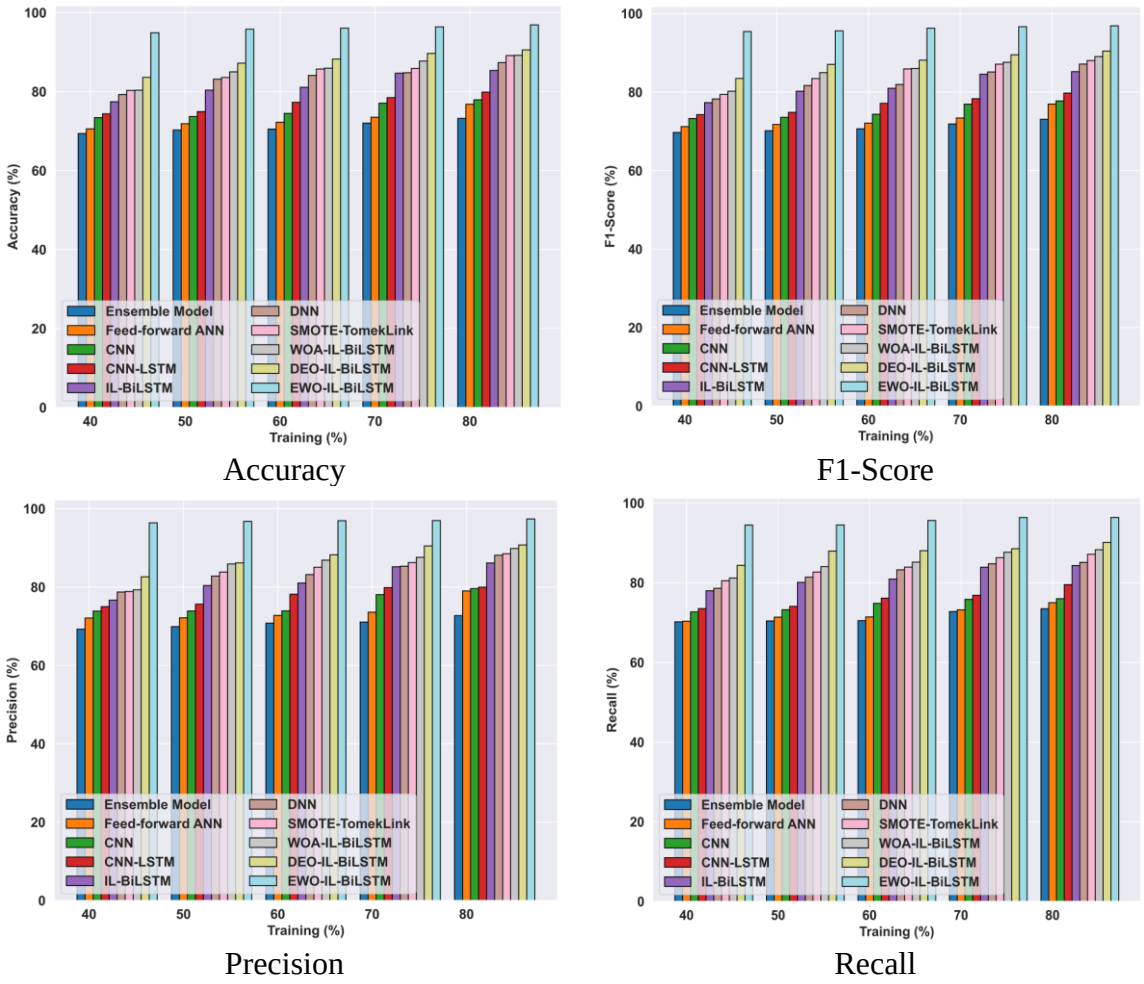


Figure 7. Comparative analysis based on TP for the WSN-DS dataset.

5.3.2. Comparative analysis based on TP for the WSN-BFSF dataset

The proposed EWO-IL-BiLSTM model is evaluated with other models based on multiple training percentages using the WSN-BFSF dataset, which is illustrated in Figure 8. At 80% training, the proposed model obtains a high detection accuracy of 97.06%, which is 11.09% greater than the DNN model. Similarly, the proposed model achieves a F1-Score of 96.78%, which is 10.6% higher than the DNN model. The proposed model attains a high precision of 97.59% and outperforms the DNN model with 11.06% improvement rate. Moreover, the recall value of 95.98% is obtained by the proposed model with 11.11% improvement over the DNN model. Specifically, the integration of the EWO algorithm enhances the convergence rate of the proposed EWO-IL-BiLSTM model for intrusion detection and outperforms other models.

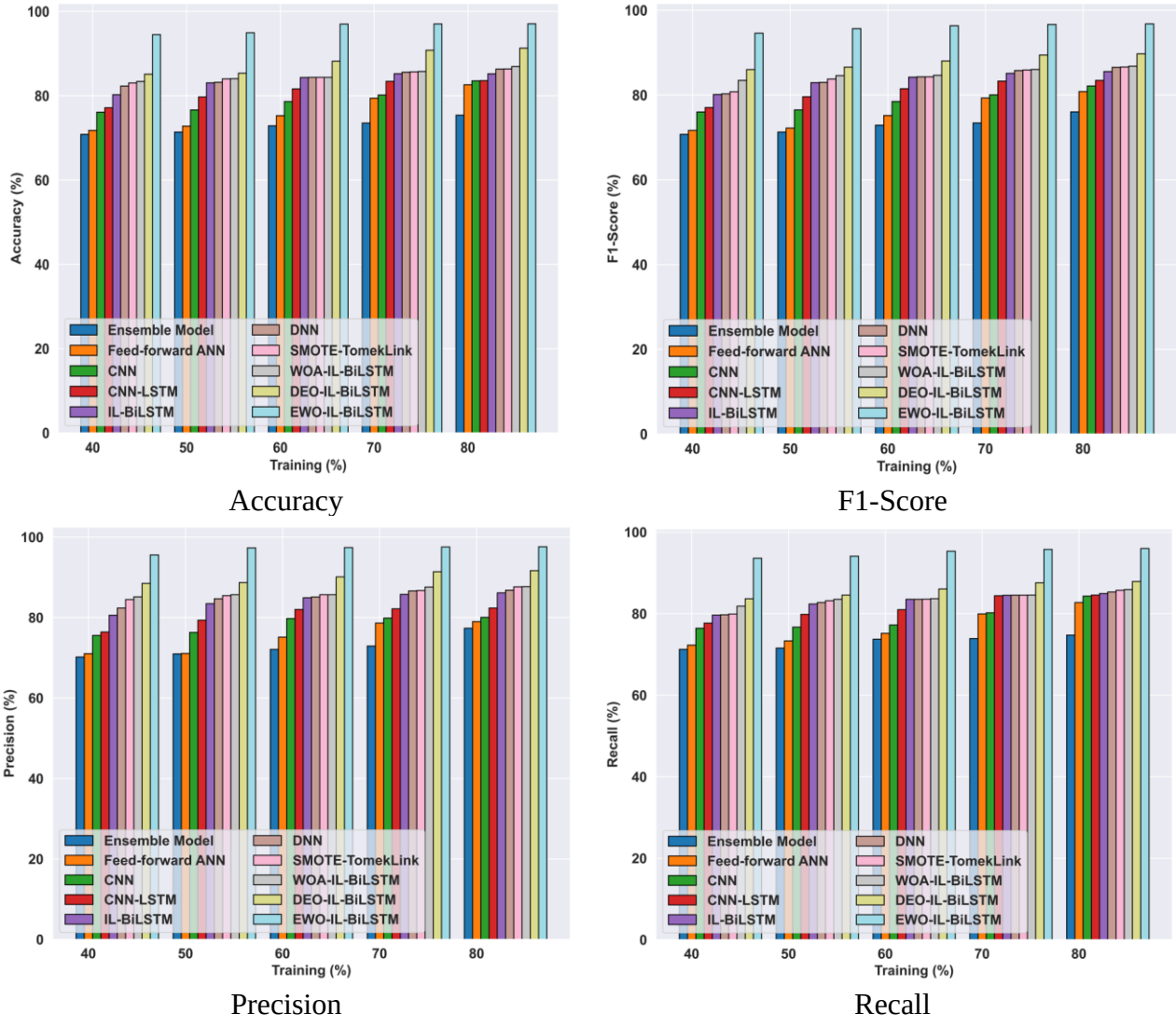


Figure 8. Comparative analysis based on TP for the WSN-BFSF dataset.

5.3.3. Comparative analysis based on TP for the CIC IoMT 2024 dataset

The proposed EWO-IL-BiLSTM model is evaluated with other models based on multiple training percentages using the CIC IoMT 2024 Dataset, which is illustrated in Figure 9. At 80% training, the

proposed model obtains a high detection accuracy of 96.95%, which is 10.5% greater than the DNN model. Similarly, the proposed model achieves a F1-Score of 96.85%, which is 10.65% higher than the DNN model. The proposed model attains a high precision of 97.45% and outperforms the DNN model with 9.86% improvement rate. Moreover, the recall value of 96.26% is obtained by the proposed model with 11.4% improvement over the DNN model. Specifically, the integration of the EWO algorithm enhances the convergence rate of the proposed EWO-IL-BiLSTM model for intrusion detection and outperforms other models.

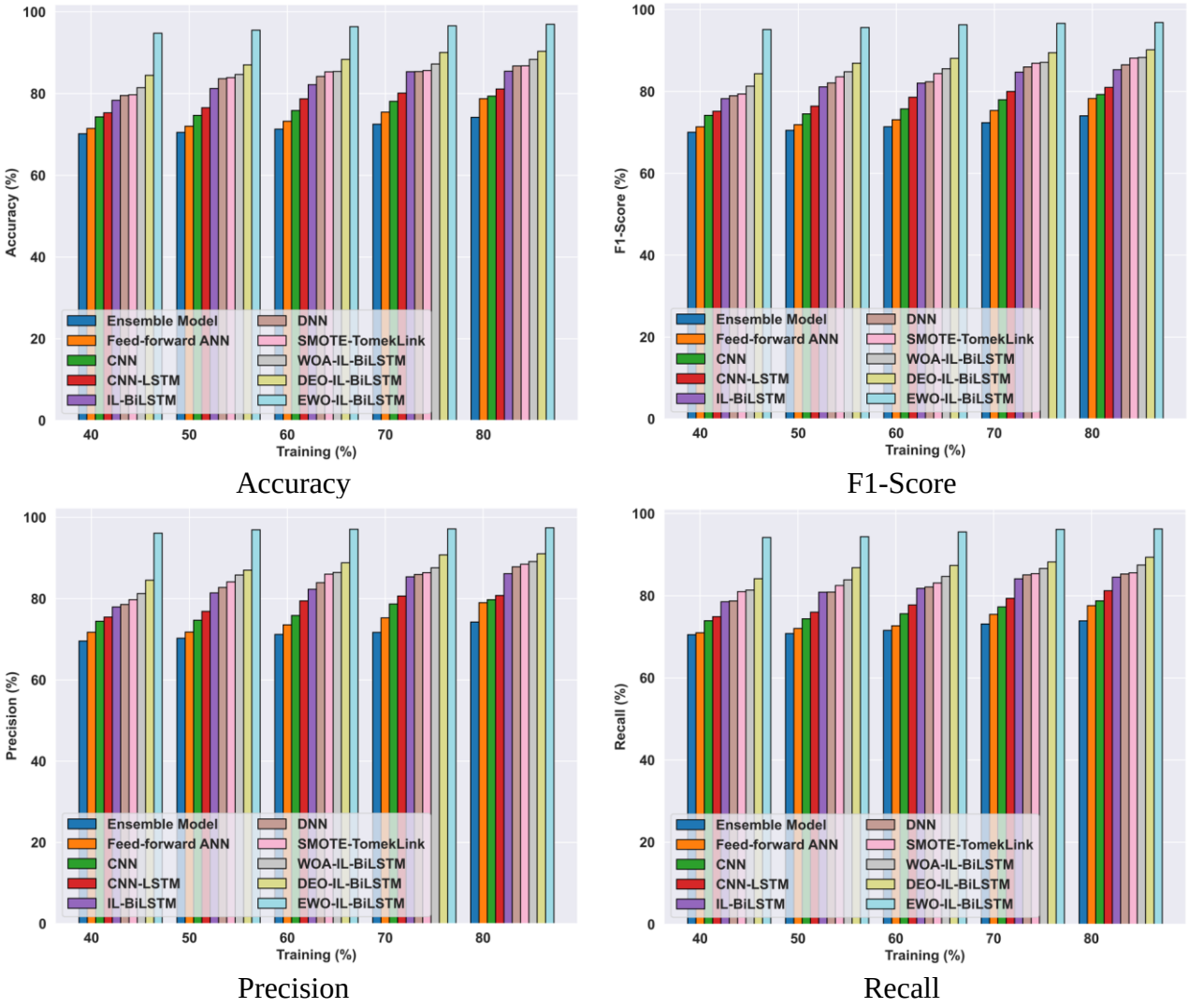


Figure 9. Comparative analysis based on TP for the CIC IoMT 2024 dataset.

5.3.4. Comparative analysis based on K-fold for the WSN-DS dataset

The proposed EWO-IL-BiLSTM model is evaluated with other models based on multiple k-fold values using the WSN-DS dataset, which is illustrated in Figure 10. At a 10-fold value, the proposed model obtains a maximum accuracy of 96.58%, which is 8.25% greater than the DNN model. Similarly, the proposed model achieves a F1-Score of 96.91%, which is 9.38% higher than the DNN model. The proposed model attains a high precision of 97.82% and outperforms the DNN model with 8.77% improvement rate. Moreover, the recall value of 96.02% is obtained by the proposed model with 7.99% improvement over the DNN model. Specifically, the integration of the EWO algorithm enhances the

convergence rate of the proposed EWO-IL-BiLSTM model for intrusion detection and outperforms other models.

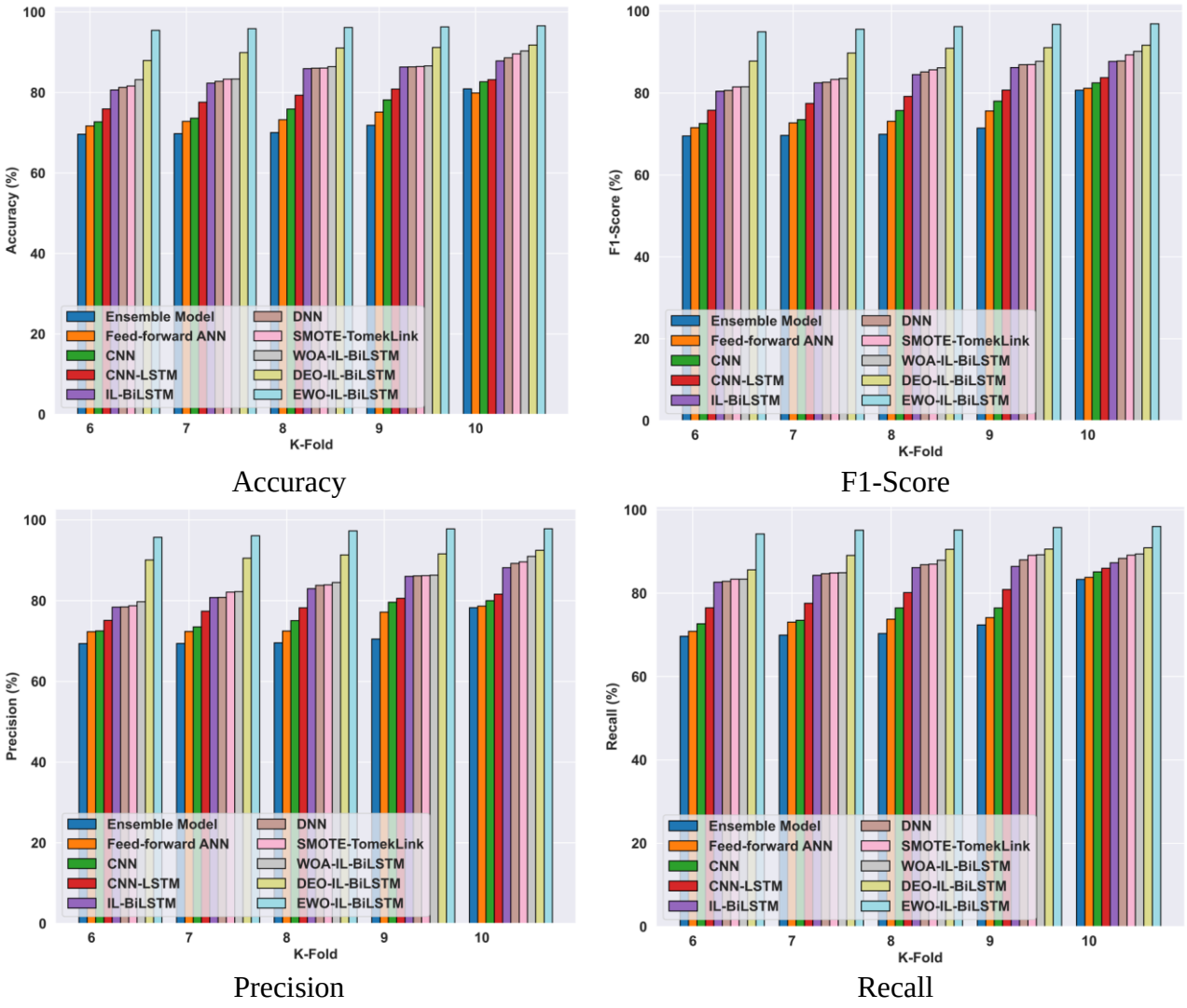


Figure 10. Comparative analysis based on k-fold for the WSN-DS dataset.

5.3.5. Comparative analysis based on K-fold for the WSN-BFSF dataset

The proposed EWO-IL-BiLSTM model is evaluated with other models based on multiple k-fold values using the WSN-BFSF dataset, which is illustrated in Figure 11. At a 10-fold value, the proposed model obtains a maximum accuracy of 96.87%, which is 13.93% greater than the DNN model. Similarly, the proposed model achieves a F1-Score of 96.42%, which is 12.38% higher than the DNN model. The proposed model attains a high precision of 97.09% and outperforms the DNN model with 15.6% improvement rate. Moreover, the recall value of 95.75% is obtained by the proposed model with 10.26% improvement over the DNN model. Specifically, the integration of the EWO algorithm enhances the convergence rate of the proposed EWO-IL-BiLSTM model for intrusion detection and outperforms other models.

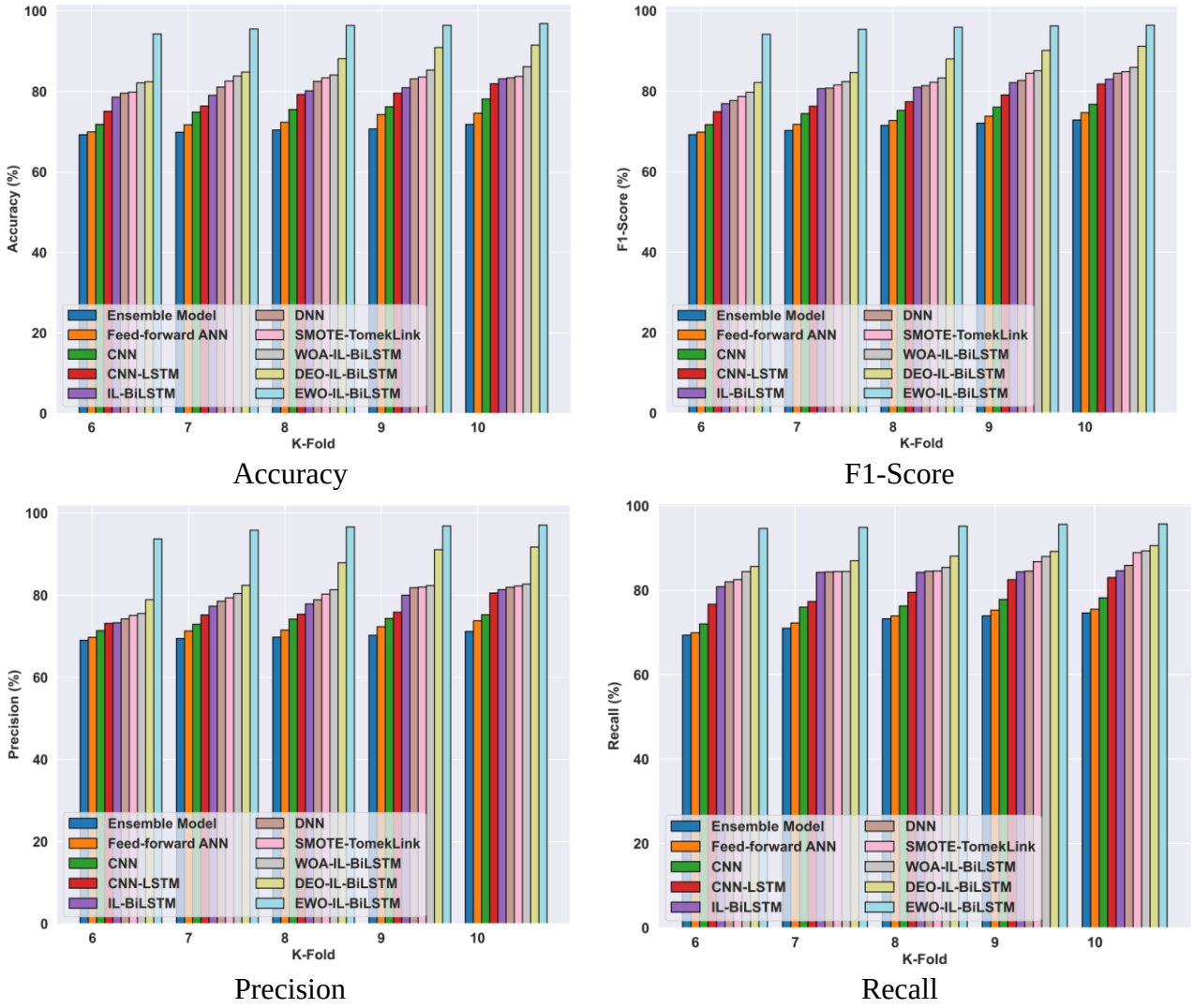


Figure 11. Comparative analysis based on k-fold for the WSN-BFSF dataset.

5.3.6. Comparative analysis based on K-fold for the CIC IoMT 2024 dataset

The proposed EWO-IL-BiLSTM model is evaluated with other models based on multiple k-fold values using the CIC IoMT 2024 Dataset, which is illustrated in Figure 12. At a 10-fold value, the proposed model obtains a maximum accuracy of 96.68%, which is 10.04% greater than the DNN model. Similarly, the proposed model achieves a F1-Score of 96.75%, which is 10.64% higher than the DNN model. The proposed model attains a high precision of 97.58% and outperforms the DNN model with 10.91% improvement rate. Moreover, the recall value of 95.93% is obtained by the proposed model with 8.14% improvement over the DNN model. Specifically, the integration of the EWO algorithm enhances the convergence rate of the proposed EWO-IL-BiLSTM model for intrusion detection and outperforms other models.

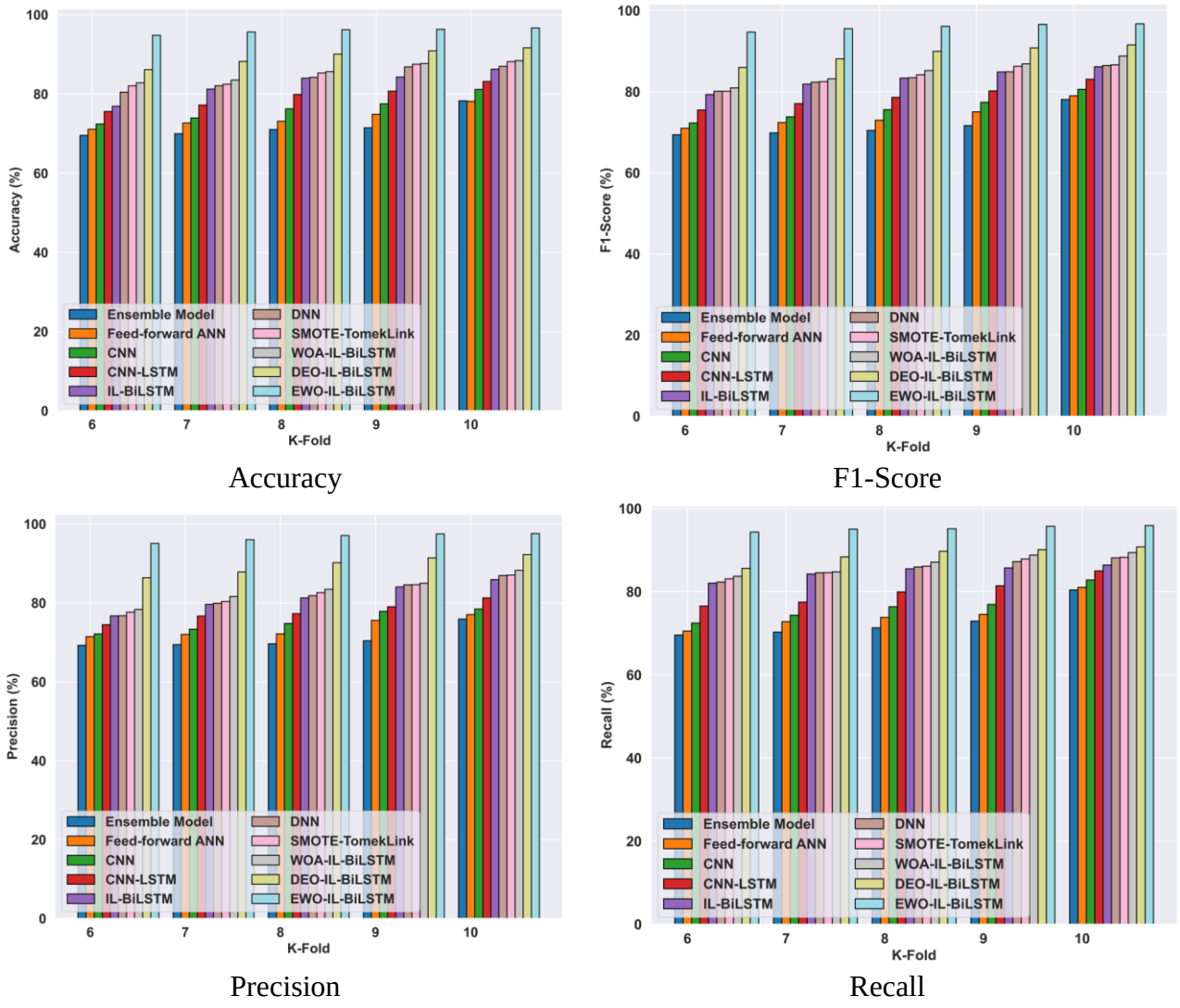
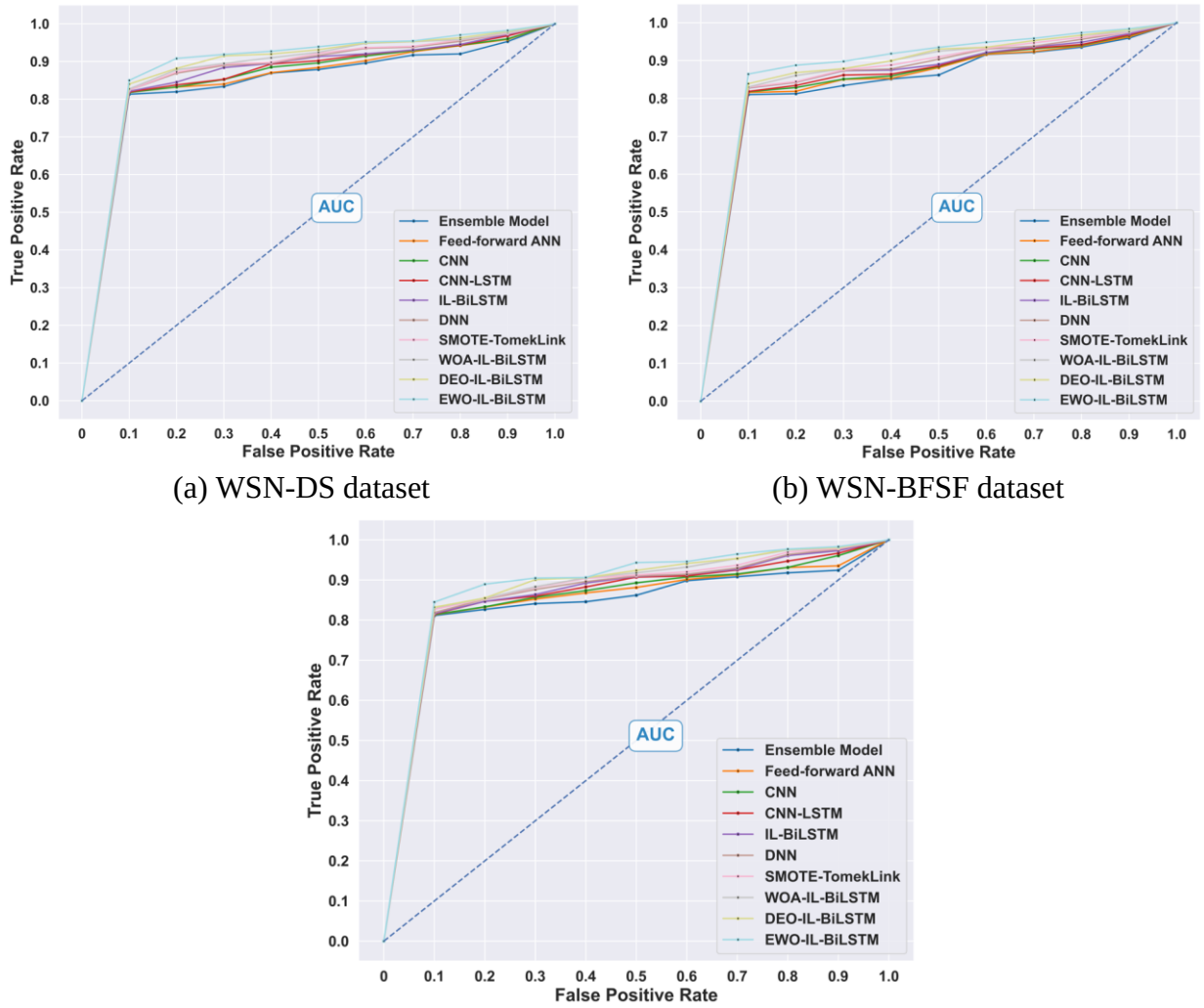


Figure 12. Comparative analysis based on k-fold for the CIC IoMT 2024 dataset.

5.4. ROC analysis

The ROC analysis is conducted using three databases, the WSN-DS, WSN-BFSF, and CIC IoMT 2024 dataset, which range from 0 to 1, as depicted in Figure 13. Evaluation results show that the proposed model gains high sensitivity for intrusion detection based on the true positive rate (TPR) and false positive rate (FPR). The proposed model attains a high TPR of 1 and outperforms other models, such as the Ensemble Model of 0.85, Feed-forward ANN of 0.91, CNN of 0.92, CNN-LSTM of 0.93, IL-BiLSTM of 0.94, DNN of 0.95, SMOTE-TomekLink of 0.96, WOA-IL-BiLSTM of 0.95, and the DEO-IL-BiLSTM of 0.97 for the WSN-DS dataset. The developed approach demonstrates superior performance compared to the techniques with a score above 0.985. The ROC analysis using these datasets demonstrates that the accuracy of the proposed detection model is better than the methods, which is mainly due to the improved learning and convergence rates.



(a) WSN-DS dataset

(b) WSN-BFSF dataset

(c) CIC IoMT 2024 dataset

Figure 13. ROC analysis.

5.5. Comparative discussion

Models that deal with the detection of intrusion in WSN are facing many difficulties in the accurate recognition of intrusion events in these networks. The models have data complexity, poor generalizability, and high computation time and energy. Indeed, in terms of the diversity of data as well as the complexity of modern networks, data breaching is complicated by further challenges in effective intrusion detection. In addition, traditional optimization algorithms could face issues in fine-tuning parameters for the optimal performance of WSN. Hence, the newly proposed EWO-based IL-BiLSTM model can address these shortcomings by incorporating IL with a BiLSTM model, which acquires intricate patterns and time dependencies hidden in the data that help in accurate intrusion detection while reducing false errors. The proposed model surpasses the challenges and brings about a superior intrusion detection capability to the WSNs compared to other models. Specifically, the evaluation with multiple and diverse datasets improves the generalizability of the model in unseen data. The proposed model attains superior performance at 80% of training and 10-fold in cross-validation. Furthermore, the proposed EWO-IL-BiLSTM model achieves a high accuracy of 97.06%, an F1-score of 96.78%, a precision of 97.59%, and a recall of 95.98% based on TP. Similarly, the model attains a

high accuracy of 96.87%, F1-Score of 96.42%, precision of 97.09%, and recall of 95.75% based on K-fold using the WSN-BFSF dataset. Tables 1–3 explain the evaluation results of the proposed model and compare them with other models using multiple datasets.

Table 1. Comparative discussion table using the WSN-DS dataset.

Methods/Metrics	WSN-DS dataset							
	TP-80				K-fold 10			
	Accuracy	F1-Score	Precision	Recall	Accuracy	F1-Score	Precision	Recall
Ensemble Model [21]	73.21	73.09	72.71	73.48	80.91	80.71	78.26	83.32
Feed-forward ANN [22]	76.79	76.95	79.01	75.01	79.90	81.15	78.66	83.81
CNN [28]	77.92	77.76	79.61	76.00	82.68	82.49	80.02	85.12
CNN-LSTM [29]	79.88	79.76	79.98	79.54	83.19	83.74	81.61	85.99
IL-BiLSTM [30]	85.35	85.22	86.15	84.31	87.85	87.73	88.17	87.29
DNN [31]	87.34	87.14	88.12	85.12	88.61	87.83	89.25	88.35
SMOTE-TomekLink [32]	89.13	88.06	88.50	87.14	89.62	89.35	89.62	89.12
WOA-IL-BiLSTM [26]	89.19	89.06	89.85	88.28	90.33	90.20	90.99	89.43
DEO-IL-BiLSTM [27]	90.56	90.43	90.74	90.13	91.80	91.68	92.48	90.89
EWO-IL-BiLSTM	**96.89**	**96.88**	**97.37**	**96.40**	**96.58**	**96.91**	**97.82**	**96.02**

Table 2. Comparative discussion table using the WSN-BFSF dataset.

Methods/Metrics	WSN-BFSF dataset							
	TP-80				K-fold 10			
	Accuracy	F1-Score	Precision	Recall	Accuracy	F1-Score	Precision	Recall
Ensemble Model [21]	75.38	76.02	77.34	74.76	71.82	72.87	71.18	74.63
Feed-forward ANN [22]	82.62	80.82	79.00	82.73	74.60	74.66	73.81	75.53
CNN [28]	83.52	82.13	80.05	84.31	78.12	76.74	75.29	78.24
CNN-LSTM [29]	83.58	83.45	82.37	84.55	81.93	81.79	80.58	83.03
IL-BiLSTM [30]	85.21	85.53	86.13	84.94	83.14	82.98	81.38	84.65
DNN [31]	86.30	86.52	86.79	85.32	83.38	84.48	81.95	85.92
SMOTE-TomekLink [32]	86.34	86.60	87.63	85.74	83.74	84.86	82.25	88.96
WOA-IL-BiLSTM [26]	86.93	86.80	87.70	85.92	86.16	85.91	82.73	89.35
DEO-IL-BiLSTM [27]	91.29	89.72	91.64	87.88	91.52	91.18	91.78	90.59
EWO-IL-BiLSTM	**97.06**	**96.78**	**97.59**	**95.98**	**96.87**	**96.42**	**97.09**	**95.75**

Table 3. Comparative discussion table using the CIC IoMT 2024 dataset.

Methods/ Metrics	WSN-BFSF dataset							
	TP-80				K-fold 10			
	Accuracy	F1-Score	Precision	Recall	Accuracy	F1-Score	Precision	Recall
Ensemble Model [21]	74.20	74.08	74.25	73.90	78.28	78.10	75.90	80.42
Feed-forward ANN [22]	78.73	78.28	79.00	77.58	78.14	79.00	77.04	81.05
CNN [28]	79.38	79.26	79.76	78.77	81.16	80.57	78.44	82.83
CNN-LSTM [29]	81.11	80.99	80.77	81.21	83.16	83.09	81.27	85.00
IL-BiLSTM [30]	85.45	85.33	86.14	84.52	86.28	86.16	85.90	86.41
DNN [31]	86.77	86.54	87.84	85.29	86.97	86.46	86.93	88.12
SMOTE-TomekLink [32]	86.78	88.16	88.48	85.56	88.17	86.64	87.03	88.27
WOA-IL-BiLSTM [26]	88.38	88.31	89.14	87.49	88.43	88.81	88.23	89.40
DEO-IL-BiLSTM [27]	90.33	90.20	91.04	89.38	91.64	91.51	92.25	90.79
EWO-IL-BiLSTM	**96.95**	**96.85**	**97.45**	**96.26**	**96.68**	**96.75**	**97.58**	**95.93**

5.6. Statistical analysis

The statistical significance analysis of the proposed EWO-IL-BiLSTM model is evaluated with other models to evaluate the model's statistical significance for intrusion detection. Here, the proposed model is evaluated based on the T-statistic values and the P-value based on performance metrics. Specifically, the proposed EWO-IL-BiLSTM model achieves p-values below 0.05, indicating that the results are statistically significant. The statistical analysis of the EWO-IL-BiLSTM model using the WSN-DS, WSN-BFSF, and CIC IoMT 2024 datasets is depicted in Table 4.

Table 4. T-test analysis.

Models / Metrics			Ensemble Model	Feed-forward ANN	CNN	CNN-LSTM	IL-BiLSTM	DNN	SMOTE-TomekLink	WOA-IL-BiLSTM	DEO-IL-BiLSTM	**EWO-IL-BiLSTM**
WSN-DS Dataset	**Accuracy**	T-Statistic	2.49	2.29	2.06	2.53	2.98	3.40	3.17	3.51	3.51	3.34
		P-value	0.07	0.08	0.11	0.06	0.04	0.03	0.03	0.02	0.02	0.03
	F1-Score	T-Statistic	2.24	1.81	2.09	2.52	2.99	2.99	3.47	3.55	3.52	2.64
		P-value	0.09	0.14	0.10	0.07	0.04	0.04	0.03	0.02	0.02	0.04
	Precision	T-Statistic	2.53	1.40	1.62	2.63	3.03	3.17	3.51	3.72	3.35	3.15
		P-value	0.06	0.23	0.18	0.06	0.04	0.03	0.02	0.02	0.03	0.03
	Recall	T-Statistic	1.88	2.34	2.73	2.33	2.91	3.36	3.00	3.18	3.64	2.34
		P-value	0.13	0.08	0.05	0.08	0.04	0.03	0.04	0.03	0.02	0.04

Continued on next page

Models / Metrics			Ensemble Model	Feed-forward ANN	CNN	CNN-LSTM	IL-BiLSTM	DNN	SMOTE-TomekLink	WOA-IL-BiLSTM	DEO-IL-BiLSTM	**EWO-IL-BiLSTM**
WSN-BFSF Dataset	**Accuracy**	T-Statistic	2.43	2.25	2.16	3.26	3.62	2.77	2.78	2.36	2.32	2.83
		P-value	0.07	0.09	0.10	0.03	0.02	0.05	0.05	0.08	0.08	0.03
	F1-Score	T-Statistic	2.29	2.27	2.32	3.26	3.55	3.33	3.45	2.81	2.62	3.53
		P-value	0.08	0.09	0.08	0.03	0.02	0.03	0.03	0.05	0.06	0.02
	Precision	T-Statistic	2.00	2.28	2.80	3.51	3.57	3.43	2.77	2.28	2.39	3.97
		P-value	0.12	0.08	0.05	0.02	0.02	0.03	0.05	0.08	0.07	0.02
	Recall	T-Statistic	2.59	2.21	1.71	2.87	3.54	3.57	3.56	3.09	2.77	2.87
		P-value	0.06	0.09	0.16	0.05	0.02	0.02	0.02	0.04	0.05	0.04
CIC IoMT 2024 Dataset	**Accuracy**	T-Statistic	2.14	2.04	2.19	2.83	3.11	3.59	3.71	3.35	3.33	3.21
		P-value	0.10	0.11	0.09	0.05	0.04	0.02	0.02	0.03	0.03	0.03
	F1-Score	T-Statistic	2.28	2.08	2.19	2.82	3.16	3.04	3.36	3.45	3.35	3.06
		P-value	0.08	0.11	0.09	0.05	0.03	0.04	0.03	0.03	0.03	0.04
	Precision	T-Statistic	2.27	1.88	2.10	3.00	3.18	3.33	3.53	3.62	3.20	3.73
		P-value	0.09	0.13	0.10	0.04	0.03	0.03	0.02	0.02	0.03	0.02
	Recall	T-Statistic	2.21	2.28	2.29	2.59	3.12	2.95	2.87	3.18	3.48	2.54
		P-value	0.09	0.09	0.08	0.06	0.04	0.04	0.05	0.03	0.03	0.03

5.7. Computational complexity analysis

The computational time complexity analysis is conducted to examine the time required for the proposed EWO-IL-BiLSTM model to perform intrusion detection. Figure 14 illustrates the computational time analysis of the proposed model compared with other models for multiple iterations. At the 100^{th} epoch, the proposed model is evaluated and achieves a minimum computation time of 123.04 seconds. However, other models need a high computational time of 123.79s with the Ensemble Model, Feed-forward ANN of 123.10s, CNN of 123.16s, CNN-LSTM of 123.25s, IL-BiLSTM of 123.27s, DNN of 123.36s, SMOTE-TomekLink of 123.46s, WOA-IL-BiLSTM of 123.58s, and DEO-IL-BiLSTM of 123.79s.

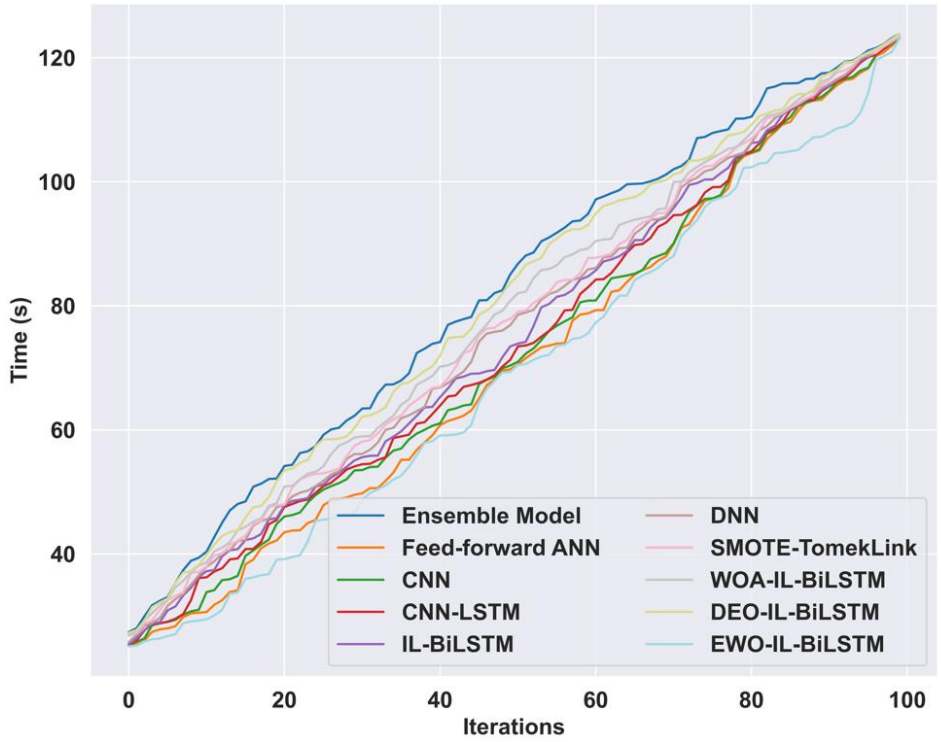
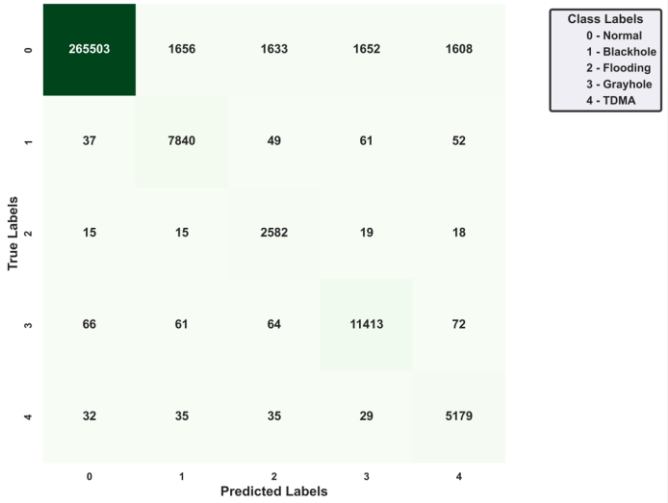


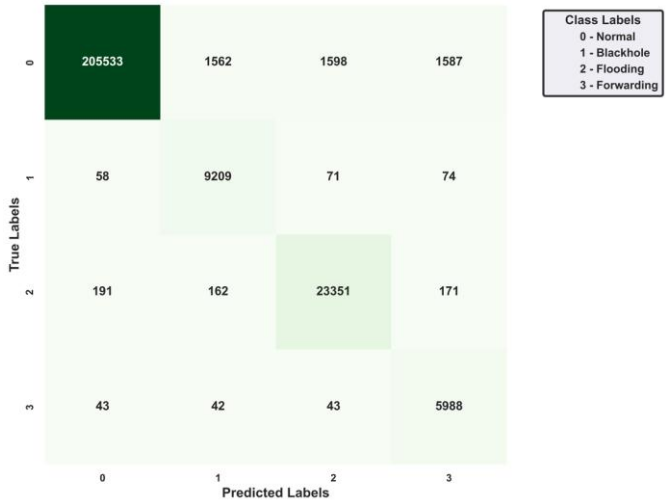
Figure 14. Computational complexity analysis.

5.8. Confusion matrix

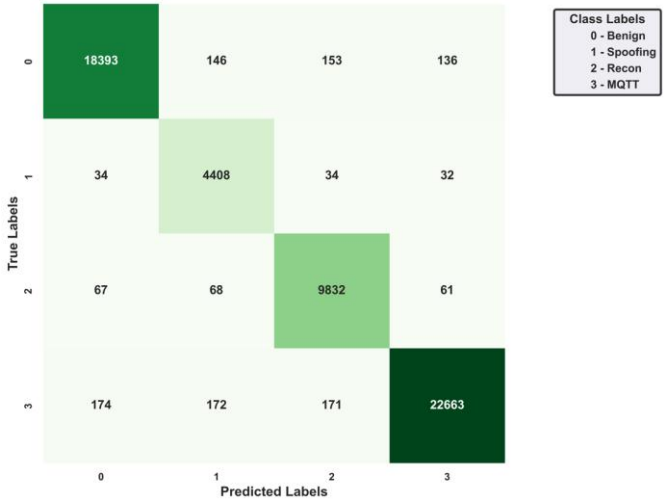
The confusion matrix is used to visualize the intrusion detection capabilities of the proposed EWO-IL-BiLSTM model using the WSN-DS, WSN-BFSF, and CIC IoMT 2024 datasets. It compares the predicted labels with the labels of the dataset to identify accurate and inaccurate detections. The EWO-IL-BiLSTM model detects the input data into five classes, such as 0-Normal, 1-Blackhole, 2-Flooding, 3-Grayhole, and 4-TDMA using the WSN-DS dataset. Similarly, the model predicts four classes with the WSN-BFSF and CIC IoMT 2024 datasets. Here, the proposed EWO-IL-BiLSTM model correctly detects 18393 data as Benign, 4408 as Spoofing, 9832 as Recon, and 22663 as MQTT and incorrectly predicted a few data points using the CIC IoMT 2024 dataset. Comparatively, the proposed model incorrectly detects a very small amount of data. Hence, the proposed EWO-IL-BiLSTM model effectively performs intrusion detection from WSNs. Figure 15 illustrates the confusion matrix of the proposed EWO-IL-BiLSTM model.



(a) WSN-DS dataset



(b) WSN-BFSF dataset



(c) CIC IoMT 2024 dataset

Figure 15. Confusion matrix.

6. Conclusions

In this research, we introduce an innovative approach to intrusion detection systems through the integration of EWO and incentive learning within a BiLSTM framework. The EWO algorithm process enhances the model's ability to capture complex temporal dependencies in network data. Additionally, the incorporation of incentive learning introduces a reward-based mechanism during model training, encouraging continuous performance improvement. By synergistically leveraging EWO and incentive learning, the proposed method addresses critical challenges in intrusion detection, achieving superior accuracy and robustness compared to traditional approaches. The EWO-based incentive learning for BiLSTM represents a significant advancement in intrusion detection technology, promising enhanced security and resilience in dynamic cyber threat landscapes. The findings indicate that the proposed

models demonstrate strong performance in both scenarios, with the WSN-BFSF dataset achieving a metric value accuracy of 97.06%, F1-Score of 96.78%, precision of 97.59%, and recall of 95.98% at 80% training. Moreover, setting up the real-world implementation and monitoring processes is critical in the system design to favor the stages of WSN intrusion detection. Furthermore, incorporating hybrid, explainable DL techniques will be the main focus of future research to enhance model performance.

Author contributions

Afnan M. Alhassan: Conceptualization, methodology, data curation, formal analysis, investigation, writing – original draft, visualization; Nouf I. Altmami: Validation, supervision, writing – review & editing, project administration, resources. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Data availability and access

This study utilizes publicly accessible datasets, namely the WSN-DS Dataset [23], WSN-BFSF Dataset [24], and CIC IoMT 2024 Dataset [25].

Acknowledgments

The authors would like to thank the Deanship of Scientific Research at Shaqra University for supporting this work.

Conflicts of interest

The authors declare no conflict of interest.

References

1. G. M. Borkar, L. H. Patil, D. Dalgade, A. Hutke, A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept, *Sustain. Comput.: Inform. Syst.*, **23** (2019), 120–135. https://doi.org/10.1016/j.suscom.2019.06.002
2. J. S. Pan, F. Fan, S. C. Chu, H. Q. Zhao, G. Y. Liu, A lightweight intelligent intrusion detection model for wireless sensor networks, *Secur. Commun. Netw.*, **2021** (2021), 5540895. https://doi.org/10.1155/2021/5540895
3. M. Safaldin, M. Otair, L. Abualigah, Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks, *J. Ambient Intell. Human. Comput.*, **12** (2021), 1559–1576. https://doi.org/10.1007/s12652-020-02228-z
4. S. Jiang, J. Zhao, X. Xu, SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments, *IEEE Access*, **8** (2020), 169548–169558. https://doi.org/10.1109/ACCESS.2020.3024219

5. S. Otoum, B. Kantarci, H. T. Mouftah, A novel ensemble method for advanced intrusion detection in wireless sensor networks, In: *Icc 2020-2020 IEEE international conference on communications (icc)*, Ireland: IEEE, 2020. https://doi.org/10.1109/ICC40277.2020.9149413
6. W. Zhang, D. Han, K. C. Li, F. I. Massetto, Wireless sensor network intrusion detection system based on MK-ELM, *Soft Comput.*, **24** (2020), 12361–12374. https://doi.org/10.1007/s00500-020-04678-1
7. V. Gowdhaman, R. Dhanapal, An intrusion detection system for wireless sensor networks using deep neural network, *Soft Comput.*, **26** (2022), 13059–13067. https://doi.org/10.1007/s00500-021-06473-y
8. A. Singh, J. Nagar, S. Sharma, V. Kotiyal, A Gaussian process regression approach to predict the k-barrier coverage probability for intrusion detection in wireless sensor networks, *Expert Syst. Appl.*, **172** (2021), 114603. https://doi.org/10.1016/j.eswa.2021.114603
9. A. Mehmood, S. Khan, B. Shams, J. Lloret, Energy-efficient multi-level and distance-aware clustering mechanism for WSNs, *Int. J. Commun. Syst.*, **28** (2015), 972–989. https://doi.org/10.1002/dac.2720
10. A. Mehmood, J. Lloret, S. Sendra, A secure and low-energy zonebased wireless sensor networks routing protocol for pollution monitoring, *Wirel. Commun. Mob. Comput.*, **16** (2016), 2869–2883. https://doi.org/10.1002/Fwcm.2734
11. A. Mehmood, M. M. Umar, H. Song, ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks, *Ad Hoc Netw.*, **55** (2017), 97–106. https://doi.org/10.1016/j.adhoc.2016.10.007
12. V. Patel, J. Gheewala, An efficient session key management scheme for cluster based wireless sensor networks, In: *2015 IEEE International advance computing conference (IACC)*, India: IEEE, 2015, 963–967. https://doi.org/10.1109/IADCC.2015.7154847
13. M. M. Umar, A. Mehmood, H. Song, A survey on state-of-the-art knowledge-based system development and issues, *Smart Comput. Rev.*, **5** (2015), 498–509. https://doi.org/10.6029/smartcr.2015.06.001
14. A. Mehmood, H. Song, J. Lloret, Multi-agent-based framework for secure and reliable communication among open clouds, *Netw. Protoc. Algorithms*, **6** (2014), 60–76. https://doi.org/10.5296/npa.v6i4.6028
15. M. Zhou, Y. Wang, Z. Tian, Y. Lian, Y. Wang, B. Wang, Calibrated data simplification for energy-efficient location sensing in the internet of things, *IEEE Internet Things J.*, **6** (2019), 6125–6133. https://doi.org/10.1109/JIOT.2018.2869671
16. C. Wang, H. Lin, R. Zhang, H. Jiang, SEND: A situation-aware emergency navigation algorithm with sensor networks, *IEEE Trans. Mobile Comput.*, **16** (2017), 1149–1162. https://doi.org/10.1109/TMC.2016.2582172
17. J. Su, A. X. Liu, Z. Sheng, Y. Chen, A partitioning approach to RFID identification, *IEEE/ACM Trans. Netw.*, **28** (2020), 2160–2173. https://doi.org/10.1109/TNET.2020.3004852
18. O. A. Osanaiye, A. S. Alfa, G. P. Hancke, Denial of service defense for resource availability in wireless sensor networks, *IEEE Access*, **6** (2018), 6975–7004. https://doi.org/10.1109/ACCESS.2018.2793841
19. T. T. H. Le, T. Park, D. Cho, H. Kim, An effective classification for DoS attacks in wireless sensor networks, In: *2018 Tenth international conference on ubiquitous and future networks (ICUFN)*, Czech Republic: IEEE, 2018, 689–692. https://doi.org/10.1109/ICUFN.2018.8436999

20. R. Kaur, G. Kumar, K. Kumar, A comparative study of feature selection techniques for intrusion detection, In: *2015 2nd International conference on computing for sustainable global development (INDIACom)*, India: IEEE, 2015, 2120–2124.
21. S. A. Birahim, A. Paul, F. Rahman, Y. Islam, T. Roy, M. A. Hasan, et al., Intrusion detection for wireless sensor network using particle swarm optimization based explainable ensemble machine learning approach, *IEEE Access*, **13** (2025), 13711–13730. https://doi.org/10.1109/ACCESS.2025.3528341
22. A. Singh, J. Amutha, J. Nagar, S. Sharma, A deep learning approach to predict the number of k-barriers for intrusion detection over a circular region using wireless sensor networks, *Expert Syst. Appl.*, **211** (2023), 118588. https://doi.org/10.1016/j.eswa.2022.118588
23. WSN Dataset. Available from: https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds/data.
24. WSN-BFSF Dataset. Available from: https://www.kaggle.com/datasets/celilokur/wsnbfsfdataset/data.
25. CIC IoMT 2024 Dataset. Available from: https://www.unb.ca/cic/datasets/iomt-dataset-2024.html.
26. E. M.Maseno, Z. Wang, Hybrid wrapper feature selection method based on genetic algorithm and extreme learning machine for intrusion detection, *J. Big Data*, **11** (2024), 24. https://doi.org/10.1186/s40537-024-00887-9
27. B. Deore, S. Bhosale, Adaptive dolphin atom search optimization-based DRNN for network intrusion detection system, *SN Comput. Sci.*, **4** (2023), 578. https://doi.org/10.1007/s42979-023-02006-6
28. J. Y. Kim, J. W. Kim, H. J. Kim, M. S. Shim, E. J. Choi, CNN-based network intrusion detection against denial-of-service attacks, *Electronics*, **9** (2020), 916. https://doi.org/10.3390/electronics9060916
29. A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, R. Ahmad, CNN-LSTM: hybrid deep neural network for network intrusion detection system, *IEEE Access*, **10** (2022), 99837–99849. https://doi.org/10.1109/ACCESS.2022.3206425
30. Q. Zhu, C. Fung, R. Boutaba, T. Basar, GUIDEX: A game-theoretic incentive-based mechanism for intrusion detection networks, *IEEE J. Sel. Areas Commun.*, **30** (2012), 2220–2230. https://doi.org/10.1109/JSAC.2012.121214
31. V. Shakya, J. Choudhary, D. P. Singh, Deep learning based intrusion detection system for WSN, *Procedia Comput. Sci.*, **258** (2025), 2101–2106. https://doi.org/10.1016/j.procs.2025.04.460
32. M. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, S. Aryal, MLSTL-WSN: machine learning-based intrusion detection using SMOTE Tomek in WSNs, *Int. J. Inf. Secur.*, **23** (2024), 2139–2158. https://doi.org/10.1007/s10207-024-00833-z

AIMS Press