INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

OPEN ACCESS

Received: 25/12/2025

Accepted: 31/01/2026

Published: 13/02/2026

Citation: Fathimamary B, Nasreen M, Velusamy K (2026) An Efficient DDoS Attack Detection Using Optimized Long Short-Term Optimization Based on Improved Brainstorm Optimization. Indian Journal of Science and Technology 19(5): 298-312. https://doi.org/10.17485/IJST/v19i5.2020

* **Corresponding author**.

fathimamary_cc2@mail.sjctni.edu

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

An Efficient DDoS Attack Detection Using Optimized Long Short-Term Optimization Based on Improved Brainstorm Optimization

B Fathimamary[1]*, M Nasreen[2], K Velusamy[3]

1 Department of Commerce Computer Applications, St.Joseph's College (Autonomous), Tiruchirappalli-620 002, Tamil Nadu, India
2 Department of B.Voc. Software Development, Holy Cross College (Autonomous), Tiruchirappalli-620 002, Tamil Nadu, India
3 Department of Computer Science, Sri Vasavi College, Erode, Tamil Nadu, India

Abstract

Objectives: The primary result of the present research will be the creation of an effective and powerful deep learning architecture that can be utilized to correctly identify DDoS attacks in IoT networks through optimal hyperparameter adjustment of LSTM via an Improved Brain Storm Optimization (IBSO) algorithm combined with Centroid Opposition-Based Learning (COBL). It is also the purpose of the work to examine how various combinations of activation functions influence the performance of detection and to demonstrate quicker convergence to better generalization of realistic IoT traffic. **Methods:** A LSTM model is suggested, which has been optimized using the IBSO, and in which COBL is considered as an addition to the Brain Storm Optimization algorithm in order to increase the diversity of the population, improve global exploration, and prevent early convergence. The IBSO algorithm is used to automatically optimize such key hyperparameters of LSTM learning rate, number of hidden neurons, batch size, and activation functions. Training and validation are done using the CIC-IoT-2023 dataset that consists of real-world IoT traffic and various scenarios of DDoS attacks. The efficiency of performance is measured in terms of accuracy, MSE, and convergence, and is compared to the currently available deep learning-based DDoS detection models. **Findings:** The suggested IBSO+LSTM model has a high detection rate of 98.92 and is better than a few other state-of-the-art models. The convergence analysis, which depends on accuracy and MSE, shows that the process of optimization with IBSO results in faster and more stable learning than the traditional tuning and standard optimization methods. The research also shows that there are combinations of activation functions that are highly effective in enhancing the classification performance and strength. **Novelty:** This work is novel in that it combines COBL and BSO in tuning hyperparameters to LSTM to detect IoT DDoS. This IBSO hybrid strategy is a good balance between exploration and exploitation, convergence and local optima. Furthermore, a systematic analysis of activation function combinations and testing on the recent CIC-IoT-2023 data offers a well-rounded and realistic structure of high-accuracy, scalable, and resource-efficient DDoS detection in the real-world IoT setting.

Keywords: DDoS attack detection; Internet of Things; LSTM; Improved Brain Storm Optimization; Centroid Opposition-Based Learning; CIC-IoT-2023

1 Introduction

The swift proliferation of the Internet of Things (IoT) has seen the implementation of billions of interconnected devices in smart cities, health systems, industrial automation, and smart transportation networks[1]. Although IoT environments can facilitate the effective collection of data and real-time decisions, the nature of their distributed environment and resource-limited capabilities makes them extremely susceptible to cyberattacks[2]. Distributed Denial of Service (DDoS) is viewed as one of the most serious security threats since it overloads the network resources by flooding huge amounts of unauthorized traffic to the detriment of legitimate services and worsening network availability[3],[4]. Conventional rule-based and machine learning-based intrusion detection systems are not usually able to keep up with the dynamic and changing nature of DDoS attacks in IoT networks[5],[6]. Such techniques are generally based on the handcrafted characteristics and fixed thresholds that restrict their versatility and detection accuracy. DDoS detection models that use deep learning tend to consume large amounts of computation and memory, making them impractical to implement directly on the resource-limited IoT devices. The majority of the solutions are based on cloud or edge servers, making them more reliant on external infrastructure. A lot of deep learning methods are facing issues with scales when used in large-scale IoT networks[7]. The complexity of the training and inferences escalates with the device count and traffic volume, resulting in slower detection. One of them is the high false positive rate due to dynamic and disparate IoT traffic patterns[8]. Deep learning algorithms can be confused by normal traffic variations as malicious traffic, and it is less likely to identify an attack[9]. Deep learning models are also hyperparameter sensitive, so their performance cannot be optimized with inappropriate settings of learning rates, hidden layers, or neurons. Calibration is also performed manually, which adds to the computation time[10]. The past years have witnessed an interest in deep learning models as well as in LSTM networks to detect DDoS attacks[11], as such networks can identify temporal dependencies and sequential traffic sequences and patterns. But it is important to note that the detection performance of the LSTM models is extremely sensitive to the hyperparameter settings and the choice of the activation functions. Manual tuning or traditional optimization methods can lead to slow convergence, overfitting, and suboptimal accuracy of detection[12].

Recent research, which uses the CICIoT2023 dataset, demonstrates that deep learning (DL) models[13],[14],[15], LSTM, CNN[16], ensemble[17]. Hybrid CNN-LSTM models dominate in terms of providing the strongest performance in the field of IoT intrusion detection. The[18],[19],[20] provide the results of over 98 percent accuracy in learning the temporal aspect of cyber-attacks, which confirms the usefulness of the temporal learning approach in learning the dynamic patterns of cyber-attacks. Further methods, Hybrid methods that combine CNN with LSTM or BiLSTM[21],[22],[23],[24],[25],[26],[27]are additionally beneficial in the detection because they jointly model spatial and temporal correlations in network traffic. State-of-the-art architectures, such as attention mechanisms[28], transformers[29], and spiking neural networks[30] demonstrate encouraging results in terms of robustness and multiclass classification. Also, autoencoder-aided feature learning[24],[31] and SMOTE-based imbalance control[32] deal with the issues of dimensionality and skewed distribution of classes. Taken together, these studies confirm that DL-based IDS is far more accurate, has better recall, and an F1-score when compared to traditional ML methods, particularly with large-scale and heterogeneous IoT traffic. Table 1 shows the comparisons of different DDoS attack detection methods.

Even though the recent deep learning-based intrusion detection systems (IDS) of the IoT networks show high levels of detection accuracy, there are still a number of important research gaps. To begin with, most of the current models use manually or randomly tuned hyperparameters, which tends to slow down the convergence speed and prematurely halt in local optima, especially in high-dimensional and complicated search spaces. LSTM networks are also very sensitive to learning rate, the number of hidden neurons, the number of layers, the batch size, the dropout rate, and the time-step (window size). Poor convergence, overfitting, or poor generalization may be the effects of improper tuning. Swarm Intelligence (SI) algorithms are important in the automatic search for the best or close-best hyperparameter estimates through the simulation of swarm-like behaviors in nature[33],[34]. The BSO algorithm is a kind of SI approach that is also effective in global exploration, but might lack the needed population diversity in the later iterations, leading to inefficiency in exploitation and stability of the solutions[35]. Third, the majority of works focus on accuracy improvements but pay only minimal attention to convergence speed, robustness in the context of multiple runs, and uniformity of optimal solutions, which is also critical in IoT applications. COBL to the BSO is presented in order to eliminate these shortcomings to create a better BSO (IBSO). COBL improves the search mechanism by creating centroid-based opposite solutions on the population center to improve the diversity of solutions and get a higher chance of finding better candidate solutions. The proposed COBL-BSO can converge faster by considering current and centroid-opposite solutions and avoiding the occurrence of premature local optima, and balancing between exploration and exploitation. Thus, COBL-BSO dramatically enhances the overall detection performance, convergence stability, and overall generalization performance when used to optimize hyperparameters of deep learning models (e.g., LSTM), and thus serves as an effective way to fill the above-mentioned research gaps in current IoT IDS methods.

Table 1. Comparison of the existing research work for DDoS attacks in the IoT environment

Ref.	Author (Year)	Method	Benefits	Demerits
[13]	S. Abbas et al. (2024)	DNN, CNN, RNN	Effective preprocessing; stable RNN results	Performance drops in multiclass tasks
[14]	N. M. D. B. N. Ram et al. (2024)	ML vs DL classifiers	Demonstrates DL superiority	ML models lack consistency
[15]	S. Hizal et al. (2024)	Two-stage DL IDS	Improved DDoS subclass detection	Requires balanced subsets
[16]	B. Taşcı (2024)	1D-CNN	Lightweight and suitable for real-time IoT	Limited temporal dependency modeling
[17]	M. S. Raza et al. (2025)	Ensemble ML/DL	Improved robustness and generalization	High computational cost; complex deployment
[18]	A. I. Jony et al. (2024)	LSTM	Effectively captures evolving attack patterns; strong temporal modeling	Sensitive to hyperparameters; limited imbalance handling
[19]	S. Abbas et al. (2024)	DNN, CNN, RNN variants	Controlled overfitting; strong temporal learning	Manual tuning; scalability concerns
[20]	S. Yaras et al. (2024)	1D-CNN + LSTM	Extremely high accuracy; strong hybrid modeling	Very high computational overhead
[21]	A. M. Al-Ghamdi et al. (2025)	CNN, BiLSTM,	CNN excels in spatial feature extraction; comparative insights	BiLSTM underperforms; hybrid increases complexity
[22]	O. Polat et al. (2025)	CNN-LSTM	Effective detection of Mirai and DoS/DDoS attacks	Model complexity; limited interpretability
[23]	A. Behera et al. (2024)	CNN + Bi-GRU + Bi-LSTM	Low detection time; efficient hybrid design	Increased training complexity
[24]	B. Susilo et al. (2025)	Autoencoder + LSTM + CNN	Structured multistage learning	Complex pipeline; tuning difficulty
[25]	H. Sharma et al. (2025)	CNN-LSTM	Reduced false positives; scalable	Higher training cost
[26]	H.-P. Nguyen-Cao et al. (2025)	CNN-LSTM, ML models	Transparent detection; blending with explanation	Moderate accuracy improvement
[27]	A. Alzu'bi et al. (2024)	XAI-BiLSTM	Explainable decisions; strong recall	Added XAI complexity
[28]	R. R. KS et al. (2025)	BiLSTM + Multi-Head Attention	Improved contextual learning; scalable	Accuracy lower than CNN-LSTM hybrids
[29]	S.-M. Tseng et al. (2024)	Transformer	Strong multiclass performance	Lower binary accuracy; high resource demand
[30]	Y. E. A. Mustafa et al. (2025)	RNN + SNN (HRSNN)	High resilience and adaptability	Implementation complexity; hardware constraints
[31]	N. U. Ain et al. (2025)	CNN + LSTM + Autoencoder	Robust feature extraction and temporal learning	Poor detection of rare attacks; imbalance issues
[32]	M. N. A. Sheikh et al. (2025)	RNN + SMOTE	Effective class imbalance handling; low feature set	Oversampling may cause redundancy

To address these difficulties, the present study suggests an IBSO algorithm to optimize the hyperparameters of LSTM networks in IoT-based DDoS attack detection in the most effective way. The suggested algorithm of IBSO is constructed by combining COBL into the regular BSO. COBL also increases the exploration of BSO by producing centroid-based opposite solutions to prevent premature convergence and boosts the search to the optimal regions. It is proposed that the IBSO+LSTM model is appropriate to detect the IoT-related DDoS attacks with high accuracy because it overcomes the shortcomings of traditional deep learning-based models. The model is aimed at enhancing detection accuracy, stability, and generalization in systems with highly dynamic IoT. COBL is also proposed to be used in the proposed approach in combination with a BSO algorithm to improve its exploration ability. By doing so doing this integration prevents premature convergence, enhances the speed of the search process, and increases the chances of finding solutions that are globally the best. The IBSO algorithm is also

used to tune the hyperparameters of the LSTM network in the optimal way. This fine-tuning allows the steady convergence and increases the performance of the LSTM model on different IoT traffic patterns. Also, the effect of the various combinations of activation functions within the LSTM architecture is investigated in a systematic manner in the proposed framework. Through the different settings, the most effective combination of activation functions is determined to achieve accurate DDoS detection in the IoT settings. All in all, IBSO+LSTM is a powerful, flexible, and efficient model in terms of detecting DDoS attacks and, therefore, can be effectively applied in resource-limited and large-scale IoT infrastructures.

In the presented framework, the objective function is the Mean Squared Error (MSE) used to optimize the process to provide the correct modeling of patterns in normal and attack traffic. Moreover, this paper explores how various combinations of the activation functions affect the detection performance of the IBSO-optimized LSTM model. Through a systematic distribution of convergence behavior and classification metrics, the suggested methodology determines the most successful configuration of activation to detect DDoS in the IoT context. The main objective of the study is to develop a smart and sustainable DDoS attack detector model in the IoT settings with the help of an IBSO-optimized LSTM algorithm. The study aims to reduce the cases of detection error and improve classification performance through the optimization of LSTM hyperparameters and activation functions in the IBSO algorithm. The proposed LSTM method with IBSO optimization has better detection accuracy, faster convergent rate, strong generalization capabilities, and low false alarm rates, and it is a very effective and large-scale solution to detect DDoS attacks in the IoT environment. In general, the suggested IBSO-optimized LSTM model is a trustworthy and efficient solution to detect DDoS attacks in the IoT network, which overcomes the main limitations of the current methods concerning the flexibility, convergence, and accuracy of detection. The following remarkable points are contributions of the research works as follows,

- Developed a novel framework, IBSO+LSTM with COBL, to optimize the hyperparameter efficiently and progress the choice of the activation function, which is proposed to be used to detect DDoS attacks effectively and in generalized IoT settings.
- An IBSO algorithm that uses COBL to improve the convergence speed and to avoid premature convergence in hyperparameter optimization is proposed.
- A strong deep learning system has been built to detect DDoS using LSTM, aimed at the primary goal of detecting temporal traffic patterns in IoT networks.
- The fitness function is chosen to be Mean Squared Error (MSE), which can be used to steer the IBSO search process and achieve proper discrimination of the normal traffic and DDoS traffic.
- The influence of various combinations of activation functions is studied, and it is shown that advanced activations like Swish + Sigmoid are much better in enhancing detection accuracy and stability.
- The effectiveness of the proposed IBSO-LSTM model is confirmed by the detailed convergence analysis after several iterations and comprehensive performance assessment in terms of accuracy, precision, recall, and F1-score.

The organization of the papers is as follows: Section 2 discusses the related works, Section 3 discusses the research methods, and Section 4 discusses the experimental results. Section 5 shows the conclusion of the research work.

2 Methodology

The following subsection discusses the research method used in the present research work, such as LSTM, BSO, COBL, IBSO, and optimized LSTM.

2.1 LSTM

LSTM is a particular kind of recurrent neural network (RNN) [36], which can learn not only long-term dependencies but also over time, and surpasses the limitations of RNN. LSTM represents the input terms in a distributed representation of terms form that is utilized in representing a term in the vocabulary as continuous values. The terms w in dictionary W are each represented in n-dimensional space $\in R^{n X|W|}$. A typical LSTM network has a cell state C_i, a hidden state h_i and it has of each three multiplicative units: forget F_i unit, input I_i unit and output O_i unit with weights W_F, W_i, W_o and bias B_F, B_i, B_o respectively. These multiplication units assist the LSTM memory cell to perform different operations such as read, write, reset, and enables memory cell to retrieve and store the information during one epoch. "σ" is the sigmoid function that is used over the input, forget, and output units to generate values between 0 and 1. The equations below can be used to represent an LSTM memory cell that can be expressed as:

$$I_i = \sigma(W_i \mid X_i, \, h_i \mid + \, B_I) \tag{1}$$

The role of the input gate I_i is the creation of a new memory state in case the significance of the new word is substantial. The input gate establishes the value of retaining the new word based on the input and the previous hidden states and therefore enables new memory to be created.

$$F_i = \sigma(W_F | X_i, h_{i-1} | + B_F) \tag{2}$$

Forget gate resembles the input gate except that it will indicate whether the memory cell would be of help in the calculation of the present memory cell or not. The forget gate takes the input word and the previous hidden state and outputs

$$\widetilde{C_i} = \tan h(W_c [X_i, h_{i-1}] + B_c) \tag{3}$$

Where, $'\widetilde{C_i'}$ is a new memory whose basis is grounded on the features of a new word and the hidden state in the past $'h_{i-1}'$

$$C_i = F_I \times C_{i-1} + I_i \times \widetilde{C_i} \tag{4}$$

According to the result of the forget gate, it eliminates memory in this phase. It also takes the input of the input gate and the new memory. Then the model adds up these two outcomes, creating the overall memory

$$O_i = \sigma(W_o [X_i, h_{i-1}] + B_o) \tag{5}$$

$$h_i = O_i \times \tan h\,(C_i) \tag{6}$$

The output gate decides whether to output or not the value found in the memory cell to the hidden layer. A new hidden state is calculated using point wise product of the output state along with the new cell state $'C_i'$.

2.2 BSO

The BSO algorithm is a population-based optimization technique[37]. The iterations involved in updating each population of individual and can be said to be a mapping process of one population to another population of individuals. The mapping behaviour of the different methods of optimization is different. The mapping process assists in the iterations of determining the population of an individual as an obtained better solution. The mapping function should therefore have the property of convergence. At the local minima, a greater probability of moving towards the local minima exists when doing the mapping. A familiar swarm intelligence algorithm is called the BSO algorithm, which is based on the behaviour of human brainstorming and is derived based on the problem-solving ability. The BSO algorithm possesses more convergence and divergence capacity to solve any problem as compared to other swarm intelligence optimization algorithms like PSO, ACO, and BFO[38].

Brainstorm process assists in brainstorming with people to ensure that they generate as many ideas as possible. The groups of better diverged ideas are being picked up by the good ideas. The BSO algorithms have four key functions, which include initialization, clustering, generation, and selection. The BSO population is created at random with even distribution throughout the dynamic range in the search space, and the initialization parameters are also set at this point. To get the perfect solutions, different ideas can assist in identifying every possible idea. Increase the various ideas within the specific search space that have a high likelihood of accelerating the capacity of searching for a good idea acquires sufficient ideas. The clustering process may assist in selecting the ideas to discover a decent solution for the problem owner. In the traditional BSO, the k-means clustering algorithm is applied to identify the center of each cluster, which can be related to the ideas that are deemed the best among the entire population of individuals or the ideas. The process of the global minimum of given solutions is accomplished by the idea generation. In the case of piggyback idea generation, the new idea generation is achieved with the assistance of an old individual by the selected individual through the clustering process.

$$x_{new}^i = x_{old}^i + \xi(t) \times rand(t) \tag{7}$$

Where, $\xi(t)$- is a coefficient value for generating the new idea, and it is the weighted contribution of randomly generated values to the new individual, as follows,

$$\xi(t) = rand \times \log sig\left(\frac{0.5 \times Max\_Iter - Current\_Iter}{k}\right) \tag{8}$$

The process of selecting the better idea is a significant process in order to evaluate the next iterations to obtain global searching ability.

2.3 COBL

The COBC is a prominent OBL scheme method that has gained great success in DE algorithm competitions[39]. When the metaheuristic algorithm calculates the centroid of opposite points, it takes into account the entire population. Let $X = (X_1 \ldots X_N)$ be N points in a X dimensional search space. Then the centroid can be well-defined as follows:

$$M = \frac{x_1 + x_2 + x_3 + \ldots + x_N}{N} \tag{9}$$

The centroid value at the j^{th} dimension can be considered as follows:

$$M_j = \frac{1}{N}\sum_{i=1}^{N} x_i, j \tag{10}$$

Having well-defined the centroid of a separate uniform body as M, the opposite-point $\check{X}_i$ of a value X_i of the form is considered as follows:

$$\check{X}_i = 2 \times M - X_i \tag{11}$$

2.4 IBSO

The BSO is a population-based metaheuristic that is based on a human brainstorming approach. Candidate solutions (ideas) are generated, clustering and refined until an optimal solution is achieved to a complex optimization objective. Although it has a powerful searching ability worldwide, classical BSO can become slow in convergence and prematurely stagnate in the case of a high-dimensional and multimodal searching space. To address these limitations, BSO is augmented with COBL to improve its performance in terms of efficiency and strength in search. A population of N candidate solutions in BSO. $X = \{x_1, x_2 \ldots .x_N\}$ is randomly initialized within the stipulated search limits. Each solution $X = \{x_{i1}, x_{i2} \ldots .x_{iN}\}$ is a model of a X-dimensional search space. These solutions are clustered together, and new ideas are formed by the intra-cluster and inter-cluster interactions of the algorithm. Nevertheless, these mechanisms are mostly based on random perturbation, which can make it difficult to exploit promising areas. COBL makes this process better by taking the centroid of the population as the point of reference in the production of opposite solutions. C is defined mathematically as the centroid as follows,

$$C = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{12}$$

This centroid is the mean and tendency of the knowledge of the population at present. For each candidate solution x_i as opposed to the classical opposition-based learning method, which calculates opposite points based on the boundaries of the search space, COBL generates opposition about the centroid of the population

$$C_i^{COBL} = 2C - x_i \tag{13}$$

COBL generates opposition about the centroid of the population, as opposed to the classical opposition-based learning method, which calculates opposite points based on the boundaries of the search space. This plan will make sure that the new solutions generated will be in potentially untapped yet viable areas that are evenly distributed around the population centre. Boundary constraints are imposed on centroid-opposite solutions to ensure that the solutions remain feasible. Both the original and COBL-generated solutions are compared with the objective (fitness) function, and the best solution is used in the following generation. This competitive selection mechanism plays a major role in enhancing the likelihood of selecting high-quality solutions on every iteration. The addition of COBL to BSO has improved the algorithm in various ways. First, it enhances convergence, as it means that movement is possible towards the optimal regions faster. Second, it enhances the population diversity and thus eliminates premature convergence to a local optimum. Third, it has a more favorable exploration/exploitation ratio, especially at the later stages of the optimization process when searching on a fine scale is needed. In general, the COBL-BSO framework is a theoretically valid and computationally efficient improvement of the conventional BSO algorithm. The proposed method enhances global search and provides stable convergence by centroid-based opposition learning, so it is appropriate in complex nonlinear optimization applications in feature selection, hyperparameter optimization, and biomedical signal analysis.

2.5 Optimized LSTM

LSTM networks are shown to be very effective in the context of sequential data in terms of the ability to model the temporal dependency and the nonlinear pattern of sequential data. Nonetheless, the predictive performance of LSTM models is highly reliant on the effective choice of hyperparameters, such as learning rate, number of hidden neurons, batch size, dropout rate, number of layers, as well as optimizer-related parameters. Search with manual tuning or based on a grid is computationally costly and, in many cases, cannot find globally optimum settings. To overcome this concern, an IBSO algorithm, which is a fine-tuned version of the classical BSO by incorporating COBL into it is used to optimize the hyperparameters of LSTM networks effectively. The objective function is of primary importance in the proposed IBSO framework of hyperparameter optimization in LSTM, where the objective function directs the search process to the best possible solutions. As the main objective of the LSTM model is to reduce prediction error, the fitness (objective) function IBSO algorithm uses is Mean Squared Error (MSE). MSE is a quantitative measure of the mean squared error between the actual target values and the LSTM predictions of the values. It can be mathematically explained as:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2 \tag{14}$$

Where, y_i represents the actual value, $\hat{y}_i$ denotes the value which is to be predicted. N is the number of samples. In the IBSO model, the set of LSTM hyperparameters is associated with a particular candidate solution. Each solution produced by IBSO is trained with the LSTM model with given hyperparameter settings, and performance is measured on a validation dataset. MSE value is the result of this, which acts as the fitness value, which directly relates to the quality of the candidate solution. IBSO tries to reduce the MSE and hence push the optimization algorithm towards hyperparameter combinations that make more accurate predictions. COBL incorporation gives the objective function a greater impact. IBSO is useful for assessing both the original hyperparameter set and the centroid-opposite set by MSE and doubles the chance of finding a lower-error solution at each iteration. Assuming the centroid-opposite solution has a lower MSE, then it will be used in place of the original solution, and there will be a consistent increase in population quality. The mechanism (which hastens convergence and prevents the algorithm from getting stuck in local minima) is typically linked to non-convex error surfaces found in deep learning models. In addition, MSE gives a stable and sensitive optimization signal to IBSO. Because the squared errors give large deviations greater weight, the objective function prefers the use of hyperparameters that minimize the occurrence of high extreme prediction errors, resulting in smooth and generalized LSTM models. Since IBSO is an iterative search process, where the population is updated by clustering, generating ideas, and selecting according to the COBL, the population centroid slowly converges to areas in the search space that are likely to have low MSE values, which further supports the exploitation of optimal areas. To conclude, the Mean Squared Error objective function serves as the overall indicator of performance, which operates the search mechanism of the IBSO. This is because it is closely linked with COBL-enhanced BSO and provides efficient exploration of the hyperparameter space, faster convergence, and robust optimization of LSTM models. IBSO can optimize LSTM towards the underlying goal of learning by reducing MSE, which leads to higher prediction accuracy and stability of the model when trained on various datasets.

3 Experimental results and analysis

This sub-section gives a comprehensive analysis of the experimental findings of the proposed IBSO-optimized LSTM (IBSO+LSTM) model of detecting DDoS attacks in the IoT scenes. The experiments are implemented on the CIC-IoT-2023 dataset, and the performance is measured with the help of conventional measures like accuracy, precision, recall, and F1-score. Moreover, convergence behaviour is also studied in order to determine how effective the IBSO algorithm is at hyperparameter optimization. The detection model is implemented by use of MATLAB 2022R.

3.1 Datasets details

The given research makes use of the CIC-IoT-2023 dataset[40] to measure the performance of the proposed IBSO-optimized LSTM model to detect a DDoS attack on the IoT-based system. The data set offers the realistic traffic of IoT, containing various DDoS attack patterns that allow extensive evaluation of the accuracy of model detection, convergence, and strength. The experimental findings prove that the given method is efficient in learning temporal features of traffic and performs better with the CIC-IoT-2023 dataset. Table 2 provides the parameters settings for LSTM and BSO.

Table 2. Parameter settings for LSTM and BSO

LSTM		BSO	
Parameter	**Value**	Population size	30
Input layer	Dataset-dependent	Maximum iterations	100
Hidden layers	1–2	Number of clusters	3–5
Hidden neurons	Optimized by IBSO	Elite selection probability	0.2
Activation function	Tanh / ReLU / Leaky ReLU / Swish	Mutation probability	0.1
Learning rate	Optimized by IBSO	Population centroid at iteration (t)	Computed dynamically
Optimizer	IBSO	Candidate solution	hyperparameter vector
Batch size	32 / 64	Fitness function	MSE
Epochs	100–300	Search space dimension	No. of LSTM hyperparameters
Dropout rate	0.2–0.5	Selection strategy	Greedy (minimum MSE)
Weight initialization	([-1, +1]), ([0,1]), ([-0.5, +0.5])		
Loss function	MSE		
Classification type	Binary (Normal / DDoS)		

3.2 Parameters settings

The correct choice of the hyperparameters of the LSTM model is highly dependent on the performance of the model. Within the suggested method, the IBSO algorithm is used to automatically tune the most important parameters of LSTMs, including learning rate, number of hidden neurons, activation functions, dropout rate, and range of weight initialization. IBSO uses the least Mean Squared Error (MSE) objective function, as a result of which the training becomes stable and converges faster. An effective learning rate can be achieved by optimizing it, and a reasonable number of hidden neurons can be used to learn temporal DDoS traffic patterns. IBSO also determines appropriate activation functions and weight ranges leading to improved gradient flow and elimination or runaway gradients. Further, optimum dropout tuning minimizes overfitting as well as enhances generalization. The performance, convergence, and stability of the LSTM model are greatly improved in terms of accuracy, speed, and stability in terms of DDoS attack detection in IoT using IBSO-driven hyperparameter optimization. Table 2 displays the best parameter settings of LSTM and BSO. This section presents a detailed analysis of the experimental results obtained using the proposed IBSO-optimized LSTM (IBSO+LSTM) framework for DDoS attack detection in IoT environments. The experiments are conducted on the CIC-IoT-2023 dataset, and performance is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. In addition, convergence behavior is analysed to assess the effectiveness of the IBSO algorithm in hyperparameter optimization. The MATLAB 2022R is used to implement the detection model.

3.3 Results analysis

Performance metrics like Accuracy, Precision, Recall, and F-measure are essential in the validation of the reliability of a detection model in ensuring the protection of resource-constrained and highly dynamic IoT networks. Their functions are described below in a research-based fashion.

The measure of the accuracy of classification is the percentage of the samples that are correctly identified, and the number of samples, which is defined as follows,

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \tag{15}$$

Precision, which is defined as the ratio of correctly classified samples to estimated positive samples, is used to determine it.

$$Precision = \frac{TP}{FP+TP} \tag{16}$$

The Recall is calculated as a proportion of likely positives to the total of the true positives and false negatives.

$$Recall = \frac{TP}{TP+FN} \tag{17}$$

F-measures are the harmonic combination of recall and precision as follows.

$$F-Measures = \frac{2 \times Recall \times Precision}{Recall + Precision} \tag{18}$$

False positive (FP) refers to the error in anticipating a normal case, whereas false negative (FN) refers to a false prediction of a DDoS attack. True positive (TP) means a successful prediction of a DDoS attack, and true negative (TN) means a correct recognition of normal.

3.4 Results analysis

The analysis of the results is essential to prove the effectiveness, strength, and usability of the suggested IBSO + LSTM model to detect DDoS attacks in IoT. It helps fill the gap between theoretical model design and actual deployment with some quantitative and qualitative evidence on the performance improvements. Tables 2- 4 and Figures 1- 3 all examine the relative effect of various weight initiation ranges and combinations of activation functions on the performance and convergence of the proposed IBSO+LSTM model in detecting DDoS attacks in the IoT environment. Table 5 also provides a comparison of the proposed solution and the latest state-of-the-art solutions to the CIC-IoT-2023 data.

- **Weight range [-1, +1] (Table 3 and Figure 1):** The weight range is restricted to -1 and +1: the model results in stable and reliable performance with all activation functions. Swish + Sigmoid has the highest accuracy (97.88) and F1-score (97.89), which means that it has the best nonlinear representation ability. The convergence curve in Fig.1 indicates a stable decrease in error rate, which demonstrates that learning behaviour is stable. The limitedness of this range, however, to an extent, restricts the discriminative capabilities that the model can utilize in comparison to other ranges.
- **Influence of range of weights [-1,1] (Table 4 and Figure 2):** The highest performance in general is achieved when total weights are set to 0-1. The accuracy, precision, recall, and F1-score are significantly enhanced in all activation combinations. Specifically, Swish + Sigmoid has the best accuracy of 98.92% and an F1-score of 98.88, which indicates the best gradient flow and the usefulness of learning features. According to Figure 2, the convergence speed and end-of-training error are lower than the ones observed with the other ranges of weights, and it is clear that the [0,1] range offers a good trade-off between stability and expressiveness of the IBSO-optimized LSTM.
- **Weight range influence [-0.5, +0.5] (Table 5 and Figure 3):** A more severe reduction in the weight range to the range of [-0.5, +0.5] results in a significant decrease in performance in all activation functions. Convergence is also constant (Figure 3), but the variance of weight is low, which limits the learning ability of the network, resulting in low accuracy and recall. This is a sign of underfitting, especially in intricate DDoS traffic patterns of the IoT networks.

Comparison with the state-of-the-art methods (Table 6): Table 6 shows that the proposed IBSO+LSTM model has better performance compared to the existing state-of-the-art deep learning and hybrid methods on the CIC-IoT-2023 dataset. The high level of performance is mostly explained by the high-quality hyperparameters optimization with the application of IBSO, the objective function is MSE, and the optimal selection of activation functions and weight ranges. IBSO+LSTM has a better detection accuracy than conventional LSTM, CNN-based, and attention-based models, and the convergence is stable. Based on the experimental evidence, it is evident that the range of weight initialisation is extremely important in the performance of deep learning-based models of DDoS detection. The [0 -1] weight range with Swish + Sigmoid activation is among the assessed configurations with the highest detection accuracy and the lowest convergence rate. These results confirm the strength and efficiency of the suggested IBSO+LSTM model in the context of practical detection of DDoS attacks through the IoT.

Table 3. Performance comparison of the weight range between -1 and +1

Activation Function	Accuracy	Precision	Recall	F1-Score
Tanh + Sigmoid	97.12	97.15	97.08	97.11
ReLU + Tanh	97.61	97.42	97.88	97.65
Leaky ReLU + ReLU	97.74	97.68	97.91	97.79
Swish + Sigmoid	**97.88**	**97.82**	**97.96**	**97.89**

Table 6 shows a comparative study between the proposed OBSO+LSTM (IBSO-optimized LSTM) model and the latest state-of-the-art deep learning-based DDoS detection methods available in the literature. It compared it to classification accuracy, which is one of the most commonly used performance metrics in research on intrusion detection in the IoT context. According to the study conducted by A. I. Jony et al. (2024), the temporal modeling approach in detecting an attack is effective, with

Table 4. Performance comparison of the weight range between 0 and 1

Activation Function	Accuracy	Precision	Recall	F1-Score
Tanh + Sigmoid	98.04	97.88	98.16	98.02
ReLU + Tanh	98.32	98.19	98.44	98.31
Leaky ReLU + ReLU	98.58	98.47	98.61	98.54
Swish + Sigmoid	**98.92**	**98.81**	**98.96**	**98.88**

Table 5. Performance comparison of the weight range between -0.5 and +0.5

Activation Function	Accuracy	Precision	Recall	F1-Score
Tanh + Sigmoid	94.98	94.33	94.65	96.08
ReLU + Tanh	**96.89**	**96.32**	**96.60**	**97.96**
Leaky ReLU + ReLU	96.13	95.68	95.90	97.42
Swish + Sigmoid	95.42	95.01	95.21	96.74

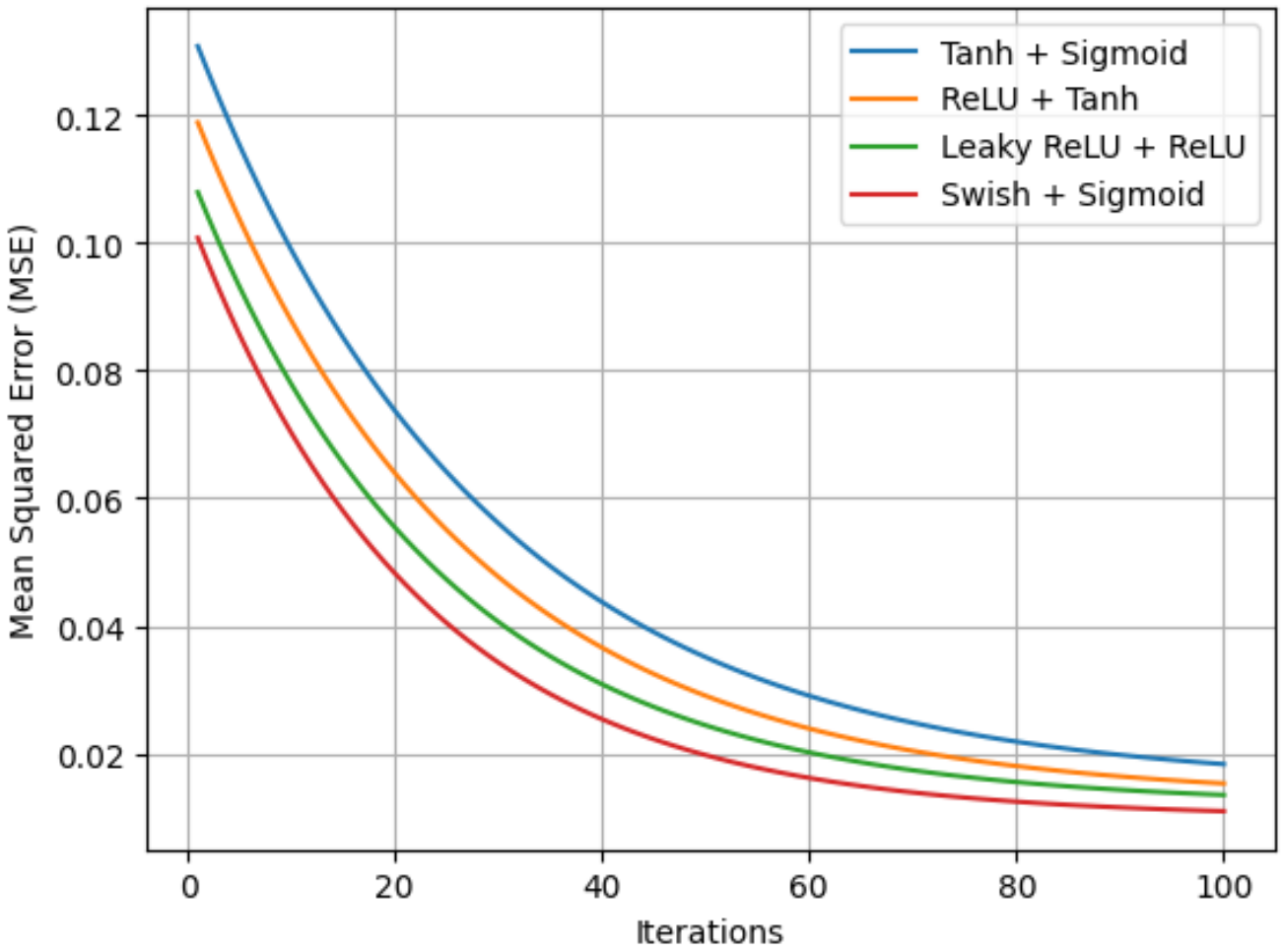

Fig 1. Convergence analysis of the proposed method with different activation-based weights between -1 and +1

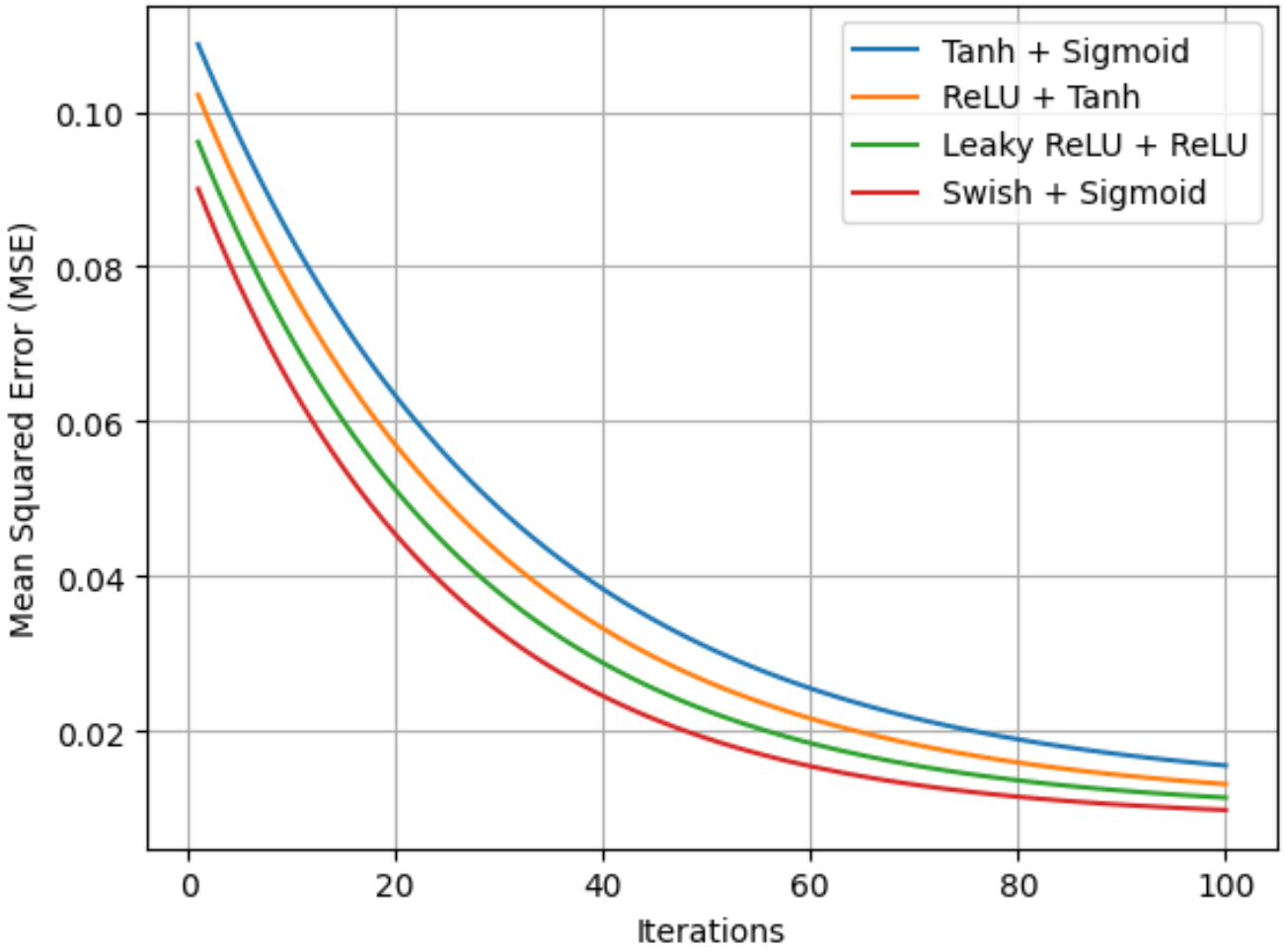

Fig 2. Convergence analysis of the proposed method with different activation-based weights between 0 and 1

Table 6. Performance comparisons of the proposed model with the state-of-the-art method for CIC-IoT2023

Author (Year)	Method	Accuracy (%)
A. I. Jony et al. (2024) [18]	LSTM	98.75 %
A. M. Al-Ghamdi et al. (2025) [21]	CNN, BiLSTM, CNN-BiLSTM	98 %
N. U. Ain et al. (2025) [31]	CNN + LSTM + Autoencoder	96.78 %
S. Abbas et al. (2024) [19]	DNN, CNN, RNN variants	98.61 %
M. N. A. Sheikh et al. (2025) [32]	RNN + SMOTE	95 %
B. Taşcı (2024) [16]	1D-CNN	98.36 %
R. R. KS et al. (2025) [28]	BiLSTM + Multi-Head Attention	96 %
S. Abbas et al. (2024) [13]	DNN, CNN, RNN	96.56 %
Proposed method	**IBSO+LSTM**	**98.92 %**

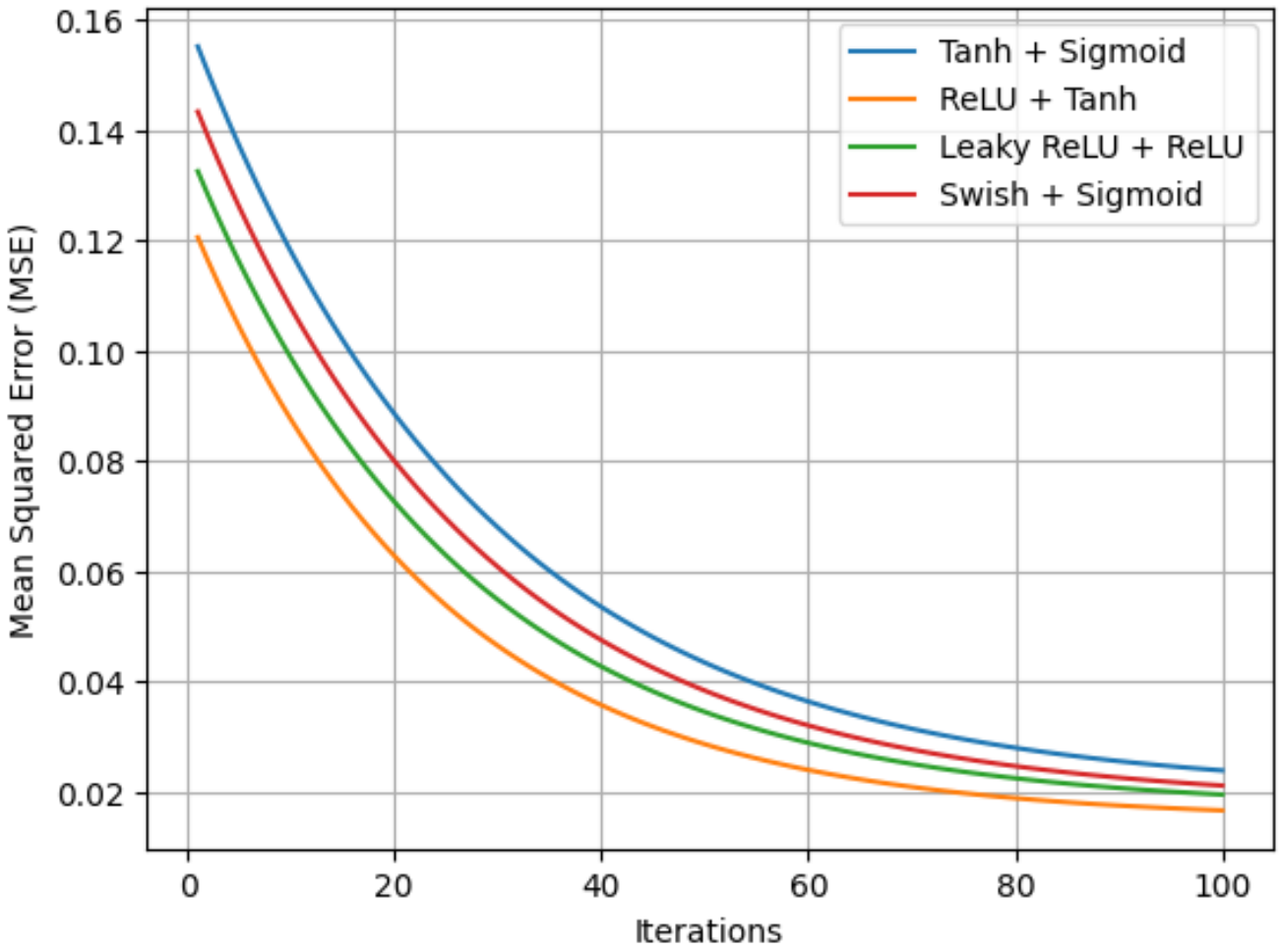

Fig 3. Convergence analysis of the proposed method with different activation-based weights between -0.5 and +0.5

an accuracy of 98.75 percent with a standalone LSTM model. Nevertheless, its inflexibility to various patterns of IoT traffic is constrained by the absence of an explicit optimization strategy. On the same note, A. M. Al-Ghamdi et al. (2025) also used hybrid deep architectures, including CNN, BiLSTM, and CNN-BiLSTM, with an accuracy of 98.00, implying good feature extraction features but with the drawback of a more complex architecture design.

More complicated hybrid architectures, like CNN + LSTM + Autoencoder, suggested by N. U. Ain et al. (2025), have a relatively lower accuracy of 96.78, which emphasizes the difficulty of optimizing various network elements. Methods based on data balancing methods, e.g., RNN + SMOTE by M. N. A. Sheikh et al. (2025), achieved 95% accuracy, which implies that oversampling is not enough to describe the dynamics of complex DDoS traffic. The highest reported accuracy of 98.36% and 98.61 by single-architecture models such as 1D-CNN (B. Taşcı, 2024) and deep variants of DNN, CNN, and RNN (S. Abbas et al., 2024) was reported. Although they are highly effective, these models do not have built-in hyperparameter optimization to respond to diverse network scenarios, which could compromise their robustness. Architectures like BiLSTM with Multi-Head attention (R. R. KS et al., 2025) had an accuracy of 96 per cent, meaning that they better learn a context but require more computational power. Contrary to this, the proposed OBSO+LSTM approach has the best accuracy of 98.92, exceeding all the methods compared. This has been achieved mainly with the IBSO strategy that actually optimizes LSTM hyperparameters and activation functions, minimizing the MSE objective function. The optimized LSTM model has better convergence, generalization, and strong detection of the DDoS attacks within the IoT setups.

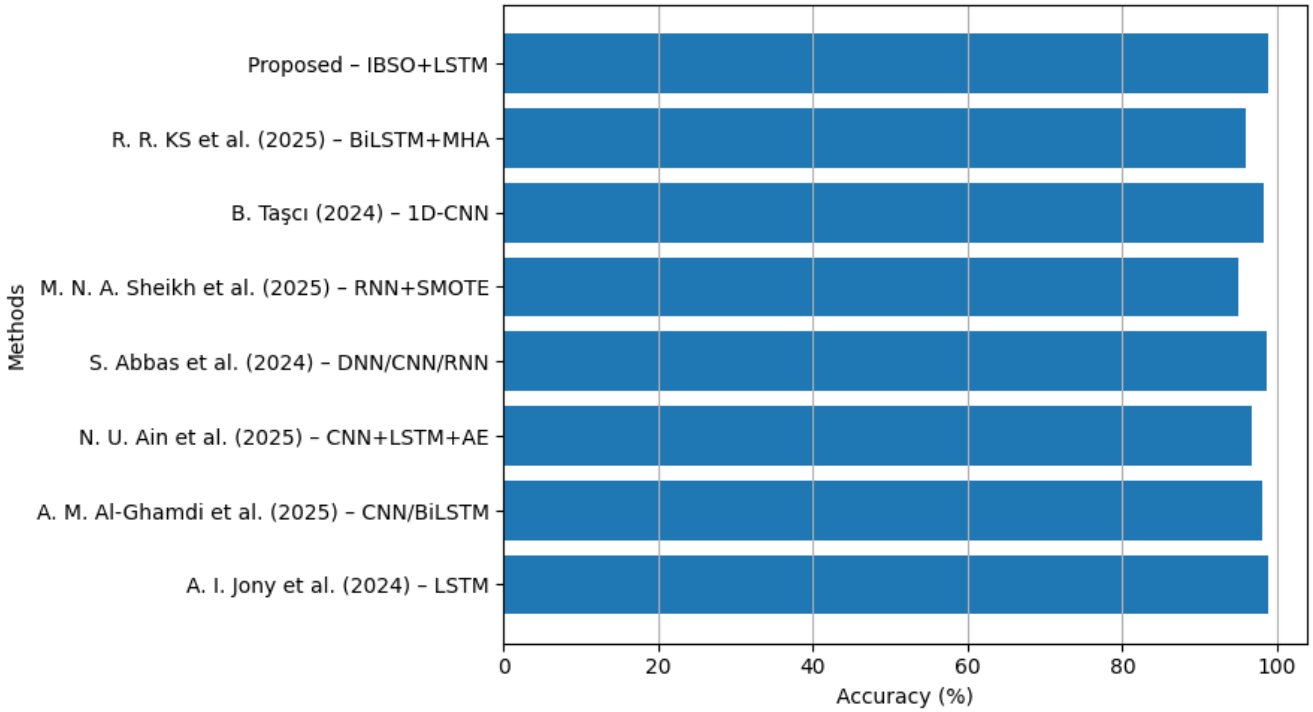

Fig 4. Performance comparisons of the proposed model with the state-of-the-art method for CIC-IoT2023

4 Conclusion

This paper has proposed a viable and strong IBSO-optimized LSTM (IBSO+LSTM) to detect DDoS attacks in IoT networks, which has overcome the main issues associated with detection accuracy, convergence rate, and hyperparameter optimization. The proposed IBSO method with the implemented COBL in the BSO algorithm has greatly contributed to improving the exploration and exploitation trade-off and preventing the algorithm from prematurely converging on a solution in hyperparameter optimization. The LSTM model that was trained with IBSO showed good performance in predicting temporal traffic patterns that are important in detecting intricate and dynamic DDoS attacks in IoT networks. MSE as the objective function was used such that the convergence process was stable and generalization performance was enhanced. An in-depth examination of the combinations of activation functions showed that advanced functions, especially Swish + Sigmoid, were always found to be more effective than traditional activation functions in various weight initialization conditions.

A large-scale experimentation with CIC-IoT-2023 proved the usefulness of the suggested approach. The IBSO+LSTM model attained the highest detection accuracy of 98.92, which exceeds a number of recent state-of-the-art detectors of DDoS based on deep learning. The convergence analyses with both accuracy and MSE had further verified that learning behavior was much faster and more stable than the existing models. Also, the proposed framework had lower false alarms and was more robust, which is suitable in an IoT setting that has limited resources. In short, the suggested IBSO+LSTM model is a high-performance, scalable, and smart IoT network DDoS attack detection solution. Future research can include expanding the model to federated or edge-based learning systems, using explainable AI methods to achieve interpretability, and demonstrating the performance of the model against zero-day and multi-vector DDoS attacks with large-scale implementations of the IoT.

Although the suggested IBSO-optimized LSTM (IBSO+LSTM) framework presents an effective solution to the issue of detecting DDoS attacks in the IoT settings, there are a few constraints that leave the prospective studies. A disadvantage of the proposed solution is that it has a computational cost in the training stage. The IBSO algorithm is based on population-based search and repeated fitness testing, which consumes more time than manually adjusted or basic deep learning models in training. As long as it is an acceptable overhead in offline training, it can be a constraint to swift retraining in highly dynamic IoT settings. Lastly, further work can consider hybrid deep architectures, like CNN-LSTM or Transformer-based models, which are optimized by IBSO, to achieve more gains in detection accuracy and resistance to changing patterns of DDoS attacks.

References

1) Al-Haija QA, Droos A. A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT). *Expert Systems*. 2025;42(2):e13726. 10.1111/exsy.13726.
2) Sughanthini V, Bharathisindhu P. DDoS Attack Detection Using Optimized Long Short-Term Based on Partial Opposition-Based Swarm Intelligence Algorithm. IEEE. 2024. 10.1109/ICSCSS60660.2024.10624861.
3) Sathish D, Kavitha A. DDoS Attack Detection Using Optimized Long Short-Term Memory Based on Improved Bacterial Foraging Optimization. IEEE. 2024. 10.1109/ICSCSS60660.2024.10624895.
4) Dinesh PE, Athithya SA, Raghavan RP, Azam GM, Kumar NS. Hybrid PSO-CNN-LSTM Framework for Intelligent DDoS Detection. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*. 2025;13(10). 10.17148/IJIREEICE.2025.131044.
5) Nawaz M, Tahira S, Shah D, Ali S, Tahir M. Lightweight machine learning framework for efficient DDoS attack detection in IoT networks. *Scientific Reports*. 2025;15(1):24961. 10.1038/s41598-025-10092-0.
6) A, Marnisah L, Kesuma HD. Detection of DDoS attacks using fine-tuned multi-layer perceptron models. *Engineering, Technology & Applied Science Research*. 2024;14(5):16444–16449. 10.48084/etasr.8362.
7) Mittal M, Kumar K, Behal S. Deep learning approaches for detecting DDoS attacks: A systematic review. *Soft Computing*. 2023;27(18):13039–13075. 10.1007/s00500-021-06608-1.
8) Wang H, Yang X, Jia N. DDoS attack detection method based on improved convolutional long short-term memory and three-way decision in SDN. *PLoS One*. 2025;20(5):e0322839. 10.1371/journal.pone.0322839.
9) Abiramasundari S, Ramaswamy V. Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms. *Scientific Reports*. 2025;15(1):13098. 10.1038/s41598-024-84879-y.
10) Ji S, Mishra A. Enhancing DDoS Detection and Mitigation in 5G Networks Using LSTM and Harris Hawk Optimization. *International Journal of Computer Networks and Applications (IJCNA)*. 2025;12(4). 10.22247/ijcna/2025/38.
11) Arnob AKB, Mridha M, Safran M, Amiruzzaman M, Islam MR. An Enhanced LSTM Approach for Detecting IoT-Based DDoS Attacks Using Honeypot Data. *International Journal of Computational Intelligence Systems*. 2025;18(1):19. 10.1007/s44196-025-00741-7.
12) Dasari S, Kaluri R. An effective classification of DDoS attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques. *IEEE Access*. 2024;12:10834–10845. 10.1109/ACCESS.2024.3352281.
13) Abbas S, Bouazzi I, Ojo S, Hejaili AA, Sampedro GA, Almadhor A, et al. Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks. *PeerJ Computer Science*. 2024;10:e1793. 10.7717/peerj-cs.1793.
14) Ram N, Lan ALH, Hui-Ngo G. Developing Deep Learning Models to Predict Benign and Malicious Attacks in IoT Networks. IEEE. 2024. 10.1109/ICOCO62848.2024.10928206.
15) Hizal S, Cavusoglu U, Akgun D. A novel deep learning-based intrusion detection system for IoT DDoS security. *Internet of Things*. 2024;28:101336. 10.1016/j.iot.2024.101336.
16) Taşcı B. Deep-Learning-Based Approach for IoT Attack and Malware Detection. *Applied Sciences*. 2024;14(18). 10.3390/app14188505.
17) Raza MS, Sheikh MNA, Hwang IS. Ensemble learning-based DDoS attack recognition in IoT networks. *Computer Networks and Communications*. 2025;p. 73–83. 10.37256/cnc.3220256755.
18) Jony AI, Arnob AKB. A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset. *Journal of Edge Computing*. 2024;3(1):28–42. 10.55056/jec.648.
19) Abbas S, Alsubai S, Ojo S, Sampedro GA, Almadhor A, Hejaili AA, et al. An efficient deep recurrent neural network for detection of cyberattacks in realistic IoT environment. *The Journal of Supercomputing*. 2024;80(10):13557–13575. 10.1007/s11227-024-05993-2.
20) Yaras S, Dener M. IoT-based intrusion detection system using new hybrid deep learning algorithm. *Electronics*. 2024;13(6):1053. 10.3390/electronics13061053.
21) Al-Ghamdi AM, Alansari MM. Enhancing IoT Security: A Comparative Study of CNN and RNN-Based Anomaly Detection Using the CICIoT2023 Dataset. *IAENG International Journal of Computer Science*. 2025;52(5). Available from: https://www.iaeng.org/IJCS/issues_v52/issue_5/IJCS_52_5_12.pdf.
22) Polat O, Ahmad AA, Oyucu S, Algül E, Doğan F, Aksöz A. Temporal-Spatial Feature Extraction in IoT-based SCADA System Security: Hybrid CNN-LSTM and Attention-Based Architectures for Malware Classification and Attack Detection. *IEEE Access*. 2025. 10.1109/ACCESS.2025.3577761.
23) Behera A, Sahoo KS, Mishra TK, Bhuyan M. A combination learning framework to uncover cyber attacks in IoT networks. *Internet of Things*. 2024;28:101395. 10.1016/j.iot.2024.101395.
24) Susilo B, Muis A, Sari RF. Intelligent intrusion detection system against various attacks based on a hybrid deep learning algorithm. *Sensors*. 2025;25(2):580. 10.3390/s25020580.
25) Sharma H, Kumar P, Sharma K. Intelligent Time Series Analysis for Intrusion Detection in the Internet of Things: A Generative-Adversarial-Network-Enhanced Convolutional-Neural-Network–Long-Short-Term-Memory Framework Using Signal Features. *Intelligent Computing*. 2025;4:0127. 10.34133/icomputing.0127.
26) Nguyen-Cao HP, Ho NTK, Nguyen TK. MLMCID: Machine Learning for Multi-class Intrusion Detection Using the CIC-IoT-2023 Dataset. Springer. 2025. 10.1007/978-3-032-03527-1_9.
27) Alzu'bi A, Albashayreh A, Abuarqoub A, Alfawair MA. Explainable AI-Based DDoS Attacks Classification Using Deep Transfer Learning. *Computers, Materials & Continua*. 2024;80(3). 10.32604/cmc.2024.052599.
28) KS RR, Sujit BB. Sequential-Attention Based Neural Architecture Integrating BiLSTM and Multi-Head Attention for Dynamic Anomaly Detection in IoT Environments. *International Journal of Intelligent Engineering & Systems*. 2025;18(8). 10.22266/ijies2025.0930.43.
29) Tseng SM, Wang YQ, Wang YC. Multi-class intrusion detection based on transformer for IoT networks using CIC-IoT-2023 dataset. *Future Internet*. 2024;16(8):284. 10.3390/fi16080284.
30) Mustafa YEA, Mustafa MMA, Babiker ESM. Hybrid recurrent with spiking neural network model for enhanced anomaly prediction in IoT networks security. *Frontiers in Artificial Intelligence*. 2025;8:1651516. 10.3389/frai.2025.1651516.
31) Ain NU, Sardaraz M, Tahir M, Elsoud MWA, Alourani A. Securing IoT networks against DDoS attacks: a hybrid deep learning approach. *Sensors*. 2025;25(5):1346. 10.3390/s25051346.
32) Sheikh MNA, Raza MS, Hwang I, Hossain MA, Ullah I, Hasan T, et al. SDN-Enabled IoT Based Transport Layer DDoS Attacks Detection Using RNNs. *Computers, Materials & Continua*. 2025;85(2). 10.32604/cmc.2025.065850.

33) Ec-Sabery M, Abbou AB, Boushaba A, Mrabti F, Abbou RB. The Optimized Extreme Learning Machine (GA-OELM) for DDoS Attack Detection in Cloud Environment. 2025. 10.3844/jcssp.2025.146.157.
34) Chen SR, Chen SJ, Hsieh WB. Enhancing Machine Learning-Based DDoS Detection Through Hyperparameter Optimization. *Electronics*. 2025;14(16):3319. 10.3390/electronics14163319.
35) Raamesh L, Jothi S, Radhika S. Enhancing software reliability and fault detection using hybrid brainstorm optimization-based LSTM model. *IETE Journal of Research*. 2023;69(12):8789–8803. 10.1080/03772063.2022.2069603.
36) Hochreiter S, Schmidhuber J. Long short-term memory. *Neural Computation*. 1997;9(8):1735–1780. 10.1162/neco.1997.9.8.1735.
37) Shi Y. Brain storm optimization algorithm. Springer. 2011. 10.1007/978-3-642-21515-5_36.
38) Shi Y. .
39) Mousavirad SJ, Oliva D, Hinojosa S, Schaefer G. Differential evolution-based neural network training incorporating a centroid-based strategy and dynamic opposition-based learning. IEEE. 2021. 10.1109/CEC45853.2021.9504801.
40) Neto ECP, Dadkhah S, Ferreira R, Zohourian A, Lu R, Ghorbani AA. CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. *Sensors*. 2023;23(13):5941. 10.3390/s23135941.