SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V13I10P102

Volume 13 Issue 10, 14-27, October 2026
© 2026 Seventh Sense Research Group®

Original Article

Effective Intrusion Detection and Classification in VANET Environments Using Deep Learning Model with Optimization Algorithms

R. Raja Kumar[1], T. Suresh[2], K. Sekar[3]

[1,2]*Department of Computer Science and Engineering, Annamalai University, Tamil Nadu, India.*
[3]*Department of Computer Science and Engineering, Chadalawada Ramanamma Engineering College (Autonomous), Tirupati, India.*

[2]*Corresponding Author : sureshaucse@gmail.com*

Received: 18 July 2026 Revised: 21 September 2026 Accepted: 15 October 2026 Published: 30 October 2026

Abstract *- VANET (Vehicular Ad Hoc Network) is an innovative transportation technology that improves road safety and traffic management through communication and data sharing between vehicles. The attackers create various kinds of assaults to oppose the operational tasks of the network environment in VANET. Then, identifying the attacks in VANET method is extremely essential to give reliable and secure communication among each vehicle within the system. Because of this, the Intrusion Detection System (IDS) is needed in VANET to offer safety from outside attacks like Botnet, Denial of Service (DoS), and so on. These may identify assaults and provoke a response, lowering the effects on the target system. This paper develops an Intelligent Intrusion Detection and Classification using Deep Learning Model and Metaheuristic Optimization Algorithms (IIDC-DLMMOA) method in VANET Environments. The main intention of IIDC-DLMMOA technique relies on developing an effective structure for IDS in VANET communications. The hiking optimization algorithm (HOA) performs feature selection by identifying the input features that contribute most to the classification process. For the classification process, the proposed IIDC-DLMMOA designs a spatial-temporal attentive with long short-term memory (STA-LSTM) system. At last, the hyperparameter tuning optimizes a classification model of STA-LSTM method through a Multi-Objective Mantis Search Algorithm (MOMSA) by selecting the best parameter values. The developed IIDC-DLMMOA system is verified on the real-time benchmark database, and the stimulated outcomes are in comparison with other advanced techniques.*

Keywords *- VANET, Intrusion Detection, Deep Learning, Multi-Objective Mantis Search Algorithm, Feature Selection, Vehicles-To-Everything.*

1. Introduction

Current improvements in the Internet of Things (IoT) and communication systems gained greater interest in the transportation field through smart and emergent vehicle applications [1]. Vehicular Ad Hoc Networks (VANETs) are considered effective smart transport tools, which show the way to several applications mostly connected to road safety as well as human day-to-day operations, namely reducing damage to public infrastructure, alerting to accidents, and giving data regarding weather, Internet facility, and traffic congestion [2]. VANET allows generally dual communications: vehicles to connect with roadside infrastructure (V2I) and vehicles to communicate with other vehicles (V2V). Vehicles typically employ fixed Roadside Units (RSUs) portals for sharing crucial driving environment information [3]. Additionally, further mobile nodes support the information transfer in VANET affiliated with vehicles-to-everything (V2X) communication, like bikes and walkers. But, occasionally, current obstacles like buildings may disturb VANET communication relations, which leads to data loss [4]. Other concern belongs to the higher node mobility, triggering various interruptions as it is positioned far away from the vehicle's location, that's why Unmanned Aerial Vehicles (UAVs), usually termed drones, had arisen in VANET, boosting investigators for examining its capability to fly across cities to send messages effortlessly through evading problems in the field [5].

Numerous research studies were done to prevent attacks in VANET, normally through utilizing cryptographic devices [6]. However, this method can't identify or avoid certain threats. Black holes, Denial of Service (DoS), Sybil, and Grey hole are a few instances of threats that can't be prohibited through conventional approaches [7]. A probable resolution to this issue has been the use of Intrusion Detection System (IDS). This will recognize threats and activate a response by

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

decreasing the impacts on the particular systems. Conventional IDSs believe that an attacker's behaviour may be obvious in regular network processes [6]. Signature detection systems relate the attacker's behavior by identified threats, believing no fresh threats might occur.

The use of these smart methods permits the IDS to study earlier attacks and find fresh ones [8]. Currently, combining Artificial Intelligence (AI) in IDS increases their capability to detect potential threats in V2X system [9]. Additionally, machine learning (ML) may enforce IDS, which can identify zero-day and unknown threats and raising its detection capability eventually.

This paper introduces an IIDC-DLMMOA method in VANET Environments. Initially, the Linear Scaling Normalization (LSN) is applied for data pre-processing stage. The Feature Selection (FS) is then executed by the Hiking Optimization Algorithm (HOA). For the classification process, the IIDC-DLMMOA designs a spatial-temporal attentive with long short-term memory (STA-LSTM) system.

At last, the hyperparameter tuning optimizes a classification model of STA-LSTM method through Multi-Objective Mantis Search Algorithm (MOMSA) by selecting the best parameter values. The developed IIDC-DLMMOA system is verified on the real-time benchmark dataset.

2. Literature Review

Dalal [10] proposed a general structure for addressing those problems, including 3 modules. Firstly, the Self-Improved Kookaburra Optimization Algorithm enhances cluster creation, considers link lifetime and mobility patterns, trust, and improves efficacy and flexibility of the network. Secondly, an Improved LSTM paradigm was presented for ID, including quality of the link and trust metrics for diminishing false alarms. Hassan et al. [11] presented a hybrid method that utilizes automatic feature engineering through correlation-based FS (CFS) and PCA to decrease feature matrix size once a sequence of thick coverings was leveraged for identification.

The proposed usage of PCA and CFS on the ML pipeline serves double gains. The security safeguarded through the vehicular system may simply be cooperated in malignant traffic by IoT's significant development. One factor is identifying malignant traffic in Vehicular networks. In [12], a secured authentication method by threat mitigation and routing is executed by utilizing the best DL procedure and planned SecureAuth protocol.

Chen et al. [13] proposed a fresh hybrid procedure called VAN-IDS. The procedure integrates physical features and packet study. Temporal possessions of packets were examined employing Bi-LSTM, whereas vehicles' physical characteristics were assessed through LightGBM. It also presents numerous threat vectors, cooperating privacy, and security. To enrich the current VANET IDS precision and realism. Behura et al. [14] suggested an elevated multi-objective process for addressing those difficulties by refining CHS and guaranteeing safe data communication. An identified malignant activity case, the protocol joins Autoencoder and Isolation forest methods for threat classification, reinforced through elevated FS.

Arya et al. [15] suggested a method for ID that relied on the FL of diverse NN for smart cities. It preserves resources and time through the well-organized ID methodology. Initially, vehicles employ an FL approach for developing DL-aided attack classification. The model use ensemble of federated heterogeneous NN has been made for every vehicle, comprising remotely as well as locally trained classifiers.

ALMahadin et al. [16] anticipated a DL paradigm to detect intrusions derived from GRU on VANET network traffic for addressing these challenges. Consumer electronics technology is effectively presented to the market in two forms: there are strong advantages to the client for deploying these technologies, and it is necessary through supervisory instruction, which avoids the practice of substitutes.

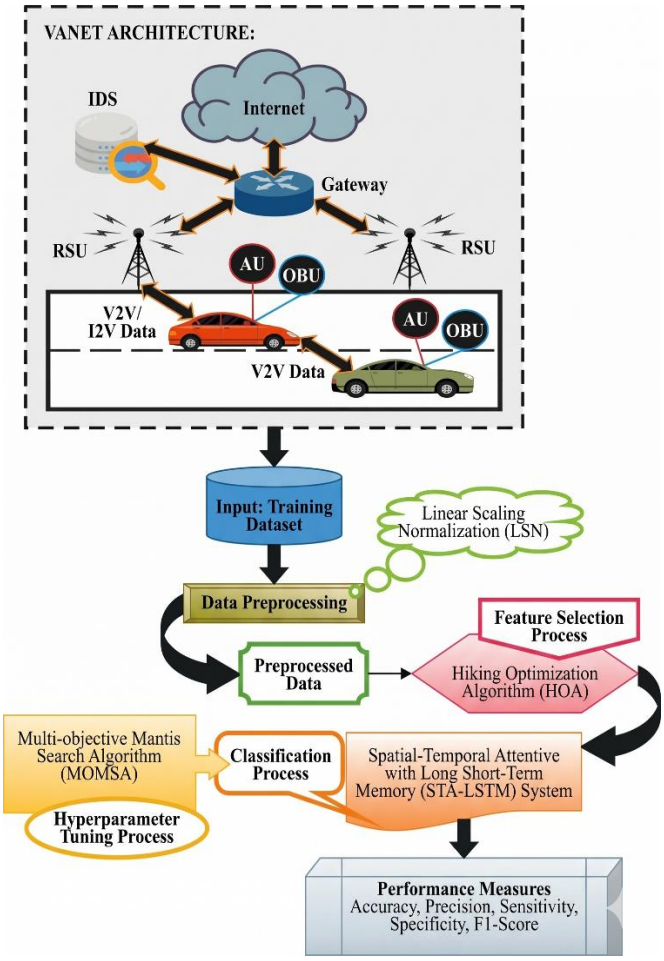


Fig. 1 Workflow of IIDC-DLMMOA method

3. Materials and Methods

In this study, a novel IIDC-DLMMOA approach is developed in VANET Environments. The main intention of IIDC-DLMMOA technique relies on developing an effective structure for intrusion detection in VANET communications. Figure. 1 illustrates the workflow of IIDC-DLMMOA method.

3.1. Data Normalization: LSN Model

The data pre-processing step first applies LSN to convert raw data into a clean and suitable format. LSN is a data preprocessing method applied to rescale values of the feature into the particular field, normally [0, 1]. In IDS for VANETs, this model ensures that individual input features contribute to the learning process, avoiding bias owing to opposing value scales [17]. It enhances the convergence speed and precision of DL methods by removing the superiority of higher-magnitude features. Linear normalization is mainly valuable in VANET environments, whereas data from different resources (like position, speed, and packet size) varied considerably. By converting the data uniformly, the system can well identify subtle abnormalities. This preprocessing stage is important for improving the stability and performance of classification methods applied in VANET-based intrusion detection.

3.2. Feature Selection Process: HOA

Followed by preprocessing step, the FS process is executed by the HOA to identify the informative features from input data. HOA is stimulated by the skill of mountaineers once they try to meet land, namely, rocks, mountains, and hills [18]. During the HOA model, the real speed of all variables, for example: every individual, is adjusted by the function of Tobler presented in Equation. (1), follows that the speed upgrade is attained according to the best location discovered, the present location, and the Sweep Factor (SF).

Conceptual hiker speed upgraded equation is presented in Equation. (1):

$$w_{i,t} = 6e^{-3.5|S_{i,t}+0.05|} \tag{1}$$

Whereas $w_{i,t}$ characterizes the hiker speed i at time t or at iteration t, and $S_{i,t}$ refers to slope of the mountain terrain or path that can be displayed in Equation. (2):

$$S_{i,t} = \frac{dh}{dx} = tan\theta_{i,t} \tag{2}$$

Whereas dx and dh characterize the distance difference and elevation change passed by the hiker, individually; $\tan\theta_{i,t}$ represents the mountain land's slope angle.

The real speed equation is presented in Equation. (3):

$$w_{i,t} = w_{i,t-1} + \gamma_{i,t}\left(\beta_{best} - \alpha_{i,t}\beta_{i,t}\right) \tag{3}$$

Whereas $y_{i,t}$ signifies randomly generated numbers; $w_{i,t-1}$,$w_{i,t}$ characterize the initial and current speeds, correspondingly; β_{best} symbolizes optimal place, $\alpha_{i,t}$ is SF.

The hiker's-updated location is calculated using Equation. (4):

$$\beta_{i,t+1} = \beta_{i,t} + W_{i,t} \tag{4}$$

Here, $\beta_{i,t}$ epitomizes the location of hiker i at tth time; $\beta_{i,t+1}$ signifies the upgraded location.

The effective performance of the HOA is as demonstrated:

Initialization: All hikers represent decision variables, and is given a starting position by calculating its novel location afterward a particular time utilizing the function of Tobler hiking Equation. (19), thus upgrading the searching area. The fitness was estimated, and the top fitness is measured as the main solution, for example: the best value.

Iteration Procedure: In all iterations, the leader's position is updated, while the other hikers are modified according to their leader's location, land slopes, and their speed.

Location Upgrade: The locations of the hikers are constantly upgraded, guaranteeing they stay inside the lower and upper limits of the problem.

Convergence and Termination: Outputting the best value afterward achieves the maximal iteration counts or satisfies the convergence settings.

The Fitness Function (FF) evaluates the performance and the number of chosen attributes. It aims to improve results while reducing the number of features used. Based on these two criteria, the FF is used to evaluate each candidate solution.

$$Fitness = \alpha * ErrorRate + (1-\alpha) * \frac{\#SF}{\#All_F} \tag{5}$$

Now, $ErrorRate$ signifies the classification error rate (0-1), $\#SF$ implies the count of selected features, $\#All_F$ indicates the total features, α is applied to evaluate the subset length.

3.3. IDS Classification Process: STA-LSTM

In addition, the IIDC-DLMMOA model designs a STA-LSTM system for the classification process. The LSTM network is a kind of RNN intended for learning longer-term dependency in sequential data [19]. Diverse conventional RNN LSTMs diminish the problem of vanishing gradient by integrating gating mechanisms and memory cells. An LSTM

handles sequential patterns by upholding a cell state, c_t upgraded at every time step t through an integrating 3 gates

1. Input Gate (i_t): It assess how much of the information stored in the cell states need to be updated.

$$i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i) \quad (6)$$

where x_t specifies the vectorized input at time t, h_{t-1} implies the hidden layer (HL) from the preceding time-step, U_i and W_i are the weighted matrices for recurrent and input connections, correspondingly, and b_i implies the biased vector. The function σ depicts the nonlinear activation function of sigmoid.

2. Forget Gate (f_t): It controls how much information from the preceding cell state in retained for the next step.

$$f_t = \sigma\left(W_f x_t + U_f h_{t-1} + b_f\right) \quad (7)$$

Here U_f and w_f are the trainable weighted matrices for recurrent and input transformation and b_f denotes the bias term.

3. Output Gate (o_t): It determines the output cell state information to the HL.

$$o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o) \quad (8)$$

Now U_o and W_o are the weighted matrices for recurrent and input connection, and b_0 depicts the vector bias.

The c_t state was upgraded by retaining relevant information from the previous memory and adding new information selected by the input gate.

$$c_t = f_t \odot c_{t-1} + i_t \odot \tanh(W_c x_t + U_c h_{t-1} + b_c) \quad (9)$$

Here c_{t-1} denotes the memory cell, U_c and W_c implies weighted matrices for recurrent and input connections, $\odot$ implies element-wise multiplication.

$$h_t = o_t \odot \tanh(c_t) \quad (10)$$

The LSTM processes historic positional information (x, y) over a predefined temporal window. The model processes input sequence through LSTM layers to learn temporal patterns, followed by a fully connected layer for prediction and MSE for loss calculation.

$$\mathcal{L} = \frac{1}{N}\sum_{i=1}^{N} \| y_i - \hat{y}_i \|^2 \quad (11)$$

Now $\hat{y}$ and y_i implies the predicted and actual sets, correspondingly, and N denotes the training sample counts.

The capability LSTM is effectively capturing temporal patterns in sequential data, but face many limitations in practical responsiveness, deals with noisy or sparse data. STA-LSTM extends standard LSTM by integrating Attention Mechanism (AM) to learn significant temporal or spatial dependencies effectively. The attention layer assigns higher weights to significant time steps, thus refining their contribution toward the final output.

1. Attention Score Calculation: The attention score at each step t is obtained using the HL h_t and learned learnable context vector u:

$$\alpha_t = \frac{\exp\left(u^T \tanh(W_a h_t + b_a)\right)}{\Sigma_{k=1}^{T} \exp\left(u^T \tanh(W_a h_k + b_a)\right)} \quad (12)$$

Here b_a represents a biased vector, T denotes the entire time steps, and W_a is weighted matrix.

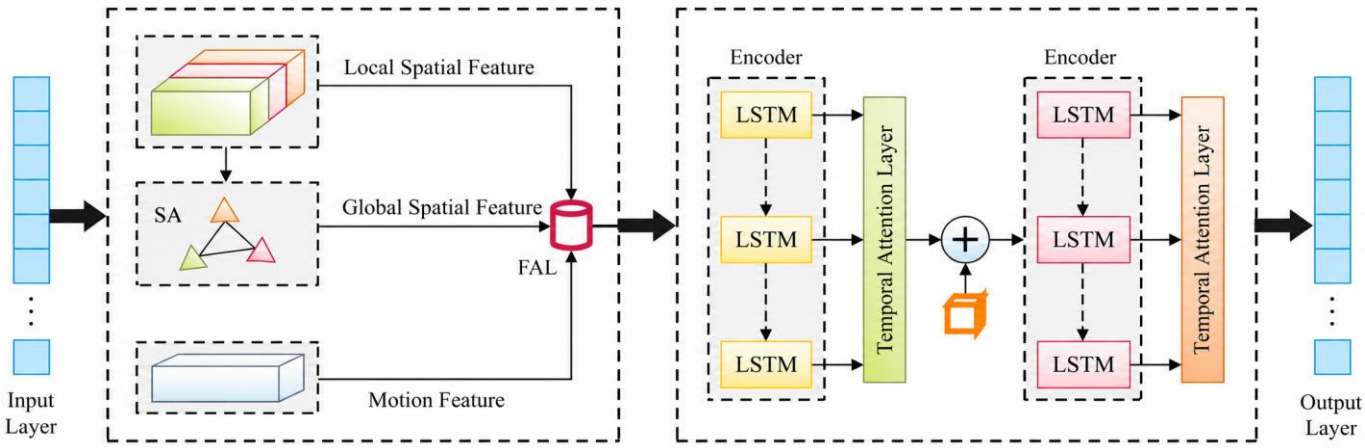


Fig. 2 Architecture of STA-LSTM Model

2. Weighted Hidden State: The HL are multiplied by their equivalent attention weights and combined to form the context vectors c:

$$c = \sum_{t=1}^{T} \alpha_t \, h_t \tag{13}$$

3. Final outcome: The vector c fed to an activation function and fully connected layer to generate the final result:

$$y = W_c c + b_c \tag{14}$$

Now b_c denotes the bias vector and W_c implies the weighted matrix.

The STA-LSTM process sequences coordinate data while selecting significant spatial and temporal patterns using AM. Its architecture involves positional input layer, multiple LSTM layer, attention layer, and a regression output. By prioritizing significant movements, it performs effectively in irregular sequences, AM further increases computational complexity, Figure.2 presents the structure of STA-LSTM.

3.4. Parameter Optimizer: MOMSA

At last, the hyperparameter tuning optimizes a classification model of STA-LSTM method through MOMSA by selecting the best parameter values. The basic concept of MOMSA originates from the preying behavior of the mantis, incorporating the search tactic of mantis in the searching procedure [20]. The searching procedure of the mantis includes 4 major steps: initialization (the waiting), the development, the exploration, and the sexual cannibalism dynamic stages. The model utilizes Pareto benefit to assess candidate solutions and preserves a not dominated group which meets slowly to the Pareto boundaries over outside archiving mechanisms. Non-dominant Ranking (NDR) is an essential element which use Crowding Distance (CD) to maintain solution diversity and minimize local convergence within the Pareto front. These mechanisms calculate the solution's density on the Pareto boundaries, guaranteeing the uniform distribution and diversity of solutions in the targeted area. This segment broadly presents the conceptual framework, mathematical equations and execution modes of MOMSA optimizer model.

3.4.1. Initialization Stage

MOMSA is relied on the MSA that draws stimulation from the particular behavior of mantises and possess several benefits. During the initialization stage, MOMSA makes a first population including mantis individuals (search agents) signifying possible solutions. The location of every mantis is formulated as shown:

$$Z_i(t) = rand \cdot (Z^{up} - Z^{low}) + Z^{low} \tag{15}$$

Whereas $Z^{low}$and Z^{up} epitomize the upper and lower limits of the searching region size i, correspondingly.

3.4.2. Exploration Stage

The exploration stage model the hunting behavior of the mantis, separated into dual behavioral manners: ambusher and pursuer. The behavior of the pursuer incorporates Levy flight (LF) distribution with standard distribution features.

$$Z_i(t+1) = \begin{cases} Z_i(t) + \tau_1 \times \big(Z_i(t) - Z_\alpha(t)\big) + |\tau_2| \cdot U \times \big(Z_\alpha(t) - Z_b(t)\big), r_1 < r_2 \\ Z_i(t) \times U + \Big(Z_\alpha(t) + r_3 \times \big(Z_b(t) - Z_c(t)\big)\Big) \times (1 - U), else \end{cases} \tag{16}$$

Whereas τ_1 is produced by the FL approach; $|\tau_2| \sim N(0,1); r_1, r_2, r_3 \in [0,1]$ means randomly generated numbers; $Z_a(t), Z_b(t), Z_c(t)$ denote select at random from the present population.

3.4.3. Exploitation Stage

During the exploitation stage, if prey approaches, the mantis starts an attack.

$$Z_i(t+1) = \begin{cases} Z_i(t) + r_{10} \times \big(Z_a - Z_b(t)\big), & r_{11} < r_{12} \\ \dfrac{Z_i(t) + Z^*(t)}{2} + v_s \cdot d_{si}(t), & else \end{cases} \tag{17}$$

Whereas $Z^*(t)$ characterizes the present best solution for the population. d_{si} refers to distance among present and best solutions. v_s denote striking speed of the mantis. r_{10}, r_{11}, r_{12} means arbitrarily made in [0,1].

$$d_{si}(t) = Z^*(t) - Z_i(t) \tag{18}$$

$$v_s = \frac{1}{1 + e^{i\rho}} \tag{19}$$

3.4.4. Sexual Cannibalism Dynamics

This mechanism represents the female mantis's behavior through three stages: attracting the male, mating through a uniform crossover operation, and feeding on the male. Random values guide the movement and mating processes, while the feeding ratio determines the feeding behavior.

3.4.5. Non-Dominated Sorting (NDS)

NDS ranks candidate solutions by comparing their objective values. A solution dominates another when it

performs equally well or better across all objectives and achieves a better value for at least one objective. Solutions that are not dominated by any other candidate form the Pareto.

$$PS = \{z \in Z | \nexists\, y \in Z, y < z\} \quad (20)$$

3.4.6. Crowding Distance (CD) Mechanism

CD mechanism helps maintain variation among the non-dominated solutions in MOMSA. It measures the spacing between solutions in the objective space and helps avoid the accumulation of candidates in a small region.

$$CD_j^i = \frac{f_j^{i+1} - f_j^{i-1}}{f_j^{\max} - f_j^{\min}} \quad (21)$$

Whereas $f_j^{\min}$ and $f_j^{\max}$ signify the minimum and maximum J_{th} objective function values.

MOMSA uses a fitness function to evaluate the classification performance of each candidate solution. The classification error rate used as the fitness value, and the optimization process aims to reduce this value to improve classification results.

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{no\ of\ misclassified\ samples}{Total\ no\ of\ samples} * 100 \quad (22)$$

4. Experimental Analysis

Here, the performance outcomes of IIDC-DLMMOA technique is tested under CIC-IDS2017 database [21]. The dataset consists of 30,800 samples across 12 traffic categories, as listed in Table 1. The total number of features is 78 only 45 were selected.

Figure. 3 presents the intrusion detection results of the IIDC-DLMMOA method using the CIC-IDS2017 dataset. Figures. 3a and 3b show the confusion matrices obtained with the 70:30 data split, illustrating the classification results for each class. Figure. 3c presents the PR curves, while Figure. 3d displays the ROC curves for the different class labels.

Table 2 and Figure. 4 represent the intrusion detection of IIDC-DLMMOA system on CIC-IDS2017 database. On 70% TRAPH, the IIDC-DLMMOA system gets average $accu_y$, $prec_n$, $sens_y$, $spec_y$, and $F1_{score}$ of 99.15%, 93.80%, 92.49%, 99.53%, and 93.06%, correspondingly. Moreover, based on 30% TESPH, the proposed IIDC-DLMMOA algorithm accomplishes average $accu_y$, $prec_n$, $sens_y$, $spec_y$, and $F1_{score}$ of 99.16%, 94.34%, 92.70%, 99.54%, and 93.41%, correspondingly.

Table 1. Details of CIC-IDS2017 database

	Type of Traffic	Samples
CIC-IDS2017 Database"	"Benign"	3000
	"Bot"	1800
	"DDoS"	3000
	"DoS GoldenEye"	3000
	"DoS Hulk"	3000
	"DoS Slowhttptest"	3000
	"DoS Slowloris"	3000
	"FTP-PATATOR"	3000
	"PortScan"	3000
	"SSH-PATATOR"	3000
	"WebAttack BruteForce"	1500
	"WebAttack XSS"	500
	Total	**30800**

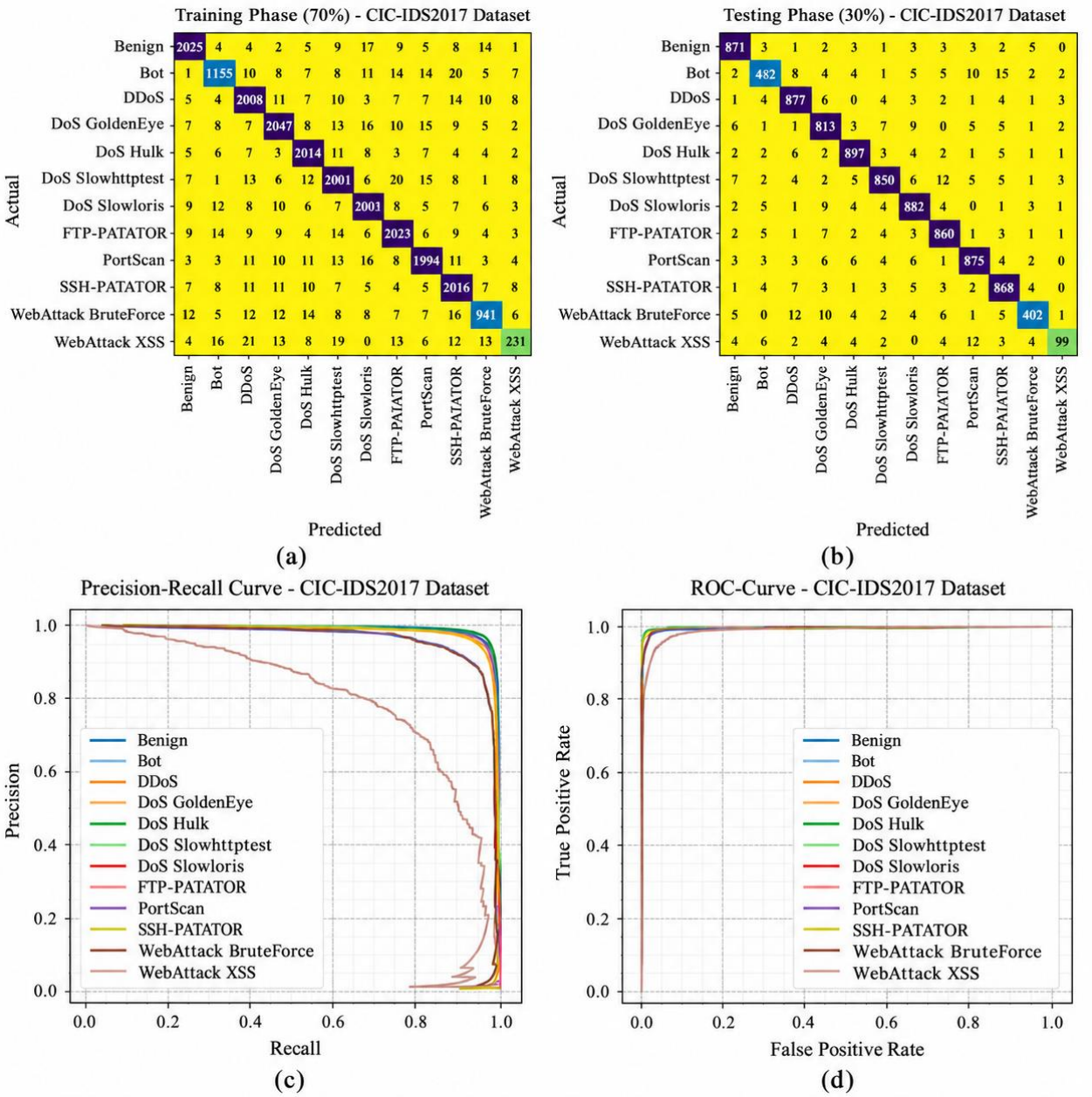


Fig. 3 CIC-IDS2017 database (a-b) confusion matrices and (c-d) curves of PR and ROC

Table 2. Intrusion detection of IIDC-DLMMOA algorithm on CIC-IDS2017 database

Classes	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	$F1_{score}$
TRAPH (70%)					
Benign	99.32	96.70	96.29	99.65	96.50
Bot	99.14	93.45	91.67	99.60	92.55
DDoS	99.08	94.67	95.89	99.42	95.28
DoS GoldenEye	99.10	95.56	95.34	99.51	95.45
DoS Hulk	99.29	95.63	97.11	99.53	96.36
DoS Slowhttptest	99.00	94.39	95.38	99.39	94.88
DoS Slowloris	99.18	95.43	96.11	99.51	95.77
FTP-PATATOR	99.12	95.16	95.88	99.47	95.51

PortScan	99.14	95.59	95.54	99.53	95.57
SSH-PATATOR	99.07	94.47	96.05	99.39	95.25
WebAttack BruteForce	99.17	92.89	89.79	99.65	91.31
WebAttack XSS	99.18	81.63	64.89	99.75	72.30
Average	99.15	93.80	92.49	99.53	93.06
TESPH (30%)					
Benign	99.34	96.14	97.10	99.58	96.62
Bot	98.99	93.23	89.26	99.60	91.20
DDoS	99.19	95.02	96.80	99.45	95.90
DoS GoldenEye	98.97	93.66	95.31	99.34	94.48
DoS Hulk	99.30	96.14	96.87	99.57	96.50
DoS Slowhttptest	99.06	96.05	94.24	99.58	95.13
DoS Slowloris	99.11	94.84	96.29	99.42	95.56
FTP-PATATOR	99.22	95.34	96.63	99.50	95.98
PortScan	99.15	95.52	95.84	99.51	95.68
SSH-PATATOR	99.08	94.35	96.34	99.38	95.33
WebAttack BruteForce	99.19	94.15	88.94	99.72	91.47
WebAttack XSS	99.36	87.61	68.75	99.85	77.04
Average	99.16	94.34	92.70	99.54	93.41

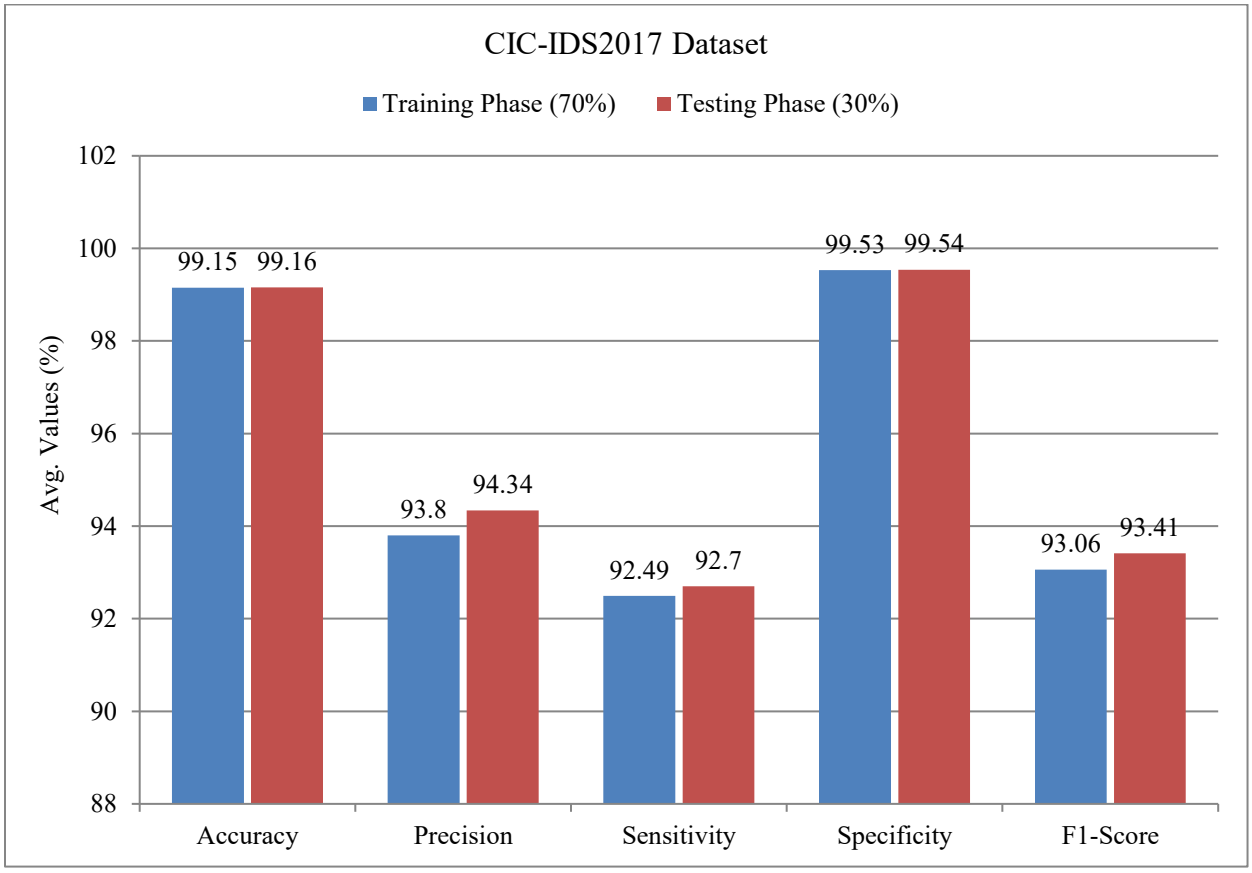


Fig. 4 Average of IIDC-DLMMOA approach on CIC-IDS2017 database

In Figure. 5, the training (TRNG) $accu_y$ and validation (VALID) $accu_y$ analysis of IIDC-DLMMOA approach on CIC-IDS2017 database is showed. The figure indicating that both $accu_y$ analysis exhibitions a growing tendency, which notified the competence of the IIDC-DLMMOA with optimal outcomes across several iterations.

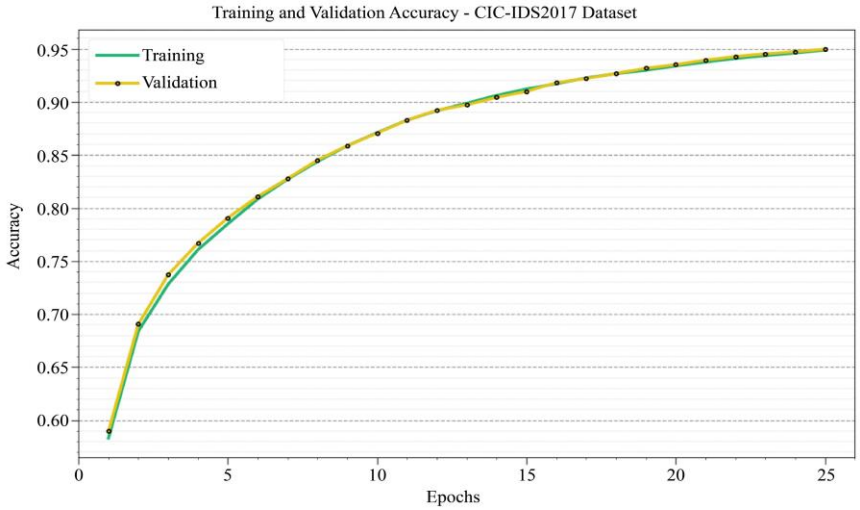


Fig. 5 $Accu_y$ Analysis of IIDC-DLMMOA methodology on CIC-IDS2017 database

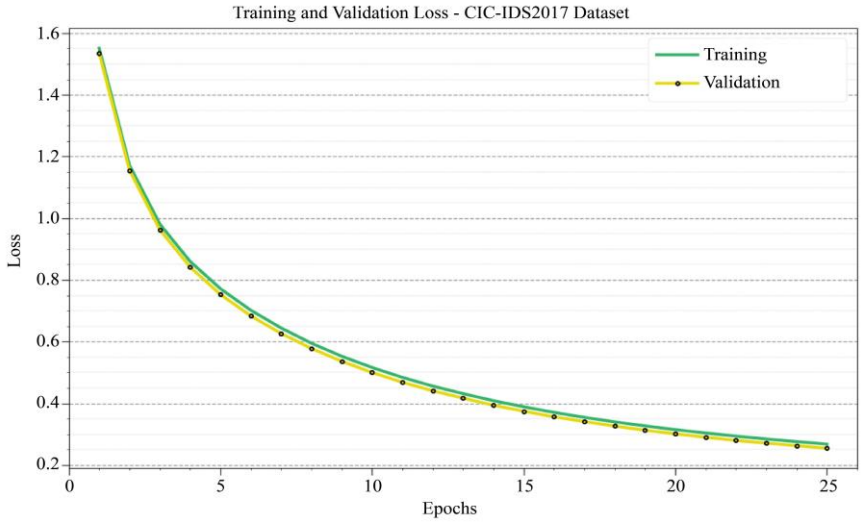


Fig. 6 Loss graph of IIDC-DLMMOA technique on CIC-IDS2017 database

Figure. 6 represents the training and validation loss curves of IIDC-DLMMOA framework on the CIC-IDS2017 dataset. Both loss values decrease over the training process, indicating that the model gradually reduces its prediction errors on the training and validation data.

Table 3. Comparative outcomes of IIDC-DLMMOA system on CIC-IDS2017 database

	Method	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$
C-IDS2017 Database	Hybrid ML	92.13	92.88	89.19	89.18
	1D-CNN	89.59	90.64	90.71	91.80
	DBN Method	93.94	90.52	91.27	97.35
	Adaptive boost	89.99	89.52	90.12	95.98
	Stacking Model	95.70	91.36	90.99	97.81
	Bagging Method	98.26	90.95	90.25	96.18
	XGBoost+RF	95.63	91.43	89.45	89.67
	IIDC-DLMMOA	99.16	94.34	92.70	99.54

Table 3 signifies the comparative study of IIDC-DLMMOA algorithm on CIC-IDS2017 database with recent methodologies. The table values specify that the IIDC-DLMMOA algorithm has obtained better performance with maximum $accu_y, prec_n$, $sens_y$, and $spec_y$ of 99.16%, 94.34%, 92.70%, and 99.54%, correspondingly. Meanwhile, the existing models such as Hybrid ML, 1D-CNN, DBN, Adaptive Boost, Stacking, Bagging, and XGBoost+RF have got worst performance.

As well, the proposed IIDC-DLMMOA algorithm examines under ToN-IoT database [22]. It holds 119957 instances under nine class as portrayed in Table 4. There are 42 attributes in total, but only 31 attributes were selected.

Table 4. Details of ToN-IoT database

	Class Labels	No. of Samples
ToN-IoT Database	"Normal"	78369
	"MiTM"	336
	"DoS"	5440
	"DDoS"	5987
	"Password"	6016
	"Injection"	5867
	"XSS"	5951
	"Ransomware"	5976
	"Backdoor"	6015
	Total Samples	119957

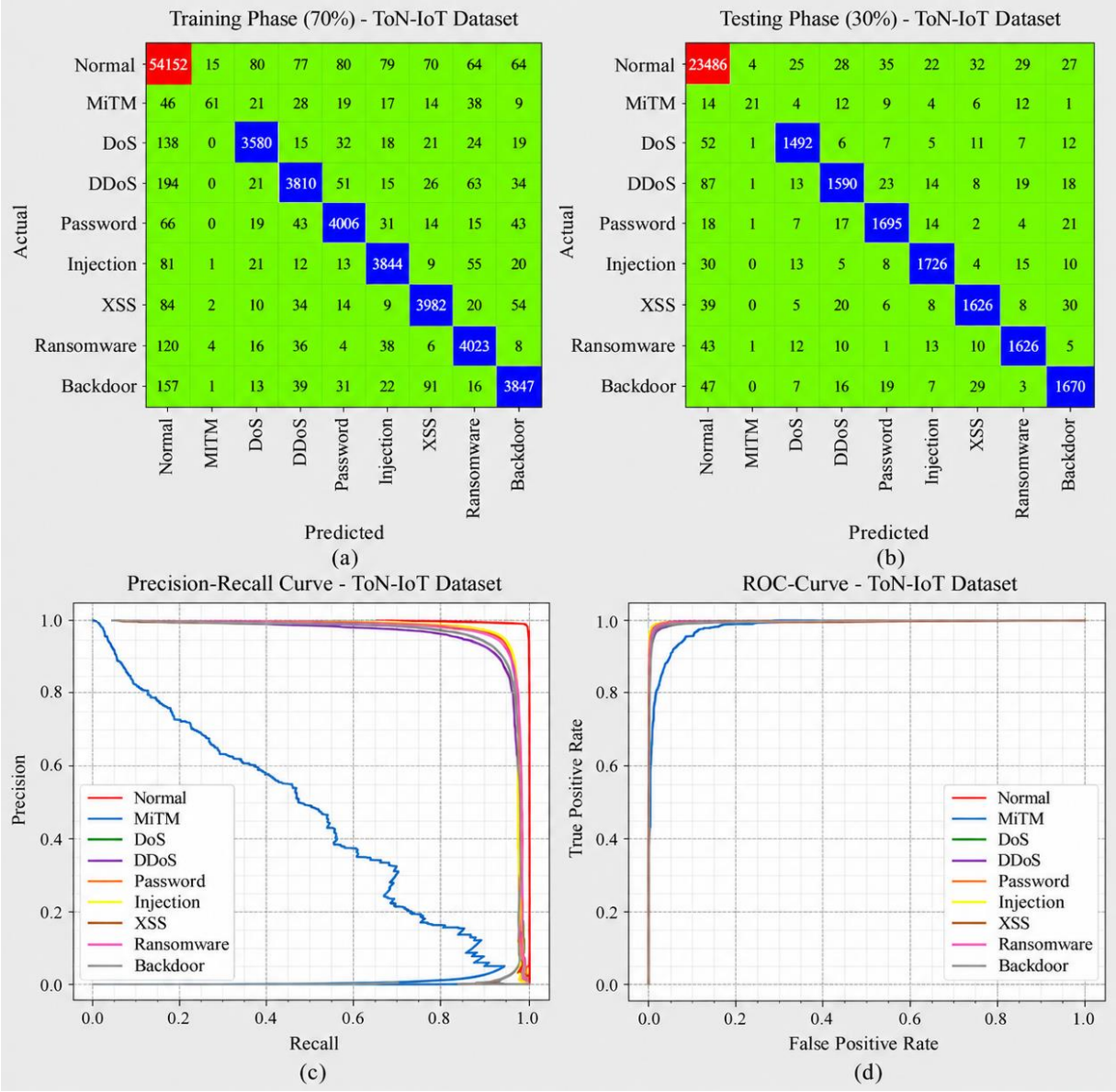


Fig. 7 ToN-IoT database (a-b) confusion matrices and (c-d) curves of PR and ROC

Figure. 7 presents the intrusion detection outcomes of the IIDC-DLMMOA method using the ToN-IoT dataset. Figures. 7a and 7b show the confusion matrices for the 70:30 data split, indicating the classification results for each class. Figure. 7c presents the PR curves, while Figure. 7d shows the ROC curves for the different class labels.

Table 5 presents the intrusion detection of IIDC-DLMMOA on ToN-IoT database. Based on 70% TRAPH, the IIDC-DLMMOA system gets average $accu_y$, $prec_n$, $sens_y$, $spec_y$, and $F1_{score}$ of 99.29%, 92.06%, 86.26%, 99.42%, and 87.80%, correspondingly.

Furthermore, based on 30% TESPH, the proposed IIDC-DLMMOA algorithm achieves average $accu_y$, $prec_n$, $sens_y$, $spec_y$, and $F1_{score}$ of 99.35%, 92.18%, 86.56%, 99.47%, and 88.11%, respectively.

Table 5. Intrusion detection of IIDC-DLMMOA technique on ToN-IoT database

Classes	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	$F1_{score}$
TRAPH (70%)					
Normal	98.31	98.39	99.03	96.97	98.71
MiTM	99.74	72.62	24.11	99.97	36.20
DoS	99.44	94.68	93.06	99.75	93.86
DDoS	99.18	93.06	90.41	99.64	91.72
Password	99.43	94.26	94.55	99.69	94.40
Injection	99.47	94.38	94.77	99.71	94.57
XSS	99.43	94.07	94.61	99.69	94.34
Ransomware	99.37	93.17	94.55	99.63	93.85
Backdoor	99.26	93.88	91.23	99.69	92.53
Average	99.29	92.06	86.26	99.42	87.80
TESPH (30%)					
Normal	98.52	98.61	99.15	97.32	98.88
MiTM	99.81	72.41	25.30	99.98	37.50
DoS	99.48	94.55	93.66	99.75	94.10
DDoS	99.17	93.31	89.68	99.67	91.46
Password	99.47	94.01	95.28	99.68	94.64
Injection	99.52	95.20	95.31	99.75	95.25
XSS	99.39	94.10	93.34	99.70	93.72
Ransomware	99.47	94.37	94.48	99.72	94.43
Backdoor	99.30	93.09	92.88	99.64	92.98
Average	99.35	92.18	86.56	99.47	88.11

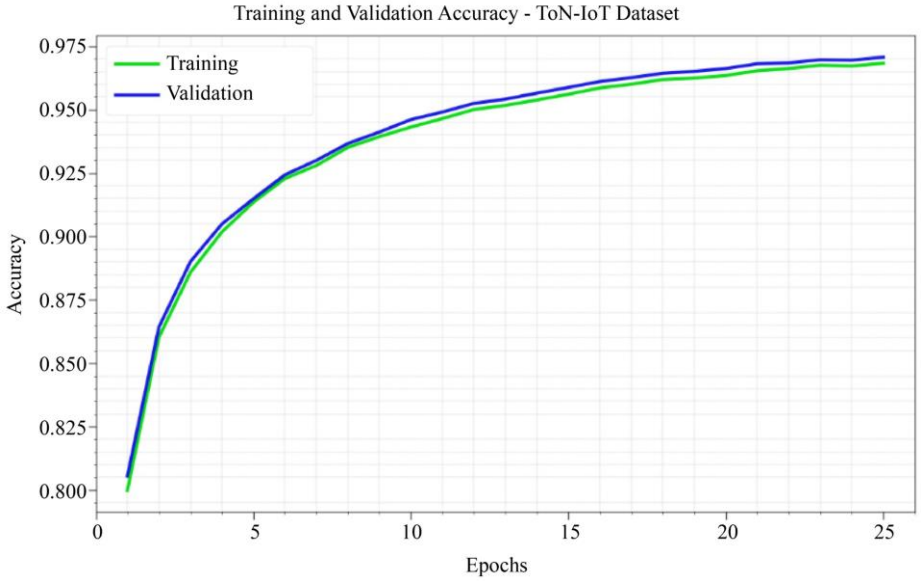


Fig. 8 $Accu_y$ curve of IIDC-DLMMOA using ToN-IoT database

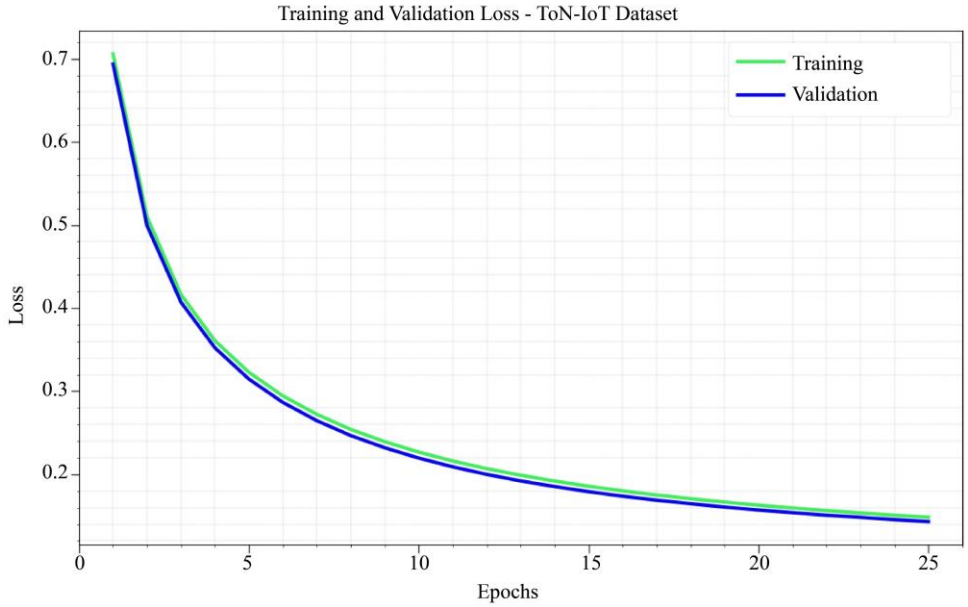


Fig. 9 Loss analysis of IIDC-DLMMOA using ToN-IoT database

In Figure. 8, the TRNG $accu_y$ and VALID $accu_y$ analysis of IIDC-DLMMOA algorithm using ToN-IoT database is shown. The outcome highlighting that both $accu_y$ values exhibitions a rising trend, which notified the capability of the IIDC-DLMMOA with higher outcomes across several iterations.

Figure. 9 shows the training and validation loss curves of IIDC-DLMMOA on the ToN-IoT dataset. Both curves decrease as training progresses, indicating that the model gradually reduces its errors on the training and validation data.

Figure. 10 signifies the comparative study of IIDC-DLMMOA methodology on ToN-IoT database with recent models [23-25]. The proposed IIDC-DLMMOA model has obtained better performance with maximum $accu_y, prec_n$, $sens_y$, and $spec_y$ of 99.35%, 92.18%, 86.56%, and 99.47%, correspondingly.

Meanwhile, the existing models such as LR, k-NN, NB, CNN-BiLSTM, CCNN-LSTM, CNN-GRU, and SVM have got worst performance under various metrics.

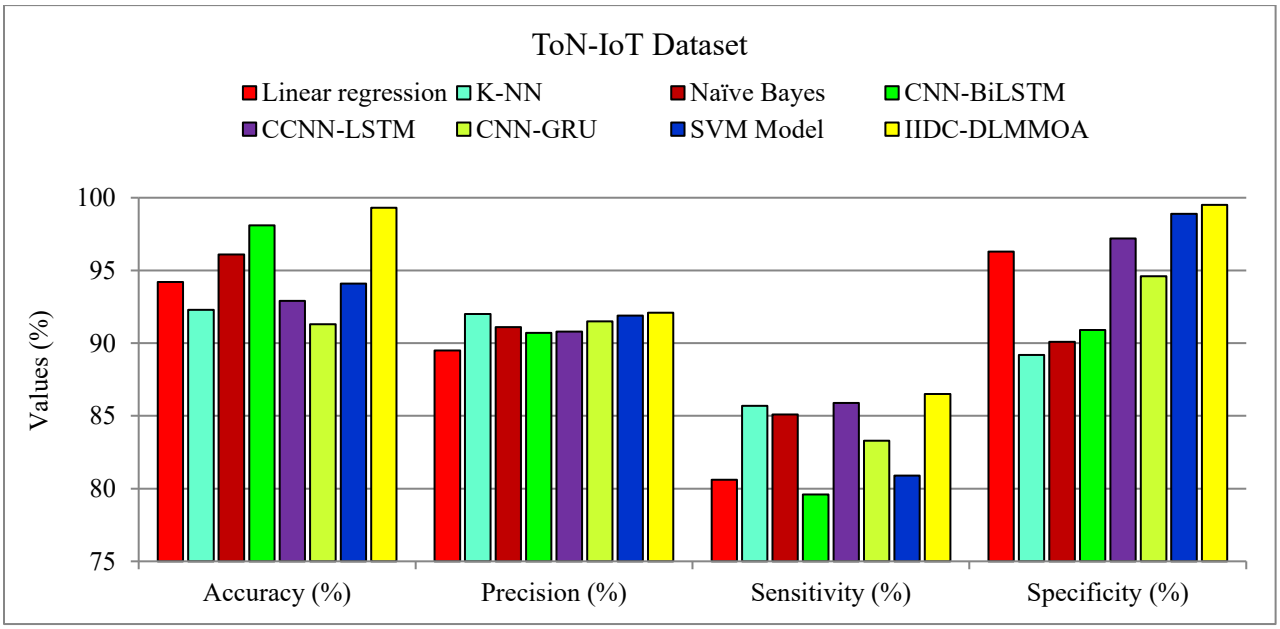


Fig. 10 Comparative analysis of IIDC-DLMMOA model using ToN-IoT database

5. Conclusion

In this manuscript, a novel IIDC-DLMMOA in VANET Environments has been developed. The main intention of IIDC-DLMMOA technique relies on developing an effective structure for intrusion detection in VANET communications. Following that, the FS process is executed by the HOA to select the most significant features from input data. For the classification process, the proposed IIDC-DLMMOA model designs a STA-LSTM system. At last, the hyperparameter tuning optimizes a classification model of STA-LSTM method through MOMSA by selecting the best parameter values. The developed IIDC-DLMMOA system is verified using the real-time benchmark dataset, and the stimulated outcomes are in comparison with other advanced techniques.

References

[1] Nourhene Ben Rabah, and Hanen Idoudi, *A Machine Learning Framework for Intrusion Detection in VANET Communications*, Emerging Trends in Cybersecurity Applications, Springer, pp. 209-227, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ammar Haydari, and Yasin Yilmaz, "RSU-based Online Intrusion Detection and Mitigation for VANET," *Sensors*, vol. 22, no. 19, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Fabio Gonçalves et al., "A Systematic Review on Intelligent Intrusion Detection Systems for VANETs," *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Dublin, Ireland, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] B. Karthiga et al., "Intelligent Intrusion Detection System for VANET using Machine Learning and Deep Learning Approaches," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Junwei Liang et al., "A Novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on Differences of Traffic Flow and Position," *Applied Soft Computing*, vol. 75, pp. 712-727, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Hind Bangui, Mouzhi Ge, and Barbora Buhnova, "A Hybrid Data-Driven Model for Intrusion Detection in VANET," *Procedia Computer Science*, vol. 184, pp. 516-523, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Fuad A. Ghaleb et al., "Misbehavior-aware On-demand Collaborative Intrusion Detection System using Distributed Ensemble Learning for VANET," *Electronics*, vol. 9, no. 9, pp. 1-17, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ila Naqvi, Alka Chaudhary, and Anil Kumar, "A Systematic Review of the Intrusion Detection Techniques in VANETS," *TEM Journal*, no. 2, pp. 900-907, 2022. [Google Scholar] [Publisher Link]

[9] Esraa Al-Ezaly, Ahmed Abo-Elfetoh, and Sara Elhish, "Pollution Reduction using Intelligent Warning Messages in VANET," *Journal of Intelligent Systems and Internet of Things*, vol. 3, no. 2, pp. 57-67, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Kusum Dalal, "Ensuring Secure Transmission in VANET: Optimal Clustering and Improved LSTM-Based Intrusion Detection," *International Journal of Communication Systems*, vol. 38, no. 4, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Fayaz Hassan et al., "A Hybrid Approach for Intrusion Detection in Vehicular Networks using Feature Selection and Dimensionality Reduction with Optimized Deep Learning," *PLOS One*, vol. 20, no. 2, pp. 1-18, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Gurjot Kaur, and Deepti Kakkar, "A Secure Lightweight Authentication Model with Interference Aware Routing and Attack Detection Approach in VANET," *Cluster Computing*, vol. 28, no. 2, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] Xiuzhen Chen et al., "Fast and Practical Intrusion Detection System based on Federated Learning for VANET," *Computers and Security*, vol. 142, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Aradhana Behura, Arun Kumar, and Puneet Kumar Jain, "A Multi-Objective Approach for Secure Cluster based Routing and Attack Classification in VANETs," *Peer-to-Peer Networking and Applications*, vol. 18, no. 3, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] Monika Arya et al., "Intruder Detection in VANET Data Streams using Federated Learning for Smart City Environments," *Electronics*, vol. 12, no. 4, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ghayth ALMahadin et al., "VANET Network Traffic Anomaly Detection using GRU-based Deep Learning Model," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4548-4555, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Fatma S. Alrayes et al., "Privacy-Preserving Approach for IoT Networks using Statistical Learning with Optimization Algorithm on High-Dimensional Big Data Environment," *Scientific Reports*, vol. 15, no. 1, pp. 1-27, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Ke Wu et al., "Low-Carbon Economic Optimization for Flexible DC Distribution Networks based on the Hiking Optimization Algorithm," *Energy Informatics*, vol. 8, no. 1, pp. 1-28, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ayub Bokani, Elaheh Yadegaridehkordi, and Salil S. Kanhere, "LSTM-H: A Hybrid Deep Learning Model for Accurate Livestock Movement Prediction in UAV-Based Monitoring Systems," *Drones*, vol. 9, no. 5, pp. 1-18, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] Rong Yang et al., "Multi-Objective Optimization of Parking Charging Strategy for Extended-Range Hybrid Electric Vehicle based on MOMSA," *World Electric Vehicle Journal*, vol. 16, no. 4, pp. 1-29, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] H.N. Chethan, Network Intrusion Dataset (CIC-IDS- 2017). [Online]. Available: https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset

[22] CIC-ToN-IoT Dataset. [Online]. Available: https://www.kaggle.com/datasets/dhoogla/cictoniot

[23] Ankit Manderna et al., "Vehicular Network Intrusion Detection using a Cascaded Deep Learning Approach with Multi-variant Metaheuristic," *Sensors*, vol. 23, no. 21, pp. 1-24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] Mostafa Mahmoud El-Gayar, Faheed A. Alrslani, and Shaker El-Sappagh, "Smart Collaborative Intrusion Detection System for Securing Vehicular Networks Using Ensemble Machine Learning Model," *Information*, vol. 15, no. 10, pp. 1-20, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Cynthia Anthony, Walid Elgenaidi, and Muzaffar Rao, "Intrusion Detection System for Autonomous Vehicles using Non-tree based Machine Learning Algorithms," *Electronics*, vol. 13, no. 5, pp. 1-19, 2024. [CrossRef] [Google Scholar] [Publisher Link]