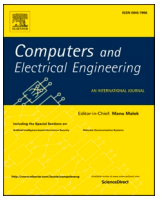
Computers and Electrical Engineering 108 (2023) 108704

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng



Sea turtle foraging algorithm with hybrid deep learning-based intrusion detection for the internet of drones environment☆

José Escorcia-Gutierrez [a,*], Margarita Gamarra [b], Esmeide Leal [c], Natasha Madera [d], Carlos Soto [e], Romany F. Mansour [f], Meshal Alharbi [g], Ahmed Alkhayyat [h], Deepak Gupta [i,j]

[a] Department of Computational Science and Electronics, Universidad de la Costa, CUC, Barranquilla, 080002, Colombia
[b] Department of System Engineering, Universidad del Norte, Puerto Colombia, 081007, Colombia
[c] Faculty of Engineering, Universidad Autónoma del Caribe, Barranquilla, 080020, Colombia
[d] Biomedical Engineering Program, Universidad Simón Bolívar, Barranquilla, 080002, Colombia
[e] Mechanical Engineering Program, Universidad Simón Bolívar, Barranquilla, 080002, Colombia
[f] Department of Mathematics, Faculty of Science, New Valley University, El-Kharja 72511, Egypt
[g] Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Alkharj 11942, Saudi Arabia
[h] College of Technical Engineering, The Islamic University, Najaf, Iraq
[i] Department of Computer Science & Engineering, Maharaja Agrasen Institute of Technology, Delhi, India
[j] UCRD, Chandigarh University, Gharuan, Mohali, Punjab, India

ARTICLE INFO

Edited by Guest Editor: Prof. Ali Kashif Bashir

Keywords:
Intrusion detection
Deep learning
Internet of drones
Metaheuristics
Feature selection

ABSTRACT

The Internet of Drones (IoD) allows for coordinated control of airspace for Unmanned Aerial Vehicles (UAVs), also known as drones. The decreasing costs of processors, sensors, and wireless connectivity have made it possible to use UAVs in many variety of military to civilian applications. While most applications utilizing the drones in the IoD have been real-time related, users are now interested in obtaining real-time services from drones that are tailored to a specific fly zone. This study develops a Sea Turtle Foraging Algorithm with Hybrid Deep Learning-based Intrusion Detection (STFA-HDLID) as a algorithm that recognizes and categorizes intrusions in the IoD environment. For this purpose, it is necessary to implement data pre-processing to standardize the input data via min-max normalization. Additionally, the feature selection process is also based on the STFA. Finally, a Deep Belief Network (DBN) with a Sparrow Search Optimization (SSO) algorithm is used for classification. A comprehensive experimental analysis is performed on a benchmark dataset to demonstrate the performance of the STFA-HDLID, which achieves maximum accuracy of 99.51% and 98.85% on the TON_IoT and UNSW-NB15 datasets, respectively, outperforming other techniques.

☆ This paper was recommended for publication by Associate Editor Prof. Ali Kashif Bashir

* Corresponding author.
E-mail addresses: jescorci56@cuc.edu.co (J. Escorcia-Gutierrez), mrgamarra@uninorte.edu.co (M. Gamarra), esleal@uac.edu.co (E. Leal), natasha.madera@unisimon.edu.co (N. Madera), carlos.soto@unisimon.edu.co (C. Soto), romanyf@sci.nvu.edu.eg (R.F. Mansour), Mg.alharbi@psau.edu.sa (M. Alharbi), ahmedalkhayyat85@iunajaf.edu.iq (A. Alkhayyat), deepakgupta@mait.ac.in (D. Gupta).

https://doi.org/10.1016/j.compeleceng.2023.108704
Received 14 October 2022; Received in revised form 22 March 2023; Accepted 24 March 2023
Available online 29 March 2023

1. Introduction

Unmanned Aerial vehicles (UAV), commonly referred to as drones, are increasingly being utilized for various applications, including environment monitoring, traffic surveillance, rescue operations, and disaster management [1]. With the Internet of Things (IoT) adoption, UAV networks are rapidly transforming into the Internet of Drones (IoD), which presents opportunities for exploring more complex drone applications. Drone, as a powerful tool, can provide advanced transmission and computational resources in 6 G and 5 G networks [2]. Nevertheless, due to limited resources on drones, Multi-access Edge Computing (MEC) is a powerful offloading technology that can be integrated with IoD networks for off-loading tasks at network edges [3]. Additionally, Blockchain (BC) technology is used to secure IoD networks. With the increasing amount of data captured by UAVs, quick processing will become neccesary. Therefore, Artificial Intelligence (AI) services can be installed on UAVs by utilizing advanced Deep Learning (DL) and Machine Learning (ML) systems [4].

Network security has recently become a significant research field, primarily advancing the Internet and communication methods. Various systems, such as Network Intrusion Detection Systems (NIDSs) and firewalls, are employed to secure assets and networks [5]. NIDSs are used to monitor the network traffic for suspicious and malicious behavior. The primary ideology behind IDS was proposed in 1980, and numerous IDS products were formulated to meet network security requirements [6]. However, in recent decades, massive transmission and network technology advancements have increased network size, the volume of data generated, and the number of applications. An IDS is a network monitoring software for suspicious activities or policy violations with related to cybercrime and generates a report to the managing system [7].

IDS can be referred to as network security. Similar to a firewall, it differs from a firewall in the way it looks for intrusions [8]. The firewall prevents external intrusions and limits access between networks to control intrusion. On the other hand, IDS will evaluates an intrusion that has already occurred and then sends an alarm signal. Many estimations have been established using ML. At the same time, this study utilizes DL, a branch of ML that attempts to model higher-level extractions in data through model structures with non-linear transformations [9]. Deep learning is selected because of its emphasis on computing methods for information representation. It can be applied in a way that it could exibits classification invariance concerning a wide range of distortions and transformations [10], enabling us to train a network with a more extensive set of observations and extract signals from it. Deep learning techniques employ more complex features in the higher layer and simple features in the lower layer [11,12].

This study presents the STFA-HDLID algorithm to recognize and categorize intrusions in the IoD environment. The STFA approach is utilized for the feature selection process, and a Deep Belief Network (DBN) with a Sparrow Search Optimization (SSO) algorithm is employed for classification. The SSO algorithm optimizes the hyperparameters of the DBN model. An extensive experimental analysis is conducted on a benchmark dataset to demonstrate the improved performance of the STFA-HDLID algorithm.

The rest of the paper is organized as follows. Section 2 presents a detailed literature review, while Section 3 describes the proposed model. Section 4 provides experimental validation, and Section 5 presents the concluding remarks.

2. Related works

Perumalla et al. [13] introduced an oppositional Aquila Optimizer-oriented feature selection (FS) with ML-assisted IDS (OAOFS-MLIDS) in the IoD network to establish secure access control through intrusion detection. The above-mentioned technique primarily pre-processes network data using minimal-maximal normalization and involves the OAOFS approach for selecting feature subsets to achieve this. Furthermore, the Coyote Optimization Algorithm (COA), combining with the XGBoost method is used to classify and recognize intrusions in the IoD network. In their recent research article, Praveena et al. [14] presented a Deep Reinforcement Learning (DRL) method optimized by the Black Widow Optimization (BWO) algorithm [15] for detecting intrusions in drone networks. The DRL approach incorporates an improved RL-oriented DBN for intrusions detection. The BWO algorithm was employed to optimize the parameters of the DRL method, resulting in enhancing the ID performance for drone networks.

In their study, Ramadan et al. [16] made significant progress in advancing FANET-ID approaches by introducing a realistic analytics structure that employs DL techniques to investigate FANET-ID threats. The structure is based on RNN and involves data collection from the network and big data analytics for Anomaly Detection (AD). The agent logs realistic FANET data for analysis. Similarly, Tan et al. [17] developed an ID technique based on DBN, which was optimized using the Particle Swarm Optimization (PSO) algorithm . They first stablished a DBN-based classification technique and then used PSO to determine the optimal number of hidden layer nodes for the DBN infrastructure.

Whelan et al. [18] have developed a new drone intrusion detection technique using one-class classifiers. Principal Component Analysis (PCA) can be used to reduce the dimensionality of sensor logs, and one-class classifier methods were generated for each sensor. The chosen count of one-class classifiers includes Local Outlier Factor, One-Class SVM, and AE-NN. Ouiazzane et al. [19] have proposed a method related to Muli-Agent system and ML approaches for detecting DoS cyber-attacks that target drone networks. The devised method is autonomous and characterized by its high performance. It recognizes unknown and known DoS attacks in drone networks with low false-positives, high accuracy, and false-negatives rates. Unlu et al. [20] presented an independent mechanism for detecting and tracking UAVs that utilizes a lower-angle camera and a static wide-angle camera on a rotating turret. To efficiently use time and memory, the authors have developed an integrated multi-frame DL detection approach, in which the frame from the zoomed camera on the turret is overlaid on the wide-angle static frame the cameras.

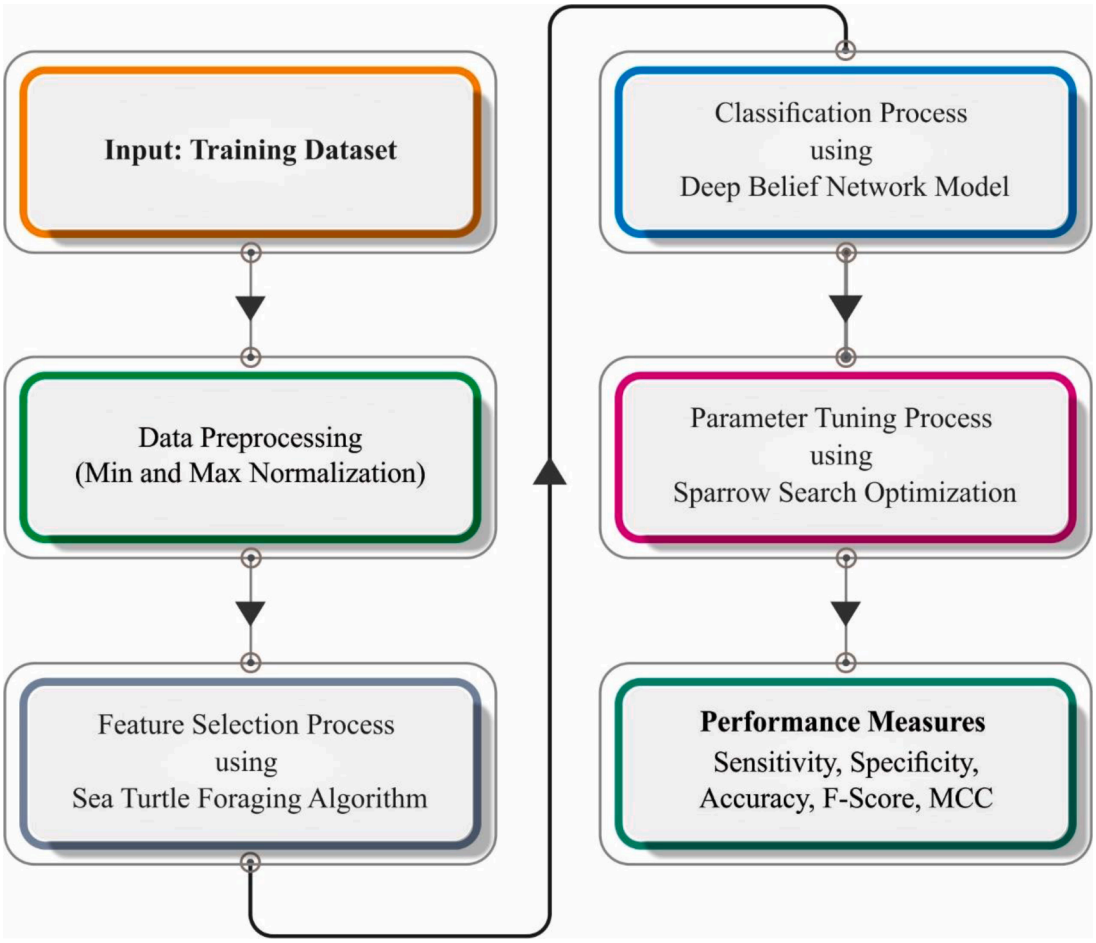


Fig. 1. Workflow of the STFA-HDLID approach.

3. The proposed model

This study introduces a new STFA-HDLID algorithm for intrusion detection and classification in the IoD environment. The STFA-HDLID algorithm first undergoes data pre-processing at the initial stage to standardize the input data via min-max normalization. Next, the STFA approach is utilized for feature selection process. Finally, the SSO with the DBN model is used for the classification process. Fig. 1 demonstrates the working flow of the STFA-HDLID system.

3.1. Feature selection using STFA technique

This study uses the STFA approach for the feature selection process. It has been identified that sea turtles are able to detect Dimethyl Sulfide (DMS) and use it to locate regions with highest concentration of prey [21]. Sea turtles travel toward food sources that release the most potent odor, using active and passive methods aided by ocean currents. The stages of the STFA technique are explained in detail below:

Step 1. Initialize the position of N sea turtles arbitrarily in a D dimensional searching space.

$$T_i(0) = \left[t_i^1,\ t_i^2,\ \ldots,\ t_i^D\right] \tag{1}$$

whereas $i = 1$ to N.

Step 2. The velocity of all the turtles, $V_i(0)$, is arbitrarily initialized as $\xi^{v_i^1, v_i^2}, \ldots, v_i^D]$. The velocity of each turtles, v_i, is constrained to within $[v\_\min^d, v\_\max^d]$ for all dimension d:

$$v\_\max^d = \lambda\left[XUB^d - XLB^d\right] \tag{2}$$

$$v\_\min^d = -v\_\max^d \tag{3}$$

XUB^d and XLB^d represent the upper and lower bounds, respectively, of d^{th} dimensional of searching spaces. λ is a real number between zero and one.

Step 3. *M* food sources are arbitrarily created and denoted as Eq. (4) for $j = 1$ to M. The fitness value of each food source is then defined.

$$K_j = \left[k_j^1,\ k_j^2,\ \ldots,\ k_j^D\right] \tag{4}$$

Step 4. The fitness of each turtle is estimated, and the most robust turtle is defined as:

$$I = \text{argmax}_i[f(T(t))] \tag{5}$$

here, $f(T(t))$ denotes the fitness of turtle i at time t.

Step 5. Compute the ocean's present velocity at the turtles' positions, $VC_i = [vc_i^1,\ vc_i^2,\ \ldots,\ vc_i^D]$:

$$VC_i(t) = \gamma[T_I(t) - T(t)] \tag{6}$$

Step 6. The velocity of all the sea turtles is updated using the Eq. (7):

$$\begin{aligned} V_i(t+1) &= V_i(t) + VC(t) \\ &+ \left[\frac{f(T_i(t)) - f(T_i(t-1))}{f(T_i(t-1))}\right][T_i(t) - T_i(t-1)] \end{aligned} \tag{7}$$

whereas $T_i(t)$ denotes the location of turtles i at time t and $f(T_i(t))$ represents the fitness of turtle i at time t.

Step 7. Compute the strength of DMS odor in the food source j which can be sensed by turtle i, $C_{ij}(t)$ by relating the turtles' fitness with the fitness of food sources. If the turtle's fitness is superior to that of the food source, the strength of odors in that food source is obtained as zero. Conversely, when the turtle's fitness is lesser compared to the food sources, the strength of odors in that food source is defined as follows:

$$C_{ij}(t) = \frac{f(K_j)}{\sum_{q=1}^{M} f(K)} e^{-\left[\frac{d_{ij}^2}{2\sigma^2(t)}\right]} \tag{8}$$

Here, $f(K_j)$ represents the fitness of food sources j. d_{ij} implies the distance between turtle i and food source j, and σ(t) controls how far the DMS odor spreads; it reduces exponentially with time:

$$\sigma(t) = \sigma_0 e^{-\left[\frac{t}{T}\right]} \tag{9}$$

Step 8. Recognize the optimum food source for turtle i. An optimum food source has the maximum value of $C(t)$ among every food source.

$$J = \text{argmax}\left[C_{ij}\right] \tag{10}$$

Step 9. Upgrade the place of all the turtles.

$$T_i(t+1) = T_i(t) + \eta V_i(t+1) + C_{iJ}(t)[K_J - T(t)] \tag{11}$$

Step10. : Verify the end condition. When every one of them is met, this technique ends. If not, two conditions are verified: i) When the value of t/T is an integer, return to step 3; ii) If the value of t/T is not an integer, go back to step 4.

The fitness function (FF) considers the count of selected features and the classifier's accuracy. It aims to minimize the set size of selected features and maximize classification accuracy. Hence, the following FF is used to evaluate individual solutions:

$$Fitness = \alpha * \ ErrorRate + (1-\alpha) * \frac{\#SF}{\#All\_F} \tag{12}$$

Where ErrorRate indicates the classification error rate using the selected feature. It can be evaluated as the percentage of improper classifications to the total number of classifications generated within the range of [0, 1]. (ErrorRate denotes complement of classification accuracy), $\#SF$ points the number of selected attributes, and $\#All\_F$ represents the total number of features in the original data. α is used to control the significance of subset length and classification quality.

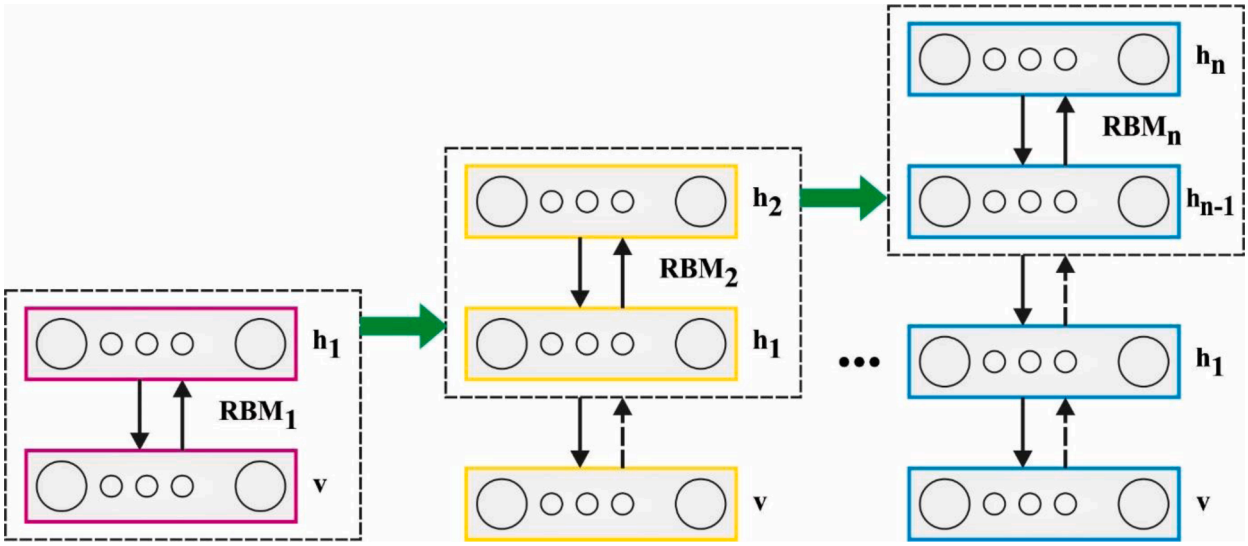


Fig. 2. DBN architecture.

Table 1
Details on TON_IoT Dataset.

Label	Attack Type	No. of Records
C-1	Backdoor	1000
C-2	DDoS	1000
C-3	DoS	1000
C-4	Injection	1000
C-5	MITM	1000
C-6	Password	1000
C-7	Ransomware	1000
C-8	Scanning	1000
C-9	XSS	1000
C-10	Benign	1000
Total Number of Attacks		**10,000**

3.2. Data classification using DBN model

This study employs the DBN model for intrusion detection and classification. The DBN is an efficient DL technique that comprises several RBMs for classifying datasets [22]. The learned activation unit of the initial RBM serves as the input for subsequent RBMs in the stack. Furthermore, the DBN is an undirected graphical method in which the visible parameter is connected to a hidden unit via undirected weight. Nevertheless, the there is no connection between visible and hidden parameters. Fig. 2 illustrates the framework of the DBN technique. The energy functions ($E(m, n, \theta)$), likelihood distribution p_d, visible parameter (m), and hidden unit (n) are arithmetically formulated as follows:

$$-logp_d(m,n)\alpha E(m,n,\theta) = -\sum_{i=1}^{|V|}\sum_{j=1}^{|Q|} w_{ij}m_i n_j - \sum_{i=1}^{|V|} b_i m_i - \sum_{j=1}^{|Q|} a_j n_j \tag{13}$$

Whereas $\theta = (w, b, a)$ denotes the parameter set, b_i and a_j represent bias, w_{ij} signifies the symmetric weights among the visible parameters (m), and α characterizes the learning rate. In the DBN, the number of hidden and visible layers is denoted by $|Q|$ and $|V|$. The conditional likelihood distribution of hidden units (n) and visible parameters (m) is determined as follows:

$$p_d\left(n_j \middle| m, \theta\right) = sigm\sum_{i=1}^{|V|} w_{ij}m_i + a_j \tag{14}$$

$$p_d(m_i|n,\theta) = sigm\sum_{j=1}^{|Q|} w_{ij}n_i + b_j \tag{15}$$

Here, $sigm\ (M) = \left(\frac{1}{1+e^{-m}}\right)$ characterizes the sigmoid function, and the parameter θ signifies learned exploiting contrastive divergence. In the DBN classification, the parameter θ is obtained by applying RBM as follows:

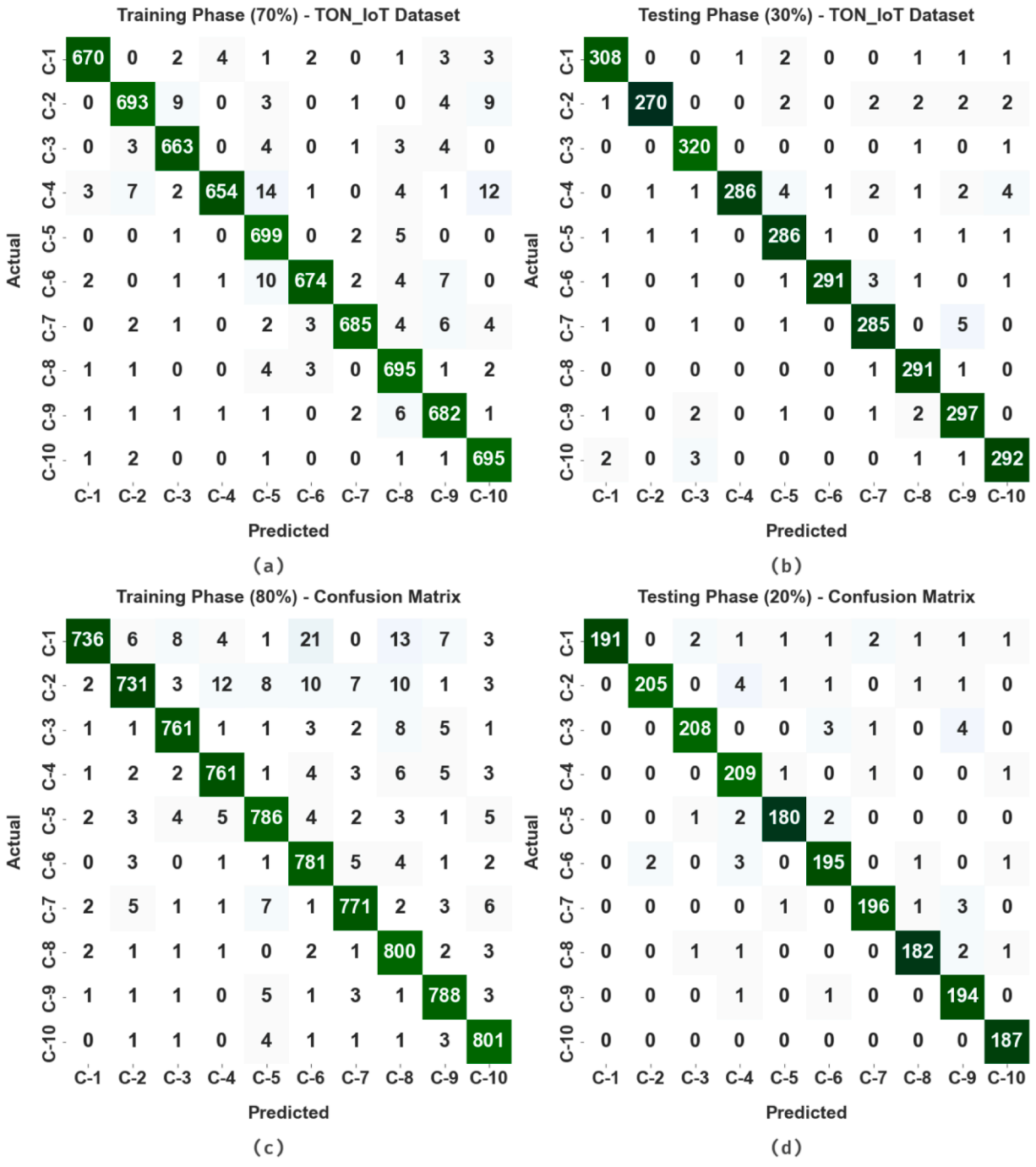


Fig. 3. Confusion matrices of STFA-HDLID approach under TON_IoT dataset: (a) 70% of TR dataset, (b) 30% of TS dataset, (c) 80% of TR dataset, and (d) 20% of TS dataset.

Table 2
Result analysis of STFA—HDLID algorithm with 70:30 of TR and TS data under the TON_IoT dataset.

Labels	Accuracy	Sensitivity	Specificity	F-Score	MCC
Training Phase (70%)					
Backdoor	99.66	97.67	99.87	98.24	98.05
DDoS	99.40	96.38	99.75	97.06	96.73
DoS	99.54	97.79	99.73	97.64	97.39
Injection	99.29	93.70	99.90	96.32	95.97
MITM	99.31	98.87	99.36	96.68	96.33
Password	99.49	96.15	99.86	97.40	97.12
Ransomware	99.57	96.89	99.87	97.86	97.63
Scanning	99.43	98.30	99.56	97.20	96.89
XSS	99.41	97.99	99.57	97.08	96.76
Benign	99.47	99.14	99.51	97.41	97.13
Average	**99.46**	**97.29**	**99.70**	**97.29**	**97.00**
Testing Phase (30%)					
Backdoor	99.57	98.09	99.74	97.93	97.69
DDoS	99.57	96.09	99.93	97.65	97.43
DoS	99.63	99.38	99.66	98.31	98.11
Injection	99.43	94.70	99.96	97.11	96.84
MITM	99.40	97.61	99.59	96.95	96.62
Password	99.67	97.32	99.93	98.31	98.13
Ransomware	99.43	97.27	99.67	97.10	96.79
Scanning	99.60	99.32	99.63	97.98	97.77
XSS	99.33	97.70	99.52	96.74	96.38
Benign	99.43	97.66	99.63	97.17	96.86
Average	**99.51**	**97.51**	**99.73**	**97.53**	**97.26**

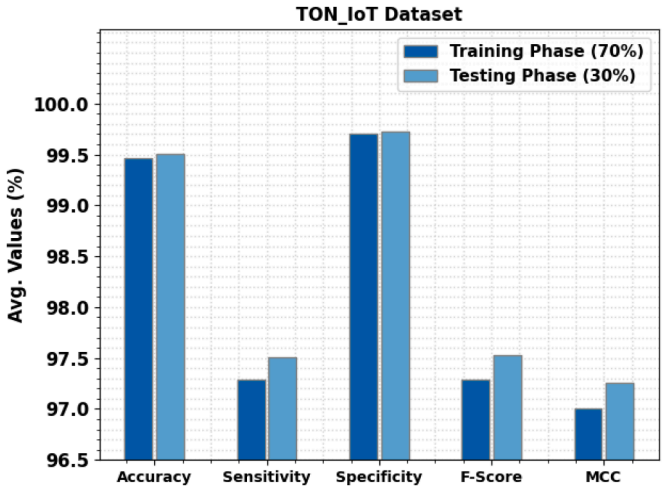


Fig. 4. Average analysis of STFA-HDLID approach with 70:30 of TR and TS data under the TON_IoT dataset.

$$p_d(m) = \sum_n p_d(n|\theta) p_d(m|n,\theta) \tag{16}$$

The value of $p_d(m|n,\theta)$ is retained, describing θ from RBM; later, $p_d(n|\theta)$ is interchanged employing successive RBM that treats the previous RBM hidden layers as a visible number.

3.3. Parameter tuning using SSO algorithm

At the final stage, the SSO algorithm adjusts the hyperparameters related to the DBN method, drawing inspiration from sparrows' anti-predation and foraging behaviors [23]. The foraging behavior of the sparrow corresponds to the roles of followers and discoverers. In each iteration of the global search food, the sparrows with the best position are carefully chosen as discoverers who provide foraging areas and direction for every follower. The rest of the sparrows are followers who compete for food by following the discoverers. The anti-predation behaviors of the sparrows correspond to the early warning and reconnaissance mechanisms. A few sparrows conduct reconnaissance and provide earlier warnings. They give up food and fly to a new position if danger is found. The following matrix represents the sparrow population (n sparrows):

Table 3
Result analysis of STFA-HDLID algorithm with 70:30 of TR and TS data under the TON_IoT dataset.

Labels	Accuracy	Sensitivity	Specificity	F-Score	MCC
Training Phase (80%)					
Backdoor	99.08	92.12	99.85	95.21	94.77
DDoS	99.01	92.88	99.68	94.87	94.35
DoS	99.45	97.07	99.71	97.19	96.89
Injection	99.35	96.57	99.65	96.70	96.34
MITM	99.29	96.44	99.61	96.50	96.10
Password	99.20	97.87	99.35	96.06	95.64
Ransomware	99.35	96.50	99.67	96.74	96.38
Scanning	99.24	98.40	99.33	96.33	95.93
XSS	99.45	98.01	99.61	97.28	96.98
Benign	99.49	98.52	99.60	97.50	97.23
Average	**99.29**	**96.44**	**99.61**	**96.44**	**96.06**
Testing Phase (20%)					
Backdoor	99.50	95.02	100.00	97.45	97.21
DDoS	99.50	96.24	99.89	97.62	97.35
DoS	99.40	96.30	99.78	97.20	96.87
Injection	99.25	98.58	99.33	96.54	96.14
MITM	99.55	97.30	99.78	97.56	97.31
Password	99.25	96.53	99.56	96.30	95.88
Ransomware	99.55	97.51	99.78	97.76	97.51
Scanning	99.55	97.33	99.78	97.59	97.34
XSS	99.35	98.98	99.39	96.76	96.43
Benign	99.80	100.00	99.78	98.94	98.84
Average	**99.47**	**97.38**	**99.71**	**97.37**	**97.09**

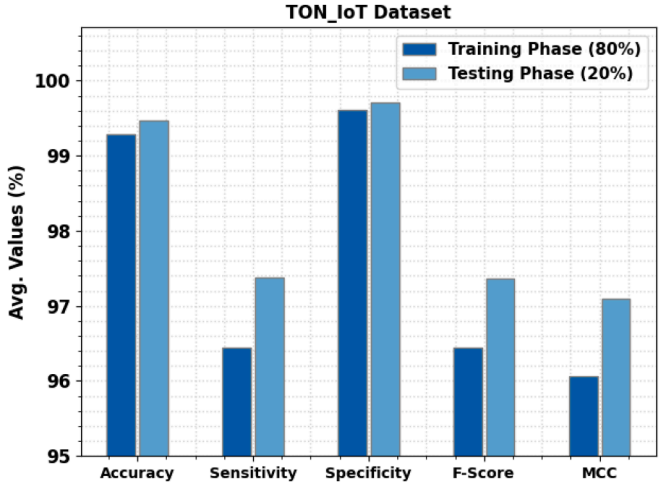


Fig. 5. Average analysis of STFA-HDLID approach with 80:20 of TR and TS data under the TON_IoT dataset.

$$X = \begin{bmatrix} X_1^1 & X_1^2 & \cdots & X_1^d \\ X_2^1 & X_2^2 & \cdots & X_2^d \\ & & \vdots & \\ X_n^1 & X_n^2 & \cdots & X_n^d \end{bmatrix} \tag{17}$$

In Eq. (17), *n*indicates the total number of sparrows in the population, and *d* represents the dimension that needs improvement. The fitness of each sparrow in the population is calculated by Eq. (18):

$$X = \begin{bmatrix} f([X_1^1 & X_1^2 & \cdots & X_1^d]) \\ f([X_2^1 & X_2^2 & \cdots & X_2^d]) \\ & & \vdots & \\ f([X_n^1 & X_n^2 & \cdots & X_n^d]) \end{bmatrix} \tag{18}$$

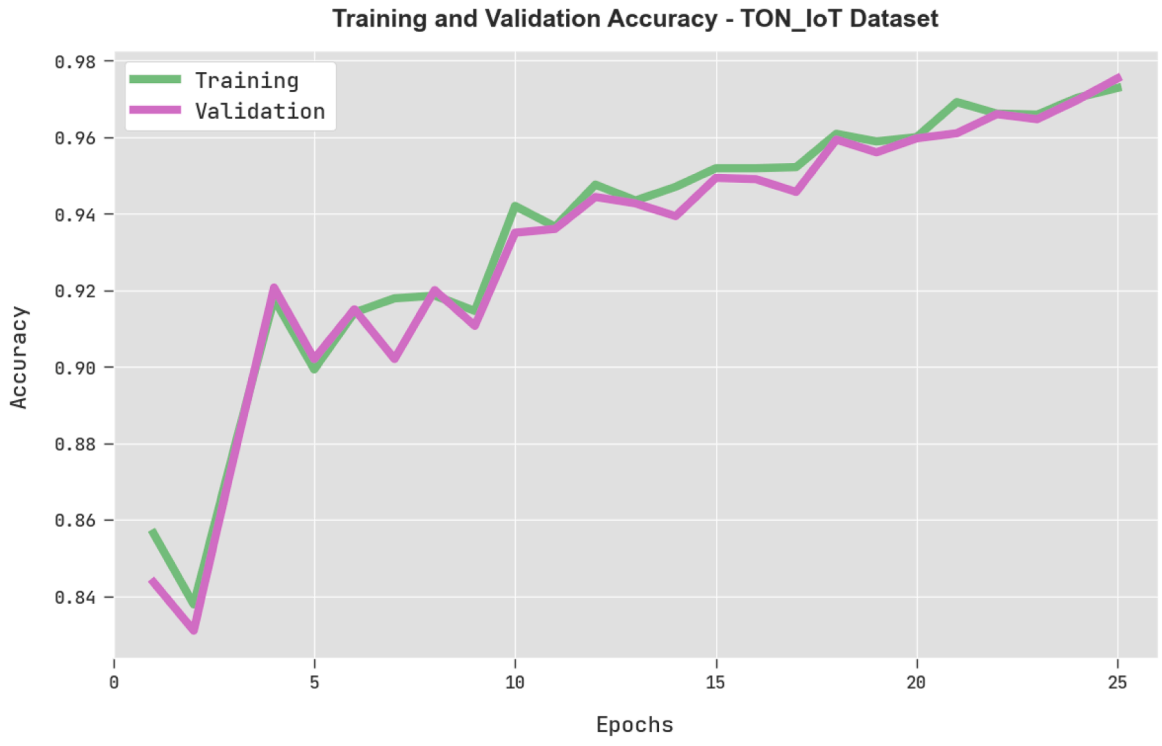


Fig. 6. TRA and VLA analysis of STFA-HDLID approach under TON_IoT dataset.

Fig. 7. TRL and VLL analysis of STFA-HDLID approach under TON_IoT dataset.

Table 4
Details on UNSW-NB15 dataset.

Label	Class	No. of Samples
C-1	Worms	174
C-2	Shell Code	1511
C-3	Reconnaissance	13,987
C-4	Normal	93,000
C-5	Generic	58,871
C-6	Fuzzers	24,246
C-7	Expoits	44,525
C-8	DoS	16,353
C-9	Backdoor	2329
C-10	Analysis	2677
Total Number of Samples		**257,673**

Where X represents the fitness of various discoverers, the sparrow with the best fitness values is the first to achieve food, leading the whole population as discoverers. The location is updated as follows:

$$X_{i,j}^{t+1=}\begin{cases} x_{i,j}^{t}\cdot exp\left(\dfrac{-i}{\alpha\cdot iter_{\max}}\right)' R_2 < S_T \\ x_{i,j}^{t}+Q\cdot L,\ R_2 \geq S_T \end{cases} \tag{19}$$

In Eq. (19), t refers to the number of existing iterations; $X_{i,j}^{t+1}$ indicates the *j-th* parameter location of the *i-th* individual in the $t+1$ iterations of the population.$iter_{\max}$ shows the maximal number of iterations. α indicates a random number uniformly distributed within [0,1]. Q denotes a uniform distribution random number; L indicates a 1 × d matrix with every component being 1. S_T represents the alert threshold between [0.5, 1], and R_2 indicates that the warning value ranges from zero to one. If $R_2 \geq S_T$, the warning is generated, and the sparrow has discovered the predator. Now, every sparrow leaves the warning zone. If $R_2 < S_T$ implies no predator fly closer, and the discoverers continue exploring in a large area. The location of followers is updated using Eq. (20):

$$X_{i,j}^{t+1=}\begin{cases} Q\cdot\ \exp\left(\dfrac{x_{worst}^{t}-x_{i,j}^{t}}{i^2}\right)' i > n\Big/2 \\ x_{p}^{t+1}+\left|X_{i,j}^{t}-X_{p}^{t+1}\right|\cdot A^{+}\cdot L,\ i \leq n\Big/2 \end{cases} \tag{20}$$

The expression, X_{worst}^{t} indicates the worst location of the existing population, while χ_p^{t+1} shows the better location of the existing population. $A^{+}=A^{T}(AA^{T})^{-1}$, where A is a 1 × d matrix, and each component in the row vector is randomly assigned 1 or − 1. n represents the size of the sparrow population, and some sparrows give alerts when the population is foraging. When a natural predator approaches, the follower and discoverer will give up the food and fly to other positions. SD (usually 10% to 20%) sparrows are arbitrarily selected from all generations in the population to provide an earlier warning:

$$X_{i,j}^{t+1}=\begin{cases} X_{best}^{t}+\beta.\left|X_{i,j}^{t}-X_{best}^{t}\right|, & f_i > f_g \\ X_{i,j}^{t}+K.\left(\dfrac{X_{i,j}^{t}-X_{worst}^{t}}{(f_i > f_w)}\right), & f_i = f_g \end{cases} \tag{21}$$

In Eq. (21), X_{best}^{t} indicates the present global optimal location. β denotes a random number under the uniform distribution, and K represents a random number uniformly distributed within [1,1]. f_i, f_g, and f_w represent the fitness value, globally optimal and global worst fitness values of the present population. The value of ε is set to avoid divide-by-zero errors. The condition $f_i > f_g$ means that the sparrow was at the edge of the population and was attacked by the predator, while $f_i = f_g$ means that the sparrow is in the center of the population and realizes the threat of being attacked by the predator and should approach other sparrows.

The SSO approach improves FF to achieve higher classifier efficiency by determining a positive integer that signifies the best performance of candidate results. This study's minimized classifier error rate is represented as FF, as provided in Eq. (22).

$$\begin{aligned} &fitness(x_i)=ClassifierErrorRate(x_i) \\ &=\frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples}*100 \end{aligned} \tag{22}$$

4. Results and discussion

The proposed model was simulated using Python 3.6.5 tool on a PC with an i5–8600k processor, GeForce 1050Ti 4GB graphics card, 16GB RAM, 250GB SSD, and 1 TB HDD. The parameter settings were: learning rate: 0.01, dropout: 0.5, batch size: 5, epoch count: 50, and activation function: ReLU. This section assesses the intrusion detection performance of the STFA-HDLID algorithm on two benchmark datasets: the TON_IoT dataset and the UNSW-NB15 dataset. The TON_IoT dataset comprises 10,000 samples with ten class

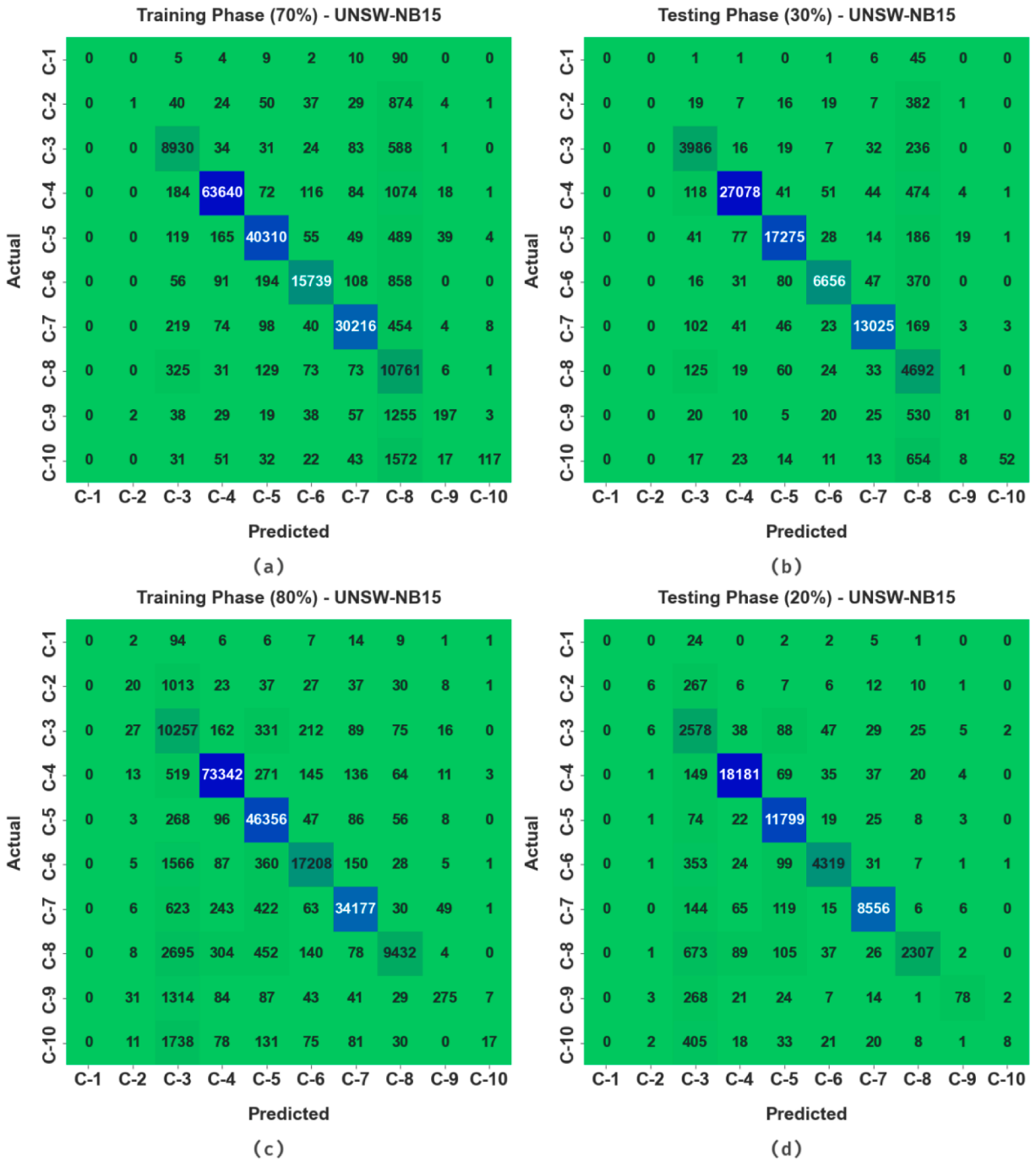


Fig. 8. Confusion matrices of STFA-HDLID approach under UNSW-NB15 dataset (a) 70% of TR dataset, (b) 30% of TS dataset, (c) 80% of TR dataset, and (d) 20% of TS dataset.

labels (as shown in Table 1) considering heterogeneous data sources collected from IoT and Industrial IoT (IIoT) sensor Telemetry datasets. It is considered the new generations of Industry 4.0/IoT and Industrial IoT (IIoT) datasets, designed to evaluate the fidelity and efficiency of cybersecurity applications based on AI models. The raw network packets of the UNSW-NB 15 dataset were created by the IXIA PerfectStorm tool in the Cyber Range Lab of UNSW Canberra to generate a hybrid of real modern normal activities and synthetic recent attack behaviors. The tcpdump captured 100GB of raw traffic (e.g., Pcap files).

The confusion matrices generated by the STFA-HDLID algorithm for the TON_IoT dataset are shown in Fig. 3. Indicating that the method has proficiently recognized ten class labels under all aspects.

Table 2 and Fig. 4 present the results of the STFA-HDLID algorithm on 70% of the TR and 30% of the TS dataset in the TON_IoT

Table 5
Result analysis of STFA—HDLID approach with 70:30 TR and TS data under the UNSW-NB15 dataset.

Labels	Accuracy	Sensitivity	Specificity	F-Score	MCC
Training Phase (70%)					
Backdoor	99.93	00.00	100.00	00.00	00.00
DDoS	99.41	00.09	100.00	00.19	01.75
DoS	99.01	92.15	99.40	90.95	90.43
Injection	98.86	97.62	99.56	98.41	97.53
MITM	99.14	97.77	99.54	98.11	97.55
Password	99.05	92.33	99.75	94.84	94.36
Ransomware	99.21	97.12	99.64	97.68	97.21
Scanning	95.62	94.40	95.71	73.17	73.12
XSS	99.15	12.03	99.95	20.48	28.56
Benign	99.01	06.21	99.99	11.58	23.04
Average	**98.84**	**58.97**	**99.35**	**58.54**	**60.36**
Testing Phase (30%)					
Backdoor	99.93	00.00	100.00	00.00	00.00
DDoS	99.42	00.00	100.00	00.00	00.00
DoS	99.01	92.78	99.37	91.20	90.69
Injection	98.76	97.36	99.55	98.26	97.31
MITM	99.16	97.93	99.53	98.16	97.62
Password	99.06	92.44	99.74	94.81	94.33
Ransomware	99.21	97.11	99.65	97.72	97.25
Scanning	95.72	94.71	95.79	73.94	73.85
XSS	99.16	11.72	99.95	20.05	28.27
Benign	99.04	06.57	99.99	12.25	24.33
Average	**98.85**	**59.06**	**99.36**	**58.64**	**60.36**

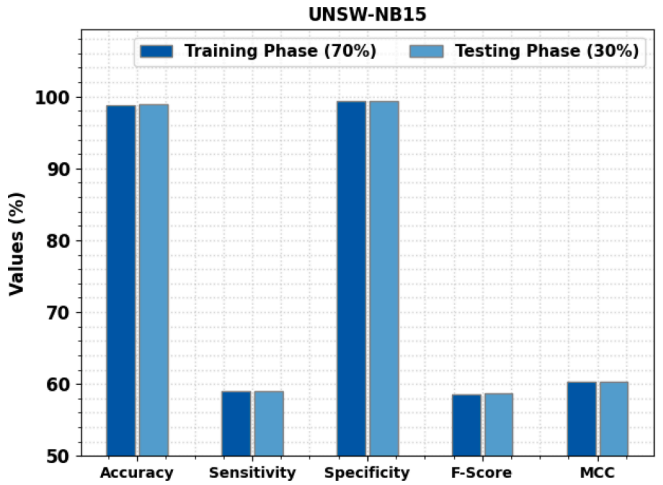


Fig. 9. Average analysis of STFA-HDLID approach with 70:30 of TR and TS data under UNSW-NB15 dataset.

dataset. The obtained outcomes demonstrate an enhanced performance in both cases. For instance, with 70% of the TR dataset, an average $accu_y$, $sens_y$, $spec_y$, F_{score},and $MCC$of 99.46%, 97.29%, 99.70%, 97.29%, and 97.00%, respectively, were achieved. Similarly, with 30% of the TS dataset, an average $accu_y$, $sens_y$, $spec_y$, F_{score},and $MCC$of 99.51%, 97.51%, 99.73%, 97.53%, and 97.26%, correspondingly.

Table 3 and Fig. 5 present the results of the STFA-HDLID algorithm on 80% of the TR and 20% of the TS dataset on the TON_IoT dataset. The outcomes indicate an improved performance in both cases. For example, with 80% of the TR dataset, an average $accu_y$, $sens_y$, $spec_y$, F_{score},and $MCC$of 99.29%, 96.44%, 99.61%, 96.44%, and 96.06%, respectively, were performed. Meanwhile, with 20% of the TS dataset, an average $accu_y$, $sens_y$, $spec_y$, F_{score},and $MCC$of 99.47%, 97.38%, 99.71%, 97.37%, and 97.09%, correspondingly.

Fig. 6 displays the Training Accuracy (TRA) and Validation Accuracy (VLA) achieved by the STFA-HDLID approach under the TON_IoT dataset. The experimental result indicates that the algorithm achieved maximum values of TRA and VLA, with VLA being greater than TRA.

Fig. 7 shows the Training Loss (TRL) and Validation Loss (VLL) obtained by the STFA-HDLID algorithm in the TON_IoT dataset. The experimental result demonstrates that the algorithm exhibited minimal TRL and VLL, with VLL being lesser than TRL.

Table 4 shows that the UNSW-NB15 dataset contains 257,673 samples with ten class labels. Fig 8. Displays the confusion matrices generated by the STFA-HDLID algorithm on the UNSW-NB15 dataset, indicating that the approach has effectively recognized all ten

Table 6
Result analysis of STFA-HDLID approach with 70:30 of TR and TS data under UNSW-NB15 dataset.

Labels	Accuracy	Sensitivity	Specificity	F-Score	MCC
Training Phase (80%)					
Backdoor	99.93	00.00	100.00	00.00	00.00
DDoS	99.38	01.67	99.95	03.03	04.98
DoS	94.79	91.83	94.96	65.63	66.25
Injection	98.91	98.44	99.18	98.49	97.64
MITM	98.71	98.80	98.68	97.21	96.39
Password	98.56	88.66	99.59	92.08	91.37
Ransomware	98.96	95.97	99.58	96.95	96.33
Scanning	98.04	71.93	99.82	82.39	82.36
XSS	99.16	14.39	99.95	24.04	32.17
Benign	98.95	00.79	99.99	01.55	06.48
Average	**98.54**	**56.25**	**99.17**	**56.14**	**57.40**
Testing Phase (20%)					
Backdoor	99.93	00.00	100.00	00.00	00.00
DDoS	99.37	01.90	99.97	03.57	07.24
DoS	94.96	91.48	95.16	66.50	66.95
Injection	98.84	98.30	99.14	98.38	97.48
MITM	98.65	98.73	98.62	97.13	96.26
Password	98.63	89.31	99.60	92.44	91.76
Ransomware	98.93	96.02	99.53	96.86	96.22
Scanning	98.02	71.20	99.82	81.91	81.93
XSS	99.30	18.66	99.96	30.06	37.75
Benign	99.00	01.55	99.99	03.02	09.66
Average	**98.56**	**56.72**	**99.18**	**56.99**	**58.53**

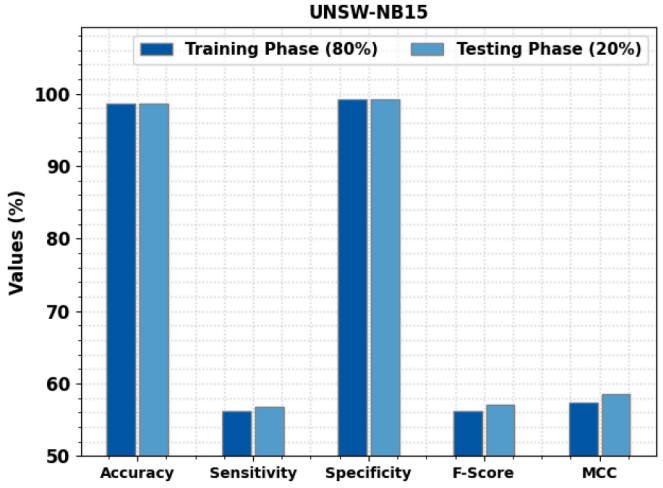


Fig. 10. Average analysis of STFA-HDLID approach with 80:20 of TR and TS data under the UNSW-NB15 dataset.

class labels in all aspects.

The results of the STFA-HDLID algorithm on 70% of the TR and 30% of the TS datasets on the UNSW-NB15 dataset are presented in Table 5 and Fig. 9. The outcomes indicate an improved performance in both cases. For example, with 70% of the TR dataset, an average $accu_y$, $sens_y$, $spec_y$, F_{score},and $MCC$of 98.84%, 58.97%, 99.35%, 58.54%, and 60.36%, correspondingly, were achieved. Parallelly, with 30% of the TS dataset, an average $accu_y$, $sens_y$, $spec_y$, F_{score},and $MCC$of 98.85%, 59.06%, 99.36%, 58.64%, and 60.36%, respectively.

Table 6 and Fig. 10 illustrate the results of the STFA-HDLID algorithm on 80% of the TR and 20% of the TS dataset on the UNSW-NB15 dataset. The results point an enhanced performance in both cases. For example, with 80% of the TR dataset, an average $accu_y$, $sens_y$, $spec_y$, F_{score},and $MCC$of 98.54%, 56.25%, 99.17%, 56.14%, and 57.40%, correspondingly, were performed. At the same time, with 20% of the TS dataset, an average $accu_y$, $sens_y$, $spec_y$, F_{score},and $MCC$of 98.56%, 56.72%, 99.18%, 56.99%, and 58.53%, respectively.

The TRA and VLA achieved by the STFA-HDLID algorithm on the UNSW-NB15 dataset are shown in Fig. 11. The experimental results indicate a maximum value of TRA and VLA, with VLA being greater than TRA.

Fig. 12 displays the TRL and VLL obtained by the STFA-HDLID algorithm under the UNSW-NB15 dataset. The experimental outcomes show that minimal values of TRL and VLL have been reached. Notably, the VLL is lower than TRL.

Table 7 and Fig. 13 report comparative intrusion detection results of the STFA-HDLID algorithm on the TON_IoT dataset [13]. The

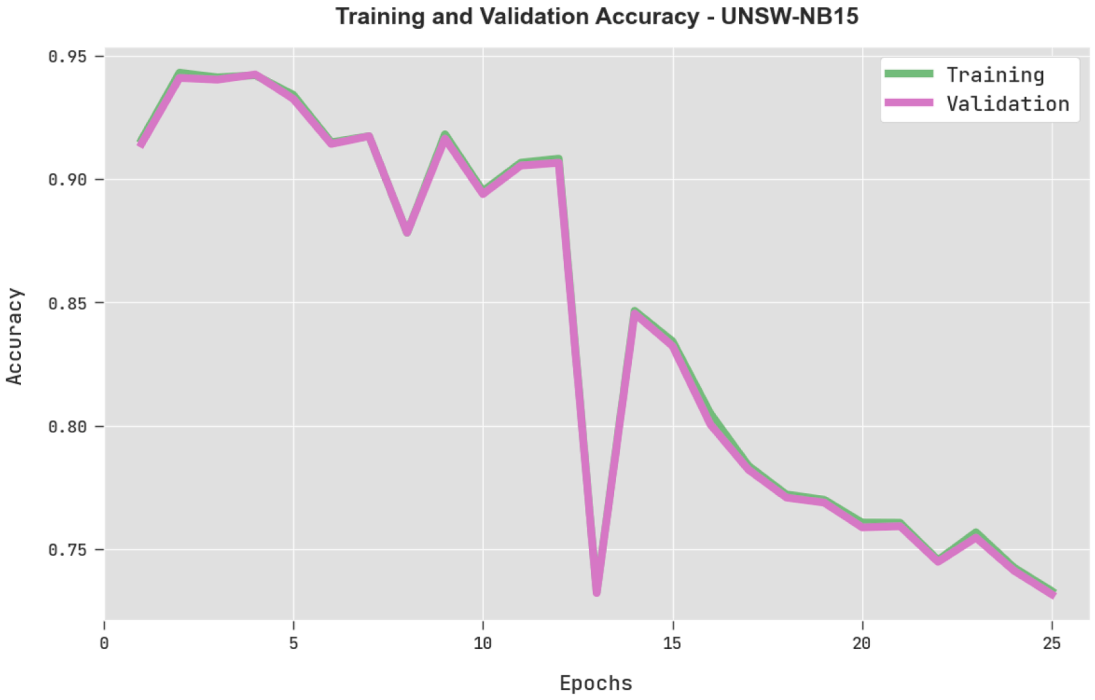


Fig. 11. TRA and VLA analysis of STFA-HDLID approach under UNSW-NB15 dataset.

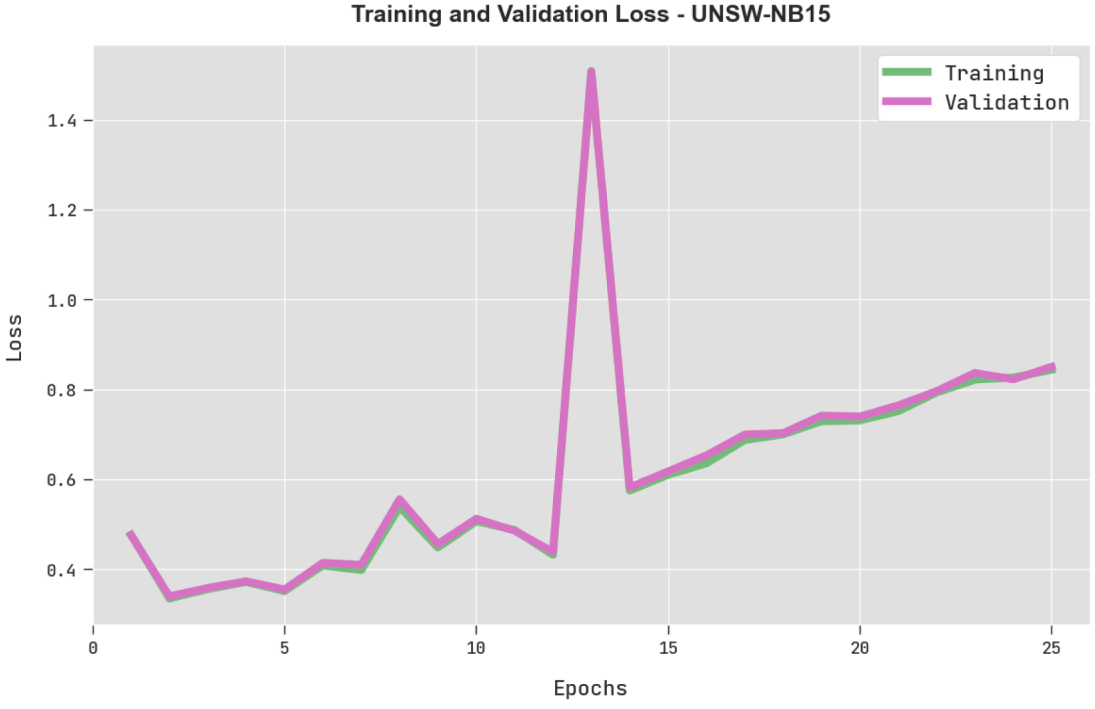


Fig. 12. TRL and VLL analysis of STFA-HDLID approach under the UNSW-NB15 dataset.

Table 7
Comparative analysis of STFA-HDLID approach with existing algorithms under the TON_IoT dataset.

Methods	Accuracy	Sensitivity
STFA-HDLID	99.51	99.73
LSTM-RNN	97.70	96.92
LR	96.64	96.68
KNN	97.53	97.05
SVM	97.99	96.07
CNN	98.62	94.19

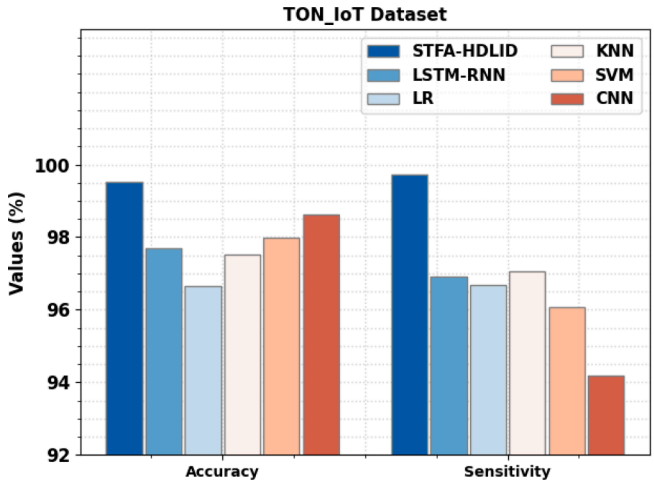


Fig. 13. Comparative analysis of STFA-HDLID approach with existing algorithms under the TON_IoT dataset.

Table 8
Comparative analysis of STFA-HDLID approach with existing algorithms under the UNSW-NB15 dataset.

Methods	Accuracy	Sensitivity
STFA-HDLID	98.85	99.36
LSTM-RNN	98.02	97.44
LR	96.34	97.17
KNN	98.34	97.55
SVM	97.46	97.21
CNN	96.55	96.72

results show that the LR method performs poorly, whereas the LSTM-RNN, KNN, and SVM methods have achieved relatively close classifier outcomes. The CNN model has attained a reasonable results with $accu_y$ of 98.62% and $sens_y$ of 94.19%. However, the presented STFA-HDLID algorithm has accomplished higher performance with $accu_y$ of 99.51% and $sens_y$ of 99.73%.

Table 8 and Fig. 14 depict comparative intrusion detection outcomes of the STFA-HDLID algorithm on the UNSW-NB15 dataset. The results show that the LR approach exhibited poor classification performance, whereas the LSTM-RNN, CNN, and SVM techniques achieved closer classifier results.

The KNN technique achieved a reasonable outcome with an $accu_y$ of 98.35% and a $sens_y$ of 97.55%. However, the presented STFA-HDLID approach demonstrate better performance with an $accu_y$ of 98.85% and a $sens_y$ of 99.36%. Thus, the STFA-HDLID algorithm can enhance intrusion detection in the IoD environment.

5. Conclusion

In this study, a new intrusion detection and classification algorithm called STFA-HDLID was developed for the IoD environment. Initially, the proposed algorithm underwent data pre-processing, in which min-max normalization was used to standardize the input data. Additionally, the STFA approach was utilized for the feature selection, and finally, the SSO with the DBN model was used for classification. The SSO algorithm was applied for optimal modification of the hyperparameters related to the DBN model. A comprehensive experimental analysis was conducted on a benchmark dataset, demonstrating the improved performance of the STFA-

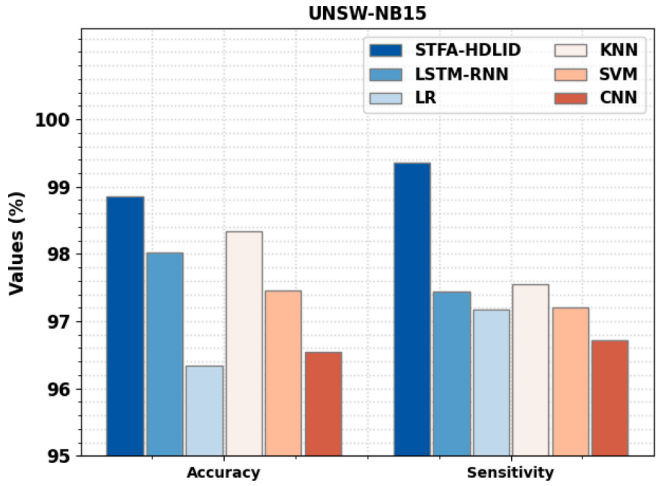


Fig. 14. Comparative analysis of STFA-HDLID approach under the UNSW-NB15 dataset.

HDLID algorithm over other recent techniques. Therefore, the proposed algorithm can achieve security in the IoD environment. Outlier detection algorithms could be employed in the future to further enhance the security performance of the STFA-HDLID algorithm compared to other methods.

Ethics approval

This article does not contain any studies with human participants performed by any of the authors.

Consent to participate

Not applicable.

Informed consent

Not applicable.

Declaration of Competing Interest

The authors declare that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

Data availability

Data sharing not applicable to this article as no datasets were generated during the current study.

References

[1] Shrestha R, Omidkar A, Roudi SA, Abbas R, Kim S. Machine-learning-enabled intrusion detection system for cellular connected UAV networks. Electronics 2021; 10(13):1549.
[2] Fotohi R, Abdan M, Ghasemi S. A Self-Adaptive Intrusion Detection System for Securing UAV-to-UAV Communications Based on the Human Immune System in UAV Networks. J Grid Comput 2022;20(3):1–26.
[3] Khan AA, Khan MM, Khan KM, Arshad J, Ahmad F. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. Comput Netw 2021;196:108217.
[4] Abu Al-Haija Q, Al Badawi A. High-performance intrusion detection system for networked UAVs via deep learning. Neural Comput Applic 2022:1–16.
[5] Basan E, Lapina M, Mudruk N, Abramov E. Intelligent intrusion detection system for a group of UAVs. In: International Conference on Swarm Intelligence. Cham: Springer; 2021. p. 230–40.
[6] Whelan J, Almehmadi A, El-Khatib K. Artificial intelligence for intrusion detection systems in unmanned aerial vehicles. Comput Electr Eng 2022;99:107784.
[7] Bouhamed O, Bouachir O, Aloqaily M, Al Ridhawi I. Lightweight ids for uav networks: a periodic deep reinforcement learning-based approach. In: 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE; 2021. p. 1032–7.
[8] Moustafa N, Jolfaei A. Autonomous detection of malicious events using machine learning models in drone networks. In: *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for* 5G *and beyond*; 2020. p. 61–6.
[9] Veerappan CS, Loh PKK, Chennattu RJ. Smart Drone Controller Framework—Toward an Internet of Drones. AI and iot for smart city applications. Singapore: Springer; 2022. p. 1–14.

[10] Guerber C, Royer M, Larrieu N. Machine Learning and Software Defined Network to secure communications in a swarm of drones. J Inf Secur Applic 2021;61:102940.
[11] Mansour RF, Soto C, Soto-Díaz R, Escorcia Gutierrez J, Gupta D, Khanna A. Design of integrated artificial intelligence techniques for video surveillance on iot enabled wireless multimedia sensor networks. Int J Interact Multimedia Artif Intell 2022;7(5):14–22. p.
[12] Mansour RF, Escorcia-Gutierrez J, Gamarra M, Villanueva JA, Leal N. Intelligent video anomaly detection and classification using faster RCNN with deep reinforcement learning model. Image Vision Comput 2021;112:104229.
[13] Perumalla S, Chatterjee S, Kumar AS. Modelling of oppositional Aquila Optimizer with machine learning enabled secure access control in Internet of drones environment. Theoret Comput Sci 2022.
[14] Praveena V, Vijayaraj A, Chinnasamy P, Ali I, Alroobaea R, Alyahyan SY, Raza MA. Optimal deep reinforcement learning for intrusion detection in UAVs. CMC-Comput Mater Continua 2022;70(2):2639–53.
[15] Althubiti S, Escorcia-Gutierrez J, Gamarra M, Soto-Diaz R, Mansour RF, Alenezi F. Improved metaheuristics with machine learning enabled medical decision support system. Comput, Mater Continua 2022;73(2):2423–39.
[16] Ramadan RA, Emara AH, Al-Sarem M, Elhamahmy M. Internet of Drones Intrusion Detection Using Deep Learning. Electronics 2021;10(21):2633.
[17] Tan X, Su S, Zuo Z, Guo X, Sun X. Intrusion detection of UAVs based on the deep belief network optimized by PSO. Sensors 2019;19(24):5529.
[18] Whelan J, Sangarapillai T, Minawi O, Almehmadi A, El-Khatib K. Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles. In: Proceedings of the 16th ACM symposium on QoS and security for wireless and mobile networks; 2020. p. 23–8.
[19] Ouiazzane S, Addou M, Barramou F. A Multiagent and Machine Learning Based Denial of Service Intrusion Detection System for Drone Networks. Geospatial intelligence. Cham: Springer; 2022. p. 51–65.
[20] Unlu E, Zenou E, Riviere N, Dupouy PE. Deep learning-based strategies for the detection and tracking of drones using several cameras. IPSJ Trans Comput Vis Applic 2019;11(1):1–13.
[21] Tansui D, Thammano A. Hybrid nature-inspired optimization algorithm: hydrozoan and sea turtle foraging algorithms for solving continuous optimization problems. IEEE Access 2020;8:65780–800.
[22] Nguyen GN, Le Viet NH, Elhoseny M, Shankar K, Gupta BB, Abd El-Latif AA. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. J Parallel Distrib Comput 2021;153:150–60.
[23] Zhang Z, He R, Yang K. A bioinspired path planning approach for mobile robots based on improved sparrow search algorithm. Adv Manuf 2022;10(1):114–30.

José Escorcia-Gutierrez received the Ph.D. degree in Computer Science and Mathematics of Security from the Universitat Rovira i Virgili in 2021 (Spain). In 2009 and 2011, he received the B.S. and M.*Sc*. degrees in Electronic Engineering from the Universidad del Norte (Colombia). His-research interests include image processing, pattern recognition, computer vision, machine learning, and medical image analysis.

Margarita Gamarra received the Ph.D. degree in Computer and Systems Engineering (2019). Received the degree in electrical and electronic engineering (2010) and M.*Sc*. in Electronic Engineering (2011) from Universidad del Norte, Colombia. She has extensive research experience in signal and image processing and machine learning, related to the medical and industrial field. She is a full-time professor at the Universidad del Norte.

Esmeide Leal received a BS. in Systems Engineering from the Universidad de Antioquia in 2000 and an MS. in Systems Engineering in 2006, and a PhD in System Engineering in 2020, both from the Universidad Nacional de Colombia. He has experience in the areas of Computer Vision, Computer Graphics and 3D Reconstruction.

Natasha Madera received the B.S. and M.Eng. degrees in Electronic Engineering from Universidad Autónoma del Caribe, respectively, in 2015 and 2020. Her research experience is addressed to digital image processing focus in medical imaging. At present, she is a professor at the Universidad Simón Bolívar since 2022.

Carlos Soto received a B.S. degree in Mechanical Engineering from the Universidad del Norte (Colombia) in 2005. He was holder an Erasmus Mundus Scholarship in a Master of Advanced Materials Science and Engineering in 2007, by Universidad Politécnica de Cataluña (Spain) and Luleå Technology University (Sweden). Currently, he is a full-time professor in the Engineering Faculty of Universidad Autónoma del Caribe.

Romany F. Mansour received the B.*Sc*. and M.*Sc*. degrees in computer science from Assiut University, Egypt, in 1998 and 2006, respectively, and the Ph.D. degree from the University of Assiut, in 2009. His-research interests include pattern recognition, computer vision, computer networks, soft computing, image processing, evolutionary computation, and machine learning.

Meshal Alharbi is PhD (Computer Science) from Durham University (UK) & MSc (Computer Science) from Wayne State University (USA). He has 10 years of Experience in Teaching/Research/Industry. His-research interests lie in the Artificial Intelligence Applications and Algorithms, Agent-Based Modelling and Simulation Applications, Disaster/Emergency Management and Resilience, Optimization Applications, and Machine Learning.

Ahmed alkhayyat is currently a dean of international relationship and manager of the word ranking in the Islamic university, Najaf, Iraq. Also, he is head of Islamic University Centre for Scientific Research. His-research interests include IoT in the health-care system, security, SDN, network coding, cognitive radio, efficient-energy routing algorithms.

Deepak Gupta is an assistant professor at Department of Computer Science and Engineering, Maharaja Agrasen institute of Technology, Delhi, India. His-research interests include Intelligent Data Analysis, Nature-Inspired Computing, Machine Learning and Soft Computing.