Mathematics

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

AIMS Mathematics, 10(12): 30068–30108.
DOI: 10.3934/math.20251322
Received: 20 September 2025
Revised: 24 November 2025
Accepted: 26 November 2025
Published: 23 December 2025

Research article

Mitigating DDoS attacks through ensemble learning models integrated with two-tier heuristic optimisation techniques for effective cyber defence

Hend Khalid Alkahtani[1], Mohammed Baihan[2], Mohammed Burhanur Rehman[3], Randa Allafi[4,*], Sultan Almutairi[5], Ibrahim Zalah[6], Nouf Atiahallah Alghanmi[7] and Mohammed Mujib Alshahrani[8]

[1] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P. O. Box 84428, Riyadh 11671, Saudi Arabia
[2] Department of Computer Science and Engineering, College of Applied Studies, King Saud University, P. O. Box 11451, Riyadh, Saudi Arabia
[3] Department of Computer Science, Applied College at Mahayil, King Khalid University, Saudi Arabia
[4] Department of Computer Science, College of Science, Northern Border University, Arar, Saudi Arabia
[5] Department of Computer Science, Applied College, Shaqra University, Shaqra 15526, Saudi Arabia
[6] Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Saudi Arabia
[7] Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh 25732, Saudi Arabia
[8] Department of Information Systems and Cybersecurity, College of Computing and Information Technology, University of Bisha, P. O. Box 551, Bisha, Saudi Arabia

* **Correspondence:** Email: Randa.allafi@nbu.edu.sa.

Abstract: The internet is the most effective means of communication in the modern world. Therefore, cyber-attacks are becoming more frequent, and their consequences are becoming increasingly severe. Distributed denial of service (DDoS) is one of the five most effective and costly cyberattacks. DDoS attacks are the most prevalent and expensive in today's evolving cybersecurity landscape. However, their ability to disrupt network services causes significant financial losses and has become an effective means of DDoS detection and prevention, both of which are essential for organisations. Network monitoring and control systems have found it challenging to recognise the numerous classes of denial of service (DoS) and DDoS attacks, as they all work exclusively. Therefore, an effective model is needed for attack detection. A previous study has established that shallow and deep learning (DL) methods are vital for identifying DDoS threats; however, there is a lack of research on time-based features and classification across numerous DDoS threat categories. This manuscript introduces an ensemble learning model integrated with two-tier heuristic optimisation techniques for effective cyber defence (ELMT2HO-ECD) methodology. The primary purpose of the ELMT2HO-ECD methodology is to provide a robust solution for detecting and mitigating DDoS attacks in real time. Initially, the ELMT2HO-ECD approach applies mean normalisation to the data to measure the feature within a specified range. Furthermore, the mountain gazelle optimiser (MGO) approach is utilised for feature extraction. For DDoS attack detection, ensemble DL models, namely convolutional long short-term memory (ConvLSTM), Wasserstein autoencoder (WAE), and temporal convolutional networks (TCN), are employed. To further enhance the performance of the three ensemble models, hyperparameter tuning is performed using the improved pufferfish optimisation algorithm (IPOA), which optimises the models' parameters to achieve higher accuracy. The ELMT2HO-ECD model is evaluated on the CICIDS2017, CICIDS2018, and CICIDS2019 datasets. Validation of the performance of the ELMT2HO-ECD model demonstrated superior accuracy of 98.93%, 98.43%, and 99.23% compared with existing techniques.

Keywords: pufferfish optimisation algorithm; ensemble learning; DDoS; cyberattack; deep learning; feature selection
Mathematics Subject Classification: 37M10

1. Introduction

Today, the Internet has become a crucial component of everyday activities. It enables interaction to be simpler. The internet of things (IoT) is becoming increasingly adopted in daily usage and business sectors [1]. IoT devices are compact and can interact with one another without a person present. The IoT is implemented on different platforms, namely smart factories, smart farms, smart homes, and expanding IoT devices. This will expose all devices to the threat of Distributed denial of service (DDoS) exploitation. IoT devices can't handle the intricate security framework due to their limited capabilities, such as processing power and storage, making them particularly susceptible [2]. If this susceptibility is not resolved, it may be exploited and used by IoT devices to execute DDoS attacks. It is presently considered a harmful threat on the Internet. DDoS attack agents attempt to prevent authorised clients from accessing services. Such attacks pose a threat due to the likelihood of real-time attacks from multiple points. Hence, until it stops, it is challenging to identify the original internet protocol (IP) address that causes this damage [3]. DDoS attacks also target legitimate networks to flood them with massive requests. When this occurs, the data units will originate from reliable sources that cannot be blocked or disabled. A single controller can direct a massive set of bots to send an enormous number of requests, thereby entirely occupying bandwidth in a DDoS attack [4]. The key role in a DDoS attack is the core function hub. These types of attacks occur very rapidly. Therefore, identifying DDoS attacks is a much stronger security approach than identifying crackers. Additionally, DDoS attacks have evolved alongside advances in security methods. Since the former types of defense depends only on identifying malicious activity or anomalies, anomaly-enabled detection is considered more advanced than signature-based detection [5]. Figure 1 illustrates the general structure of DDoS attack detection.

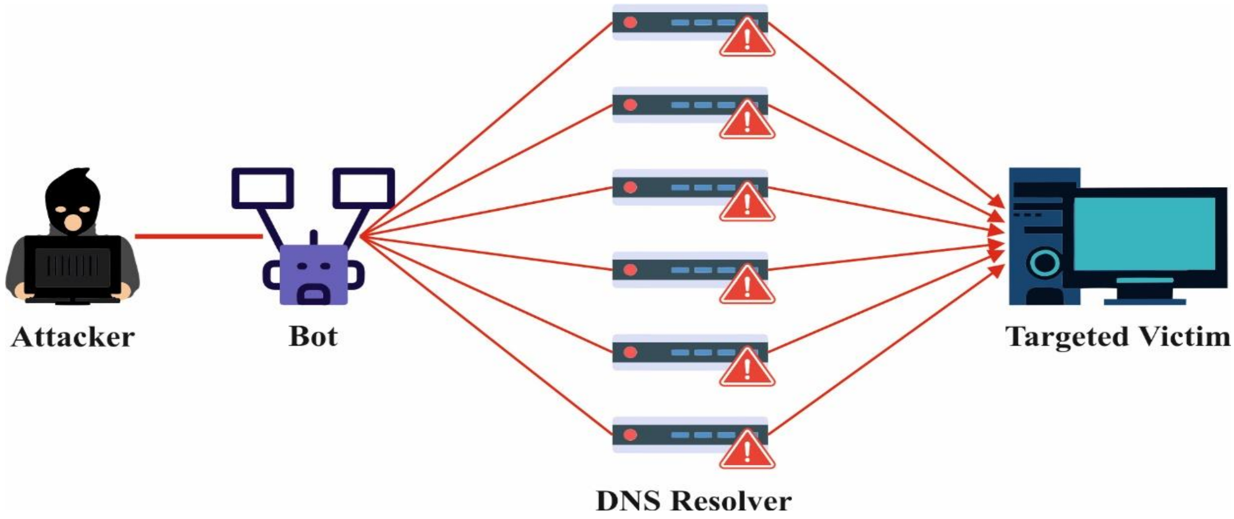


Figure 1. General structure of DDoS attack detection.

There are two major groups of DDoS attacks: Volumetric and application-layer attacks. The first attack category overloads and drains the system's bandwidth. The second attack category is more advanced and usually employs minimal bandwidth to initiate. It emphasizes specific services or applications and progressively depletes network resources [6]. DDoS attacks pose a significant obstacle and require a comprehensive strategy to mitigate and manage the associated threats. Several methods are presented for detecting, mitigating, and preventing DDoS attacks [7]. The two main detection strategies are anomaly detection (AD) and signature-based. The AD technique can recognize fresh and novel threats by detecting anomalous conditions triggered by an attack [8]. Signature-based techniques can only recognize attacks whose patterns are already documented and are ineffective against zero-day or new attacks. A notable gap exists in the analysis of DDoS attack mitigation, even as defense mechanisms are becoming more efficient and attack strategies are growing more complex [9]. As a result, new types of DDoS attacks may emerge, which current detection techniques can not handle efficiently. Deep learning (DL) models can efficiently recognize DDoS attacks because the information is classified, and the models extract features. DL frameworks, such as RNN and CNN, are constructed using a sequence of nonlinear transformation layers to perform multiple stages of information abstraction from a set of labelled inputs. Hence, DL acts as an effective method for DDoS identification [10].

This manuscript introduces an ensemble learning model integrated with two-tier heuristic optimization techniques for effective cyber defense (ELMT2HO-ECD) methodology. The primary purpose of the ELMT2HO-ECD methodology is to provide a robust solution for detecting and mitigating DDoS attacks in real time. Initially, the ELMT2HO-ECD approach applies mean normalization to the data to measure the feature within a specified range. Furthermore, the mountain gazelle optimizer (MGO) approach is utilized for feature extraction. For DDoS attack detection, ensemble DL models, namely convolutional long short-term memory (ConvLSTM), the wasserstein autoencoder (WAE), and temporal convolutional networks (TCNs), are employed. To further enhance the performance of the three ensemble models, hyperparameter tuning is performed using the improved pufferfish optimization algorithm (IPOA), which optimizes model parameters to achieve higher accuracy. The ELMT2HO-ECD model is evaluated on the CICIDS2017, CICIDS2018, and CICIDS2019 datasets. The key contributions of the ELMT2HO-ECD model are listed below.

- The ELMT2HO-ECD method applies mean normalization to standardize network traffic data, ensuring consistent feature scaling across samples. This improves training stability and improves convergence speed. It also contributes to more accurate detection by minimizing data discrepancies.
- The ELMT2HO-ECD approach utilizes the MGO model for effectual feature extraction by detecting the most relevant features from the dataset, significantly mitigating dimensionality. This optimization enhances both the accuracy of DDoS detection and computational efficiency. It allows the model to concentrate on key patterns, improving overall performance.
- The ELMT2HO-ECD model integrates ConvLSTM, WAE, and TCN to capture spatial, temporal, and deep abstract patterns in DDoS traffic, enabling robust detection across varying attack types. This hybrid architecture efficiently models both short- and long-term dependencies within the data, improving the technique's ability to detect intrinsic attack patterns with higher accuracy.
- The ELMT2HO-ECD methodology implements the IPOA method to fine-tune hyperparameters, ensuring optimal performance in detecting DDoS attacks. IPOA improves the model's ability to find the optimal parameter combination, enhancing accuracy and efficiency. This results in a more reliable and adaptive detection system.

The novelty of the ELMT2HO-ECD model lies in the hybrid integration of the bio-inspired MGO and IPOA techniques with advanced DL methods, including ConvLSTM, WAE, and TCN. This integration creates a robust, adaptive framework capable of detecting complex DDoS attack patterns. The model's capability to utilize optimization and DL methods for accurate detection in dynamic environments is a crucial distinguishing factor.

2. Literature review

The authors [11] designed a federated learning (FL) method for denial of service (DoS) attack detection and classification (FLDoSADC-DTL) through deep TL for blockchain-aided industrial IIoT infrastructure. BC tools ensure safe communication in IIoT environments. This method executes the sand cat swarm algorithm (SCSA) for feature selection. A stacked autoencoder (SAE) technique is used for the attack detection. The black widow optimization algorithm (BWOA) method is implemented for tuning. In [12], a new software defined networking (SDN)-powered DDoS threat recognition method was proposed using Tanhsoftmax-restricted Boltzmann dense machines (TS-RBDM) alongside the mean difference of public key and private key based Streebog (MDPP-Streebog) user authentication system. During registration, users entered their device details. Furthermore, in the network layer, nodes are initiated via the router/gate, and the detected data is communicated to the SDN controller to enhance network energy efficiency. The adaptive synthetic (ADASYN) technique is employed for data balancing. Lastly, the data is trained using the TS-RBDM technique. This trained DDoS detection system categorizes the sensed data as either attacked or non-attacked. By utilizing the Entropy binomial probability-based Shanon_Sano_Slias (EB-SFE) technique, the non-attacked data is encoded and transmitted to the receiving terminal. Mehmood et al. [13] presented a CNN based on conventional models and a multi-layer perceptron (MLP) to detect DDoS attacks. The model utilizes SHapley Additive exPlanations (SHAP) for key-feature detection and Bayesian optimization (BO) for hyperparameter tuning, thereby improving detection precision and overall performance.

The authors of [14] proposed a robust and scalable DDoS attack detection method for SDN-IoT environments by utilizing a multilevel deep neural network (DNN) that integrates convolutional neural networks (CNN) and long short-term memory (LSTM) to capture spatial and temporal patterns in network traffic effectively. Kanthimathi et al. [15] improve DDoS attack detection by incorporating SA-based CNNs with XGBoost, LSTM, and random forests (RF), using self-attention and weighted ensemble learning to enhance feature extraction and classification accuracy. The authors [16] developed a meta-heuristic, multi-layer ensemble deep reinforcement learning for DDoS attack detection (MMEDRL-ADM), in a cloud SDN setting. The introduced model uses metaheuristics with a DL approach on the SDN data plane. This technique proposes the african buffalo optimization (ABO)-based feature selection (ABO-FS) to reduce computational complexity and increase the recognition rate. The improved grasshopper optimization algorithm (IGOA) technique is also implemented for tuning. Fatima et al. [17] proposed a novel ensemble FS technique, ensemble FS for lightweight intrusion detection system (IDS), leveraging seven filter-based approaches. ensemble feature selection for Lightweight IDS (ELIDS) reduces features and unifies the selection of essential features recognized by separate FS models. As part of numerous learning processes, ELIDS includes strong classification methods that are widely evaluated for resumption and performance through cross-domain and in-domain testing. Hassan et al. [18] proposed a novel technique to identify DDoS attacks using a boosted elman RNN (ERNN) trained with a chaotic bacterial colony optimizer (CBCO) named CBCO-ERNN. The recommended technique utilizes CBCO to determine the optimal structure (number of hidden neurons) and parameter values (biases and weights) of the ERNN model. The CBCO is used to improve the BCO's exploitation and exploration abilities. The CBCO method is used to train the ERNN. Dhanvijay et al. [19] proposed an Ensemble of Deep Learning Models with Prediction Scoring-based Optimized Feature Sets (EDLM-PSOFS) technique by integrating Missforest imputation, shapiro-wilk and correlation-adaptive LASSO regression (CALR)-based feature selection, and global attention LSTM networks (GA-LSTM) model with attention mechanisms. The model further improves interpretability through the exploit prediction scoring system (EPSS). Li et al. [20] proposed the multimodal adaptive replay-based continual learning (Multi-ARCL) framework to enhance encrypted traffic classification by utilizing multimodal DL and adaptive replay mechanisms. It aims to maintain model stability and plasticity through deep learning (DL) and continual learning (CL) while efficiently managing silent application data. Pradeep and Shukla [21] developed a novel network anomaly detection model using the predefined-mud ring algorithm (P-MRA) model for optimal feature selection and used multi-serial stacked networks (multi-SSN), which combines convolutional autoencoder (CAE), gated recurrent unit (GRU), and Bayesian learning (BL), to accurately detect DDoS attacks in IoT networks by effectively capturing complex attack patterns and reducing false positive rates. Table 1 summarizes the existing studies on DDoS detection models.

Table 1. Summary of key literature on DDoS detection methods and techniques.

Ref.	Techniques	Metrics	Datasets	Findings and limitations
[11]	FL, FLDoSADC-DTL, SCSA, SAE, BWOA	accuracy, precision, recall, F1-score, detection rate	Edge-IIoT cybersecurity dataset	FLDoSADC-DTL outperforms in DoS detection for BC-based IIoT but faces challenges with computational load, data heterogeneity, and adversarial risks.
[12]	TS-RBDM, MDPP-Streebog authentication, SDN, ADASYN, EB-SFE	Accuracy, training time, detection rate, precision, recall	CIC DDoS 2019 Dataset	The model achieved 98% accuracy with minimal training time, outperforming existing methods, but may face scalability and real-time adaptability challenges.
[13]	MLP, CNN, SHAP, BO	True positive rate, accuracy, precision, false positive rate	CICDDoS-2019 and InSDN dataset	The model achieved 99.95% TP on CICDDoS-2019 and 99.98% on InSDN, demonstrating high detection accuracy, though it may require further validation across diverse real-world conditions.
[14]	CNN, LSTM, Multilevel DNN	Accuracy, precision, recall, F1-score, detection rate	Real-world datasets	The CNN-LSTM model outperformed existing methods in DDoS detection for SDN-IoT networks, but may face scalability and real-time deployment challenges.
[15]	SA-Enabled CNN with XGBoost, LSTM, RF, Self-Attention Mechanisms, Weighted Ensemble Learning	Accuracy, precision, recall, F1-score	CIC-DDoS2019 dataset	The proposed ensemble model achieved over 98% accuracy across existing DDoS detection methods, though it requires substantial computational resources for training.
[16]	MMEDRL-ADM, ABO-FS, IGOA	Detection rate, accuracy, precision, recall	Benchmark dataset	The MMEDRL-ADM model outperforms existing models, though it involves increased computational complexity and training time.
[17]	ELIDS, seven filter-based FS, RF	Accuracy, robustness, peak accuracy	Diverse IoT security datasets	The ELIDS model attained 23.7% higher accuracy than existing methods, but its complexity may increase computational overhead.
[18]	CBCO-ERNN, Chaos Theory	Accuracy, sensitivity, specificity, precision, F-Score	BoT-IoT, CIC-IDS2017, CIC-DDoS2019, and IoTID20 datasets	The CBCO-ERNN technique outperformed previous methods, though it may require extensive computational resources for large-scale deployments.

Continued on next page

Ref.	Techniques	Metrics	Datasets	Findings and limitations
[19]	EDLM-PSOFS, Median-based Shapiro-Wilk test, CALR, GA-LSTM, EPSS	Accuracy, precision, recall, F1-score, FPR	NSL-KDD, CIC-IDS2017	Achieved strong detection accuracy and reduced false positives, but was restricted by model complexity and interpretability at scale.
[20]	Multi-ARCL, CL, Adaptive Replay, DL	Accuracy improvement, stability-plasticity balance	NJUPT2023	Improves accuracy by 8.64% but may face challenges handling rapidly evolving silent applications.
[21]	P-MRA, Multi-SSN, CAE, GRU, BL	FPR, detection accuracy	IDS ISCX 2012 dataset	Improved detection with reduced false positives, but complex attack patterns remain challenging.

3. The proposed methodology

This paper presents the ELMT2HO-ECD methodology. The main objective of the ELMT2HO-ECD methodology is to provide a robust solution for recognizing, detecting, and mitigating DDoS attacks. The proposed ELMT2HO-ECD method uses mean normalization, dimensionality reduction, ensemble methods, and a parameter-tuning model to obtain this. Figure 2 represents the overall process of the ELMT2HO-ECD method.

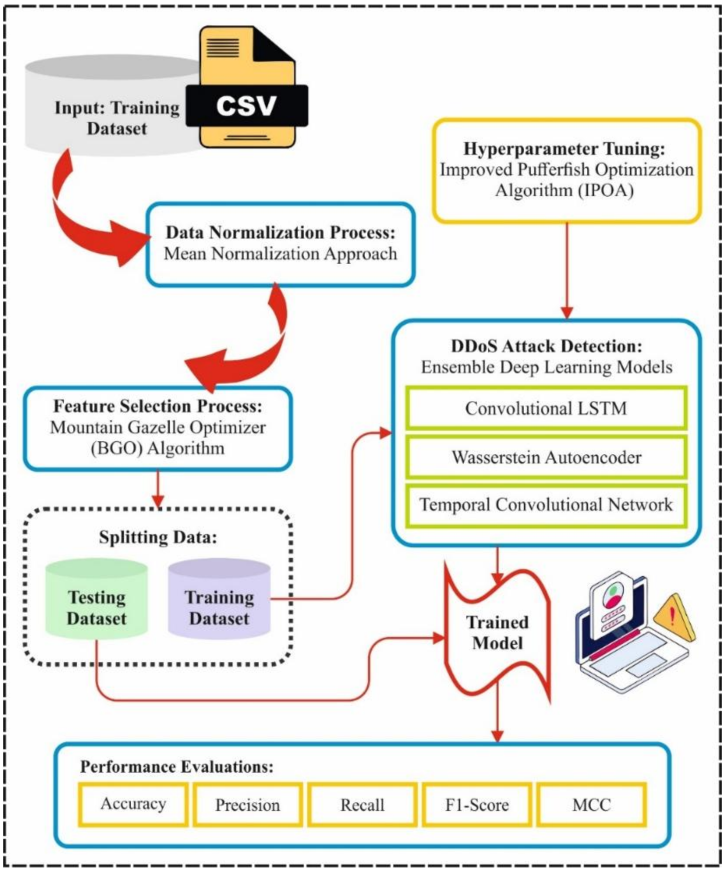

Input: Training Dataset
CSV
Hyperparameter Tuning: Improved Pufferfish Optimization Algorithm (IPOA)
Data Normalization Process: Mean Normalization Approach
DDoS Attack Detection: Ensemble Deep Learning Models
Convolutional LSTM
Wasserstein Autoencoder
Temporal Convolutional Network
Feature Selection Process: Mountain Gazelle Optimizer (BGO) Algorithm
Splitting Data:
Testing Dataset
Training Dataset
Trained Model
Performance Evaluations:
Accuracy
Precision
Recall
F1-Score
MCC

Figure 2. Overall process of the ELMT2HO-ECD method.

3.1. Data normalization

Initially, the ELMT2HO-ECD approach applies mean normalization to scale the features within a specified range [22]. The model enhances convergence and stability during training and also mitigates the impact of disparities in the feature magnitude. It also prevents specific features from dominating the learning process, thus improving the overall detection accuracy. This is also simple, computationally efficient, and remarkably effective when combined with diverse DL methods, compared with other scaling models, ensuring balanced contributions from all features.

The mean normalization method scales features by subtracting the mean and dividing by the standard deviation. In DDoS attack detection, this method supports normalized network traffic data, guaranteeing that attributes with large numerical ranges do not control those with small scales. This enhances the performance and convergence speed of ML methods for detecting DDoS attacks. Focusing the data near zero makes it easier to recognize abnormalities that deviate considerably from The usual traffic behavior. It is beneficial after using gradient-based or distance-based classifiers, as it improves stability and training precision.

3.2. MGO-based feature selection procedure

Next, the MGO method efficiently selects and recognizes the most related features [23]. This method is efficient at selecting and detecting the most relevant features, thereby enhancing accuracy and mitigating complexity. The model achieves faster convergence through its adaptive exploration-exploitation strategy and avoids local optima compared with conventional optimization techniques. MGO also dynamically balances global and local search more effectively than particle swarm optimization (PSO) and genetic algorithms (GA). The method also needs fewer iterations and effectively mitigates the risk of premature convergence. Furthermore, real-time cyber defense is enabled by the simplicity and scalability of the MGO model. The MGO also enhances detection performance by choosing features that maximize informative patterns while reducing redundancy. Thus, the model exhibits superior feature selection in high-dimensional data and also highlights clear advantages over conventional metaheuristic techniques.

The MGO is an advanced optimization model that draws on the social systems of mountain gazelles, lone territorial males, encircling maternity herds (MHs), and bachelor male herds (BMHs). Investigators employed these natural behaviors to advance a mathematical expression that enhances the optimizer. The MGO model incorporates gazelle traits: swift movement, migration, social hierarchy, and territoriality. This model proficiently inspects and is involved within the solution area by modelling the communication between MHs and BMHs and the searching actions of territorial males. This model enables MGO to efficiently optimize and solve complex problems by employing adaptive, dynamic models inspired by gazelle behavior. The mode safeguards wide-ranging study and employment in the search area, becoming a vital instrument in the optimisation.

Mountain gazelles' show sturdy territorial behavior, keep significant distances among individual territories, and arrange themselves into three classes: Herds of young males, solitary males, and mother-calf herds. Adult males frequently tackle territorial disputes, which are less potent than those of females, but younger males employ their horns more energetically than older males.

(a) Territorial solitary males (TSMs):

Once they reach adulthood, male gazelles' begin to defend their own territory. The optimal global position is determined by a mathematical expression that integrates arbitrary features and the location of another male in the bachelor herd.

$$TSM = male_{gazelle} - |(ri_1 \times BH - ri_2 \times X \times F| \times Cof_r. \tag{1}$$

(b) Maternity herds (MHs):

MHs are crucial for the birth of stronger male gazelles'; a behavior modelled to create stronger solutions by mimicking herd communication and the effects of dominant males.

$$MH = \left(BH + Cof_{1,r}\right) + \left(ri_3 \times male_{gazelle} - ri_4 \times X_{rand}\right) \times Cof_{1,r}. \tag{2}$$

where, X_{rand} depicts a vector location of a gazelle arbitrarily chosen from the population. ri_3 and ri_4 refer to integers at arbitrary locations.

(c) Bachelor male herds (BMHs):

As younger males mature, they endeavor to establish their lands and oppose recognized males. It is modelled to depict the competition between solutions to enhance their locations.

$$BMH = (X(t) - D) + \left(ri_5 \times male_{gazelle} - ri_6 \times BH\right) \times Cof_r. \tag{3}$$

Now, $male_{gaze11e}$ provides the optimal solution, and D is calculated using the existing location.

(d) Migration to search for food (MSF):

Gazelles continuously migrate in search of food, covering long distances. This behavior is modelled to improve the search, allowing the model to explore various regions of the solution space.

$$MSF = (ub - lb) \times r_7 + lb. \tag{4}$$

Now, r_7 represents an arbitrary number, and lb and ub denote the lower and upper bounds. In the MGO model, the fitness function (FF) employed is intended to find a balance among the selected feature counts in every solution (least) and the classifier's precision (highest) which is achived by utilizing this chosen feature. The Eq (10) indicates the FF to calculate solutions.

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|}. \tag{5}$$

where $\gamma_R(D)$ indicates the classification rate of error of the specified classifier. |R| characterizes chosen subset's cardinality, and $|C|$ denotes complete feature counts in the dataset; α and β are dual parameters equivalent to the significance of classifier quality and subset length.

3.3. DDoS attack detection using ensemble methods

An ensemble of DL techniques, such as ConvLSTM, WAE, and TCNs are deployed for DDoS attack detection. The ensemble models utilize the merits of each model. The ConvLSTM technique efficiently captures spatial and temporal patterns, while WAE excels at extracting latent features for anomaly representation. Likewise, the sequential dependencies are efficiently modelled by the TCN technique. The integrated model is effective at detecting intrinsic and growing attack behaviors compared with conventional single-model or shallow-learning approaches. Furthermore, incorporating diverse DL methodologies may lead to conflicts due to differing feature representations or gradient directions; however, these conflicts can be reduced by using weighted loss aggregation, coordinated backpropagation, and careful learning rate scheduling, thereby ensuring harmonious and stable training. Thus, the ensemble model achives superior detection performance and faster convergence. The technique is resilient against diverse attack patterns, making it a better choice than conventional techniques.

3.3.1. ConvLSTM model

This is use for forecasting the spatio-temporal sequence issue. In multiple-step prediction, the ConvLSTM technique fully leverages higher-dimensional spatio-temporal sequences [24]. Because of the effective process of spatio-temporal data sequences, it is extensively utilized in further investigation domains.

Unlike LSTM, ConvLSTM uses a vectorised representation of states, inputs, gating, and hidden cells, which are visualized as a sequence of vectors in a spatial grid. It employs a convolution kernel for forecasting the upcoming state of the grid cell from the neighboring input and the previous space-state:

Forgot:

$$f_t = \sigma\left(W_{xf} * X_t + W_{hf} * H_{t-1} + W_{cf} \circ C_{t-1} + b_f\right). \tag{6}$$

Input gate:

$$i_t = \sigma(W_{xi} * X_t + W_{hi} * H_{t-1} + W_{ci} \circ C_{t-1} + b_i). \tag{7}$$

Status update:

$$\tilde{C}_t = \tanh(W_{xc} * X_t + W_{hc} * H_{t-1} + b_C), \tag{8}$$

$$C_t = f_t \circ C_{t-1} + i_t \circ \tilde{C}_t. \tag{9}$$

Output gate:

$$o_t = \sigma(W_{xo} * X_t + W_{ho} * H_{t-1} + W_{co} \circ C_t + b_0), \tag{10}$$

$$H_t = o_t \circ \tanh(C_t). \tag{11}$$

Now, input X_t of the existing moment, the state C_{t-1} and the hidden H_{t-1} of the preceding moment are the input of the ConvLSTM, and the output is the state C_t and the hidden H_t of the present moment. The state C_t has a memory canvas that is updated over time steps, and the hidden H_t specifies the visible output. The Hadamard product represents element-wise multiplication; * denotes convolutional operations, sigmoid σ output $0{\sim}1$ to regulate the data flow, and the hyperbolic tangent $\tanh$ outoutputs outputsuts $-1 \sim 1$ as an activation function for scaling the candidate's values. f_t, i_t and o_t refer to the value of a gating unit; $W_{x(f,i,c,o)}$, $W_{h(f,i,c,o)}$ and $W_{c(f,i,c,o)}$ are the weighted matrices of the gate unit; the weight W is the convolution kernels that acquire the local spatial pattern. b_f, b_i, b_C, and b_o refer to scalar offsets that modify the gate's primary activation threshold. Figure 3 specifies the framework of the ConvLSTM technique.

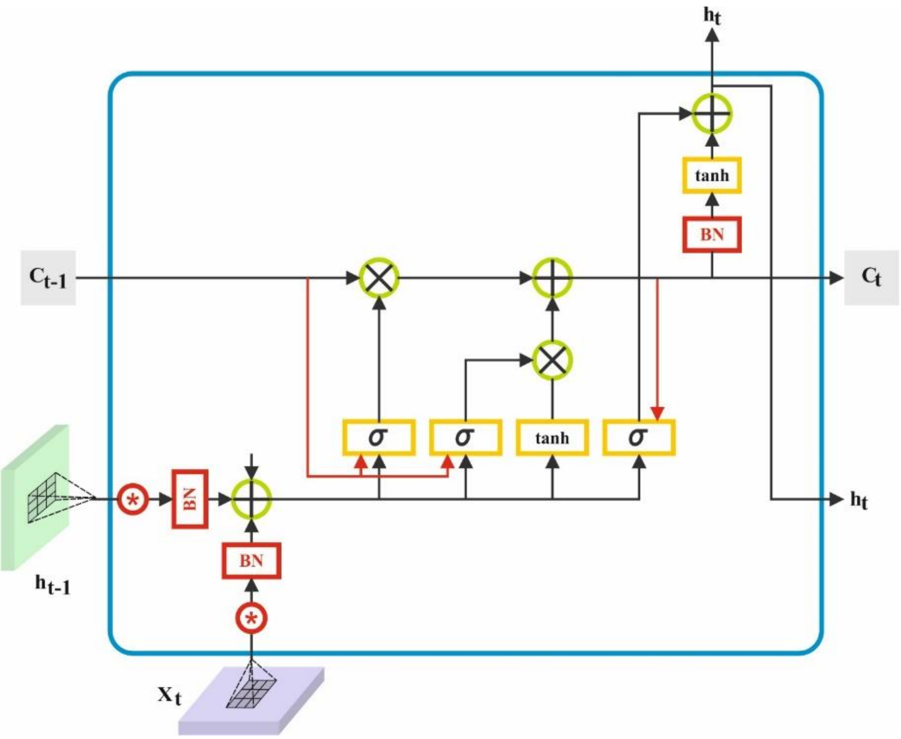


Figure 3. Structure of ConvLSTM approach.

3.3.2. The WAE method

During the WAE training, the Wasserstein distance between the latent space distribution and the input data distribution decreases [25]. Thus, a system of encoders next to decoders, each one holding trainable parameters, is employed. Like the WAE, VAE intends to decrease either the cost of reconstruction or the term of regularization depicted as $D_Z(P_Z, Q_z)$ and denoted by some arbitrary divergence metrics among Q_z and P_z.

$$\mathcal{L}_{WAE} = \mathbb{E}_{q(z|x)}[\log p(x|z)] + \lambda \cdot D_z\big(q(z|x), p(z)\big) \tag{12}$$

where, $D_z\big(q(z|x), p(z)\big)$ indicate some arbitrary divergence metrics, $\lambda > 0$ represents a hyper-parameter and $\mathbb{E}_{q(z|x)}[\log p(x|z)]$ acts as a term of reconstruction. The model has dual regularizes: Adversarial training and maximum mean discrepancy (MMD), which address this problem and improve adaptability in the latent space model. Notably, adversarial training is associated with adversarial AE. The WAE employs the Wasserstein distance to define a deterministic, direct map from the input data's latent space, addressing the inherent stochasticity of latent variables in both (generative adversarial networks) GANs and VAEs. This deterministic mapping addresses randomness and enables latent-space interpolation.

3.3.3. The TCN technique

The TCN comprises three essential units, namely residual links, extended convolutions, and causal convolutions, which combine the benefits of RNNs and CNNs. It effectively prevents the explosion gradient or gradient hourglassing that often occurs in RNNs [26]. This approach highlights time-linking in time-series predictions. Assuming the input sequence $X^{t+1} = x_0, x_1, \dots, x_T$ and the constantly directed sequences of output $Y^{T+1} = y_0, y_1, \dots, y_T$, the projected output y_t for time-step t is restricted, for instance: $x_0, x_1, \dots$, tx. These ensure that each prediction is given according to the identified data until the point, and the output prediction sequences are expressed as follows:

$$y(t) = F_\theta(x_0, x_1, \dots, x_T)(\forall)_t \in [0, T]. \tag{13}$$

where, $F_\theta()$ represents the forward propagation process in the neural network NN, and θ characterises the network parameters. The structure ensures that future data does not spread to the preceding. TCN's convolutional layer avoids the need for a specific step size by sampling thoroughly at random. As with the most significant receptive part, Conv and extended time-series dependencies are achieved at the corresponding output size. Given the 1D sequence of inputs $x \in R^n$ and $Conv$ filter mapping $0, \cdots, k-1 \in R$, the dilated $Conv$ for module s inside the sequence is defined as follow:

$$F(s) = \sum_{j=0}^{k-1} f\,(j) \cdot x_{s-d \cdot j}. \tag{14}$$

In the meantime, k symbolizes the $Conv$ kernel's dimensions and $s - d \cdot j$ seizure preceding data. The dilation d controls the sum of 0-vectors central to neighbouring $Conv$ kernels. Utilising each application of the layer of convolutional to the sequences of input, the dilation feature d gives an exponential result.

Still, as the number of layers in the network increases significantly, problems such as vanishing gradients or gradient decrease may occur, particularly in the deepest layers, particularly in methods for handling multifaceted time-series data. To tackle these difficulties, residual blocks are joined into the TCN. Each residual block includes many dilated convolution layers, weight normalization, dropout, and rectified linear unit (ReLU) for heightened regularization and strength. Furthermore, the residual block combines positive and reverse residual components, allowing the model to take bi-directional temporal dependencies. Skip connections are used to apply $1 \text{x} 1$ convolutions, allowing direct mapping of input features to the output while still requiring dimensionality adjustment. In the residual blocks, x retains the earlier layer output, and $F(x)$ retains the consequence of the procedure. Previously, $F(x)$ and x are passed through the ReLU to obtain the final output, y. This model is specified as:

$$y = ReLU\big(x + F(x)\big). \tag{15}$$

Here, x denotes input from the earlier layer, $F(x)$ indicates the transformed output, and y signifies the concluding output later utilising the ReLU.

3.4. Hyperparameter tuning using the IPOA model

Hyperparameter tuning via the IPOA optimizes the models' parameters, enhancing the three ensemble models and achieving superior accuracy [27]. This model is excellent in optimizing parameters without needing overall system knowledge. The IPOA improves convergence and eliminates the need for predefined stabilizing strategies, unlike conventional policy or value-iteration models, making it effective in intrinsic and dynamic settings. This technique also effectively handles heterogeneous and ill-conditioned data by accounting for the characteristics of both fast and slow subsystems. The data-driven technique also mitigates computational overhead while ensuring robust performance. The model's efficiency and convergence have been rigorously validated, thus highlighting its dominance over conventional tuning techniques.

The POA developed here successfully places the individual within the solution by mimicking the pufferfish's natural behavior and interactions with predators. This imitation has contributed to a two-tier development of individual placement. The primary phase, exploration, mimics the predator's attack, whereas the subsequent phase, exploitation, mimics the pufferfish's defensive change. The optimal control of fast-sampling singularly perturbed systems is efficiently addressed by designing a composite controller utilizing subsystem decomposition [28]. Moreover, a novel data-driven single-loop iterative model guarantees the cost control of uncertain systems, effectively handling fast and slow subsystem data and ill-conditioned problems, and removing the requirement for precise initial conditions [29].

3.4.1. Exploration

The model's primary step mimics the hunter's assault, tactically targeting the locations of vulnerable individuals that move slowly and are at risk of predation. By demonstrating the hunter's movement during the predatory procedure, the model improves exploration and significantly changes the POA individual's locations within the solution area. This combination of the hunter's model supports the model's exploration ability, leading to improved exploration solutions. In the POA model, each individuals' assumes the predator role, corresponding to a starving hunter seeking prey. In this search stage, individuals consider the locations of other individuals with higher performance indices, equivalent to aiming at pufferfish with the required qualities. The dynamics and definition of this predator's group inside every population are explained as follows:

$$FQ_i = \left[Y_h : G_h < G_j, h \neq i\right]s, i = 1,2, \dots, N, k \in [1,2, \dots, N]. \tag{16}$$

Here, the variable FQ_i denotes the pool of sites associated with the ith predator. y_h stands for the individual showing greater index performance than ith predator, using its individual performance index, denoted by G_h. The hunters arbitrarily choose the pufferfish from the accessible collection FQ, using the chosen candidates characterised by SP. By using Eq (17) to mimic the predator's movements, a novel location inside the solution area was established for the individual. The preceding location is upgraded according to Eq (18), thus helping a constant search for the best solutions,

$$y_{i,j}^{Q1} = y_{i,j} + e_{i,j} \times (SP_{i,j} - K_{i,j}) \times y_{i,j}, \tag{17}$$

$$Y_i = \begin{cases} Y_i^{Q1}, G_i^{Q1} \leq G_i; \\ Y_i, else. \end{cases} \tag{18}$$

where, SP_i denotes the candidates randomly selected from the group FQ, whereas SP_{ij} denotes the jth size of these candidates. The upgraded location of the ith hunter, as established by the presented model, is characterized by y^{Q1}, using its jth size specified as $y_{i,j}^{Q1}$. The performance index for this novel location is denoted G_i^{Q1}. Summaries random variables e_{ij} and adding the stochastic component to the equation. Additionally, the constant K_{ij} can take on both 1 and 2.

3.4.2. Exploitation

During the exploitation stage, the model follows the defensive tactics of particular species, thus improving the individual's spatial distribution. During an attack, it activates its defense tool by expanding into a spiky sphere across the water's surface. By imitating the hunter's response to this self-protective posture, the model can detect and improve minor changes in the candidate's location, like improving its exploitation efficacy. After computing a novel location, performance metrics are linked; when the novel location yields improved performance, it is established. On the other hand, the candidate maintains its first location. It is significant to recognize that the upgraded mechanism inside the POA relies on the performance index's development, as determined by Eqs (19) and (20).

$$y_{i,j}^{Q2} = y_{ij} + (1 - 2e_{i,j}) \times \frac{ub_j - lb_j}{t}, \tag{19}$$

$$Y_j = \begin{cases} Y_i^{Q2}, G_i^{Q2} \leq G_j; \\ Y_i, else. \end{cases} \tag{20}$$

where, y_i^{Q2} denotes the recently computed location for the ith hunter, as established by the second stage of the model, whereas $y_{i,j}^{Q2}$ denotes its jth size. G_i^{Q2} characterises the performance index at this upgraded location. The variable t indicates the iteration count, and e_{ij} denotes a randomly generated variable that alternates between $(0,1)$, thus incorporating a stochastic component within the equation.

The POA embodies a new meta-heuristic approach that draws on the interesting behavior of pufferfish, particularly their defense mechanism of expanding their bodies to avoid predators. This model is carefully designed to address complex optimization issues while overcoming the limitations of recent methods, including issues related to accuracy, computational efficiency, and convergence rates. The IPOA combines significant progress, such as a novel search tactic, adaptive parameter management, and an improved balance between exploitation and exploration. A substantial advance in the IPOA is the combination of a nonlinear, adaptive, weighted element that dynamically fine-tunes the search region on the basis of the quality of candidate solutions. This adaptable characteristic is essential for alleviating early convergence within the population and fostering diversity among solutions. The improved equation for X might yield differences in both negative and positive values, thereby enhancing the model's adaptability.

$$y_{i,j}^{Q1} = y_{i,j} + w_i \times (SP_{i,j} - K_{i,j}) \times y_{i,j}. \tag{21}$$

The weight module of the ith value is signified by w_i and is calculated utilising Eq (22):

$$w_i = \frac{\overline{f} - f_i}{f - \underline{f}}, \quad i = 1,2, \dots, N_P. \tag{22}$$

where, f_i denotes the performance index for the ith sample, and $\overline{f}$ and f denote the minimum and maximum objective values, respectively. This adaptive tactic effectively synchronizes the model's capacity for exploration and exploitation. Additionally, a significant development is the exchange of stochastic variable r using chaotic map γ, as shown in Eq (23):

$$y_{i,d} = lb_d + \gamma_t \times (ub_d - lb_d). \tag{23}$$

This study uses Bernoulli shift mapping, as described by Eq (24):

$$\gamma_t^{new} = \begin{cases} \frac{\gamma_t}{1-\beta}, 0 < \gamma_t \leq 1-\beta, \\ \frac{\gamma_t-(1-\beta)}{\beta}, 1-\beta < \gamma_t < 1 \end{cases} \tag{24}$$

where β is set to 0.4, t denotes the iteration count. Combining this with the Bernoulli shift mapping target improves the model's convergence.

Table 2 outlines the elements involved in the optimization process, which play a crucial role in balancing exploration and exploitation. These parameters ensure effective convergence, maintain the solutions' diversity, and prevent premature stagnation, making the algorithm robust for complex optimization problems.

Table 2. Hyperparameters of the IPOA technique.

Hyperparameter	Description	Typical value / range
POPU_SIZE (N)	Candidate solutions in the populations	20-50
ITER (t)	Optimum optimization iterations	100-500
SCALING_FACTOR (K)	Regulate the step size during updates	1 or 2
STOCHASTIC_VARI (e)	Introduces randomness in position updates	0-1
ADAP_WEIGHT (w)	Search intensity is adjusted arbitrarily on the basis of performance	Calculated per candidate
UPP_BOUND (ub)	Each solution dimension’s maximum value	Problem-specific
LOW_BOUND (lb)	Each solution dimension’s minimum value	Problem-specific
CHAOTIC_MAO (γ)	Bernoulli shift is used to improve diversity and convergence	0-1

Fitness selection is a significant factor that influences the IPOA performance. The hyperparameter selection method includes a solution-encoding method to calculate the efficacy of candidate solutions. As stated below, the IPOA determines precision as the foremost principle in the FF modelling.

$$Fitness = \max(P), \tag{25}$$

$$P = \frac{TP}{TP+FP}. \tag{26}$$

Here, TP and FP represent the true and false positives, respectively

4. Performance validation

The performance of the ELMT2HO-ECD technique is evaluated on the CICIDS2017, CICIDS2018, and CICIDS2019 datasets [30–32]. The CICIDS2017 dataset contains 17,500 samples across seven class labels, as shown in Table 3. There are 78 attributes, but only 18 features were chosen.

Table 3. Details of the CICIDS2017 dataset.

CICIDS2017 Dataset	
Class	No. of instances
BruteForce	2500
DoS	2500
WebAttacks	2500
Infiltration	2500
Bot	2500
DDoS	2500
PortScan	2500
Total Instances	17500

Figure 4 illustrates the convergence of fitness analysis over iterations. The outcomes indicate that the ELMT2HO-ECD model converges better across multiple iterations of the implemented data.

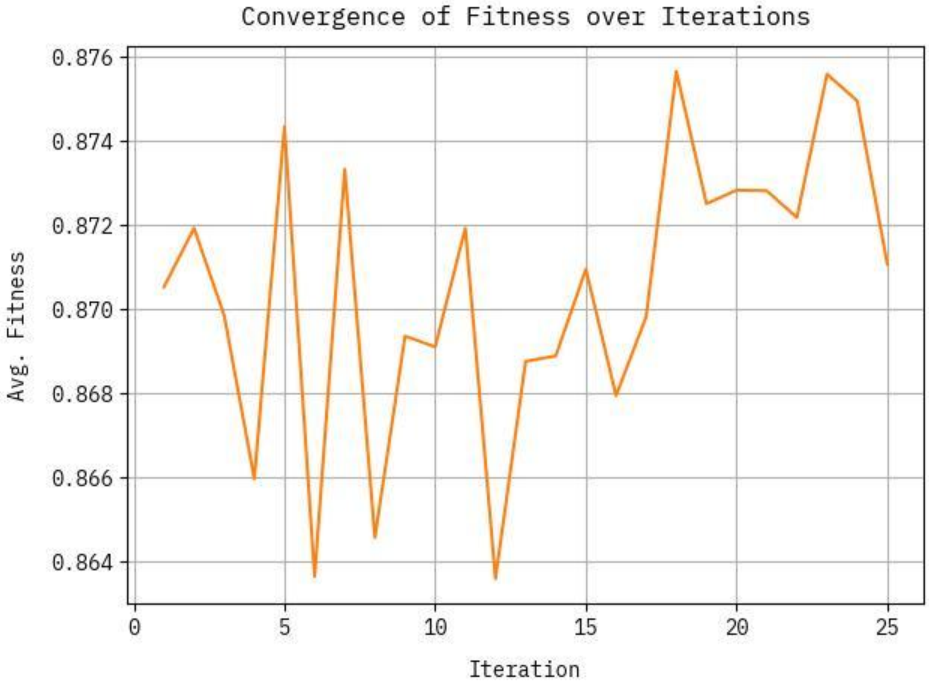
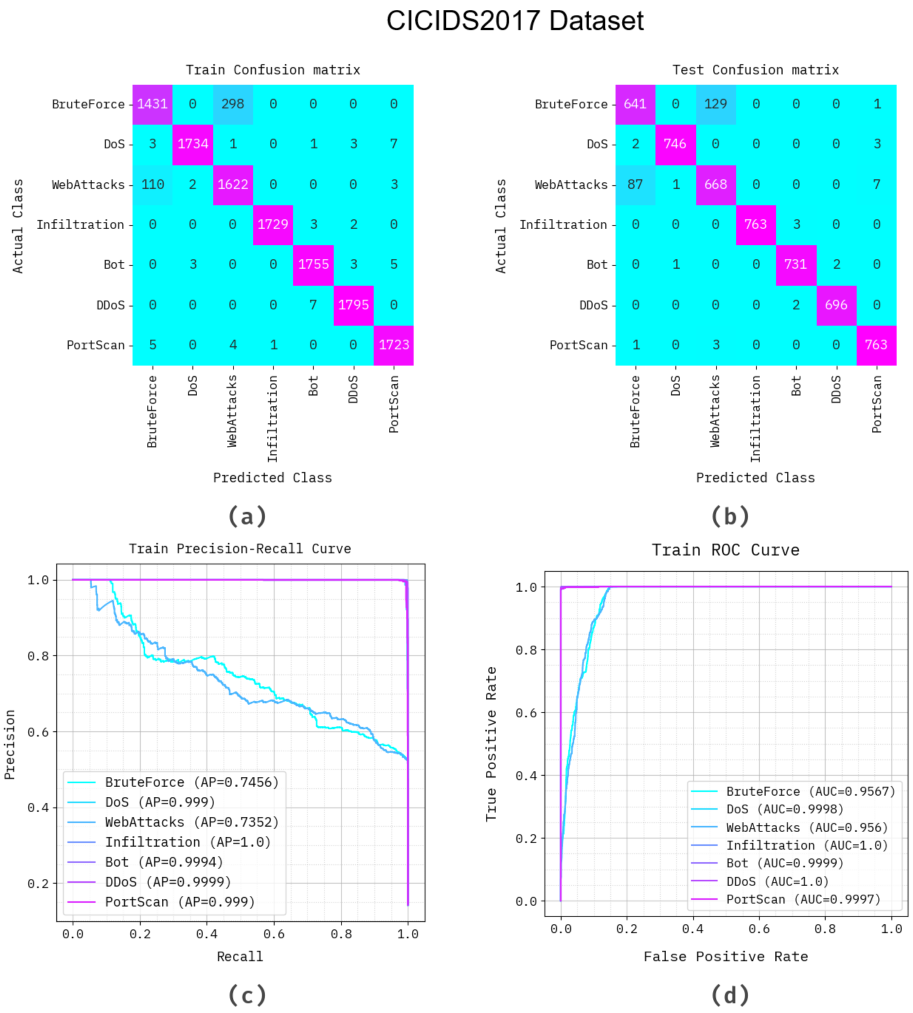


Figure 4. Convergence curve of the ELMT2HO-ECD model under various iterations.

Figure 5 shows the classifier performance of the ELMT2HO-ECD model on the CICIDS2017 dataset. Figures 5(a) and 5(b) exhibit the confusion matrices with the accuracy of each class. Figure 5(c) shows the PR study, demonstrating superior outcomes across all class labels. Ultimately, Figure 5(d) illustrates the receiver operating characteristic ROC analysis, showing high ROC values for suitable outcomes across varied classes.



Train Confusion matrix

	BruteForce	DoS	WebAttacks	Infiltration	Bot	DDoS	PortScan
BruteForce	1431	0	298	0	0	0	0
DoS	3	1734	1	0	1	3	7
WebAttacks	110	2	1622	0	0	0	3
Infiltration	0	0	0	1729	3	2	0
Bot	0	3	0	0	1755	3	5
DDoS	0	0	0	0	7	1795	0
PortScan	5	0	4	1	0	0	1723

Test Confusion matrix

	BruteForce	DoS	WebAttacks	Infiltration	Bot	DDoS	PortScan
BruteForce	641	0	129	0	0	0	1
DoS	2	746	0	0	0	0	3
WebAttacks	87	1	668	0	0	0	7
Infiltration	0	0	0	763	3	0	0
Bot	0	1	0	0	731	2	0
DDoS	0	0	0	0	2	696	0
PortScan	1	0	3	0	0	0	763

Figure 5. CICIDS2017 dataset: (a) and (b) confusion matrices, (c) curve of PR, and (d) curve of ROC.

Table 4 and Figure 6 show the attack recognition of the ELMT2HO-ECD technique under the CICIDS2017 dataset. With 70%TRPHE, the ELMT2HO-ECD methodology provides average $accuracy$, $prec_n$, $reca_l$, $F1_{score}$, and MCC of 98.93%, 96.34%, 96.20%, 96.20%, and 95.62%, respectively. Moreover, depending on 30%TSPHE, the ELMT2HO-ECD technique delivers average $accuracy$, $prec_n$, $reca_l$, $F1_{score}$, and MCC of 98.68%, 95.5%, 95.49%, 95.48%, and 94.72%, respectively.

Table 4. Attack detection of the ELMT2HO-ECD method under the CICIDS2017 dataset.

Class	$Accuracy$	$Prec_n$	$Reca_l$	$F1_{Score}$	MCC
TRPHE (70%)					
BruteForce	96.60	92.38	82.76	87.31	85.53
DoS	99.84	99.71	99.14	99.43	99.33
WebAttacks	96.59	84.26	93.38	88.59	86.74
Infiltration	99.95	99.94	99.71	99.83	99.80
Bot	99.82	99.38	99.38	99.38	99.27
DDoS	99.88	99.56	99.61	99.58	99.51
PortScan	99.80	99.14	99.42	99.28	99.16
Average	98.93	96.34	96.20	96.20	95.62
TSPHE (30%)					
BruteForce	95.81	87.69	83.14	85.35	82.95
DoS	99.87	99.73	99.33	99.53	99.46
WebAttacks	95.68	83.5	87.55	85.48	82.97
Infiltration	99.94	100	99.61	99.8	99.77
Bot	99.85	99.32	99.59	99.46	99.37
DDoS	99.92	99.71	99.71	99.71	99.67
PortScan	99.71	98.58	99.48	99.03	98.86
Average	98.68	95.5	95.49	95.48	94.72

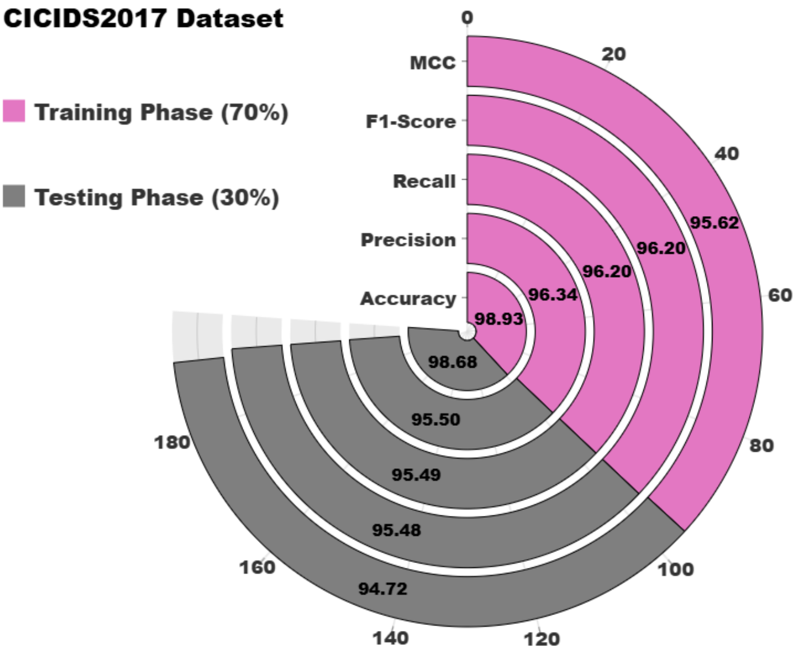


Figure 6. Average values of the ELMT2HO-ECD method with the CICIDS2017 dataset.

In Figure 7, the training (TRNG) $accuracy$ and validation (VALID) $accuracy$ performances of the ELMT2HO-ECD method with CICIDS2017 dataset are shown. both values are calculated over an interval of 0–100 epochs. The figure indicates that both *accuracy* values display an increasing trend, which shows the capability of the ELMT2HO-ECD technique with an enhanced solution through many iterations. Additionally, *accuracy* remains constant across epochs, indicating the least overfitting and suggesting a higher solution for the ELMT2HO-ECD technique.

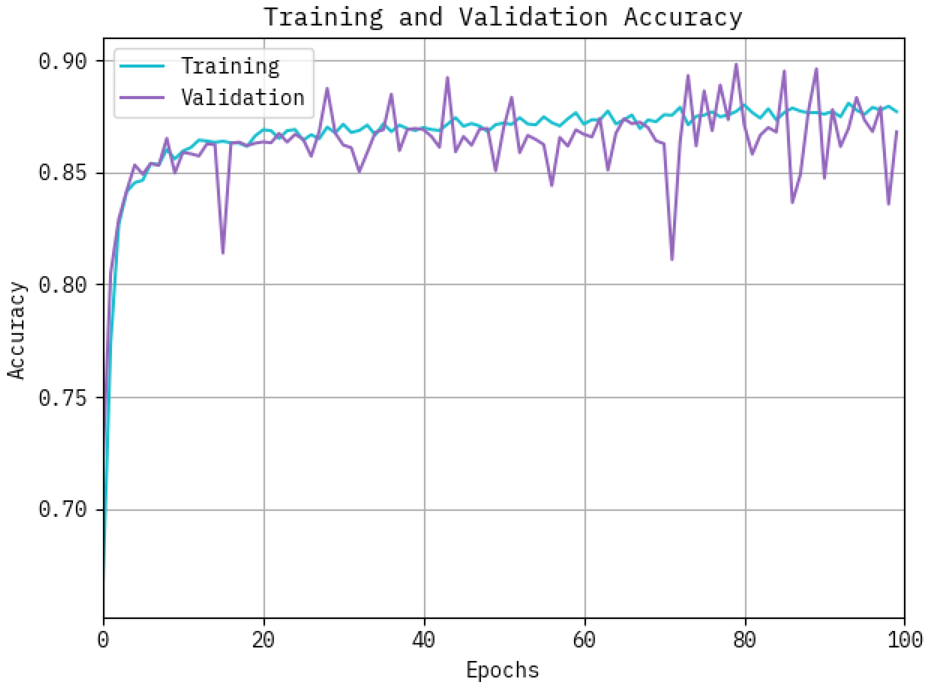


Figure 7. *Accuracy* curve of the ELMT2HO-ECD method on the CICIDS2017 dataset.

In Figure 8, the TRNG and VALID loss graphs of the ELMT2HO-ECD model on the CICIDS2017 dataset are shown. The values are calculated using an interval of 0–100 epochs. The values indicate a tendency to reduce, indicating the ELMT2HO-ECD method's proficiency in balancing trade-offs. The ongoing decrease also ensures the superior performance of the ELMT2HO-ECD technique.

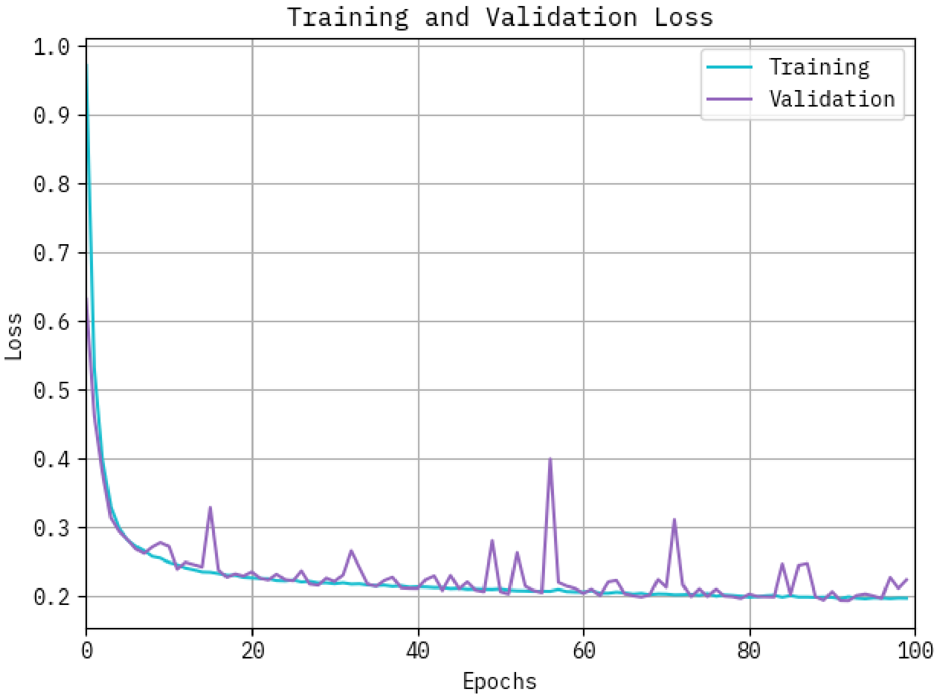


Figure 8. Loss curve of the ELMT2HO-ECD method on the CICIDS2017 dataset.

Table 5 and Figure 9 present a comparative analysis of the ELMT2HO-ECD approach against existing models on the CICIDS2017 dataset [11–19, 34–37]. Better to use all of these old approaches for comparison with the proposed approach because all of them have been validated under the same environment and evaluation measures of the proposed approach and to ensure the outperforms of the proposed approach on all of old proposed approaches. The outputs showed that the FLDoSADC-DTL, TS-RBDM, MMEDRL-ADM, EDLM-PSOFS, P-MRA, BNIDS, XG-Boost, and LSTM-AFSA models yielded lower values. However, the ELMT2HO-ECD technique demonstrated enhanced output with greater $accuracy$, $prec_n$, $reca_l$, and $F1_{score}$ of 98.93%, 96.34%, 96.20%, 96.20%, respectively.

Table 5. Comparison evaluation of ELMT2HO-ECD model under the CICIDS2017 dataset [11–19, 34–37].

CICIDS2017 Dataset				
Approach	$Accuracy$	$Prec_n$	$Reca_l$	$F1_{Score}$
FLDoSADC-DTL [11]	96.00	90.30	94.14	94.99
TS-RBDM [12]	97.45	95.63	92.95	90.99
MMEDRL-ADM [16]	98.30	94.39	90.28	91.48
EDLM-PSOFS [19]	95.78	91.98	90.88	94.06
P-MRA [34]	93.91	90.74	96.07	94.02
BNIDS [34]	96.67	92.74	95.37	95.67
XG-Boost [35]	98.30	90.92	94.81	90.17
LSTM-AFSA [37]	97.56	92.16	92.42	95.58
ELMT2HO-ECD [proposed]	98.93	96.34	96.20	96.20

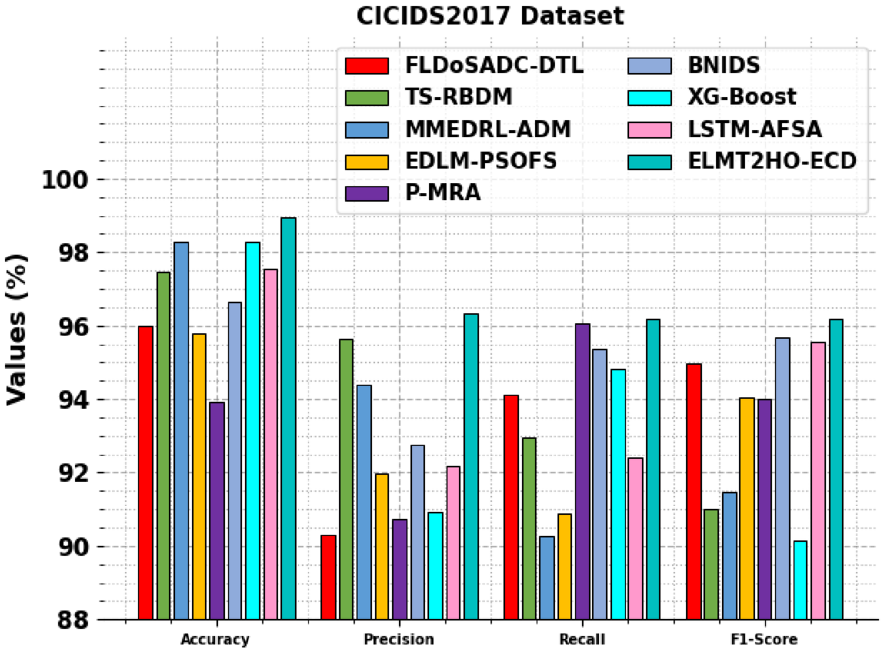


Figure 9. Comparison of the ELMT2HO-ECD model on the CICIDS2017 dataset.

Table 6 and Figure 10 specify the computational time (CT) analysis of the ELMT2HO-ECD technique versus existing models under the CICIDS2017 dataset. The FLDoSADC-DTL records a CT of 17.44, TS-RBDM takes 20.92, and MMEDRL-ADM achieves 14.52. Meanwhile, EDLM-PSOFS requires 19.18; P-MRA outperforms with a faster CT of 13.29; and BNIDS and XG-Boost follow closely with 15.30 and 15.37, respectively. LSTM-AFSA exhibits the highest CT of 22.96 seconds. Notably, the proposed ELMT2HO-ECD model significantly outperforms others, achieving the lowest CT of 5.53.

Table 6. CT analysis of the ELMT2HO-ECD model with existing models with the CICIDS2017 dataset.

CICIDS2017 dataset	
Approach	CT (sec)
FLDoSADC-DTL [11]	17.44
TS-RBDM [12]	20.92
MMEDRL-ADM [16]	14.52
EDLM-PSOFS [19]	19.18
P-MRA [34]	13.29
BNIDS [34]	15.30
XG-Boost [35]	15.37
LSTM-AFSA [37]	22.96
ELMT2HO-ECD [proposed]	5.53

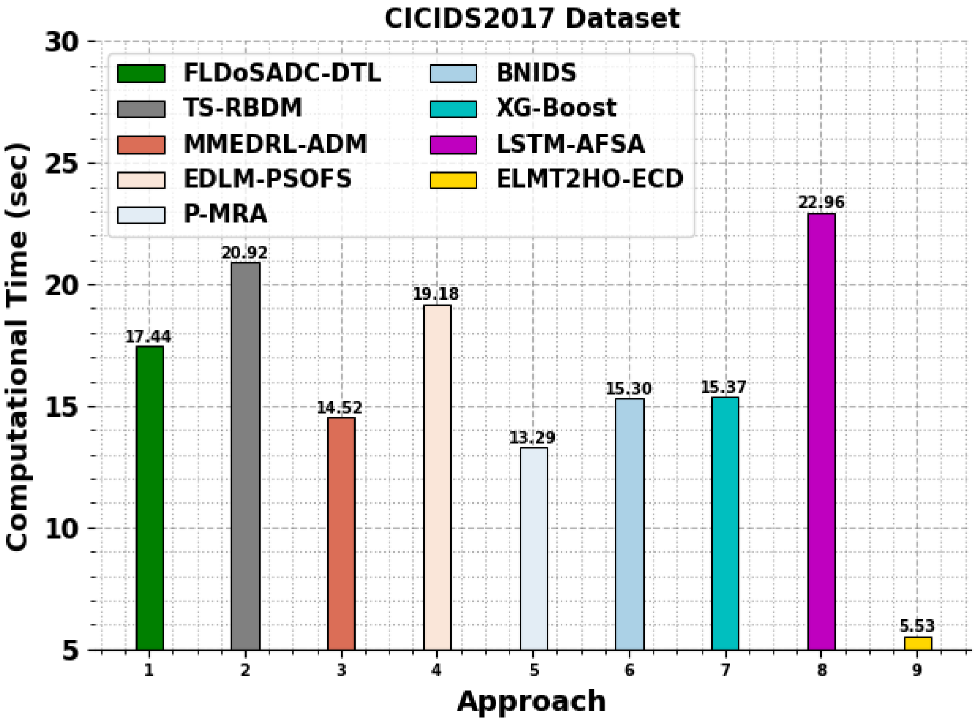


Figure 10. CT analysis of the ELMT2HO-ECD model versus existing models with the CICIDS2017 dataset.

Table 7 and Figure 11 show the ablation study analysis of the ELMT2HO-ECD approach with the CICIDS2017 dataset. The convolutional LSTM with BGO without hyperparameter tuning achived an $accuracy$ of 94.96%, $prec_n$ of 92.13%, recall of 92.10%, and F-Score of 91.61%. Additionally, the convolutional LSTM+BGO+IPOA achieved an $accuracy$ of 95.65%, $prec_n$ of 92.74%, $reca_l$ of 92.92%, and $F1_{score}$ of 92.48%. Furthermore, by utilizing the WAE with BGO without tuning provided an $accuracy$ of 96.20%, $prec_n$ of 93.26%, $reca_l$ of 93.51%, and $F1_{score}$ of 93.37%, which increased to an $accuracy$ of 96.90%, $prec_n$ of 93.88%, $reca_l$ of 94.12%, and $F1_{score}$ of 94.11% in the subsequent evaluation. Moreover, TCN with BGO without tuning achieved an $accuracy$ of 97.76%, $prec_n$ of 94.64%, $reca_l$ of 94.80%, and $F1_{score}$ of 94.78%, which improved to an $accuracy$ of 98.38%, $prec_n$ of 95.49%, $reca_l$ of 95.56%, and $F1_{score}$ of 95.67%. Finally, the ELMT2HO-ECD model outperformed all combinations with an $accuracy$ of 98.93%, $prec_n$ of 96.34%, $reca_l$ of 96.20%, and $F1_{score}$ of 96.20%, thus emphasizing the efficiency of each individual process.

Table 7. Ablation study analysis of the ELMT2HO-ECD approach under the CICIDS2017 dataset.

CICIDS2017 Dataset				
Approach	$Accuracy$	$Prec_n$	$Reca_l$	$F1_{Score}$
Convolutional LSTM+BGO (without hyperparameter tuning)	94.96	92.13	92.10	91.61
Convolutional LSTM+BGO+IPOA (with hyperparameter tuning)	95.65	92.74	92.92	92.48
Wasserstein AE+BGO (without hyperparameter tuning)	96.20	93.26	93.51	93.37
Wasserstein AE+BGO (without hyperparameter tuning)	96.90	93.88	94.12	94.11
TCN+BGO (without hyperparameter tuning)	97.76	94.64	94.80	94.78
TCN+BGO (without hyperparameter tuning)	98.38	95.49	95.56	95.67
ELMT2HO-ECD (ensemble deep learning models with BGO feature selection process and IPOA hyperparameter tuning process)	98.93	96.34	96.20	96.20

The ELMT2HO-ECD technique is analysed with the CICIDS2018 dataset [31]. It has 17500 samples across eight class labels, as shown in Table 8 below. There are 78 attributes, but only 18 features were selected.

Table 8. Details of the CICIDS2018 dataset.

CICIDS2018 Dataset	
Classes	No. of samples
“Normal”	2500
“DDoS”	2500
“DoS”	2500
“BruteForce”	2500
“Bot”	2500
“Infiltration”	2500
“Web”	2500
Total samples	17500

Figure 11 shows the convergence of the fitness analysis across iterations. The outcomes indicate that the ELMT2HO-ECD approach achieves the best convergence across diverse iterations of the data.

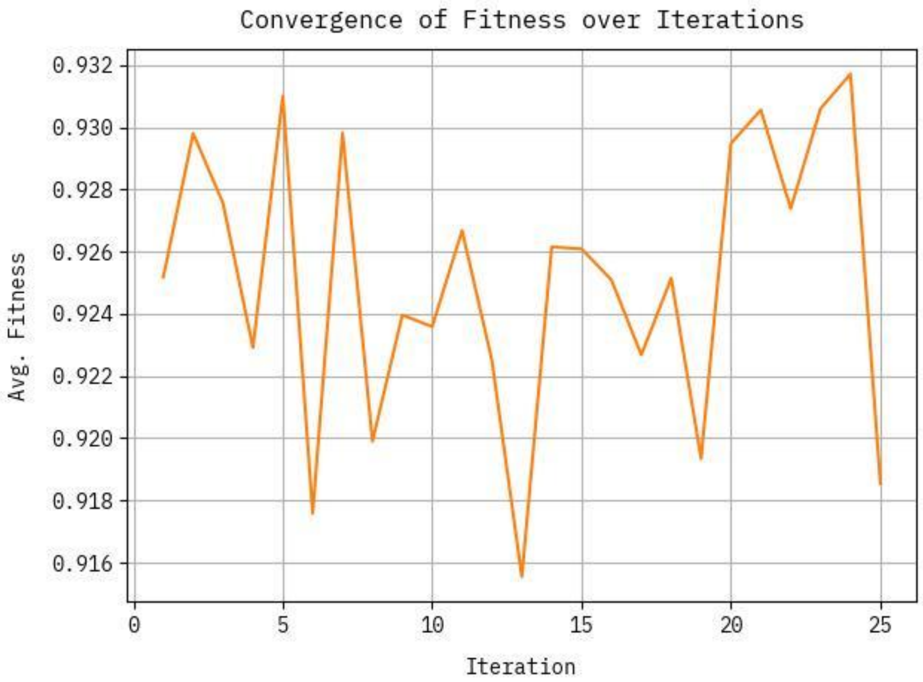


Figure 11. Convergence curve of the ELMT2HO-ECD model across various iterations.

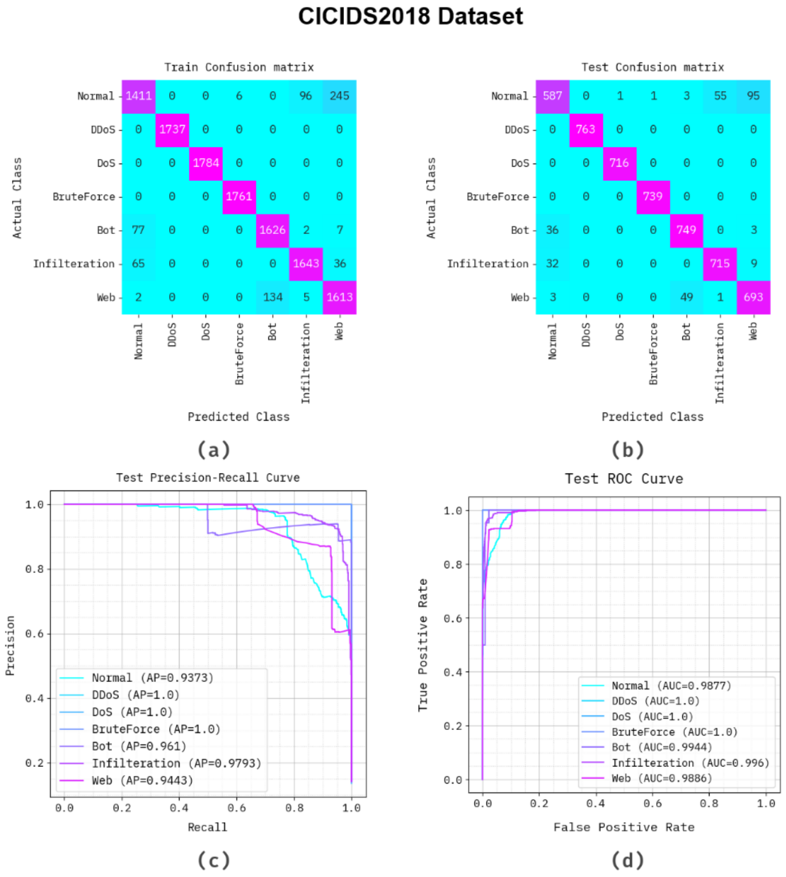


Figure 12. CICIDS2018 dataset: (a) and (b) Confusion matrices, (c) PR, and (d) ROC.

Figure 12 shows the classification performance of the ELMT2HO-ECD technique on the CICIDS2018 dataset. Figures 12(a) and 12(b) display the confusion matrices with the accuracy of each class. Figure 12(c) shows the PR study, indicating better outcomes across all class labels. Lastly, Figure 12(d) show the ROC analysis, demonstrating strong performance with high ROC values across various class labels.

Table 9 and Figure 13 show the attack recognition performance of the ELMT2HO-ECD model on the CICIDS2018 dataset. With 70%TRPHE, the ELMT2HO-ECD model delivers an average $accuracy$, $prec_n$, $reca_l$, $F1_{Score}$, and MCC of 98.42%, 94.53%, 94.49%, 94.44%, and 93.57%, respectively. Moreover, 30%TSPHE, the ELMT2HO-ECD approach provides average $accuracy$, $prec_n$, $reca_l$, $F1_{Score}$, and MCC of 98.43%, 94.54%, 94.52%, 94.47%, and 93.60%, respectively.

In Figure 14, the TRNG $accuracy$ and VALID $accu_y$ outcomes of the ELMT2HO-ECD technique on the CICIDS2018 dataset are verified. Both values are calculated 0–100 epochs. The figure underscored that both accuracy values illustrated an increasing trend, indicating that the ELMT2HO-ECD model's proficiency improved and yielded higher outcomes across various iterations. Besides, both accuracy values remain constant across epochs, indicating minimal overfitting and a better solution.

Figure 15 shows the TRNG and VALID loss curves for the ELMT2HO-ECD technique on the CICIDS2018 dataset. Both values are calculated 0–100 epochs. The values exemplify a tendency toward lessening, indicating the ELMT2HO-ECD approach's proficiency at balancing trade-offs. The steady decline ensures the overall outcome of the ELMT2HO-ECD approach.

Table 9. Attack detection of the ELMT2HO-ECD model with the CICIDS2018 dataset.

Class	$Accuracy$	$Prec_n$	$Recall$	$F1_{Score}$	MCC
TRPHE (70%)					
Normal	95.99	90.74	80.26	85.18	83.08
DDoS	100.00	100.00	100.00	100.00	100.00
DoS	100.00	100.00	100.00	100.00	100.00
BruteForce	99.95	99.66	100.00	99.83	99.80
Bot	98.20	92.39	94.98	93.66	92.63
Infiltration	98.33	94.10	94.21	94.15	93.18
Web	96.50	84.85	91.96	88.26	86.30
Average	98.42	94.53	94.49	94.44	93.57
TSPHE (30%)					
Normal	95.70	89.21	79.11	83.86	81.58
DDoS	100.00	100.00	100.00	100.00	100.00
DoS	99.98	99.86	100.00	99.93	99.92
BruteForce	99.98	99.86	100.00	99.93	99.92
Bot	98.27	93.51	95.05	94.27	93.26
Infiltration	98.15	92.74	94.58	93.65	92.57
Web	96.95	86.62	92.90	89.65	87.94
Average	98.43	94.54	94.52	94.47	93.60

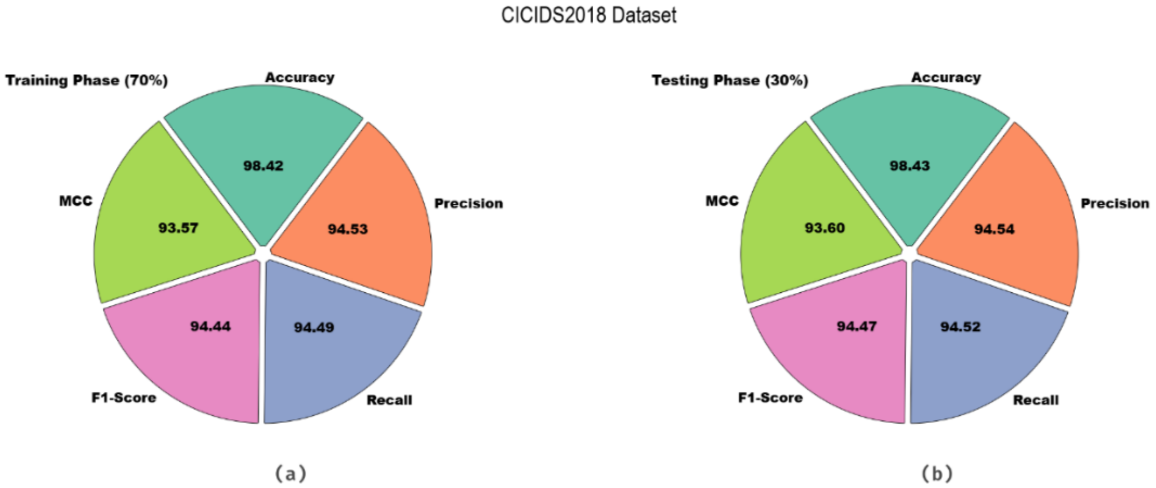


Figure 13. Average values of the ELMT2HO-ECD model with the CICIDS2018 dataset.

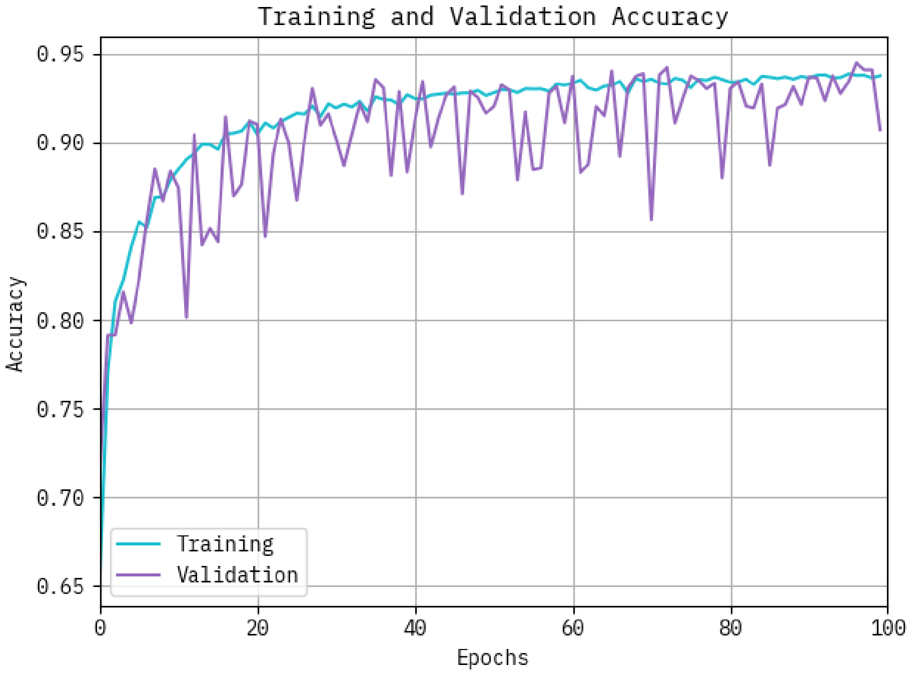


Figure 14. Accuracy curve of the ELMT2HO-ECD approach with the CICIDS2018 dataset.

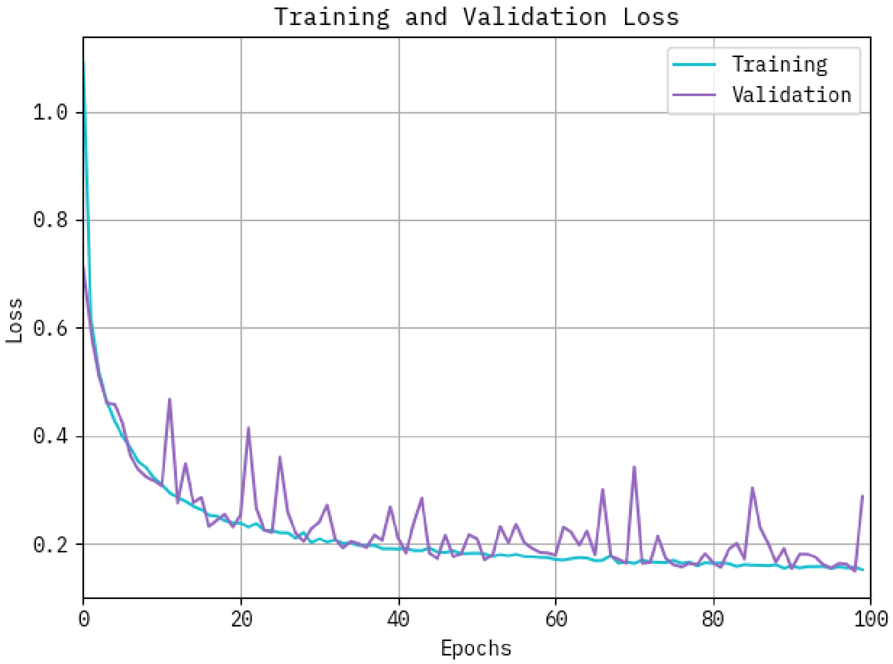


Figure 15. Loss curve of ELMT2HO-ECD approach with the CICIDS2018 dataset.

Table 10 and Figure 16 present a comparative analysis of the ELMT2HO-ECD technique against existing models on the CICIDS2018 dataset. The outcomes highlighted that the EB-SFE, CNN-LSTM, SA-CNN-XGBoost, Multi-ARCL, Multi-SSN, SecFedNIDS, and Base CNN approaches illustrated lesser values. However, the ELMT2HO-ECD method exhibited an enhanced outcome with a greater $accuracy$, $prec_n$, $reca_l$, $F1_{Score}$ of 98.43%, 94.54%, 94.52%, 94.47%, respectively.

Table 10. Comparison analysis of the ELMT2HO-ECD model under the CICIDS2018 dataset [12–21, 33–38]. Better to use all of these old approaches for comparison with the proposed approach because all of them have been validated under the same environment and evaluation measures of the proposed approach and to ensure the outperforms of the proposed approach on all of old proposed approaches.

CICIDS2018 dataset				
Approach	$Accuracy$	$Prec_n$	$Reca_l$	$F1_{Score}$
EB-SFE [12]	91.71	93.74	93.51	93.49
CNN-LSTM [14]	95.34	92.88	93.11	94.26
SA-CNN-XGBoost [15]	95.21	93.31	91.89	93.18
Multi-ARCL [20]	96.24	90.13	92.36	92.12
Multi-SSN [21]	91.15	92.96	92.99	90.76
SecFedNIDS [33]	97.03	90.65	93.06	90.24
Base CNN [38]	97.97	91.84	90.43	92.61
ELMT2HO-ECD [proposed]	98.43	94.54	94.52	94.47

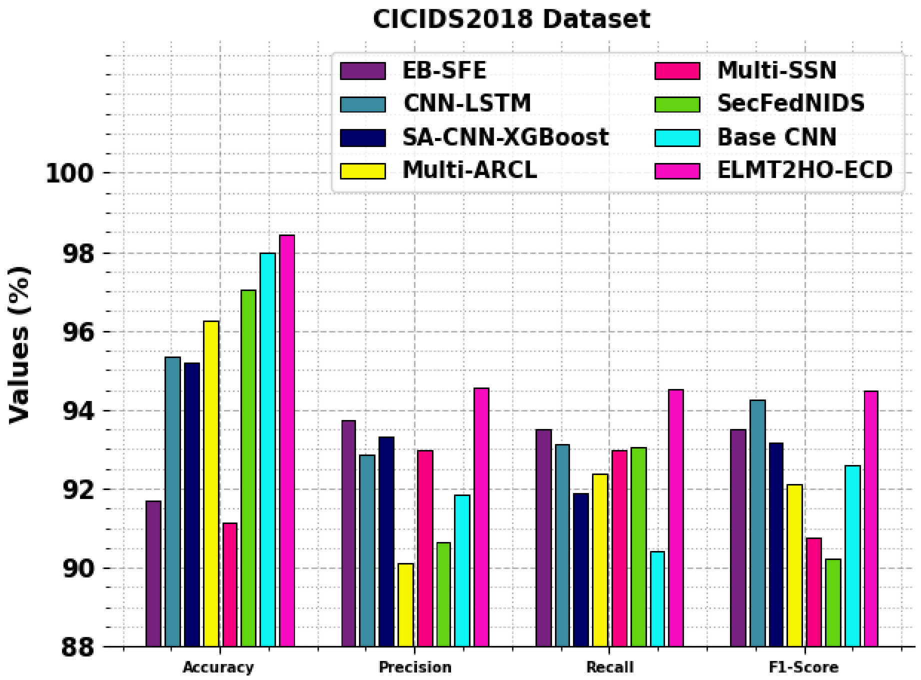


Figure 16. Comparison analysis of the ELMT2HO-ECD model with the CICIDS2018 dataset.

Table 11 and Figure 17 demonstrate the CT analysis of the ELMT2HO-ECD methodology with the existing models. The EB-SFE model records a CT of 24.93, closely followed by CNN-LSTM and Multi-SSN, both at 24.97. SA-CNN-XGBoost exhibits a slightly better CT at 23.11, while multi-ARCL exhibits the highest CT of 27.06. SecFedNIDS maintains a balanced performance of 24.21, while the Base CNN performs more efficiently at 18.81. The ELMT2HO-ECD method clearly surpasses existing methods, achieving the lowest CT of 14.48 and demonstrating enhanced computational efficiency.

Table 11. CT evaluation of the ELMT2HO-ECD methodology versus the existing models with the CICIDS2018 dataset.

CICIDS2018 dataset	
Approach	CT (sec)
EB-SFE [12]	24.93
CNN-LSTM [14]	24.97
SA-CNN-XGBoost [15]	23.11
Multi-ARCL [20]	27.06
Multi-SSN [21]	24.97
SecFedNIDS [33]	24.21
Base CNN [38]	18.81
ELMT2HO-ECD	14.48

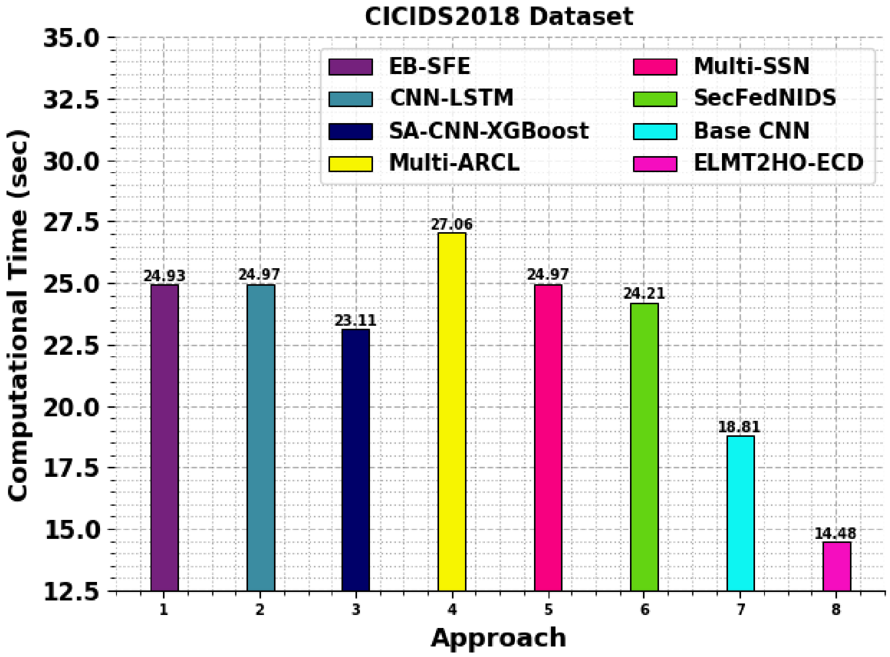


Figure 17. CT evaluation of the ELMT2HO-ECD methodology versus the existing models with the CICIDS2018 dataset.

Table 12 demonstrates the ablation study assessment of the ELMT2HO-ECD model with the CICIDS2018 dataset. The convolutional LSTM with BGO without hyperparameter tuning attained an $accuracy$ of 94.24%, $prec_n$ of 90.32%, $reca_l$ of 89.93%, and $F1_{score}$ of 90.55%. Likewise, the WAE model with BGO without tuning achieved an $accracy$ of 95.52%, $prec_n$ of 91.57%, $reca_l$ of 91.36%, and $F1_{score}$ of 92.00%, increasing to $accuracy$ of 96.25%, $prec_n$ of 92.30%, $reca_l$ of 92.21%, and $F1_{score}$ of 92.55% in subsequent evaluation. Furthermore, TCN with BGO without tuning reached an $accuracy$ of 97.12%, $prec_n$ of 92.99%, $reca_l$ of 92.74%, and $F1_{score}$ of 93.08%, which improved to an $accuracy$ of 97.84%, $prec_n$ of 93.72%, $reca_l$ of 93.63%, and $F1_{score}$ of 93.96%. However, superior results were achived by the complete ELMT2HO-ECD model with an $accuracy$ of 98.43%, $prec_n$ of 94.54%, $reca_l$ of 94.52%, and $F1_{score}$ of 94.47%, underscoring the effectiveness of each component.

Table 12. Ablation study assessment of the ELMT2HO-ECD model under the CICIDS2018 dataset.

CICIDS2018 Dataset				
Model	$Accuracy$	$Prec_n$	$Reca_l$	$F1_{Score}$
Convolutional LSTM+BGO (without hyperparameter tuning)	94.24	90.32	89.93	90.55
Convolutional LSTM+BGO+IPOA (with hyperparameter tuning)	94.90	90.95	90.57	91.41
Wasserstein AE+BGO (without hyperparameter tuning)	95.52	91.57	91.36	92.00
Wasserstein AE+BGO (without hyperparameter tuning)	96.25	92.30	92.21	92.55
TCN+BGO (without hyperparameter tuning)	97.12	92.99	92.74	93.08
TCN+BGO (without hyperparameter tuning)	97.84	93.72	93.63	93.96
ELMT2HO-ECD (ensemble deep learning models with BGO feature selection process and IPOA hyperparameter tuning process)	98.43	94.54	94.52	94.47

Furthermore, the ELMT2HO-ECD technique is examined under the CICIDS2019 dataset [32]. The CICIDS2019 dataset comprises 9,000 samples representing diverse types of network traffic, with each class containing 500 samples. It includes both benign traffic and diverse types of DDoS attacks, such as domain name system (DNS), lightweight directory access protocol (LDAP), Microsoft SQL server (MSSQL), network time protocol (NTP), network basic input/output system (NetBIOS), simple network management protocol (SNMP), and user datagram protocol (UDP). Furthermore, the dataset features other attack types, including LDAP, MSSQL, NetBIOS, Portmap, Syn, TFTP, UDP, UDP-lag, UDPLag, and WebDDoS. The dataset is constructed to support research on network intrusion detection and traffic analysis, providing diverse, labelled samples for machine learning (ML) and DL techniques. The dataset comprises 78 features, of which 34 were selected for analysis.

Figure 18 illustrates the convergence of fitness analysis over various iterations. The results demonstrate that the ELMT2HO-ECD approach achieves optimal convergence across iterations using these data.

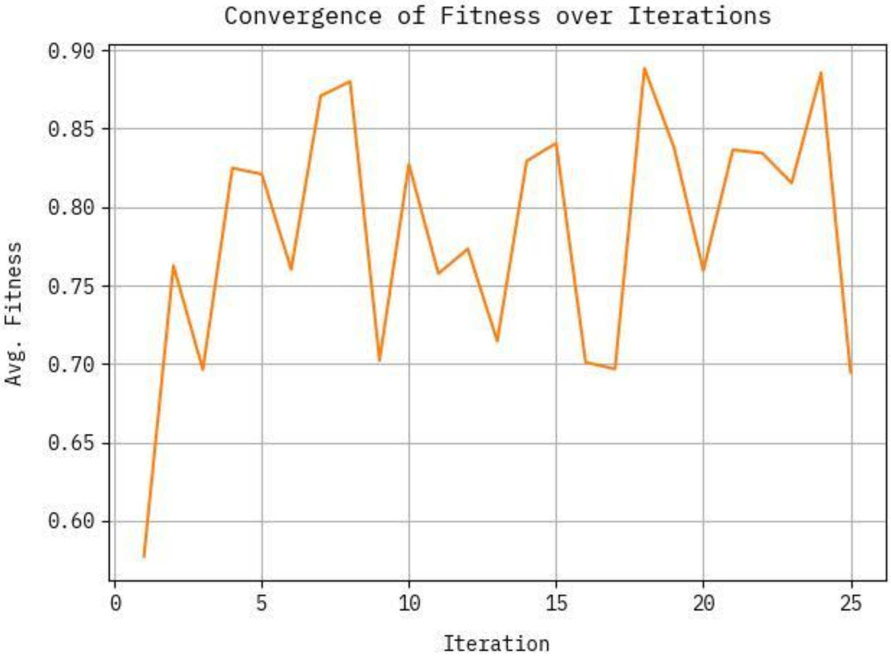


Figure 18. Convergence curve of the ELMT2HO-ECD model accros various iterations.

Figure 19 provides a thorough analysis of the ELMT2HO-ECD technique in classifying diverse attack types within the CICIDS2019 dataset. Figure 19(a) illustrates the training confusion matrix, and Figure 19(b) shows the testing confusion matrix, indicating how well the model distinguishes between benign and malicious traffic. The separate cells in the matrix depict the counts of true positives, false positives, false negatives, and true negatives for each attack class. The PR and ROC curves, shown in Figures 19(c) and 19(d), further highlight the model's robustness across diverse attack types, with higher AUC scores indicating improved classification performance. These matrices and curves collectively demonstrate the model’s robustness and accuracy in detecting diverse attack scenarios.

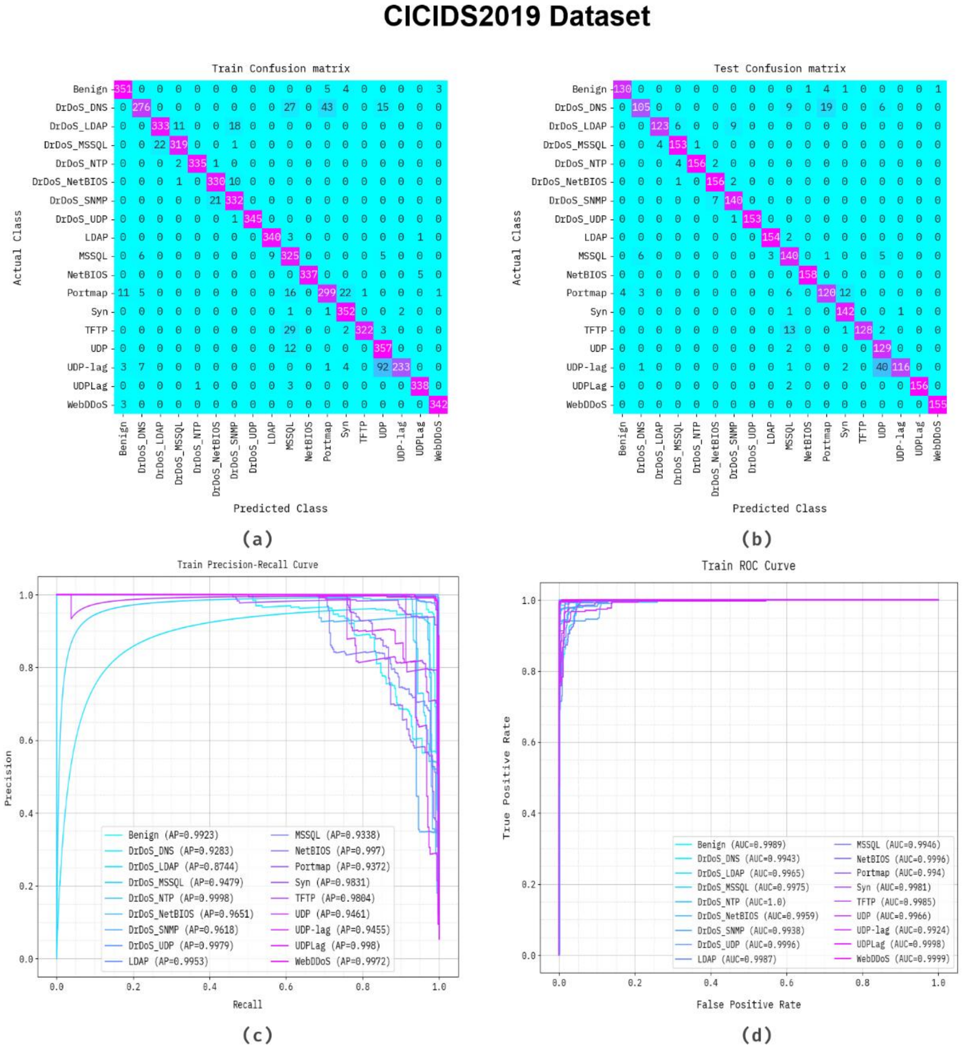


Figure 19. CICIDS2019 dataset: (a) and (b) Confusion matrices, (c) PR, and (d) ROC.

Table 13 and Figure 20 present the attack detection performance of the ELMT2HO-ECD model on the CICIDS2019 dataset with 70% TRPHE and 30% TSPHE, evaluated using multiple metrics, including $accuracy$, $prec_n$, $reca_l$, $F1_{Score}$, and MCC. Under 70% TRPHE, the model achieves high performance across various attack classes with an average $accuracy$ of 99.23%, $prec_n$ of 93.80%, $reca_l$ of 93.13%, $F1_{Score}$ of 93.13%, and MCC of 92.91%. Under 30% TSPHE, the model exhibits robust performance with an average $accuracy$ of 99.23%, $prec_n$ of 93.56%, $reca_l$ of 93.02%, $F1_{Score}$ of 92.94%, and MCC of 92.74%. The results show the technique's consistent effectiveness in detecting both benign and malicious traffic across diverse attack types.

Table 13. Attack detection of the ELMT2HO-ECD model wirh the CICIDS2019 dataset.

Class	$Accuracy$	$Prec_n$	$Reca_l$	$F1_{Score}$	MCC
TRPHE (70%)					
Benign	99.54	95.38	96.69	96.03	95.79
DrDoS_DNS	98.37	93.88	76.45	84.27	83.91
DrDoS_LDAP	99.19	93.80	91.99	92.89	92.46
DrDoS_MSSQL	99.41	95.80	93.27	94.52	94.22
DrDoS_NTP	99.94	99.70	99.11	99.41	99.37
DrDoS_NetBIOS	99.48	93.75	96.77	95.24	94.97
DrDoS_SNMP	99.19	91.71	94.05	92.87	92.45
DrDoS_UDP	99.98	100.00	99.71	99.86	99.85
LDAP	99.79	97.42	98.84	98.12	98.02
MSSQL	98.24	78.12	94.20	85.41	84.90
NetBIOS	99.92	100.00	98.54	99.26	99.22
Portmap	98.32	85.67	84.23	84.94	84.06
Syn	99.43	91.67	98.88	95.14	94.91
TFTP	99.44	99.69	90.45	94.85	94.68
UDP	97.98	75.64	96.75	84.90	84.57
UDP-lag	98.27	99.15	68.53	81.04	81.67
UDPLag	99.84	98.26	98.83	98.54	98.46
WebDDoS	99.89	98.84	99.13	98.99	98.93
Average	99.23	93.80	93.13	93.13	92.91
TSPHE (30%)					
Benign	99.59	97.01	94.89	95.94	95.73
DrDoS_DNS	98.37	91.30	75.54	82.68	82.24
DrDoS_LDAP	99.30	96.85	89.13	92.83	92.55
DrDoS_MSSQL	99.41	93.29	96.84	95.03	94.73
DrDoS_NTP	99.74	99.36	96.30	97.81	97.68
DrDoS_NetBIOS	99.56	94.55	98.11	96.30	96.08
DrDoS_SNMP	99.30	92.11	95.24	93.65	93.29
DrDoS_UDP	99.96	100.00	99.35	99.67	99.66
LDAP	99.81	98.09	98.72	98.40	98.30
MSSQL	98.11	79.55	90.32	84.59	83.78
NetBIOS	99.96	99.37	100.00	99.68	99.67
Portmap	98.19	83.33	82.76	83.04	82.09
Syn	99.33	89.87	98.61	94.04	93.80
TFTP	99.41	100.00	88.89	94.12	93.99
UDP	97.96	70.88	98.47	82.43	82.62
UDP-lag	98.33	99.15	72.50	83.75	84.03
UDPLag	99.93	100.00	98.73	99.36	99.33
WebDDoS	99.96	99.36	100.00	99.68	99.66
Average	99.23	93.56	93.02	92.94	92.74

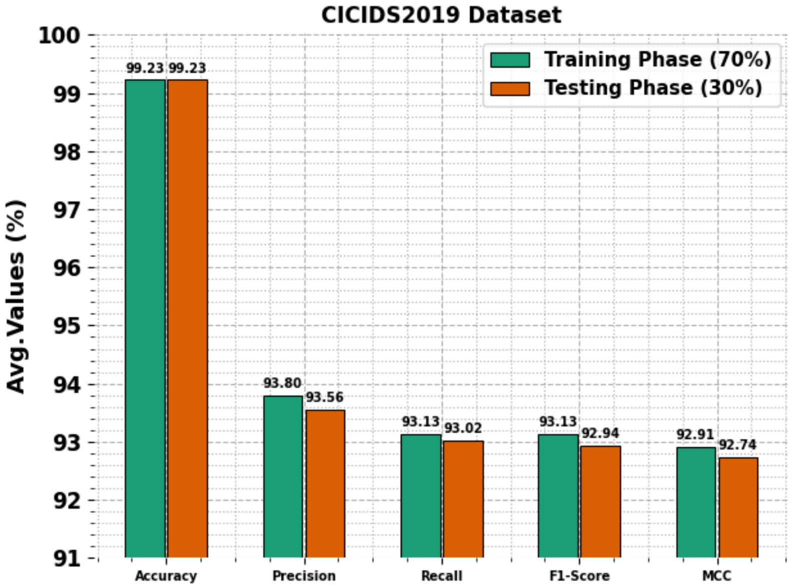


Figure 20. Average values of the ELMT2HO-ECD model with the CICIDS2019 dataset.

In Figure 21, the TRNG and VALID $accuracy$ outcomes of the ELMT2HO-ECD technique on the CICIDS2019 dataset across 0–100 epochs are illustrated. The figure shows that both $accuracy$ values exhibit increasing trends, indicating the efficiency of the ELMT2HO-ECD model and improvements in the outputs across successive iterations. Additionally, the more consistent $accu$ values across epochs indicate reduced overfitting and suggest a more robust solution.

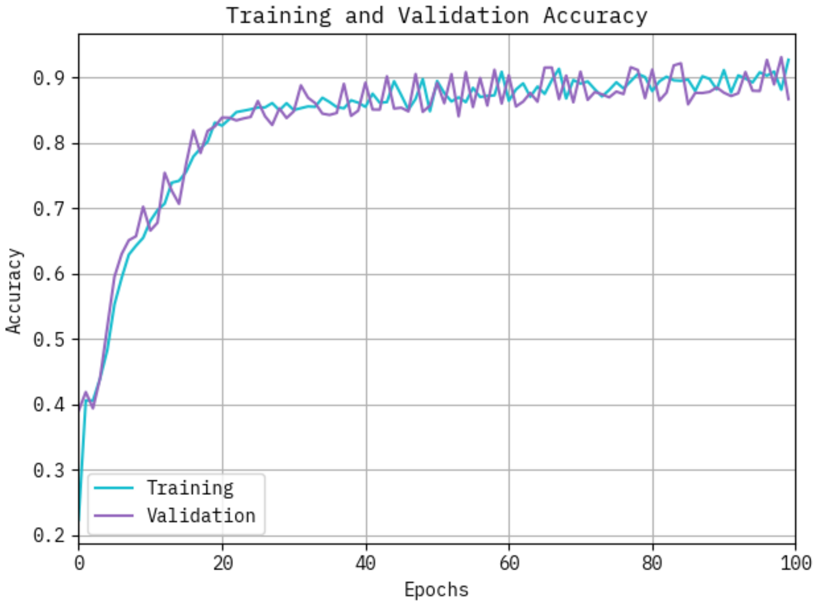


Figure 21. $Accuracy$ curve of the ELMT2HO-ECD approach on the CICIDS2019 dataset.

In Figure 22, the TRNG and VALID loss outputs of the ELMT2HO-ECD technique with the

CICIDS2019 dataset over 0–100 epochs are illustrated. The figure emphasises that both loss values exhibit decreasing trends, showing that the model is effectively learning and minimising errors during training. The training loss consistently decreases, while the validation loss also follows a similar downward trend, suggesting that the model is generalising well. Moreover, the gap between the TRNG/VALID losses remains small, further confirming the model's ability to avoid overfitting and perform efficiently.

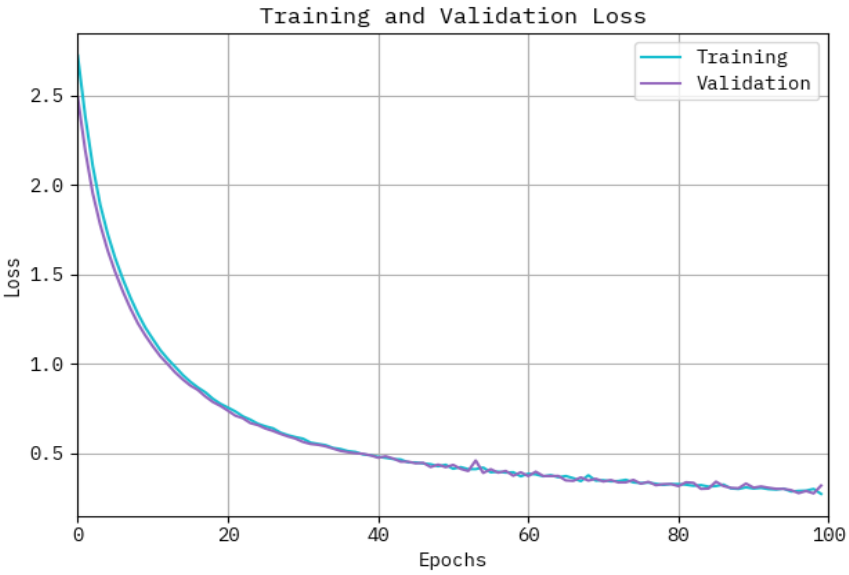


Figure 22. Loss curve of ELMT2HO-ECD approach on the CICIDS2019 dataset.

The comparison study of the ELMT2HO-ECD methodology in Table 14 and Figure 23 with the CICIDS2019 dataset shows that the ABO-FS, CBCO-ERNN, GA-LSTM, CAE-GRU-BL, SVM, CNN-radial. basis function (CNN-RBF), and CNN-LSTM-ATT techniques attained lower values. In contrast, the ELMT2HO-ECD model attained the highest $accuracy$, $prec_n$, $reca_l$, and $F1_{score}$ of 99.23%, 93.80%, 93.13%, 93.13%.

Table 14. Comparison analysis of the ELMT2HO-ECD model under the CICIDS2019 dataset [16–21, 39–41].

CICIDS2019 dataset				
Approach	$Accuracy$	$Prec_n$	$Reca_l$	$F1_{Score}$
ABO-FS [16]	95.04	89.28	89.41	89.32
CBCO-ERNN [18]	97.97	92.93	93.01	91.32
GA-LSTM [19]	97.10	89.95	90.71	90.49
CAE-GRU-BL [21]	95.39	90.88	89.28	89.27
SVM [39]	97.00	92.37	89.13	90.16
CNN-RBF [40]	98.64	90.42	91.64	91.10
CNN-LSTM-ATT [41]	95.67	89.58	90.06	89.01
ELMT2HO-ECD [proposed]	99.23	93.80	93.13	93.13

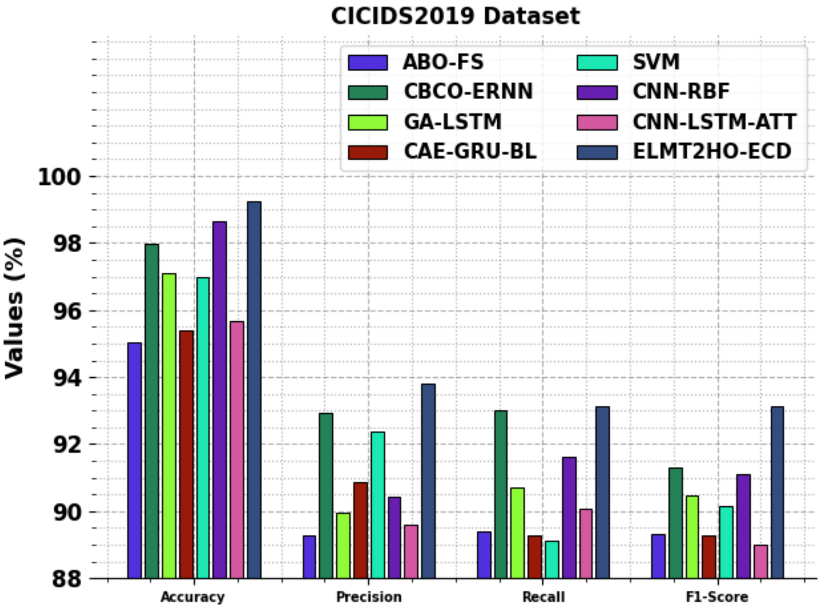


Figure 23. Comparison analysis of the ELMT2HO-ECD model with the CICIDS2019 dataset.

Table 15 and Figure 24 indicate the CT analysis of the ELMT2HO-ECD technique versus the existing methods. The ABO-FS model attained a CT of 22.58, while CBCO-ERNN performs slightly better at 22.40. GA-LSTM and CAE-GRU-BL illustrate higher CT with 28.35 and 29.86, respectively. SVM shows a relatively longer CT of 27.62, whereas CNN-RBF and CNN-LSTM-ATT are more efficient at 23.95 and 22.27 seconds, respectively. The ELMT2HO-ECD model significantly outperforms all existing techniques, achieving the lowest CT of 17.44.

Table 15. CT assessment of the ELMT2HO-ECD technique with the existing methods under the CICIDS2019 dataset.

CICIDS2019 dataset	
Technique	CT (sec)
ABO-FS [16]	22.58
CBCO-ERNN [18]	22.40
GA-LSTM [19]	28.35
CAE-GRU-BL [21]	29.86
SVM [39]	27.62
CNN-RBF [40]	23.95
CNN-LSTM-ATT [41]	22.27
ELMT2HO-ECD [proposed]	17.44

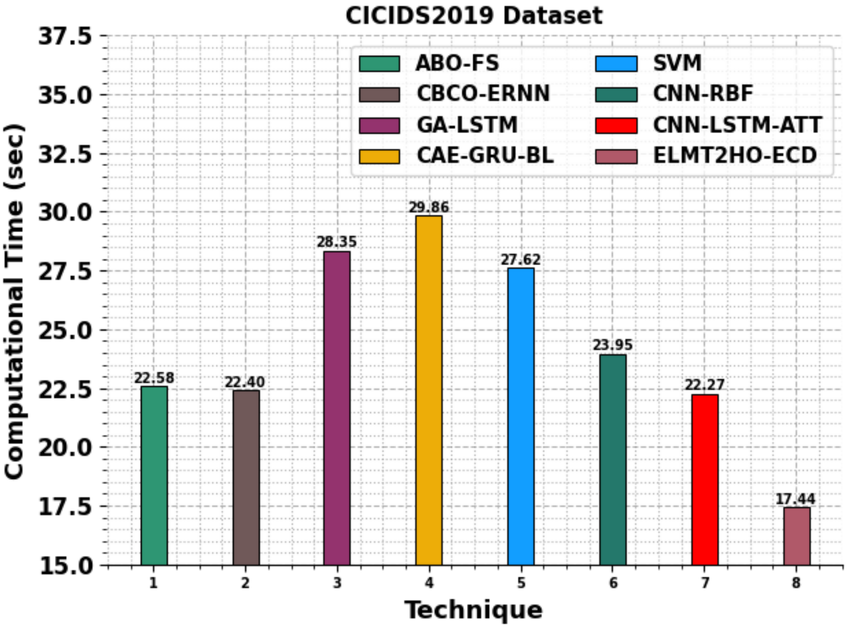


Figure 24. CT assessment of the ELMT2HO-ECD technique versus the existing methods with the CICIDS2019 dataset.

Table 16 exemplifies the ablation study evaluation of the ELMT2HO-ECD method under the CICIDS2019 dataset. The convolutional LSTM with BGO without hyperparameter tuning had an $accuracy$ of 94.77%, $prec_n$ of 89.69%, $reca_l$ of 89.29%, and $F1_{score}$ of 89.02%. Additionally, the Convolutional LSTM+BGO+IPOA combination reached an $accuracy$ of 95.39%, $prec_n$ of 90.34%, $reca_l$ of 89.87%, and $F1_{score}$ of 89.68%. Likewise, the WAE method with BGO without tuning achieved an $accuracy$ of 96.22%, $prec_n$ of 91.05%, $reca_l$ of 90.43%, and $F1_{score}$ of 90.20%, additionally increasing to an $accuracy$ of 96.99%, precision of 91.59%, $reca_l$ of 91.14%, and $F1_{score}$ of 91.02% in subsequent evaluation. Moreover, TCN with BGO without tuning resulted in an $accuracy$ of 97.76%, $prec_n$ of 92.42%, $reca_l$ of 91.85%, and $F1_{score}$ of 91.79%, which improved to an $accuracy$ of 98.44%, $prec_n$ of 92.95%, $reca_l$ of 92.50%, and $F1_{score}$ of 92.60%. Finally, the ELMT2HO-ECD method showed superior values with an $accuracy$ of 99.23%, $prec_n$ of 93.80%, $reca_l$ of 93.13%, and $F1_{score}$ of 93.13%.

Table 16. Ablation study evaluation of the ELMT2HO-ECD method with the CICIDS2019 dataset.

CICIDS2019 dataset				
Method	$Accuracy$	$Prec_n$	$Reca_l$	$F1_{Score}$
Convolutional LSTM+BGO (without hyperparameter tuning)	94.77	89.69	89.29	89.02
Convolutional LSTM+BGO+IPOA (with hyperparameter tuning)	95.39	90.34	89.87	89.68
Wasserstein AE+BGO (without hyperparameter tuning)	96.22	91.05	90.43	90.20
Wasserstein AE+BGO (without hyperparameter tuning)	96.99	91.59	91.14	91.02
TCN+BGO (without hyperparameter tuning)	97.76	92.42	91.85	91.79
TCN+BGO (without hyperparameter tuning)	98.44	92.95	92.50	92.60
ELMT2HO-ECD (ensemble deep learning models with BGO feature selection process and IPOA hyperparameter tuning process)	99.23	93.80	93.13	93.13

5. Conclusions

This paper presents the ELMT2HO-ECD methodology. The primary purpose of the ELMT2HO-ECD methodology is to provide a robust solution for detecting and mitigating DDoS attacks in real time. Initially, the ELMT2HO-ECD approach applies mean normalization to scale the features within a specified range. Furthermore, the MGO approach efficiently selects and recognizes the most related features. For DDoS attack detection, an ensemble of DL techniques, including ConvLSTM, WAE, and TCN, is employed. To further enhance the performance of the three ensemble models, hyperparameter tuning is performed using the IPOA, which optimizes model parameters to achieve higher accuracy. The ELMT2HO-ECD model is evaluated on the CICIDS2017, CICIDS2018, and CICIDS2019 datasets. The validation of the ELMT2HO-ECD model demonstrated superior accuracy of 98.93%, 98.43%, and 99.23% compared with existing techniques. The limitations of the ELMT2HO-ECD model include reliance on a specific dataset that may not fully capture the diversity of real-world DDoS attack scenarios, potentially limiting the model's adaptability to evolving threats. Additionally, the approach requires substantial computational resources, which may limit its deployment in resource-constrained environments. The model also focuses primarily on network traffic features, omitting other contextual data that could improve detection accuracy. For future work, incorporating adaptive learning mechanisms to handle growing attack patterns and exploring lightweight models for edge devices would enhance applicability. Furthermore, expanding evaluation to include multi-vector attacks and real-time implementation scenarios could provide deeper insights into practical efficiency. The ELMT2HO-ECD model can be extended to detect other network attacks, such as SQL injection or phishing, by adapting feature extraction and model layers to detect attack-specific patterns. Future study may also include a method for handling multi-vector DDoS attacks by utilizing flexible ensemble structures and hierarchical feature learning for robust detection of complex, combined threats

Author contributions

Hend Khalid Alkahtani: Conceptualization, methodology, validation, investigation, writing-original draft preparation; Mohammed Baihan: Conceptualization, methodology, writing-original draft preparation, writing-review and editing; Mohammed Burhanur Rehman: Methodology, validation, writing-original draft preparation; Randa Allafi: Software, visualization, validation, data curation, writing-review and editing; Sultan Almutairi: Validation, original draft preparation, writing-review and editing; Ibrahim Zalah: Methodology, validation, conceptualization, writing-review and editing; Nouf Atiahallah Alghanmi: Methodology, validation, original draft preparation; Mohammed Mujib Alshahrani: Validation, original draft preparation, writing-review and editing. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

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

Acknowledgments

The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Research Project under grant number RGP2/ 247/46. The authors would like to thank Ongoing Research Funding program, (ORFFT-2025-090-3), King Saud University, Riyadh, Saudi Arabia. Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R384), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number NBU-FPEJ-2025-170-06. The authors are thankful to the Deanship of Graduate Studies and Scientific Research at University of Bisha for supporting this work through the Fast-Track Research Support Program.

Data availability statement

The data supporting this study's findings are openly available in the Kaggle repository [25–27].

Conflict of interest

The authors declare that they have no conflict of interest. The manuscript was written with contributions from all authors, and all authors have approved the final version.

References

[1] M. Mittal, K. Kumar, S. Behal, Deep learning approaches for detecting DDoS attacks: A systematic review, *Soft Comput.*, **27** (2023), 13039–13075. https://doi.org/10.1007/s00500-021-06608-1

[2] M. Shurman, R. Khrais, A, Yateem, DoS and DDoS attack detection using deep learning and IDS, *Int. Arab J. Inf. Techn.*, **17** (2020), 655–661. https://doi.org/10.34028/iajit/17/4A/10

[3] S. Aktar, A. Y. Nur, Towards DDoS attack detection using deep learning approach, *Comput Secur.*, **129** (2023), 103251. https://doi.org/10.1016/j.cose.2023.103251

[4] T. Khempetch, P. Wuttidittachotti, DDoS attack detection using deep learning, *IAES International Journal of Artificial Intelligence*, **10** (2021), 382–388. http://doi.org/10.11591/ijai.v10.i2.pp382-388

[5] M. S. Elsayed, N. A. Le-Khac, S. Dev, A. D. Jurcut, Ddosnet: A deep-learning model for detecting network attacks, *2020 IEEE 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Cork, Ireland, 2020, 391–396. https://doi.org/10.1109/WoWMoM49955.2020.00072

[6] C. S. Shieh, W. W. Lin, T. T. Nguyen, C. H. Chen, M. F. Horng, D. Miu, Detection of unknown DDoS attacks with deep learning and Gaussian mixture model, *Appl. Sci.*, **11** (2021), 5213. https://doi.org/10.3390/app11115213

[7] J. G. Almaraz-Rivera, J. A. Perez-Diaz, J. A. Cantoral-Ceballos, Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models, *Sensors*, **22** (2022), 3367. https://doi.org/10.3390/s22093367

[8] M. A. Al-Shareeda, S. Manickam, M. A. Saare, DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison, *Bulletin of Electrical Engineering and Informatics*, **12** (2023), 930–939. https://doi.org/10.11591/eei.v12i2.4466

[9] A. R. Shaaban, E. Abd-Elwanis, M. Hussein, DDoS attack detection and classification via convolutional neural network (CNN), *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, Cairo, Egypt, 2019, 233–238. https://doi.org/10.1109/ICICIS46948.2019.9014826

[10] N. A. M. Alhammadi, M. Mabrouk, M. Zrigui, Recent trends on sophisticated types of flooding attacks and detection methods based on multi sensors fusion data for cloud computing systems, *Fusion: Practice & Applications*, **11** (2023), 37–56. https://doi.org/10.54216/FPA.110103

[11] M. Abdullah, H. A. Mengash, M. Maray, F. A. F. Alrslani, H. Alkhudhayr, N. A. Alghanmi, et al., Federated learning with blockchain on denial-of-service attacks detection and classification of edge IIoT networks using deep transfer learning model, *Computers and Electrical Engineering*, **124** (2025), 110319. https://doi.org/10.1016/j.compeleceng.2025.110319

[12] M. Dandotiya, R. R. S. Makwana, Secured DDoS attack detection in SDN using TS-RBDM with MDPP-Streebog based user authentication, *T. Emerg. Telecommun. T.*, **36** (2025), e70052. https://doi.org/10.1002/ett.700

[13] S. Mehmood, R. Amin, J. Mustafa, M. Hussain, F. S. Alsubaei, M. D. Zakaria, Distributed denial of services (DDoS) attack detection in SDN using optimizer-equipped CNN-MLP, *PloS One*, **20** (2025), e0312425. https://doi.org/10.1371/journal.pone.0312425

[14] Y. A. Abid, J. S. Wu, G. Q. Xu, S. H. Fu, M. Waqas, Multilevel deep neural network for distributed denial-of-service attack detection and classification in software-defined networking supported Internet of things networks, *IEEE Internet Things*, **11** (2024), 24715–24725. https://doi.org/10.1109/JIOT.2024.3376578

[15] S. Kanthimathi, S. Venkatraman, K. S. Jayasankar, T. P. Jiljith, R. Jashwanth, A Novel self-attention-enabled weighted ensemble-based convolutional neural network framework for distributed denial of service attack classification, *IEEE Access*, **12** (2024), 151515–151531. https://doi.org/10.1109/ACCESS.2024.3478764

[16] K. K. Paidipati, C. Kurangi, J. Uthayakumar, S. Padmanayaki, D. Pradeepa, S. Nithinsha, Ensemble of deep reinforcement learning with optimisation model for DDoS attack detection and classification in cloud based software defined networks, *Multimed. Tools Appl.*, **83** (2024), 32367–32385. https://doi.org/10.1007/s11042-023-16894-6

[17] M. Fatima, O. Rehman, S. Ali, M. F. Niazi, ELIDS: Ensemble feature selection for lightweight IDS against DDoS attacks in resource-constrained IoT environment, *Future Gener. Comp. Sy.*, **159** (2024), 172–187. https://doi.org/10.1016/j.future.2024.05.013

[18] M. I. T. Hussan, G. V. Reddy, P. T. Anitha, A. Kanagaraj, P. Naresh, DDoS attack detection in IoT environment using optimised Elman recurrent neural networks based on chaotic bacterial colony optimisation, *Cluster Comput.*, **27** (2024), 4469–4490. https://doi.org/10.1007/s10586-023-04187-4

[19] D. M. Dhanvijay, M. M. Dhanvijay, V. H. Kamble, Cyber intrusion detection using ensemble of deep learning with prediction scoring based optimised feature sets for IOT networks, *Cyber Security and Applications*, **3** (2025), 100088. https://doi.org/10.1016/j.csa.2025.100088

[20] Z. Y. Li, M. Y. Liu, P. Wang, W. Y. Su, T. S. Chang, X. J. Chen, et al., Multi-ARCL: Multimodal adaptive relay-based distributed continual learning for encrypted traffic classification, *J. Parallel Distr. Com.*, **201** (2025), 105083. https://doi.org/10.1016/j.jpdc.2025.105083

[21] K. J. Pradeep, P. K. Shukla, Designing a novel network anomaly detection framework using multi-serial stacked network with optimal feature selection procedures over DDOS attacks, *International Journal of Intelligent Networks*, **6** (2025), 1–13. https://doi.org/10.1016/j.ijin.2024.11.001

[22] Y. K. Beshah, S. L. Abebe, H. M. Melaku, Multi-stage adversarial defense for online DDoS attack detection system in IoT, *IEEE Access*, **13** (2025), 72657–72673. https://doi.org/10.1109/ACCESS.2025.3560186

[23] P. Odelu, C. K. Shiva, S. Sen, V. Basetti, C. S. Reddy, Forward-thinking frequency management in islanded marine microgrid utilising a heterogeneous source of generation and nonlinear control assisted by energy storage integration, *Sci. Rep.*, **15** (2025), 13794. https://doi.org/10.1038/s41598-025-97592-1

[24] T. L. Xu, Z. Q. Zhou, C. X. Wang, Y. C. Li, T. Rong, Spatio-temporal prediction of surface remote sensing data in equatorial pacific ocean based on multi-element fusion network, *J. Mar. Sci. Eng.*, **13** (2025), 755. https://doi.org/10.3390/jmse13040755

[25] A. X. Wang, B. P. Nguyen, Deterministic autoencoder using Wasserstein loss for tabular data generation, *Neural Networks*, **185** (2025), 107208. https://doi.org/10.1016/j.neunet.2025.107208

[26] E. Akhmetshin, D. Hudayberganov, R. Shichiyakh, S. Yellisetti, L. K. Pappala, et al., Intelligent federated learning boosted cyberattack detection system for Denial-Of-Wallet attacks using an advanced heuristic search with multimodal approaches, *Sci. Rep.*, **15** (2025), 14265. https://doi.org/10.1038/s41598-025-96986-5

[27] J. Li, C. Bastani, Optimising PEMFC parameter identification using improved pufferfish algorithm and CNN, *AIP Adv.*, **15** (2025), 025117. https://doi.org/10.1063/5.0251549

[28] H. Shen, C. J. Peng, H. C. Yan, S. Y. Xu, Data-driven near optimisation for fast sampling singularly perturbed systems, *IEEE T. Automat. Contr.*, **69** (2024), 4689–4694. https://doi.org/10.1109/TAC.2024.3352703

[29] H. Shen, Y. Wang, H. C. Yan, S. Y. Xu, Data-driven single-loop policy iteration control of uncertain singularly perturbed systems, *IEEE T. Automat. Contr.*, **70** (2025), 8314–8320. https://doi.org/10.1109/TAC.2025.3581141

[30] *Network Intrusion Dataset (CIC-IDS-2017)*, 2023. Available from: https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset.

[31] *IDS 2018 Intrusion CSVs (CSE-CIC-IDS2018)*, 2020. Available from: https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv.

[32] M. A. Talukder, M. A. Uddin, *CIC-DDoS2019 Dataset*, Mendeley Data, 2023. Available from: https://data.mendeley.com/datasets/ssnc74xm6r/1.

[33] D. Javeed, M. S. Saeed, I. Ahmad, P. Kumar, A. Jolfaei, M. Tahir, An intelligent intrusion detection system for smart consumer electronics network, *IEEE T. Consum. Electr.*, **69** (2023), 906–913. https://doi.org/10.1109/TCE.2023.3277856

[34] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, R. Patan, Effective attack detection in internet of medical things smart environment using a deep belief neural network, *IEEE Access*, **8** (2020), 77396–77404. https://doi.org/10.1109/ACCESS.2020.2986013

[35] S. Songma, T. Sathuphan, T. Pamutha, Optimising intrusion detection systems in three phases on the CSE-CIC-IDS-2018 dataset, *Computers*, **12** (2023), 245. https://doi.org/10.3390/computers12120245

[36] E. Osa, P. E. Orukpe, U. Iruansi, Design and implementation of a deep neural network approach for intrusion detection systems, *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, **7** (2024), 100434. https://doi.org/10.1016/j.prime.2024.100434

[37] S. S. N. Chintapalli, S. P. Singh, J. Frnda, P. B. Divakarachari, V. L. Sarraju, P. Falkowski-Gilski, OOA-modified Bi-LSTM network: An effective intrusion detection framework for IoT systems, *Heliyon*, **10** (2024), e29410. https://doi.org/10.1016/j.heliyon.2024.e29410

[38] O. D. Okey, D. C. Melgarejo, M. Saadi, R. L. Rosa, J. H. Kleinschmidt, D. Z. Rodríguez, Transfer learning approach to IDS on cloud IoT devices using optimised CNN, *IEEE Access*, **11** (2023), 1023–1038. https://doi.org/10.1109/ACCESS.2022.3233775

[39] M. Ramzan, M. Shoaib, A. Altaf, S. Arshad, F. Iqbal, A. K. Castilla, et. al., Distributed denial of service attack detection in network traffic using deep learning algorithm, *Sensors*, **23** (2023), 8642. https://doi.org/10.3390/s23208642

[40] F. L. Becerra-Suarez, I. Fernández-Roman, M. G. Forero, Improvement of distributed denial of service attack detection through machine learning and data processing, *Mathematics*, **12** (2024), 1294. https://doi.org/10.3390/math12091294

[41] M. Ouhssini, K. Afdel, M. Akouhar, E. Agherrabi, A. Abarda, Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches, *Egypt. Inform. J.*, **27** (2024), 100517. https://doi.org/10.1016/j.eij.2024.100517

AIMS Press