SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I7P120

Volume 12 Issue 7, 274-286, July 2025
© 2025 Seventh Sense Research Group®

Original Article

Optimized Cascading Long Short-Term Memory model with Latin Sampling Satin Bowerbird Optimization Algorithm for Intrusion Detection in Internet of Things

Naveen Thimmahanumaiah Hosur[1], Vasantha Kumara Mahadevachar[2], Venkatesh Prasad BS[3], Thirthe Gowda MT[4]

[1]*Department of Computer Science and Engineering, Government Engineering College, Haveri, Karnataka, India.*
[2,4]*Department of Computer Science and Engineering, Government Engineering College, Hassan, Karnataka, India.*
[3]*Department of Computer Science and Engineering, Government Engineering College, Kushalnagar, Karnataka, India.*

[1]*Corresponding Author : th.naveen@gmail.com*

Received: 15 May 2025 Revised: 17 June 2025 Accepted: 16 July 2025 Published: 31 July 2025

Abstract *- The rapid development of Internet of Things (IoT) networks has significantly increased their vulnerability to cyberattacks, so it is essential to develop effective Intrusion Detection Systems (IDS). Traditional algorithms often struggle with a high false positive rate and scalability issues in dynamic IoT environments. For addressing these challenges, this article proposed Optimized Cascading Long Short-Term Memory with Latin Sampling Satin Bowerbird Optimization (OCLSTM-LSBO) algorithm to effectively identify intrusions. The deep cascading LSTM framework captures the deep temporal dependencies in network traffic and improves the identification of difficult intrusion patterns in IoT networks. Then, employed the LSBO algorithm to fine-tune the hyperparameters of the LSTM model, which improves classification accuracy and enhances the generalization ability of the model. In the pre-processing phase, the Min-Max normalization technique is used to normalise the features in a uniform range. The OCLSTM-LSBO algorithm obtained the highest accuracy of 98.97% using the CICIoT2023 dataset and 95.62% using ToNIoT dataset for multiclass classification when compared to existing algorithms like Federated Multi Layered Deep-Learning (Fed-MLDL).*

Keywords *- Internet of Things, Intrusion Detection System, Latin sampling satin bowerbird optimization, Multiclass classification, Optimized Cascading Long Short-Term Memory model.*

1. Introduction

The development of the Internet of Things (IoT) has significantly transformed various sectors by offering unprecedented connectivity and convenience [1, 2]. Additionally, to these technological growths, IoT has brought new security problems and vulnerabilities [3]. The growing number of interconnected devices involves smart home gadgets and industrial sensors, which have a highly increased vulnerability to potential invasions [4, 5]. To safeguard these interconnected environments from malicious activities and unauthorised access, robust intrusion detection algorithms are required [6]. Furthermore, Intrusion Detection Systems (IDS) have historically been based on signature-enabled algorithms that access incoming network information against known patterns of malicious behavior [7]. Though these algorithms are successful in countering familiar threats, they require support in identifying new or growing attacks that expose IoT systems to increasing hazards [8]. With the widespread utilization of IoT devices across different industries like industrial automation, healthcare and smart homes, security vulnerabilities in IoT environments have become a major concern [9]. Different parameters of IoT, like restricted resources, ever-changing network architectures and different communication protocols, offer substantial challenges for traditional IDS architectures [10]. The determination to secure IoT networks is understood by recent cyberattacks that target essential infrastructure and consumer systems. The large-scale Mirai botnet variant exploits unsecured IoT cameras and routers for launching Distributed Denial-of-Service (DDoS) attacks against European telecom providers and disrupts services to millions of users [11]. The ransomware attacks on smart healthcare systems in the U.S disabled access for interconnected medical systems and delayed emergency services. Moreover, botnet-based infiltration of smart city traffic sensors in Asia causes manipulated traffic congestion and data [12]. These determine that modern IoT attacks are highly dynamic and resourceful, making conventional signature-based IDS inadequate. This shows the urgent requirement for scalable, intelligent and adaptive IDS models. Traditional Machine Learning (ML)-based algorithms have been employed for tasks like authentication and risk assessment, aiming to obtain high accuracy in identifying

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

potential threats [13]. However, conventional IDS techniques struggle with the dynamic and heterogeneous nature of IoT environments, which often causes high False Positive Rates (FPR) and complexity in identifying threats [14-17]. Moreover, researchers have introduced Deep Learning (DL)-based approaches for improving detection rate and minimizing false positives [18]. Though these algorithms generally impact computational resources and processing time [14]. One of the main challenges for the solution of IDS techniques is its scalability. Particularly in difficult network environments, the equally huge size is mandatory for a method to identify and overcome the ever-evolving intrusions [19]. Traditional solutions generally involved large methods that demand substantial executional resources, making it impractical for deployment in resource-constrained environments like IoT devices [20]. However, these approaches become increasingly ineffective against rapidly evolving and sophisticated intrusions [21], which necessitate updated detection methods to address the limitations of existing systems. The primary objective of this manuscript is to develop a lightweight, scalable and precise IDS especially tailored to IoT environments. To obtain this, developed an optimized DL algorithm that integrated a Cascading Long Short-Term Memory (CLSTM) model with Latin Sampling – Satin Bowerbird Optimization (LSBO) algorithm. This integration enables the model to efficiently learns temporal attack patterns when reducing false alarms, minimizing computational overhead and improving detection accuracy in binary and multiclass intrusion detection systems.

1.1. Research Gap

There is a need for a lightweight, highly accurate IDS that handles the different and dynamic nature of IoT networks while maintaining a lower false alarm rate and high generalization. Many existing researches fail to capture deep temporal dependencies in sequential network traffic data and doesn't sufficiently optimize model hyperparameters, which limits their detection performance.

1.2. Problem Statement

The development of Internet of Things (IoT) devices presents significant security challenges due to their dynamic, heterogeneous, and resource-constrained nature. Traditional IDS, especially based on signature and conventional ML-based algorithms, is inefficient in identifying unknown cyber-attacks, resulting in high False Positive (FP) and poor scalability. Existing Deep Learning (DL) algorithms failed to generalise well in real-time IoT scenarios. Hence, there is a requirement for optimized, precise and lightweight IDS to efficiently identify known and unknown intrusions across complex IoT.

1.3. Objective

The main aim of this article is to develop an effective and scalable IDS for IoT environments. This research developed Optimized Cascading Long Short-Term Memory model with Latin Sampling Satin Bowerbird Optimization (OCLSTM-LSBO), which precisely identifies binary and multiclass intrusions. The algorithm minimizes the false alarms, improves detection accuracy and processes effectively in resource-constrained environments by advanced pre-processing and hyperparameter optimization algorithms.

1.4. Contributions

The paper's significant contributions are described as follows.

- The proposed multi-layered Cascading LSTM method can capture deep temporal dependencies in network traffic, improving the identification of complex and evolving intrusion patterns in IoT networks.
- Employed the LSBO algorithm for fine-tuning key hyperparameters of the LSTM model, enhancing classification accuracy and minimises model loss, and helping improve the model's generalization ability.
- The performance of the traditional SBO algorithm is improved using Latin Sampling (LS), which enhances diversity and coverage in optimization process to ensure better exploration of the parameter space and avoid local optimum.

The balance section of the article is arranged as follows: Section 2 analyses existing algorithms with their advantages and limitations. Section 3 provides the details of the proposed algorithm. Section 4 analyses and validates the performance of the proposed algorithm. The conclusion of this research is given in Section 5.

2. Literature Review

Chandnani et al. [22] developed the Federated Multi Layered Deep-Learning (Fed-MLDL), which employed physics-enabled Hyper Parameter Optimization (HPO). Moreover, FedRIME was used in a distributed federated learning for intrusion detection, which ensures better generalization for all clients' data through fine-tuning the hyperparameters in accordance with every client. The developed Fed-MLDL with Fed-RIME have defined essential enhancements in convergence speed, stability and client-specified customization in federated learning. The developed method had high false positive rates, which minimised classification reliability and precision.

Abdelaziz et al. [23] presented the Convolutional Kolmogorov-Arnold Network (CKAN) for IDS in an IoT environment. Multi-Layer Perceptron (MLPs) layers replaced CKAN method with KAN in the traditional Convolutional Neural Network (CNN) framework. KAN provided high performance compared to MLP layers with fewer parameters. The presented algorithm has less scalability, which minimises scalability and overall performance in resource-constrained IoT environments.

Aburasain [24] suggested an Enhanced Black Widow Optimization with Hybrid Deep Learning enabled Intrusion Detection (EBWO-HDLID) algorithm in an IoT-enabled Smart Farming environment. The EBWO-HDLID algorithm captures difficult patterns and identifies intrusions, ensuring security and reliability in smart farming. In the EBWO-HDLID algorithm, the Bald Eagle Search (BES) algorithm utilized for the feature selection process. The HDL model utilized for the classification process, and hyperparameters were tuned by the EBWO algorithm. The suggested method struggles to capture complex temporal patterns and fails to detect sophisticated attack behaviors.

Abbas et al. [25] introduced an algorithm for using federated learning for identifying huge attacks on IoT devices. The introduced algorithm utilised a Deep Neural Network (DNN) for obtaining accurate classification. Before method training, the data was pre-processed by different algorithms for developing trustworthiness for classification. The introduced algorithm included feature normalization, data balancing and prediction of the model by federated learning. The manual and ineffective hyperparameter tuning minimises the adaptability over datasets.

Chen et al. [26] implemented the Synaptic Intelligent Convolutional Neural Network (SICNN) for intrusion detection in IoT dynamic environments. Confirmed with real-time modifying intrusion data, several IDS are needed for a continuous combination of training data to retrain and refine the parameters. The storage demanded through continuous input data streams and the time consumed through repetition training pose challenges for IoT intrusion detection. SICNN method uses Synaptic Intelligence (SI) for optimizing the synaptic architecture of CNN, effectively mitigating CNN's forgetfulness for past identification and simplifying model training. However, the algorithm has inconsistent feature ranges in heterogeneous data, minimises training stability and generalization ability over multiple IoT datasets.

The literature review includes a broader range of recent and relevant work related to intrusion detection in IoT environments. Here, discuss the algorithms, including Fed-MLDL, optimisation-augmented models EBWO-HDLID, hybrid CNN models and memory-efficient neural networks SICNN. The drawbacks of these models are clearly described, which provides strong motivation for the growth of the proposed OCLSTM-LSBO model.

3. Proposed section

In this manuscript, the DL-based IDS method is developed to detect intrusions in IoT environments. The datasets, such as CICIoT2023 and ToNIoT, are used in this article to detect intrusions. In the pre-processing phase, the features are normalized and scaled to a uniform range. At last, classified by using a developed CLSTM and the hyperparameters of LSTM are optimized by using the LSBO algorithm. Figure 1 represents the process of intrusion detection in an IoT environment.

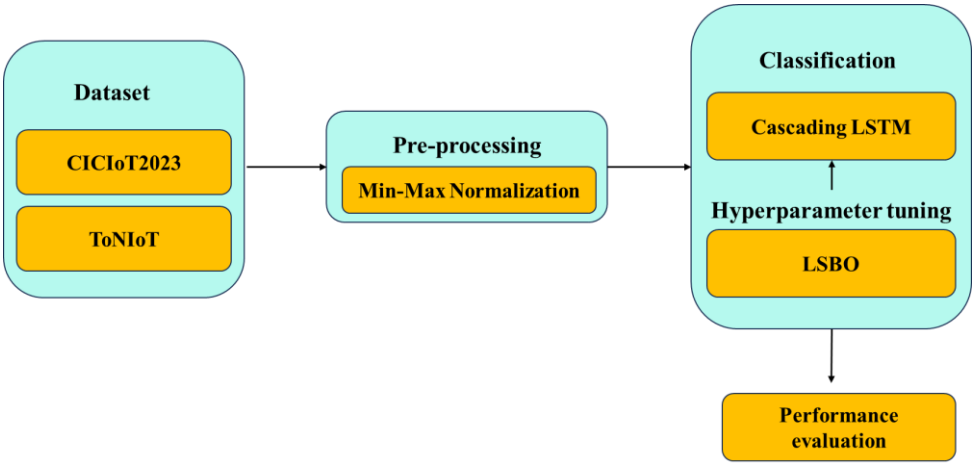

Fig. 1 Process of intrusion detection in an IoT environment

3.1. Dataset

The datasets such as CICIoT2023 [27] and ToNIoT [28] are used in this article to effectively detect intrusions in the IoT environment. These datasets are described in detail.

3.1.1. CICIoT 2023

CICIoT2023 is a dataset that supports the growth and evaluation of intrusion detection systems. This dataset is detailed and offers a broad and practical testbed to assess the efficacy of security solutions for a different range of IoT-specific cyber threats. This hosts the network behavior from 105 IoT devices across attacks, captures variability and complexity of conditions with 46 different attributes, including 33 various attack types, and these are divided into 7 classes like Spoofing, Brute Force, DoS, DDoS, Web-based and Reconnaissance. Table 1 represents the distribution of the CICIoT2023 dataset.

Table 1. Dataset description of the CICIoT2023 dataset

Parameters	Value
Number of classes	34 (1 benign class and 33 attack classes)
Number of instances	46,686,579
Number of attributes	46

3.1.2. ToNIoT

This dataset is a broadcast set of data focused on privacy and security challenges in the IoT domain. This dataset is developed primarily to analyse the impact of heterogeneity on IoT network intrusion datasets and highlights the requirement to standardize features and attack classifications. This dataset includes 4 different sub-datasets, each targeting a particular domain like smart cities, grids, factories and homes. Every sub-dataset defines a diverse group of data types, including system logs, sensor readings, network traffic logs, and metadata. The kind of attacks ranges from malware infections to DoS attacks and unauthorized access.

Table 2. Dataset description of the ToNIoT dataset

Parameters	Value
Number of classes	6 (Infiltration, Scan, DDoS, Botnet, Normal, PortScan)
Number of instances	17,168,894
Number of attributes	121

3.2. Pre-Processing using Min-Max normalization

The dimensionality of every feature in intrusion detection uses different attributes, the actual data directly used for detection analysis, and its results have high numerical levels, occupying a high weight in detection analysis. For effective model training, much significant stage, performed in data pre-processing, is normalization of data, which limits the feature values in a certain range for providing precise data detection [29, 30]. Here, Min-max normalization is considered to normalize the value of every feature in a range of 0 to 2. The mathematical expression for min-max normalisation is given as Equation (1).

$$x_{normalized} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

In the above Equation (1), x represents the present value of data features, x_{min} represents the minimum value of data features and x_{max} represents the maximum value of data features.

3.3. Classification using Cascading LSTM

The IDS method assigns an LSTM network to efficiently identify the intrusions. The ability of LSTM to preserve and adjust data over lengthy sequences provides the exceptional capability to identify attacks. The cascading LSTM is a neural network that involves a layering of several LSTM modules, one on top of the other. Developed method utilises a cascading LSTM that includes three LSTM layers. This makes it suitable for applications like IDS. The process of LSTM includes input, output and forget gates. The core of the LSTM mechanism is the input gate, which determines how much new data is incorporated into the memory cell at each time step. Validating the significance of the present input data enables LSTM to selectively strengthen its memory when retaining significant data. The process of the input gate I_t is measured by the present state X_t and past hidden state h_{t-1} in each time step t, its mathematical expression is given as Equations (2).

$$I_t = Sig(W_i[h_{t-1} \otimes X_t] + b_i) \quad (2)$$

Candidate value in the input gate is calculated by Equation (3).

$$\check{C}_t = \tanh(W_c[h_{t-1} \otimes X_t] + b_c) \quad (3)$$

In the above Equations (2) and (3), the W_i and W_c represents the weight factors, the b_i and b_c represents the bias of the input cell. After integrating weighted inputs and bias, the sigmoid activation function converts values in the range [0,1]. As the outcome, assigning the tanh function introduced the data that exhibits values in the range [0,1]. Forget gate stores the important information in the LSTM network, as that represents the degree to which past stored data is retrieved from the memory cell. This is an essential process for LSTM to obtain and capture patterns in data over long time intervals. In every time step, LSTM uses the present input data x_t and past hidden state h_{t-1} and forget gate is calculated by Equation (4).

$$F_t = Sig(W_f[h_{t-1} \otimes X_t] + b_f \quad (4)$$

In the above Equation (4), the b_f and W_f represent bias value and weight dynamics of the forget gate. Forget gate activates by processing element-wise multiplication on every component of the previous memory cell state C_{t-1}. This process determines which segments of memory are retained and which are discarded. The last configuration of updating the memory cell state C_t is designed through a dynamic relationship between a memory cell update, candidate cell state and input gate. Output O_t regulated transmission of data from a memory cell, the outcome or the following hidden state. This gate plays the essential role in determining the information as the last LSTM result in every step, and the mathematical expression is given as Equation (5).

$$O_t = Sig(W_o[h_{t-1} \otimes X_t] + b_o) \quad (5)$$

In the above Equation (5), the W_o represents the weight parameter and the b_o represents a bias vector. Modified hidden

state h_t acts as an origin point on the LSTM result in the present time step t or passed on following network layer on additional improvement, and is a mathematical formula given as Equation (6).

$$h_t = O_t \tanh \otimes (C_t) \tag{6}$$

By dynamic modulation of input gate activation, LSTM captures essential patterns and interconnections in data. In the cascading LSTM structure, the considered dropout layer is employed among LSTM layers to protect against overfitting through randomly eliminating feature subsets in training. This model, integrated with feedback recycling to an LSTM layer, provides a robust method generalization. Hyperparameters include a 0.5 dropout rate, and the stopping criteria are optimized to improve IDS performance, obtaining essential accuracies on CICIoT2023 and ToNIoT datasets. Through a complete forward pass, input data are exposed to the process in LSTM layers, resulting in prediction formation. Every LSTM unit in the network handles its inherent state, facilitates a capability for comprehension and retains significant patterns in sequential data. Efficacy of a method's prediction is evaluated by Mean Squared Error (MSE), and its mathematical expression is given in Equation (7).

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(x_i - \check{x})^2 \tag{7}$$

In the above Equation (7), the $\check{x}$ represents LSTM prediction, and x represents the original value in a dataset. By squaring values in a calculation of RMSE, huge errors receive more importance than fewer errors. RMSE is defined by Equation (8),

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \check{x})^2} \tag{8}$$

After measuring loss, LSTM initialises the backpropagation for measuring the gradient for loss related to weights and biases in every discrete time step. By processing backpropagation, the network gains the capability to learn from the errors and improve its prediction abilities across time. Parameters are optimized for minimising model loss. Using cascading LSTM for intrusion detection with CICIoT2023 and ToNIoT datasets has the potential to improve accuracy and resilience in identifying network intrusions and differences, thereby strengthening the overall security of network systems.

3.3.1. Hyperparameter using Satin Bowerbird Optimization (SBO) Algorithm

At last, tuning of the hyperparameter of C-LSTM is accomplished through the utilization of the SBO algorithm. SBO algorithm initially generates a uniform population that comprises a set of bower places. SBO algorithm has characteristics such as global optimization, feasible to implement, fewer number of parameters, robust and highly effective. Every position $(pop(i), Pos)$ is determined by variables which are assumed, and its mathematical expression is given as Equation (9),

$$pop(i).Pos = rand(1, n_{var}) \cdot (Var_{Max} - Var_{Min}) + Var_{Min}, \quad \forall_i \in n_{Pop} \tag{9}$$

It shows that the initial population value relies on the current minimal and maximal limits of the improvement parameter.

Latin Sampling (LS)

LS is a much precise sampling method that is effective for acquiring sample points. The algorithm has its essential strength, space-filling effect and convergence attributes, which are compared to random or stratified sampling algorithms. In this research, a new sample size produced through the LS algorithm provides high stability and wide implementation in SBO adjustment. LS is represented by $n \times d$ matrix. Each column, L includes an integer permutation from 1 to n, where every row of L is described as a sample point and its mathematical formula is given as Equation (10),

$$LS = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \left[\begin{pmatrix} x_{11} & \cdots & x_{1p} \\ \vdots & \ddots & \vdots \\ x_{N1} & \cdots & x_1 \end{pmatrix} \right] \tag{10}$$

In the above Equation (10), the x_i represents jth sample position, when samples are organised by random classification in terms of x, produced vector elements.

Iteration Adjustment by LS

The initial population of 30 individuals is selected randomly by LS. This algorithm is utilized for testing the complete design space with a smaller number of instances. AS the random nature of LS didn't provide optimum space-filling sampling, it iteratively produced 100 LS and sampling with the highest distance criterion among sample positions are chosen. The feature set value (30 populations and 100 maximum iterations) is updated for controlling optimization process.

The possibility of bower is evaluated by using Equations (11) and (12).

$$Prob_i = \frac{cost_i}{\sum_{k=1}^{n_{Pop}} cost_i}, \quad \forall_i \in n_{Pop} \tag{11}$$

$$cost_i = \begin{cases} \frac{1}{1+f(x)}, & f(x_i) \geq 0 \\ 1 + |f(x_i)|, & f(x_i) < 0 \end{cases} \tag{12}$$

Like other evolutionary-based optimizer, elitism is exploited for storing the optimum solution in each generation. In mating, males like each bird use their drives for decorating and developing a bower. The experienced and older males

attract much attention to the bower. These bowers have more fitness than other bowers. In the process of SBO, the position of the optimum bower produced by a bird is assessed as elite of kth iteration $(x_{elite,k})$ through the highest fitness and is capable to impact of impacting are measured based on Equation (13).

$$X_{ik}^{new} = X_{i,k}^{old} + \beta_k \left[\left(\frac{x_{jk}+x_{elite,k}}{2}\right) - X_{i,k}^{old}\right] \quad (13)$$

The roulette wheel selective method is exploited to select a better one with a good probability. In the SBO algorithm, variable β_k defines a step count, chooses the target bower, and its mathematical formula is given as Equation (14).

$$\beta_k = \frac{\alpha}{1+Prop_i} \quad (14)$$

An arbitrary modification is introduced to x_{ik} with some probability, the normal distribution is exploited through variance σ and the average of $x_{i,k}^{old}$, its mathematical expression is given as Equations (15) and (16).

$$X_{ik}^{new} \sim X_{ik}^{old} + \sigma \cdot N(0,1) \quad (15)$$

$$\sigma = Z \cdot (Var_{Max} - Var_{min}) \quad (16)$$

At last, every cycle is an old population, and the populations acquired are sorted, combined, assessed, and a novel population is produced. The SBO algorithm derived the fitness function to improve the classifier's result.

It defined positive values to signify the effective performance of the candidate solution. In this research, minimized error rate is considered as a fitness function and its mathematical formula is given as Equation (17).

$$fitness(x_i) = ClassifierErrorRate\ (x_i) = \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} \times 100 \quad (17)$$

Algorithm 1- OCLSTM-LSBO algorithm-based intrusion detection in IoT for reproducability

Input - Initialize parameters for CLSTM, population size and maximum iteration
Output - Classified labels
Pre-processing
Normalize all feature values to [0,1] using Min-Max Normalization
$x_{norm} = (x - \min(x))/\max(n) - \min(n))$
Split D into training set and test set
Define CLSTM model
    Define 3-layer LSTM with dropout between layers
    Output layer=softmax for multiclass / sigmoid for binary
    Initialize model with hyperparameters $H = \{dropout, learning\ rate, hidden\ units\}$
Optimize Hyperparameters using Latin Sampling SBO
    Generate initial population of solutions using Latin Sampling
    For $i = 1\ to\ P$
        Generate $H_i \in H_{space}\ via\ latin\ sampling$
Evaluate fitness of every solution
    For every H_i
        Train CLSTM using H_i on training set
        Evaluate accuray $1 - error\ on\ validation\ set \rightarrow Fitness(H_i)$
For $t = 1$ to Max Iteration:
    Choose elite solution H_{best} with highest fitness
    Employ SBO to update positions
    Choose target bower based on roulette selection
        Update candidate positions using SBO $H_{new} = H_{old} + \alpha \times Normal(\mu, \sigma)$
Evalute new population
Keep solution for next generation
Return H_{best} with highest fitness as optimized hyperparameters
Final Model Traininga nd Evaluation
    Train final CLSTM model using H_{best}
    Predict on test data
Return Trained OCLSTM-LSBO model and classification results.

4. Experimental Analysis

In this section, the performance of the OCLSTM-LSBO algorithm is simulated on a Python 3.12 environment equipped with an i5 processor, 8GB RAM and Windows 10 (64-bit). Also, presents the experimental outcomes for the OCLSTM-SBO algorithm with evaluation metrics and acquired outcomes with discussion.

Table 3 represents the performance comparison of T-LSBO with different DL-based algorithms like RNN, LSTM, GRU and CLSTM across two datasets, such as CICIoT2023 and ToNIoT.

Every method is evaluated on both binary and multi-class classification tasks, and metrics involve training time (s), Memory Usage (MB), loss and accuracy.

From the experimental outcomes, OCLSTM-LSBO outperforms traditional algorithms in terms of accuracy and loss, demonstrating its efficacy in capturing spatial and temporal features for intrusion detection.

While training time and memory usage are higher due to the complexity of the model, results effectively enhanced the detection performance.

Table 3. Performance evaluation of DL models on CICIoT2023 and ToNIoT datasets for intrusion detection

Methods	Tasks	Training time (s)	Memory Usage (MB)	Loss	Accuracy (%)
CICIoT2023 dataset					
RNN	Binary	68	190	0.0935	95.31
	Multi	84	230	0.1127	91.25
LSTM	Binary	72	205	0.0753	96.78
	Multi	88	256	0.1022	93.45
GRU	Binary	70	200	0.0692	97.11
	Multi	86	245	0.0967	94.10
CLSTM	Binary	85	240	0.0456	98.42
	Multi	102	310	0.0784	96.31
Proposed OCLSTM - LSBO	Binary	132	295	0.0167	99.45
	Multi	150	478	0.0241	98.97
ToNIoT dataset					
RNN	Binary	50	180	0.0813	96.12
	Multi	68	225	0.1075	90.56
LSTM	Binary	58	195	0.0689	97.02
	Multi	75	243	0.0914	92.78
GRU	Binary	56	190	0.0603	97.45
	Multi	72	238	0.0881	93.87
CLSTM	Binary	69	230	0.0417	98.85
	Multi	83	298	0.0678	94.55
Proposed OCLSTM - LSBO	Binary	76	275	0.0231	99.97
	Multi	95	450	0.0347	95.62

Table 4 represents the classification performance of various DL models like RNN, LSTM, GRU and CLSTM with OCLSTM-LSBO on binary and multiclass intrusion detection using the CICIoT2023 dataset.

For both classification tasks, the OCLSTM-LSBO algorithm outperforms the baseline method across all evaluation measures. In binary classification, the OCLSTM-LSBO obtains the highest accuracy of 99.45%, showing robust detection capabilities. Same as in multiclass classification, it provides strong performance with the highest accuracy of 98.97%. These outcomes represent the efficacy of OCLSTM-LSBO to learn temporal and spatial features, making it suitable for precise and reliable intrusion detection in complex IoT environments.

Table 4. Performance of OCLSTM-LSBO with different DL models using the CICIoT2023 dataset on binary and multiclass classification

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC (%)
Binary Classification					
RNN	98.05	97.82	97.53	97.67	97.03
LSTM	98.24	98.07	97.85	97.95	97.41
GRU	98.72	98.51	98.32	98.41	97.84
CLSTM	99.16	98.83	98.55	98.68	98.32
Proposed OCLSTM - LSBO	99.45	99.37	99.21	99.28	98.65
Multiclass Classification					
RNN	96.82	96.64	96.43	96.53	95.87
LSTM	97.25	97.19	96.89	97.03	96.21
GRU	97.73	97.45	97.17	97.30	96.58
CLSTM	98.32	98.04	97.92	97.97	96.89
Proposed OCLSTM - LSBO	98.97	98.85	98.78	98.81	97.43

Table 5 represents the classification performance of various DL models like RNN, LSTM, GRU and CLSTM with OCLSTM-LSBO on binary and multiclass intrusion detection using the ToNIoT dataset. The OCLSTM-LSBO method demonstrates high performance across both classification types. In binary classification, it obtains an accuracy of 99.95% on key metrics, effectively outperforming traditional models like RNN, LSTM, GRU and CLSTM. In multiclass classification, the OCLSTM-LSBO method obtains 95.62% accuracy and the highest AUC of 96.57%. These outcomes represent the superior ability of OCLSTM-LSBO in precisely detecting and classifying intrusions over complex IoT network environments.

Table 5. Performance of OCLSTM-LSBO with different DL models using ToNIoT dataset on binary and multiclass classification

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC (%)
Binary Classification					
RNN	97.79	97.52	97.28	97.39	96.80
LSTM	98.28	98.02	97.72	97.86	97.31
GRU	98.67	98.44	98.10	98.26	97.68
CLSTM	99.31	99.05	98.76	98.90	98.03
Proposed OCLSTM - LSBO	99.95	99.95	99.95	99.95	98.54
Multiclass Classification					
RNN	94.31	94.08	93.54	93.80	95.21
LSTM	94.79	94.36	93.87	94.11	95.68
GRU	95.01	94.85	94.19	94.51	96.06
CLSTM	95.34	95.12	94.42	94.76	96.32
Proposed OCLSTM - LSBO	95.62	95.36	94.95	95.15	96.57

Table 6 represents the 5-fold cross-validation accuracy outcomes for the OCLSTM-LSBO algorithm with different DL-based algorithms like RNN, LSTM, GRU and CLSTM on a binary task using CICIoT2023 and ToNIoT datasets. Every method is validated across five folds to assess its generalization ability and performance consistency. In both datasets, the OCLSTM-LSBO algorithm consistently obtained the highest accuracy across all folds, with a mean accuracy of 99.42% on CICIot2023 and 99.90% on ToNIoT.This demonstrates its robustness in identifying the intrusion patterns in IoT environments. Traditional algorithms like RNN and LSTM show comparatively less performance, with mean accuracy ranging from 95.26% to 96.74% on CICIoT2023 and 96.12%-96.94% on ToNIoT. CLSTM and GRU algorithms performed better than RNN and LSTM but were still outperformed by the OCLST-LSBO algorithm. These outcomes validate the ability of OCLSTM-LSBO to maintain high detection accuracy across multiple data splits, which represents high generalization, less variance and high reliability for real-time intrusion detection in IoT-based networks.

Table 6. 5-fold cross-validation accuracy of OCLSTM-LSBO on CICIoT2023 and ToNIoT datasets

K-fold values	RNN	LSTM	GRU	CLSTM	OCLSTM-LSBO
CICIoT2023 dataset					
1	95.2	96.7	97.1	98.3	99.4
2	95.3	96.8	97.2	98.4	99.5
3	95.1	96.6	97.0	98.2	99.3
4	95.4	96.9	97.1	98.4	99.4
5	95.3	96.7	97.1	98.5	99.5
Mean	95.26	96.74	97.10	98.36	99.42
ToNIoT dataset					
1	96.1	96.9	97.3	98.7	99.9
2	96.0	96.8	97.2	98.8	99.9
3	96.2	97.0	97.4	98.9	99.9
4	96.1	96.9	97.3	98.8	99.9
5	96.2	97.1	97.4	98.9	99.9
Mean	96.12	96.94	97.32	98.82	99.90

Table 7. Performance of statistical analysis and computational analysis of the proposed model

Models	Accuracy (%)	Training time (s)	Inference time (s)	Standard deviation	Confidence Interval
RNN	95.31	68	0.42	$\pm$0.10	[95.12, 95.40]
LSTM	96.78	72	0.46	$\pm$0.12	[96.56, 96.92]
GRU	97.11	70	0.44	$\pm$0.10	[96.96, 97.24]
CLSTM	98.42	85	0.53	$\pm$0.14	[98.18, 98.54]
OCLSTM-LSBO	99.45	132	0.57	$\pm$0.08	[99.34, 99.50]

Table 7 presents the comparative analysis of various DL models in terms of accuracy, training time, inference time, standard deviation and confidence interval. The proposed OCLSTM-LSBO model outperformed baseline models like RNN, LSTM, GRU and CLSTM, obtaining the highest accuracy with minimal standard deviation and a confidence

interval that shows strong stability and generalization ability. When considering the slight training and inference time compared to existing algorithms, it is justified by its substantial performance improvements.

This determined the proposed model's effectiveness in accurately learning spatiotemporal patterns and their suitability for real-time IDS on IoT.

4.1. Analysis of the Confusion Matrix and ROC Curve

In this section, the confusion matrix and ROC curve for both binary classification and multiclass classification tasks are analyzed. Figures 2 and 3 represent the confusion matrix on the CICIoT2023 dataset for binary and multiclass classification, respectively. Figure 4 represents the ROC Curve for the CICIOT2023 dataset. Figures 5 and 6 represent the confusion matrix on the ToNIoT dataset for binary and multiclass classification, respectively. Figure 7 represents the ROC Curve for the CICIOT2023 dataset.

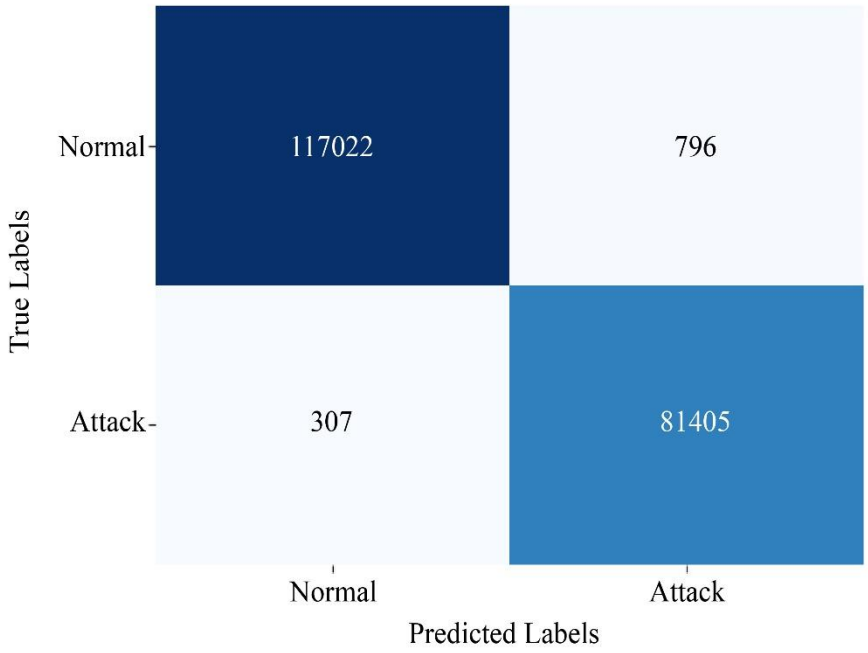

Fig. 2 On binary classification using CICIoT2023

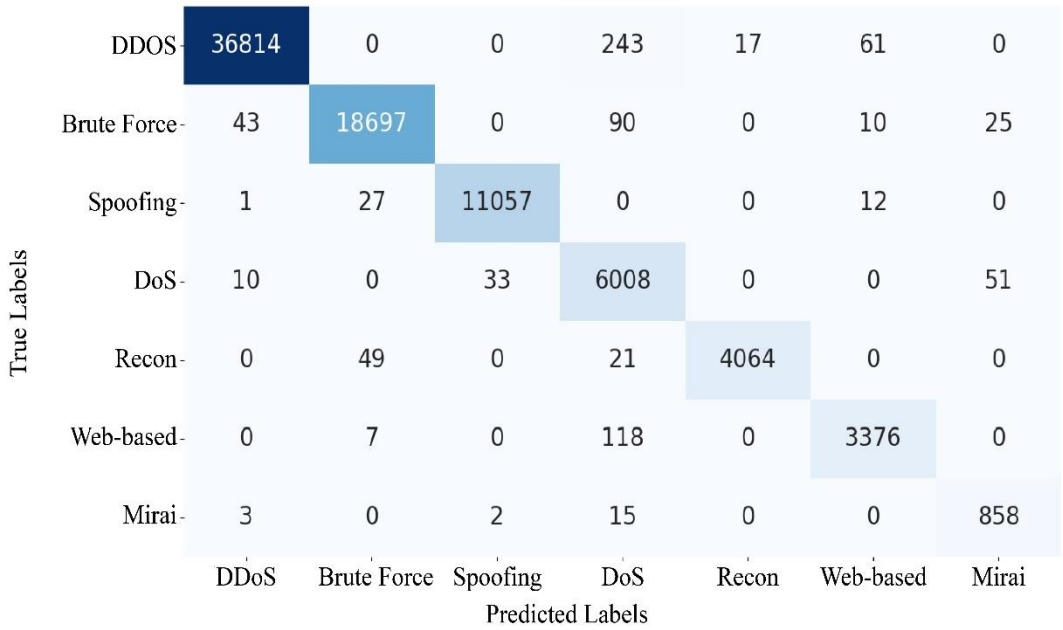

Fig. 3 On multiclass classification using CICIoT2023

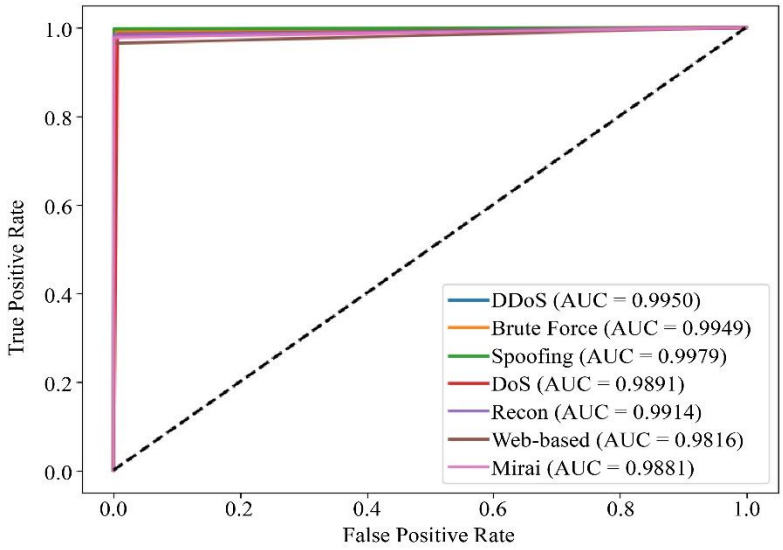

Fig. 4 ROC curve using CICIoT2023

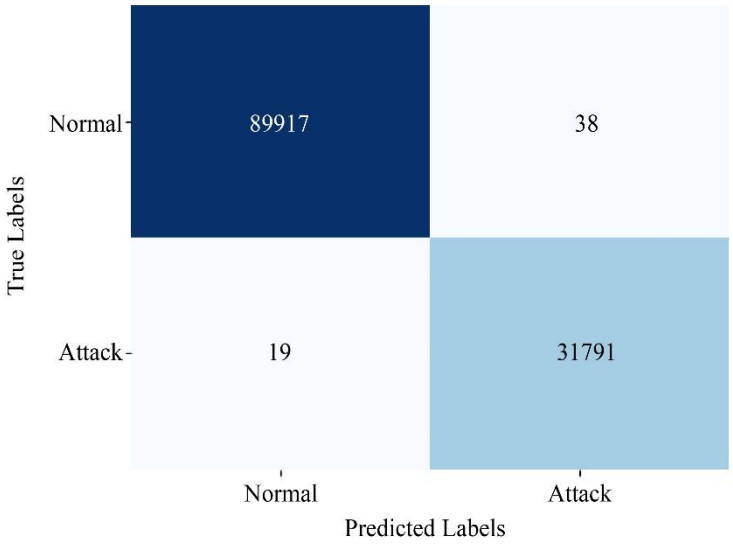

Fig. 5 On binary classification using ToNIoT

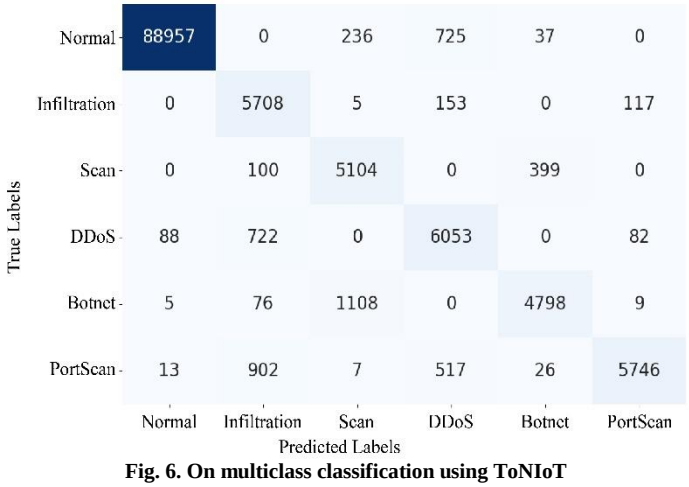

Fig. 6. On multiclass classification using ToNIoT

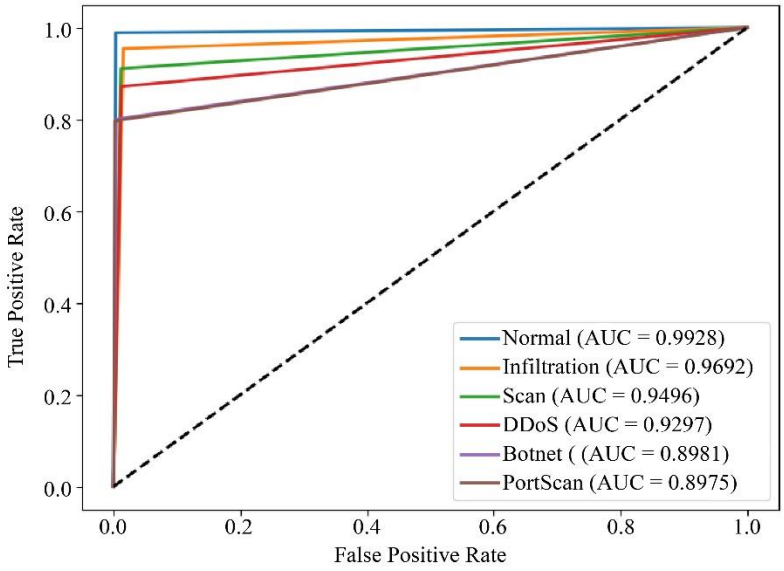

Fig. 7 ROC Curve using ToNIoT

4.2. Comparative Analysis

Table 8 compares the performance of different existing algorithms with OCLSTM-LSBO for binary and multiclass intrusion detection on CICIoT2023 and ToNIoT datasets. The OCLSTM-LSBO algorithm outperforms existing algorithms across both datasets and classification tasks. In binary classification, it obtains 99,45% accuracy on the CICIoT2023 dataset and 99,95% accuracy on the ToNIoT dataset.

In multiclass classification, it demonstrates superior generalization on CICIoT2023 datasets and high performance on the ToNIoT dataset. Compared to existing algorithms like Fed-MLDN with Fed-RIME [22], CKAN [23], EBWO-HDLID [24] and SICNN [26] offers balanced and robust detection ability for both binary and multiclass intrusion detection in IoT environments.

Table 8. Comparison of existing algorithms with OCLSTM-LSBO for intrusion detection on CICIoT2023 and ToNIoT datasets

Methods	Tasks	Datasets	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Fed-MLDN with Fed-RIME [22]	Binary and Multi-classification	CICIoT2023	99.2	NA	NA	NA
		ToNIoT	98.2	NA	NA	NA
CKAN [23]	Binary classification	CICIoT2023	99.22	99.81	99.40	99.60
		ToNIoT	99.93	99.95	99.91	99.93
	Multi classification	CICIoT2023	98.84	98.84	98.84	98.84
		ToNIoT	93.30	93.30	93.30	93.30
EBWO-HDLID [24]	Multi classification	ToNIoT	98.81	90.84	78.95	79.49
SICNN [26]	Multi classification	CICIoT2023	97.69	NA	NA	NA
Proposed OCLSTM - LSBO	Binary classification	CICIoT2023	99.45	99.37	99.21	99.28
		ToNIoT	99.95	99.95	99.95	99.95
	Multi classification	CICIoT2023	98.97	98.85	98.78	98.81
		ToNIoT	95.62	95.36	94.95	95.15

The proposed OCLSTM-LDBO model differentiates itself from existing algorithms by its hybrid combination of a deep temporal learning model with LSBO. Unlike traditional models like Fed-MLDL [22] that focus on federated optimization or CKAN [23] that employ kernel adaptations, the proposed model captures deep temporal patterns while being resource-effective and highly adaptive. Moreover, the LSBO ensures robust hyperparameter tuning, minimizing overfitting and enhancing generalization ability across heterogeneous datasets. As shown in Table 8, the proposed model obtains superior performance in terms of accuracy, precision and F1-score across all datasets, determining their advantages over recent SOTA IDS models.

4.3. Discussion

The novelty of the proposed model is a hybrid combination of CLSTM with LSBO for intrusion detection in IoT environments. Unlike traditional algorithms that lack hyperparameter optimization and fail to capture long-term dependencies in sequential traffic data, the proposed approach

addresses both drawbacks. The CLSTM efficiently learns deep temporal patterns in network traffic, and LSBO ensures optimized hyperparameter tuning for enhanced generalization and minimized model loss. In Fed-MLDL with Fed-RIME [22], which mainly focuses on federates training and CKAN [23], which modified CNN layers with KAN but lacks scalability, the proposed model determines superior performance on accuracy, precision and reduction of false positives. Additionally, unlike EBWO-HDLID [24], which uses a basic DL architecture and struggles with temporal pattern detection and SICNN [26] that suffered from inconsistency across heterogeneous data, the proposed model obtains better consistency and adaptability across all datasets. The datasets considered in this manuscript are publicly available, anonymized and gathered under controlled environments with null Personally Identifiable Information (PII) included. These datasets are gathered for academic and research purposes, ensuring compliance with data protection principles like GSPR and ethical research standards.

5. Conclusion

In this manuscript, an efficient and scalable intrusion detection model, OCLSTM-LSBO, is proposed to address the security challenges in dynamic IoT environments. The model integrates a CLSTM network with SBO for automated hyperparameter tuning, enabling the capture of deep temporal patterns while maintaining optimal model performance. The deep cascading LSTM framework captures the deep temporal dependencies in network traffic and improves the identification of difficult intrusion patterns in IoT networks. Then, employed the LSBO algorithm to fine-tune the hyperparameters of the LSTM model, which improves classification accuracy and enhances the generalization ability of the model. Min-Max normalization is employed during pre-processing to ensure uniform feature scaling, and Latin Sampling enhances the diversity of the optimization process. Experimental evaluations on benchmark datasets, CICIoT2023 and ToNIoT, reveal that the proposed method significantly outperforms traditional deep learning models, including RNN, LSTM, GRU, and CLSTM, in both binary and multiclass intrusion detection tasks. The OCLSTM-LSBO model achieves a remarkable accuracy of up to 99.95% in binary classification and demonstrates strong performance across all evaluation metrics. This confirms the model's robustness, precision, and suitability for deployment in real-time, resource-constrained IoT systems.

5.1. Limitations

The proposed OCLSTM-LSBO model needs high training time and computational resources because of its deep cascading architecture and optimization process, which limit its deployment in less powerful IoT devices. Moreover, models have not been evaluated on real-world zero-day attacks that affect their adaptability in high-dynamic threat environments.

5.2. Future Work

Future research focuses on improving the OCLSTM-LSBO method for detecting zero-day attacks by integrating adaptive learning mechanisms. Moreover, the method is extended for real-time deployment by edge computing frameworks to support continuous intrusion detection in dynamic and resource-constrained environments.

References

[1] Louai A. Maghrabi, "Automated Network Intrusion Detection for Internet of Things: Security Enhancements," *IEEE Access*, vol. 12, pp. 30839-30851, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ayoob Almotairi et al., "Enhancing Intrusion Detection in IoT Networks Using Machine Learning-Based Feature Selection and Ensemble Models," *Systems Science & Control Engineering*, vol. 12, no. 1, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Randa Allafi, and Ibrahim R. Alzahrani, "Enhancing Cybersecurity in the Internet of Things Environment Using Artificial Orca Algorithm and Ensemble Learning Model," *IEEE Access*, vol. 12, pp. 63282-63291, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Louai A. Maghrabi et al., "Enhancing Cybersecurity in the Internet of Things Environment using Bald Eagle Search Optimization with Hybrid Deep Learning," *IEEE Access*, vol. 12, pp. 8337-8345, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mansi Bhavsar et al., "Fl-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices for Transportation IoT," *IEEE Access*, vol. 12, pp. 52215-52226, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] D. Jayalatchumy et al., "Improved Crow Search-Based Feature Selection and Ensemble Learning for IoT Intrusion Detection," *IEEE Access*, vol. 12, pp. 33218-33235, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Fatma S. Alrayes et al., "Intrusion Detection in IoT Systems Using Denoising Autoencoder," *IEEE Access*, vol. 12, pp. 122401-122425, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Hayam Alamro et al., "Modelling of Bayesian-Based Optimized Transfer Learning Model for Cyber-Attack Detection in Internet of Things Assisted Resource Constrained Systems," *IEEE Access*, vol. 12, pp. 177298-177311, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Zhixin Xia et al., "PSO-GA Hyperparameter Optimized ResNet-BiGRU-Based Intrusion Detection Method," *IEEE Access*, vol. 12, pp. 135535-135550, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Aya G. Ayad, Nehal A. Sakr, and Noha A. Hikal, "A Hybrid Approach for Efficient Feature Selection in Anomaly Intrusion Detection for IoT Networks," *The Journal of Supercomputing*, vol. 80, no. 19, pp. 26942-26984, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ibrahim A. Fares et al., "TFKAN: Transformer based on Kolmogorov-Arnold Networks for Intrusion Detection in IoT Environment," *Egyptian Informatics Journal*, vol. 30, pp. 1-13, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mimouna Abdullah Alkhonaini et al., "Sandpiper Optimization with Hybrid Deep Learning Model for Blockchain-Assisted Intrusion Detection in IOT Environment," *Alexandria Engineering Journal*, vol. 112, pp. 49-62, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] Asadullah Momand, Sana Ullah Jan, and Naeem Ramzan, "ABCNN-IDS: Attention-Based Convolutional Neural Network for Intrusion Detection in IoT Networks," *Wireless Personal Communications*, vol. 136, no. 4, pp. 1981-2003, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jing Li et al., "Optimizing IoT Intrusion Detection System: Feature Selection versus Feature Extraction in Machine Learning," *Journal of Big Data*, vol. 11, no. 1, pp. 1-44, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Tin Lai et al., "Ensemble Learning Based Anomaly Detection for IoT Cybersecurity via Bayesian Hyperparameters Sensitivity Analysis," *Cybersecurity*, vol. 7, no. 1, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Shahad Altamimi, and Qasem Abu Al-Haija, "Maximizing Intrusion Detection Efficiency for IoT Networks Using Extreme Learning Machine," *Discover Internet Things*, vol. 4, no. 1, pp. 1-37, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Engy El-Shafeiy et al., "Deep Complex Gated Recurrent Networks-Based IoT Network Intrusion Detection Systems," *Sensors*, vol. 24, no. 18, pp. 1-22, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Riccardo Lazzarini, Huaglory Tianfield, and Vassilis Charissis, "A Stacking Ensemble of Deep Learning Models for IoT Intrusion Detection," *Knowledge-Based System*, vol. 279, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Gutierrez-Portela Fernando et al., "Enhancing Intrusion Detection in IoT Communications Through ML Model Generalization With a New Dataset (IDSAI)," *IEEE Access*, vol. 11, pp. 70542-70559, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] P. Sanju, "Enhancing Intrusion Detection in IoT Systems: A Hybrid Metaheuristics-Deep Learning Approach with Ensemble of Recurrent Neural Networks," *Journal of Engineering Research*, vol. 11, no. 4, pp. 356-361, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Marwa Keshk et al., "An Explainable Deep Learning-Enabled Intrusion Detection Framework in IoT Networks," *Information Sciences*, vol. 639, pp. 1-20, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Chirag Jitendra Chandnani et al., "A Physics-Based Hyper Parameter Optimized Federated Multi-Layered Deep Learning Model for Intrusion Detection in IoT Networks," *IEEE Access*, vol. 13, pp. 21992-22010, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[23] Mohamed Abd Elaziz, Ibrahim Ahmed Fares, and Ahmad O. Aseeri, "CKAN: Convolutional Kolmogorov-Arnold Networks Model for Intrusion Detection in IoT Environment," *IEEE Access*, vol. 12, pp. 134837-134851, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Rua Y. Aburasain, "Enhanced Black Widow Optimization with Hybrid Deep Learning Enabled Intrusion Detection in Internet of Things-Based Smart Farming," *IEEE Access*, vol. 12, pp. 16621-16631, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Sidra Abbas et al., "A Novel Federated Edge Learning Approach for Detecting Cyberattacks in IoT Infrastructures," *IEEE Access*, vol. 11, pp. 112189-112198, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Hui Chen et al., "Intrusion Detection Using Synaptic Intelligent Convolutional Neural Networks for Dynamic Internet of Things Environments," *Alexandria Engineering Journal*, vol. 111, pp. 78-91, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[27] CIC IoT dataset, University of New Brunswick, 2023. [Online]. Available: https://www.unb.ca/cic/datasets/iotdataset-2023.html

[28] Nour Moustafa, The TON_IoT datasets, Unsw Sydney, 2021. [Online]. Available: https://research.unsw.edu.au/projects/toniot-datasets

[29] Shankar Deva et al., "Lightweight Hybrid CAE-ELM and Enhanced Smote Based Intrusion Detection for Networks," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 6, pp. 1006-1021, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[30] Woothukadu Thirumaran Valavan, Nalini Joseph, and G. Umarani Srikanth, "Network Intrusion Detection System based on Information Gain with Deep Bidirectional Long Short-Term Memory," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 4, pp. 45-56, 2024. [CrossRef] [Google Scholar] [Publisher Link]