scientific reports

Check for updates

OPEN

African buffalo optimization with deep learning-based intrusion detection in cyber-physical systems

E. Laxmi Lydia[1], Sripada N. S. V. S. C. Ramesh[2], Veronika Denisovich[3], G. Jose Moses[4], Seongsoo Cho[5], Srijana Acharya[5]✉ & Cheolhee Yoon[6]✉

Cyber-physical system (CPS) incorporates several computing resources, networking units, interconnected physical processes, and monitoring the development and application of the computing system. Interconnection between the cyber and physical worlds initiates attacks on security problems, particularly with the enhancing complications of transmission networks. Despite the efforts to combat these problems, analyzing and detecting cyber-physical attacks from the complex CPS is challenging. Machine learning (ML)-researcher workers implemented based techniques to examine cyber-physical security systems. A competent network intrusion detection system (IDS) is essential to avoid these attacks. Generally, IDS uses ML techniques to classify attacks. However, the features used for classification are not frequently appropriate or adequate. Moreover, the number of intrusions is much lower than that of non-intrusions. This research presents an African Buffalo Optimizer Algorithm with a Deep Learning Intrusion Detection (ABOADL-IDS) model in a CPS environment. The main intention of the ABOADL-IDS model is to utilize the FS with an optimal DL approach for the intrusion recognition and identification procedure. Initially, the ABOADL-IDS model performs the data normalization process. Furthermore, the ABOADL-IDS model utilizes the ABO technique for feature selection. Moreover, the stacked deep belief network (SDBN) technique is employed for intrusion detection and identification. To improve the SDBN technique solution, the seagull optimization (SGO) technique is implemented for the hyperparameter selection. The assessment of the ABOADL-IDS technique is accomplished under NSLKDD2015 and CICIDS2015 datasets. The performance validation of the ABOADL-IDS technique illustrated a superior accuracy value of 99.28% over existing models concerning various measures.

Keywords Cyber-physical systems, Intrusion detection system, African buffalo optimization, Feature selection, Deep learning

With the assimilations of physical processes and computing resources, a Cyber-physical system (CPS) performs computation and communication via interconnected devices, allowing remote control and access to machines, devices, and systems indispensable in several industrial fields[1]. Nonetheless, the comprehensive integration of CPS comes with different security risks, which may cause severe damage to the physical object and harm the users who rely entirely on them[2]. The security mechanism aims to defend CPS devices from exterior attacks that depend on antivirus, firewalls, and encryption methods. However, this mechanism could not avoid all these attacks, particularly allowing the attacker to develop its approaches[3] continually. Intrusion Detection Systems (IDS) are essential for identifying malicious behaviours and protecting CPS from security attacks in these contexts. Specific embedded domain device software that allows adversaries to perform arbitrary code and vulnerabilities are exposed by libraries even though the emergence of real-time software for CPS is stringent[4]. This code injection attack has been standard in the general-purpose domain for several years. As more embedded applications, especially CPS applications, utilize networks, they become more vulnerable to these attacks[5].

[1]Department of Computer Science and Engineering, Vignan's Institute of Engineering for Women, Visakhapatnam, Andhra Pradesh 530046, India. [2]Department of Computer Science and Engineering, Aditya College of Engineering and Technology, Surampalem, Andhra Pradesh, India. [3]Institute of Digital Technologies and Law, Kazan Innovative University named after V. G. Timiryasov, 42 Moskovskaya str., Kazan, Russia420111. [4]Department of Computer Science and Engineering, School of Engineering, Malla Reddy University, Hyderabad, India. [5]Department of Convergence Science, Kongju National University, Gongju 32588, Korea. [6]Laboratory of Autonomous Vehicle and Block-Chain, Korean National Police University, Asan 31539, Republic of Korea. ✉email: srijana@kongju.ac.kr; bertter@police.ac.kr

Furthermore, most IDSs exploit machine learning (ML) models for attack identification. This necessitates extracting better features for various intrusions used in supervised learning for attack detection. However, appropriate and sufficient traffic data is not available often, which enables proper feature learning[6]. Compared to the number of non-intrusions, the number of intrusions is also much lesser, resulting in more difficulties in training[7]. IDS employs ML techniques for detecting malicious behaviours using training datasets[8]. Still, many researchers exploit datasets taken from the internet protocol. This dataset is not suited for intrusion detection in CPSs because they lack traffic from CPS protocol and have a slight relationship with the present equipment[9]. The classical offline ML technique does not have its models often updated while the behaviour shift occurs. Currently, it is necessary to categorize real-time attacks in vast streams of information without compromising hardware resources, like CPU and memory, with the vulnerability to take data processing to the network node and the enhancing development of Big Data systems generating an ample quantity of heterogeneous data[10]. Hence, classical offline ML methods might not be appropriate for processing events from a massive flow of information.

This research presents an African Buffalo Optimizer Algorithm with a Deep Learning Intrusion Detection (ABOADL-IDS) model in a CPS environment. The main intention of the ABOADL-IDS model is to utilize the FS with an optimal DL approach for the intrusion recognition and identification procedure. Initially, the ABOADL-IDS model performs the data normalization process. Furthermore, the ABOADL-IDS model utilizes the ABO technique for feature selection. Moreover, the stacked deep belief network (SDBN) technique is employed for intrusion detection and identification. To improve the SDBN technique solution, the seagull optimization (SGO) technique is implemented for the hyperparameter selection. The assessment of the ABOADL-IDS technique is accomplished under NSLKDD2015 and CICIDS2015 datasets. The key contribution of the ABOADL-IDS technique is listed below.

- The ABOADL-IDS model utilizes min-max scaling to normalize the data, ensuring all features fall within a standardized range. This preprocessing step assists in improving the model's performance by eliminating bias from features with different scales. It also enables more effective learning, particularly for models sensitive to input range.
- The ABO-based feature selection identifies the most relevant features, improving the technique's ability to detect intrusions accurately. Concentrating on key features mitigates the data's dimensionality, resulting in faster computation and less resource consumption. This enhances the efficiency and effectiveness of the intrusion detection process.
- The SDBN model is utilized for intrusion detection. Its DL technique enables the model to learn complex data patterns, effectively detecting advanced and previously unseen attacks. The SDBN technique's hierarchical feature learning improves the accuracy and robustness of the detection process.
- SGO-based tuning fine-tunes the model's parameters, improving its overall performance. This methodology optimizes the balance between exploration and exploitation, allowing for more precise parameter selection. As a result, the model attains improved generalization and robustness across diverse datasets.
- The novelty of the ABOADL-IDS model is in seamlessly incorporating advanced techniques like ABO for feature selection, SDBN for DL-based intrusion detection, and SGO for parameter tuning. This integration creates a cohesive framework that improves detection accuracy and minimizes computational complexity. By employing these complementary methods, the model attains enhanced performance in real-time intrusion detection with reduced resource consumption.

Related works

In[11], an Explainable AI-Enabled Intrusion Recognition method for protecting CPS (XAIID-SCPS) was designed. A Hybrid Enhanced GSO (HEGSO) technique has been implemented for the FS method. The Improved ENN (IENN) technique could be employed to determine the optimum parameters for IDS. Althobaiti et al.[12] introduced a new intellectual computation-based IDS method. This method includes preprocessing to remove the noise data. Later, this technique employs a binary bacterial foraging optimizer (BBFO) based-FS approach for optimally choosing feature subsets. Also, the GRU approach was implemented to detect intrusions. Lastly, the Nesterov-accelerated Adaptive Moment Estimation (NADAM) technique must be employed for the hyperparameter optimizer of the GRU technique. Mittal et al.[13] suggested a novel clustering technique for intrusion detection. This approach uses a new gravitational search algorithm (GSA) variant to attain optimum clusters. *Kbest* was changed to a proportionally reduced process in this developed variant with logistic-mapping-based chaotic behaviours. In[14], a privacy-conserving model named PC-IDS was designed to have two main modules. Initially, a data preprocessing module was developed for cleaning and converting real data into various layouts, achieving privacy conservation; later, an IDS was introduced utilizing PSO-based probabilities of neural networks. Kukkala et al.[15] projected a new DL-based IDS named INDRA that implements a GRU-based recurrent-AE network to identify different cyberattacks in automatic CPSs. The authors[16] suggested innovative AI-aided multimodal fusion-based IDS (AIMMF-IDS). A weighted voting-based ensemble framework combined methods through RNN, deep belief network (DBN), and BiLSTM. In[17], a DL-based IDS was implemented to identify cyberattacks on CPS using a multimodal learning method. This technique reports two IDS methods depending on DL: RNN and CNN. In the first IDS, Gramian Angular Field (GAF) was implemented to transform CPS time-series data into images. The second IDS employed RNN with a multimodal attention method to train the attack detector.

Safavat and Rawat[18] recommended secure federated learning employing an Interpolated private and public keys-ROTation (IPP-ROT)-based ECC and providing Buff; FL using Buffered Asynchronous, Aggregation based Log Sigmoid-MLP (FB-FL-BAA-LS-MLP) approaches. Firstly, the vehicles could be listed with a cloud server by producing cipher text and keys with the help of IPP-ROT and ECC techniques. Shi et al.[19] develop an effective framework for analyzing recurrent spontaneous abortion (RSA) in patients with thyroid disorders, using an integration of the Joint Self-Adaptive Sime Mould Algorithm (JASMA) and Support Vector Machine (SVM) to improve global search, optimization, and convergence for improved diagnosis and treatment. Ji et al.[20] propose

a hybrid intrusion detection approach for CPSs, incorporating AdaBoost and random forest (RF) methods. It chooses optimal features based on their significance scores and retrains the base models for improved attack detection. Arumugam et al.[21] develop an intrusion detection system for CPS by extracting statistical and flow-based features, choosing optimal features using Improved LDA, and applying a hybrid CNN-Bi-GRU classifier optimized by the BMEAOA approach for improved detection performance. Chen et al.[22] propose an improved Firefly Algorithm integrated with the Extremal Optimization (IFA-EO) approach. It introduces three strategies: a hybrid attraction model, adaptive step size, and EO integration for improved local search, balancing exploration and exploitation to improve performance. Abinash et al.[23] propose HGCNN-LSTM, a DL-based attack detection model for ICS networks, using hypergraphs to optimize CNN-LSTM thresholds and enhance the detection of data injection, DoS, and reconnaissance attacks.

Feng et al.[24] propose the dConvLSTM-DCN framework, incorporating dual ConvLSTM and Dense Convolutional Network to predict VPS availability short-term (within 30 min) and long-term (over 30 min). It effectively captures temporal and spatial correlations and utilizes a two-layer linear network for feature extraction, with direct and iterative methods for long-term predictions. Al Mazroa et al.[25] propose an automated Cyberattack Detection using Binary Metaheuristics with DL (ACAD-BMDL) method for automated cyberattack detection in CPS environments, using Z-score normalization, binary grey wolf optimizer (BGWO) for feature selection, Enhanced Elman Spike Neural Network (EESNN) for attack detection, and Archimedes Optimization Algorithm (AOA) for hyperparameter optimization. Rahim and Manoharan[26] propose a framework for CPS intrusion detection and mitigation utilizing Fractional Artificial Protozoa Optimization (FAPO)-enabled Spiking VGG-16. It involves normalizing input logs with Quantile Normalization, selecting features via Skill Optimization Algorithm (SOA), detecting intrusions with Spiking VGG-16, and classifying attacks with FAPO for mitigation. Chen et al.[27] present a hybrid 3DMA scheme for multi-user multiple-input multiple-output visible light communication (MU-MIMO-VLC) approaches, optimizing 3D resources to improve performance. It uses user grouping, frequency pairing, power multiplexing with superposition coding, and an optimal power allocation strategy, achieving higher sum rates than benchmark schemes. Markkandeyan et al.[28] propose a hybrid DL strategy for detecting malware in IoT environments, utilizing an Adaptive TensorFlow DNN with Improved Particle Swarm Optimization (IPSO) for SC duplication detection and E-LSTM for identifying suspicious actions.

Despite the improvements in intrusion detection and mitigation systems for CPS, several limitations and research gaps remain. Many existing methods encounter challenges in handling high-dimensional data, resulting in issues with feature selection and computational efficiency. Furthermore, there is a lack of scalability in several techniques when applied to large-scale, real-time CPS environments. Many approaches also face difficulty generalizing across diverse attack scenarios, limiting their efficiency in dynamic settings. Furthermore, while improving detection accuracy, optimization techniques often overlook the trade-off between exploration and exploitation. Lastly, while hybrid models exhibit potential, their complexity and requirement for extensive training data remain significant barriers to their practical deployment. Therefore, more efficient, scalable, and adaptable solutions are required to address these gaps in current research.

The proposed model

This manuscript proposes automatic intrusion recognition using the ABOADL-IDS method in the CPS platform. The main intention of the ABOADL-IDS technique is to utilize the FS with an optimal DL approach for the intrusion

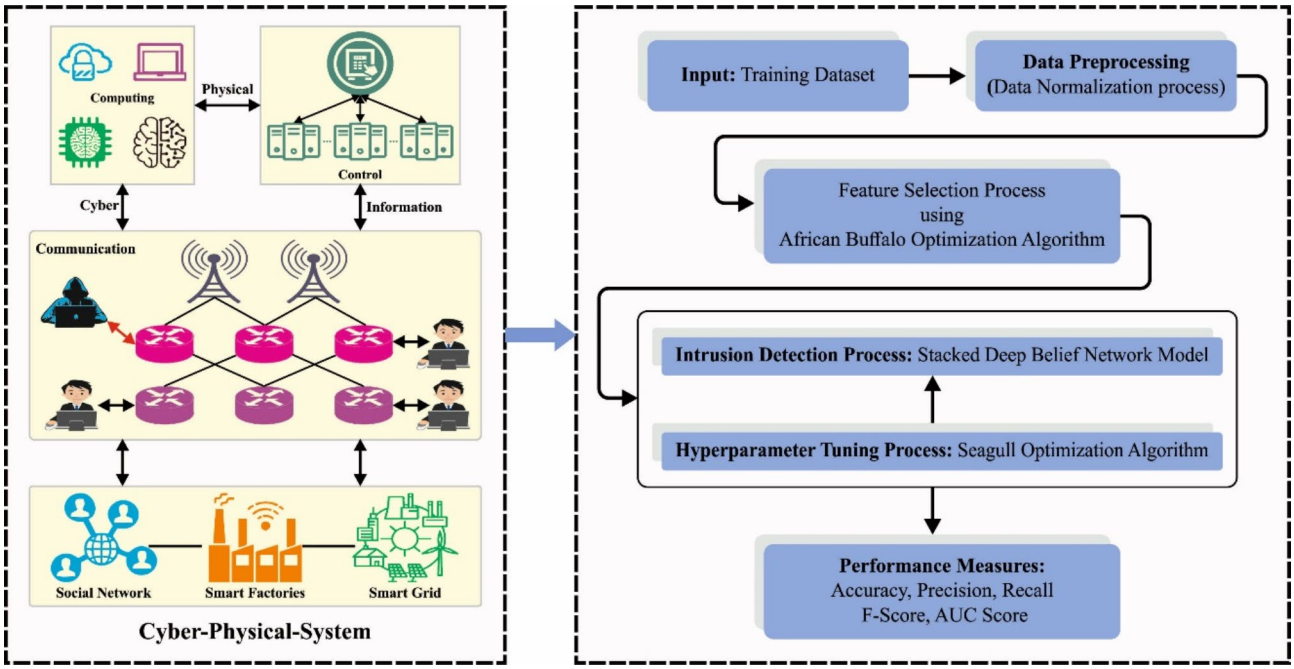

Fig. 1. Workflow of ABOADL-IDS technique.

recognition and identification procedure. It comprises data normalization, ABO-based FS, SGO-based hyperparameter tuning, and SDBN-based intrusion recognition. Figure 1 represents the workflow of the ABOADL-IDS technique.

Data normalization

Data normalization using a min-max scaling approach is mainly utilized[29]. This model is chosen due to its simplicity and effectiveness in transforming data into a standard range, typically between 0 and 1. This method ensures that all features contribute equally to the model, preventing features with larger numerical ranges from dominating the learning process. Unlike other normalization techniques, such as Z-score normalization, Min-Max scaling preserves the original distribution of the data and averts distortion. It is particularly advantageous when the model requires a specific input range, such as in neural networks, where activation functions like sigmoid or tanh work best within a bounded range. Furthermore, Min-Max scaling is computationally efficient and easy to implement, making it a preferred choice for preprocessing data in many ML tasks.

MinMax Scaler shrinks the data from the provided range, generally from zero to one. It converts data by scaling features to the offered range. It scales the values to a specific range without altering the original distributions' shape. This equation of the Min-Max normalizer method X_norm is represented in Eq. (1).

$$X\_norm = \frac{(X - X\_\min)}{X\_\max - X\_\min} \tag{1}$$

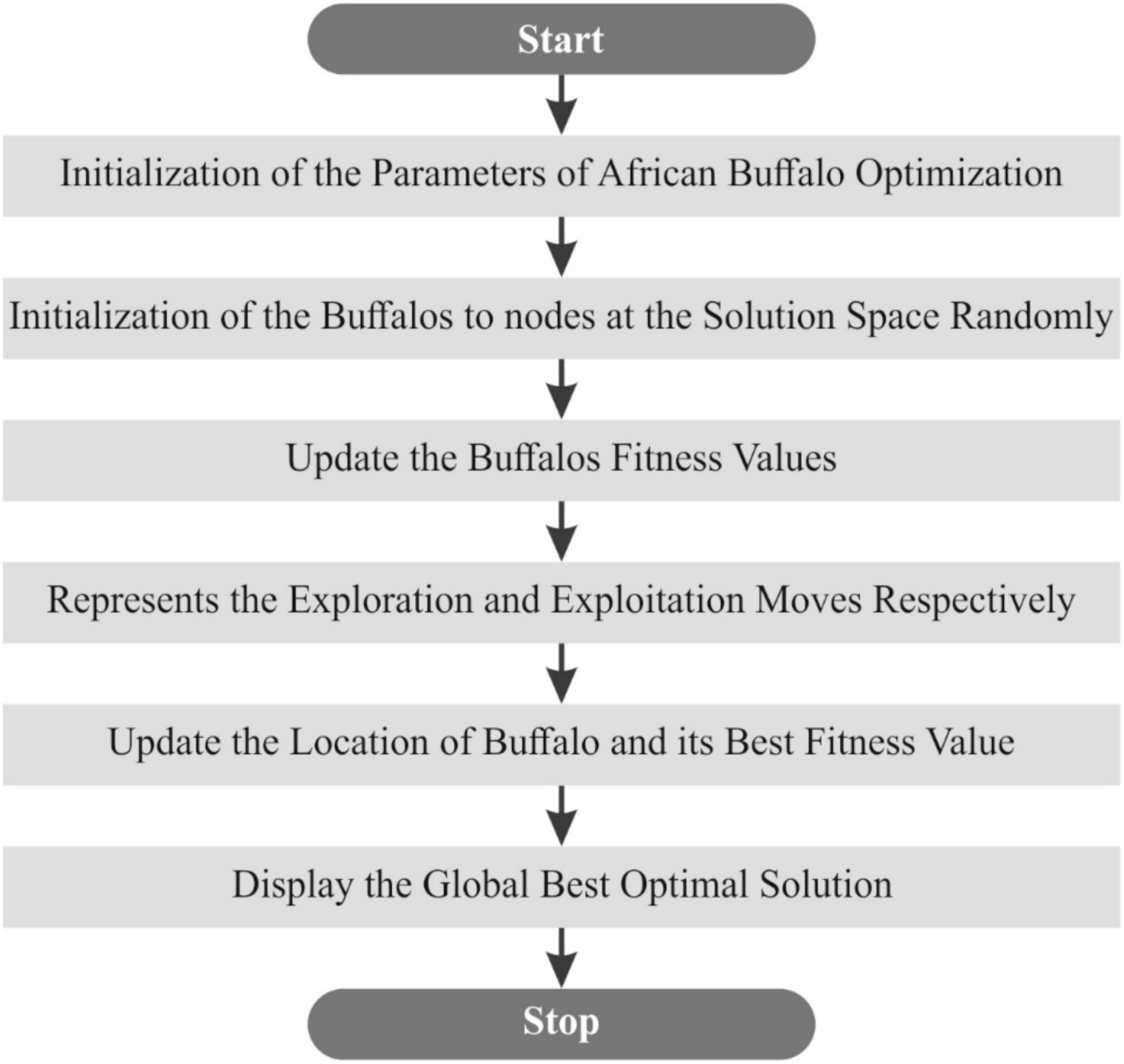

Fig. 2. Steps involved in the ABO model.

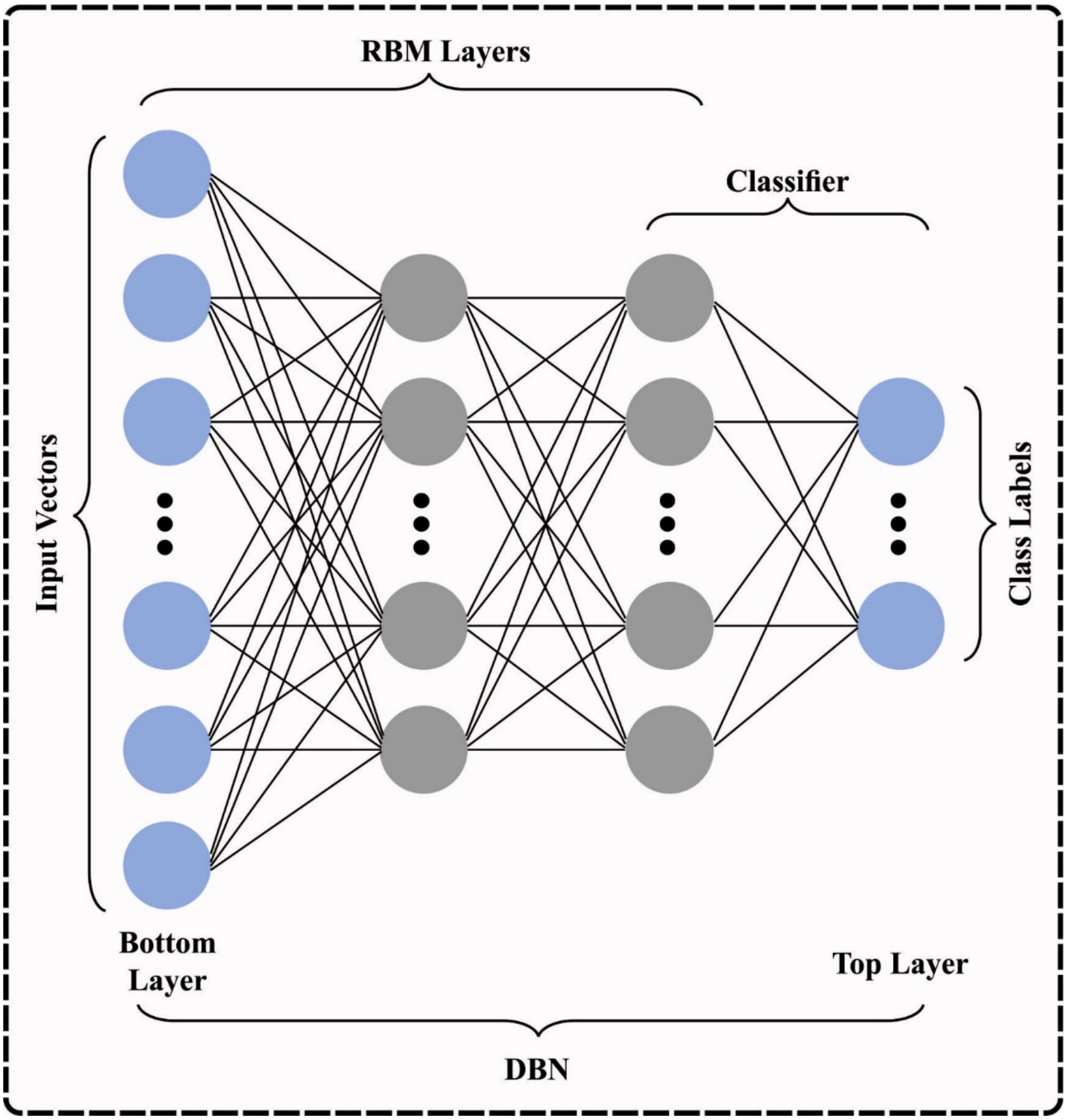

Fig. 3. Architecture of DBN.

In this case, the normalizer computation is carried out only for unknown validation, training, and testing sets.

Feature selection using ABO model

To choose a feature, the ABOADL-IDS technique designs a new ABO technique for FS[30]. This model is preferred due to its unique capability to explore the solution space and balance exploration and exploitation effectually. Inspired by the herd behaviour of African buffaloes, the ABO model utilizes a cooperative search mechanism that replicates the way buffaloes work together to find optimal grazing areas. This behaviour allows the model to avert local optima and improves the accuracy of feature selection. Compared to other optimization techniques, the ABO model is more robust in handling complex, high-dimensional datasets and is less prone to getting stuck in suboptimal solutions. Its strong global search capability and fast convergence make it an ideal choice for feature selection in ML tasks, ensuring that only the most relevant features are chosen to improve model performance. Figure 2 illustrates the ABO model.

The African buffalo's behaviour from the vast forests and grasslands of Africa assisted as a simulation for the ABO technique. While African buffaloes are consistently identified as exceptionally planned and remarkably effective herbivores, this meta-heuristic system tries to influence the natural intellect of buffaloes to generate higher-quality meta-heuristics. During this method, once the position (solution) of all the buffalo is, an optimum preceding position of that buffalo can continuously be comprised in the computation for simulating the remarkable memory capacity of these animals. Additionally, it is transferred efficiently by its vocalizations; mainly, it is distinctive "was" calls that assist various purposes like signalling danger or determining an optimum food source. This performance can be established in the method, such that the computation of novel solutions of all the buffaloes also assumes the position of the existing buffalo, which is near other buffaloes of the group are also affected. By executing this earlier defined performance of constantly upgrading the solution of all the buffalo is dependent upon their historical optimum solution and existing solution of the entire optimum buffalo from the herd, this method ABO effectively resolves the difficulty of early convergence or stagnation in the optimizer method, permitting for a wide-ranging exploration of searching space.

Process of ABO

Data: VN-count of variables in the position,

PS-the population size, ITN-the iteration counts,

$NMBM$ −the maximal iteration counts without enhancing the optimum position

Result: X-the optimum position in the population P

$P \leftarrow \emptyset, PLocal_{\max} \leftarrow \emptyset;\ bgmax \leftarrow \{0\};$

$lp1 \leftarrow randomValue(0.1,0.6), lp2 \leftarrow randomValue(0.1,0.6),$

$numBg_{max} \leftarrow 0, wk \leftarrow \{0\};$

For $i \leftarrow 1$ to ITN do

if $i = 1$ or $numBg_{max} = NMBM$ then

$numBg_{max} \leftarrow 0, wk \leftarrow \{\emptyset\},$

$For\ j \leftarrow 0\ to \leftarrow |PS - 1|\ do$

$C \leftarrow Vector\ (VN);$

$For\ k \leftarrow 0\ to\ |VN - 1|\ do$

$|\ C_k, \leftarrow randomVa1ue();$

$P_j \leftarrow C;$

$numBg_{local} \leftarrow \{0\},$

$For\ j \leftarrow 0$ to $|PS - 1|\ do$

$mk \leftarrow mk + lp1 * (Bg_{max} - P_j) + lp2 * \left(PLocal_{max,j} - P_j\right);$

$P_j \leftarrow (P_j + mk)/0.5;$

$If\ fitnessFunction\ (P_i)$ >fitnessFunction $(PLocal_{\max,i})$, then

$|PLocal_{\max,j} \leftarrow P_j;$

$If\ fitnessFunction\ (P_j)$ >fitnessFunction $(numBg_{local})$, then

$numBg_{local} \leftarrow P_j;$

$if\ fitnessFunction\ (numBg_{local})$ >fitnessFunction (bg_{max}), then

$bg_{max} \leftarrow numBg_{local}$

$numBg_{max} \leftarrow 0;$

else

$numBg_{max} \leftarrow numBg_{max} + 1$

$X \leftarrow bg_{max};$

Algorithm 1. Pseudocode of ABO

The primary formula in the ABO method defines the parameter mk that affects the novel solution of separate bison (solution) comparative to its old optimum solution (separate's optimum bison) and comparative to existing best solution (the global optimum position) as:

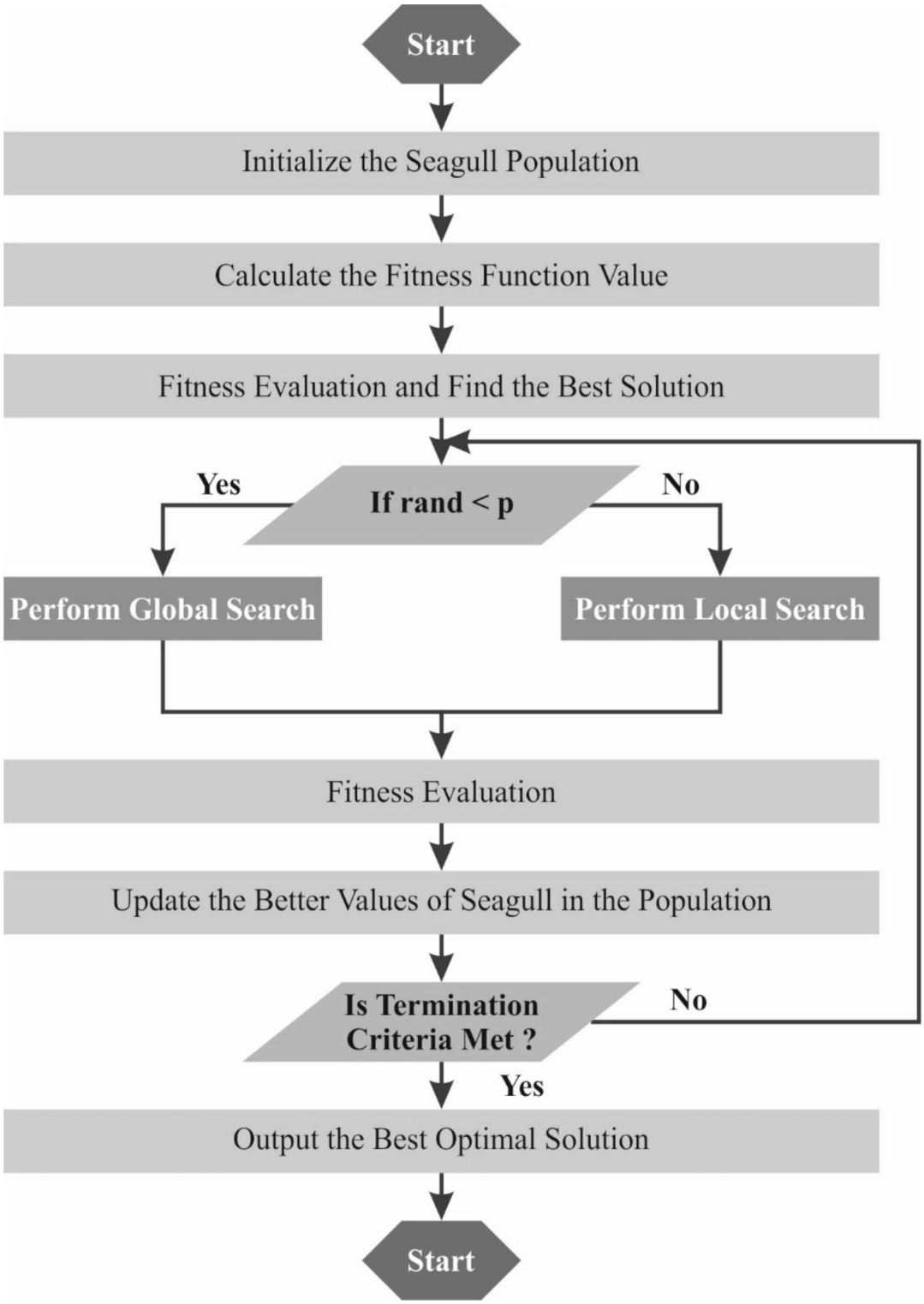

Fig. 4. Flowchart of the SGO technique.

$$mk = mk + lp1^{*}\left(bg_{\max} - P_j\right) + lp2^{*}\left(PLocal_{\max,j} - P_j\right), \tag{2}$$

In this case, P_j signifies the existing solution of buffalos j, b_{gax} denotes the global optimum position, and $PLocal_{max,j}$ represents the old optimum position of buffalos j. The parameter mk determines the novel solution P_j of buffalos j. The parameters $lp1$ and $lp2$ define if the bison follows its optimum solution or the solution of optimum global position. During all the iterations of the ABO approach, the global optimum

position and old optimum position of all the bison can also be upgraded once there is a alter. Afterwards, the procedure is repeated, and the condition for the end of the method is met.

The allocated FF evaluates the quality solution of the ABO-based FS technique[31]. The function depends primarily on the regression or classification error rate, and the feature is chosen from the input data. The fittest solution can rely on a series of features that provide minimal features with a minimal classifier error rate. The subsequent formula is used to assess the solutions' quality.

$$F_n = \alpha Err\,(O) + \beta \frac{|s|}{|f|} \tag{3}$$

In Eq. (18), $Err\,(O)$ is the optimizer error rate, s denotes the selected set of features, and f shows the overall amount of existing features. The $\alpha \in [0,1]\,, \beta = 1 - h_1$ value is accountable for the classifier errors and the quantity of nominated features. Here, h_1 depicts a parameter related to the classifier's performance or a specific aspect of the feature selection process, and its value is used to adjust the weight parameter β, affecting the overall model optimization.

Intrusion detection using SDBN model

The SDBN technique is employed to detect intrusion[32]. This model is chosen because it can automatically learn hierarchical feature representations from raw data. By stacking multiple Restricted Boltzmann Machines (RBMs) layers, SDBN captures intrinsic patterns and correlations within the data, which is significant for detecting advanced intrusions. Unlike conventional ML techniques requiring manual feature extraction, SDBN learns high-level abstractions from the raw input, improving its ability to detect unknown or zero-day attacks. Furthermore, the DL structure of SDBN allows for improved generalization, making it highly effectual on diverse and large-scale datasets. Compared to other models, SDBN's multi-layered architecture improves its robustness and performance in intrusion detection tasks by efficiently processing high-dimensional data and distinguishing subtle malicious behaviour patterns.

A DBN is a DNN stacked with the multi-layer infrastructure of RBMs. The RBM architecture comprises hidden and visible layers with hidden neurons, respectively. Visible neurons are FC with hidden neurons; no intra-layer from the VL or HL exists. There exist two major learning models: supervised and unsupervised learning. The RBM and backpropagation network (BPN) implement unsupervised and supervised learning. After implementing the RBM operation, the hidden neuron is conditionally independent once the visible state is given. Therefore, once the input vector is given, it rapidly takes unbiased samples in the posterior distribution. The two primary functions represent these models— the probability distribution and energy functions.

$$E\,(v, h; \theta) = -\sum_{i=1}^{n}\sum_{j=1}^{m} v_i h_j w_{ij} - \sum_{i=1}^{n} v_i a_i - \sum_{j=1}^{m} h_j b_j \tag{4}$$

In Eq. (4), E shows the energy with configuration on v and h visible and hidden neurons, v_i represents the binary state of i^{th} visible neurons, h_j signifies the binary state of j^{th} hidden neurons, and w_{ij} shows the weight between i^{th} and j^{th} neurons, for the parameter θ of $\{W,\ b,\ a\}$ and $v_i,\ h_j \in \{0,1\}$. Now, W refers to the symmetric weight with $n \times m$ dimension , a designates the bias of visible neuron, and b denotes the bias of hidden neuron. The energy defines the probability of configuration.

$$p\,(v_i, h_j) = \frac{e^{-E\left(v_i, h_j\right)}}{\sum_{v_i, h_j} e^{-E\left(v_i, h_j\right)}} \tag{5}$$

The denominator in Eq. (5) defines the partition function and is attained by adding each pair of hidden and visible vectors. According to the function of probability distribution, the conditional probability distribution function is resulting and given below:

$$h_j = sigmoid\left(\sum_i v_i W_{ij} + b_j\right) \tag{6}$$

$$v_i = sigmoid\left(\sum_j h_j W_{ij}^T + a_i\right) \tag{7}$$

Here, h_j indicates the probability distribution once v_i is provided, and v_i shows the probability distribution once h_j is provided.

DBN exploits pre-training, fine-tuning, and prediction. Pre-training and fine-tuning allow this method to forecast a correct outcome. During the pre-training, a series of primary parameters are attained in the input vector. SDBN is a kind of ANN design that integrates several layers of RBMs to procedure a DL approach. During the stacked DBN, several RBMs are trained greedy layer-wise. This suggests that you begin with the primary RBM and train it to capture features from the data. Afterwards, the outcome of this RBM is employed as input for the next RBM. This procedure is frequent for several layers as desired. Figure 3 signifies the structure of DBN.

NSLKDD 2015 dataset	
Classes	**No. of samples**
Normal	67,343
Anomaly	58,630
Total no. of samples	125,973

Table 1. Details of the NSLKDD2015 dataset.

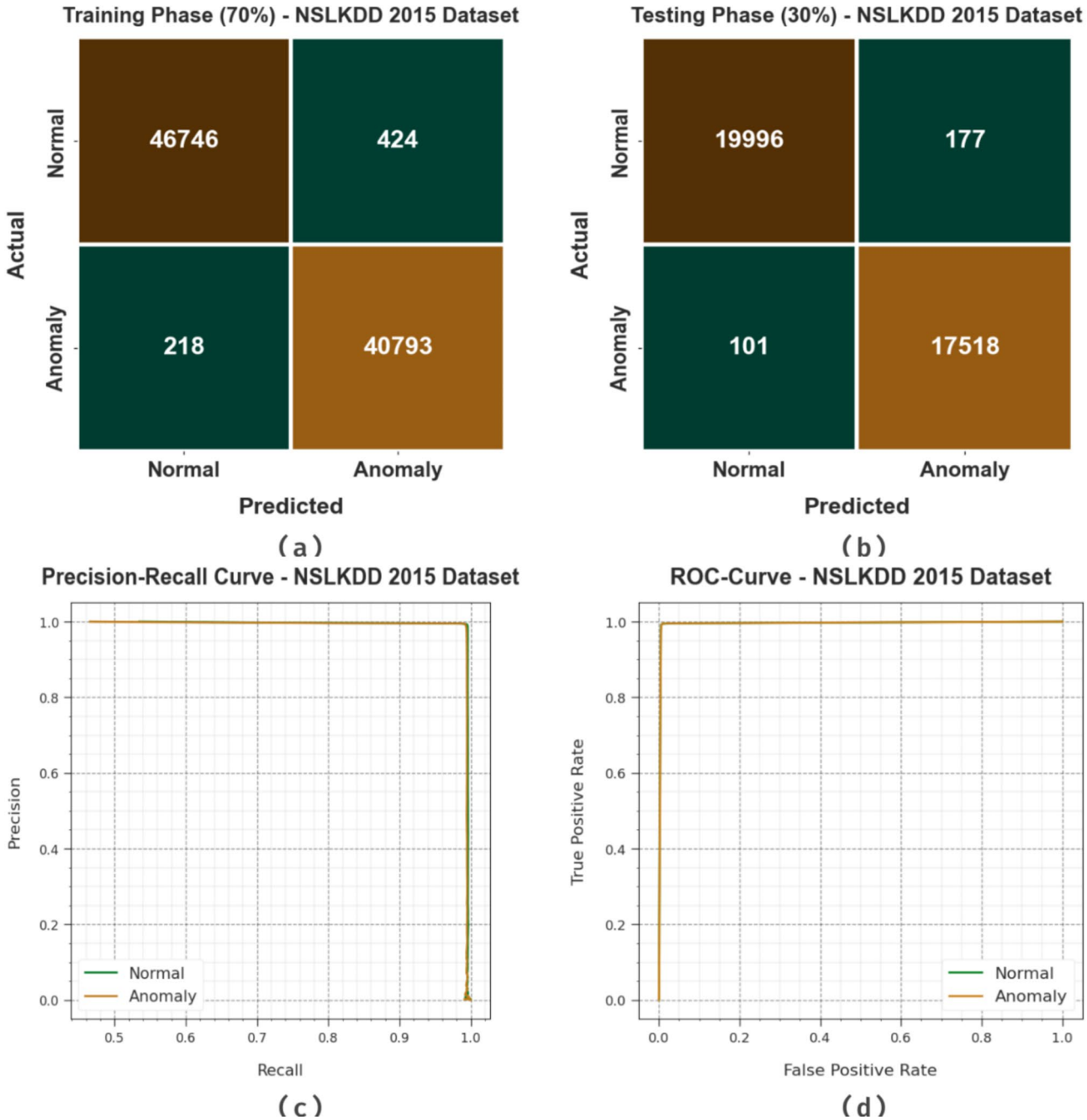

Fig. 5. NSLKDD2015 dataset (**a**, **b**) Confusion matrices, (**c**, **d**) PR and ROC curves.

NSLKDD 2015 dataset					
Classes	$Accu_y$	$Prec_n$	$Recal$	F_{score}	AUC_{score}
70% of TRAS					
Normal	99.10	99.54	99.10	99.32	99.28
Anomaly	99.47	98.97	99.47	99.22	99.28
Average	99.28	99.25	99.28	99.27	99.28
30% of TESS					
Normal	99.12	99.50	99.12	99.31	99.27
Anomaly	99.43	99.00	99.43	99.21	99.27
Average	99.27	99.25	99.27	99.26	99.27

Table 2. Detection outcome of ABOADL-IDS technique on NSLKDD2015 dataset.

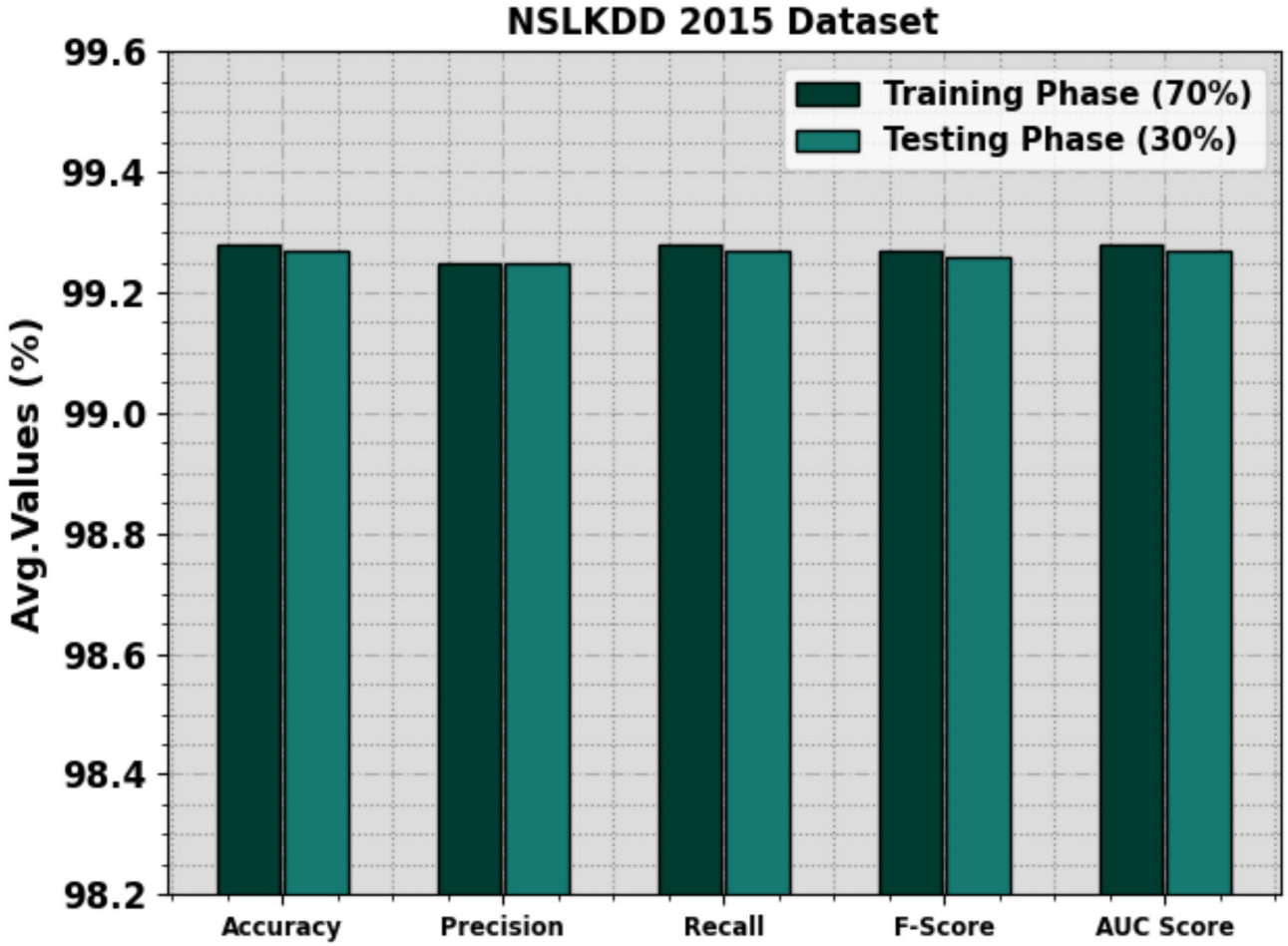

Fig. 6. Average of ABOADL-IDS technique on the NSLKDD2015 dataset.

Parameter tuning using the SGO model

Finally, the SGO model optimally chooses the parameter linked to the SDBN model[33]. This model is chosen due to its unique bio-inspired search mechanism, which replicates the intelligent foraging behaviour of seagulls. This model effectually balances exploration and exploitation, allowing it to search a vast solution space while converging towards the optimal solution. Compared to other optimization techniques, SGO is less likely to get trapped in local optima, making it more robust in finding the best parameter set. The adaptability of SGO to various optimization problems, comprising parameter tuning, improves its flexibility and effectiveness. Additionally, SGO needs fewer computational resources and iterations than some conventional methods, improving efficiency. Its ability to work well on complex, high-dimensional parameter spaces makes it an ideal choice for fine-tuning models in ML tasks. Figure 4 specifies the flow chart of the SGO technique.

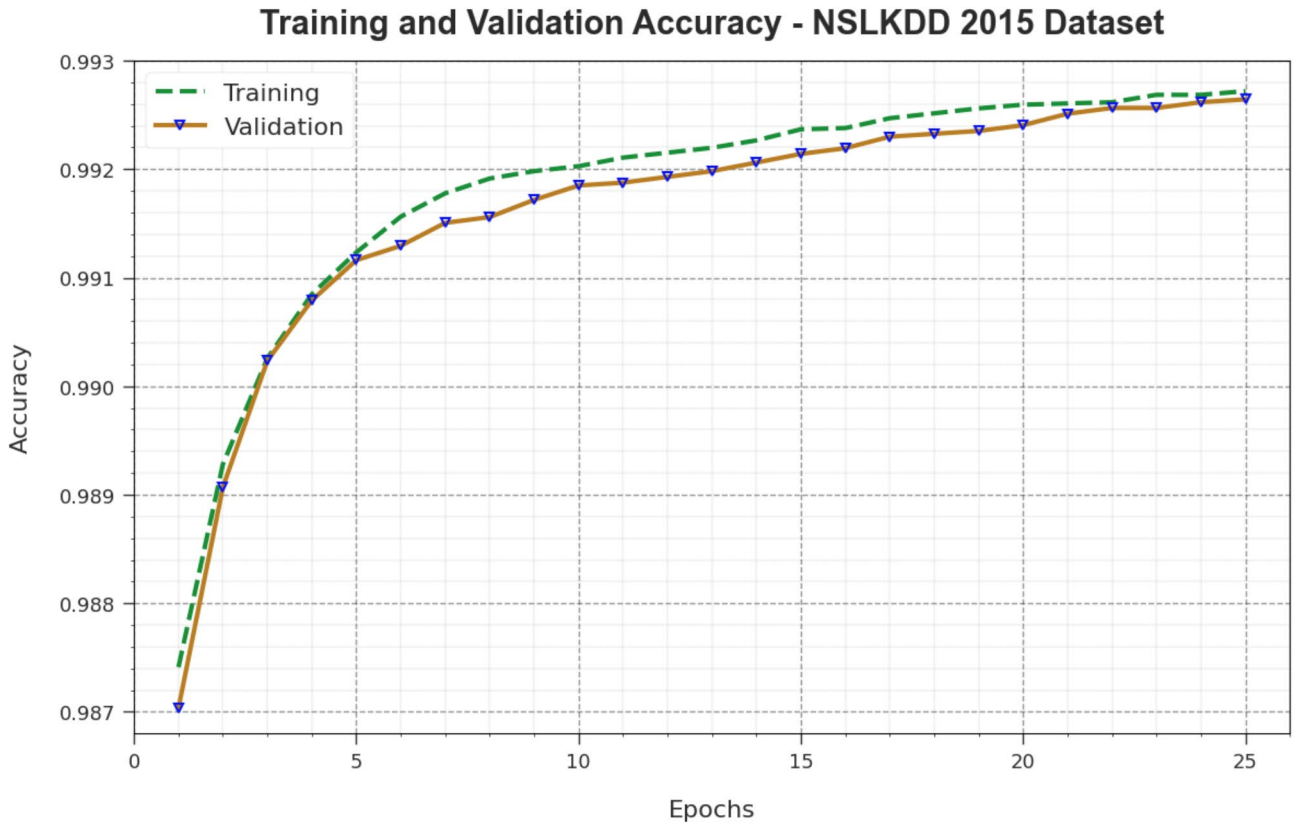

Fig. 7. $Accu_y$ curve of ABOADL-IDS technique on NSLKDD 015 dataset

The SGO approach is a recent metaheuristic intelligent approach based on seagulls' attacking and migratory strategies. Its underlying principle is to search for the global optima solution by relating local and global search development of different population individuals. At the same time, attack is a local optimization, and migration is a global optimization. Over other optimization techniques, the SGO gives the succeeding two advantages:

(1) The structure of the algorithm is open, and there aren't multiple parameters to organize, so it is very simple to resolve different types of problems;
(2) A global optimizer algorithm called SGO has increased proficiency for global search and local exploitation and deals with the problem of substantial dimension.

During the flight, it affects the local development capacity of the SGO; however, attack behaviour is the seagull attacks for food in the water and on the ground. A migration strategy is the seagull's flight in many directions suitable for survival at the existing stage but not in another location.

Migration
The SGO performs a global search by mimicking seagulls' random flying in all directions. Every random seagull should gradually meet the above three requirements in this process.

(1) Avoiding collision

The SGO evaluates the seagull's post-migration location $C_s(t)$ by dealing with the existing location of the seagull $P_s(t)$ and the additional parameter A to avoid collision between neighbouring seagull individuals:

$$C_s(t) = A \times P_s(t) \tag{8}$$

t—represents the existing iterations count; A—indicates the drive of seagulls in space;

$$A = f_c - \left(t \times \frac{f_c}{\mathrm{Max}_{iteration}}\right) \tag{9}$$

f_c—linear function reduces the A value linearly from f_c to 0; $\mathrm{Max}_{iteration}$—shows the maximal iteration count.

(2) Best position orientation

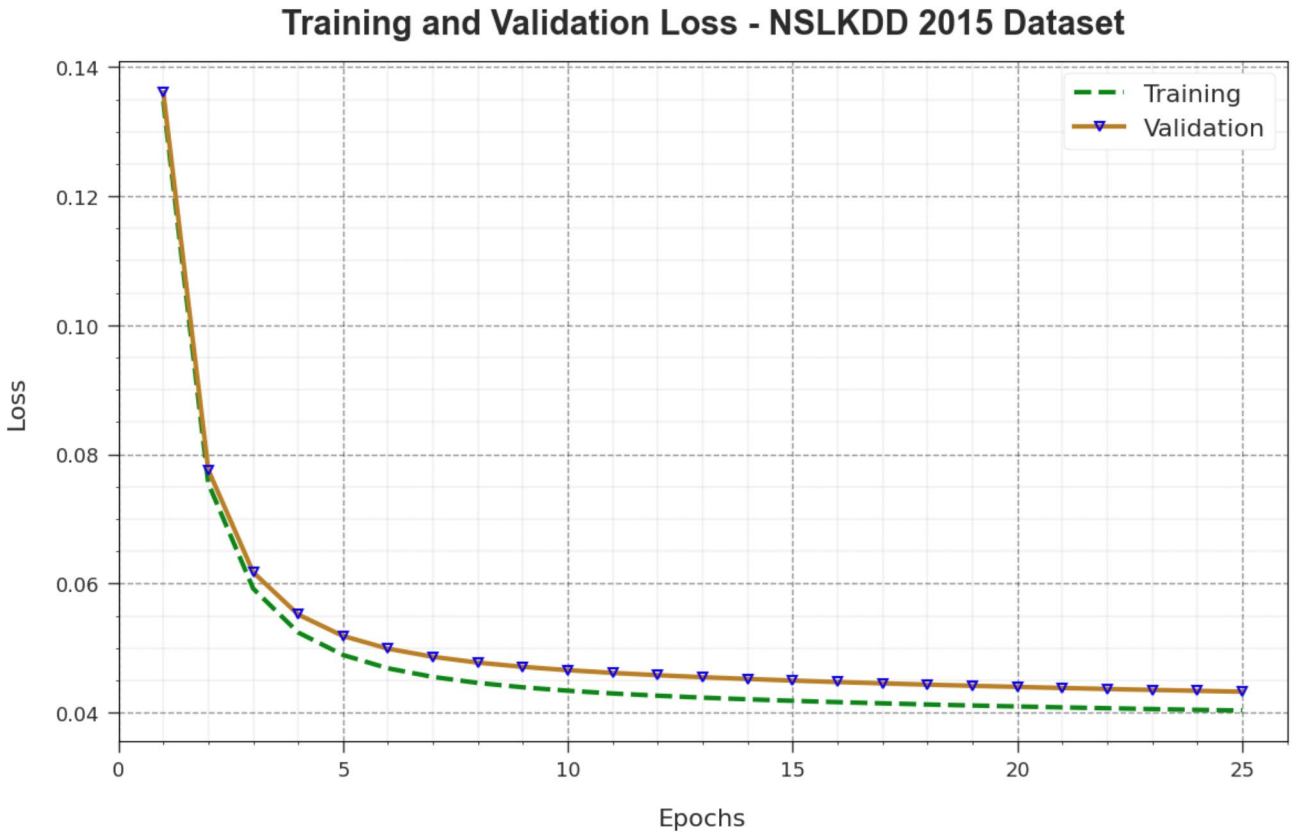

Fig. 8. Loss curve of ABOADL-IDS technique on NSLKDD2015 dataset.

CICIDS 2017 dataset	
Classes	**No. of instances**
Normal	50,000
Anomaly	50,000
Total instances	100,000

Table 3. Details of the CICIDS2015 dataset.

On the basis that the seagulls don't crash with one another, seagulls must shift towards the optimal location $M_s\,(t)$:

$$M_s\,(t) = B \times (P_{best}\,(t) - P_s\,(t)) \tag{10}$$

$P_{best}\,(t)$—optimal position for seagulls; B—random value that balances local and global optima;

$$B = 2 \times A^2 \times rd \tag{11}$$

rd—randomly generated integer [0,1].

(3) Move to the finest location

Once the abovementioned dual conditions are met, the seagull needs to travel towards the optimum location till it attains the newest location $D_s\,(t)$ that is formulated by the subsequent equation:

$$D_s\,(t) = |C_s\,(t) + M_s\,(t)| \tag{12}$$

Attack behavior
Seagulls use their weight and wings during migration to keep a specific altitude. They dive in a spiral movement near the target after discovering an objective to attack. These behaviours of seagulls in the air are represented as x , y, and z 3D planes:

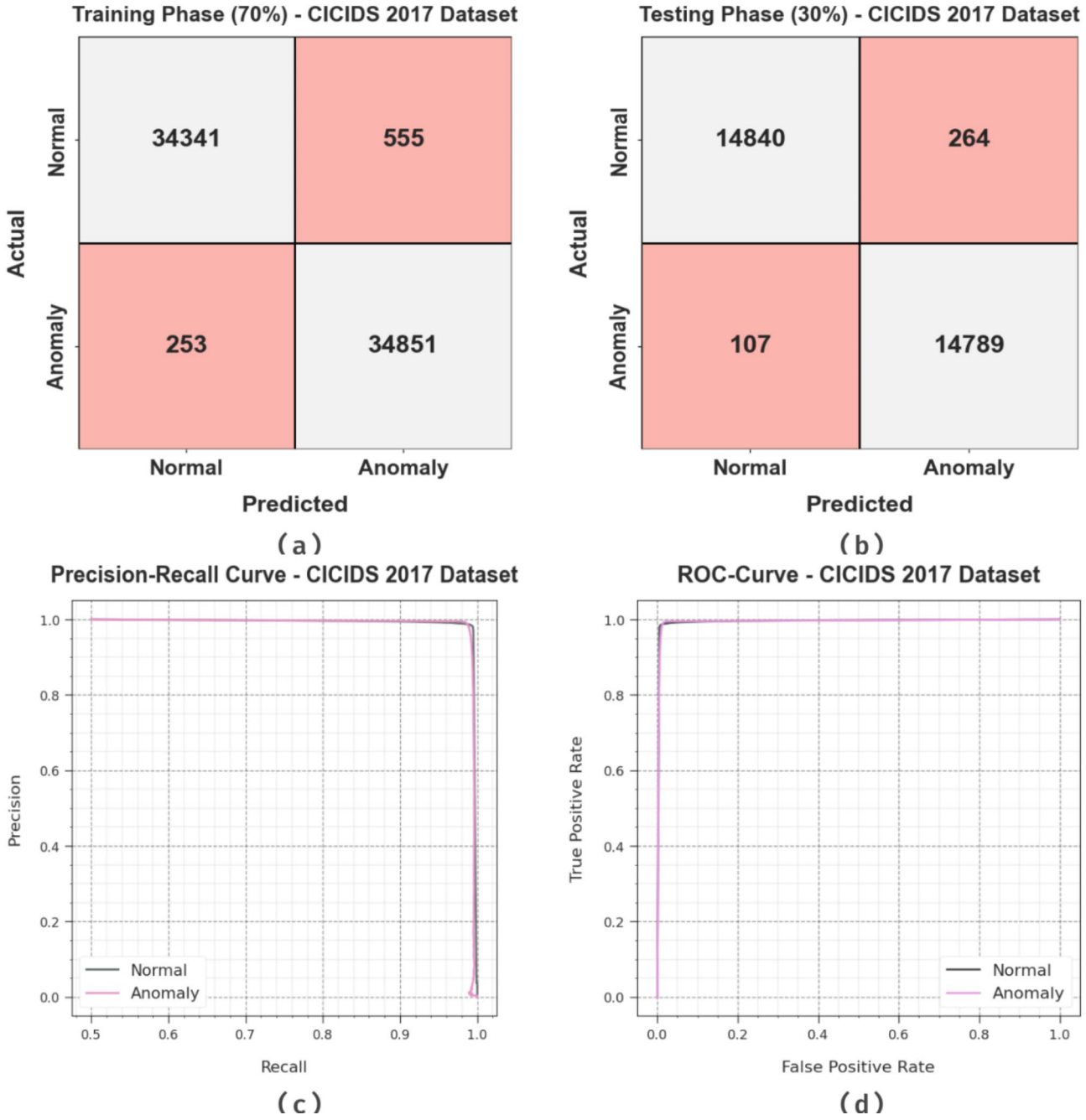

Fig. 9. CICIDS2015 dataset (**a**, **b**) Confusion matrices, (**c**, **d**) PR and ROC curves.

$$x = r \times \cos(\theta) \tag{13}$$

$$y = r \times \sin(\theta) \tag{14}$$

$$z = r \times \theta \tag{15}$$

$$r = u \times e^{\theta v} \tag{16}$$

r—the radius of the helix; θ angle value in [0,2π]; $u,\ nu$—correlation constant for helix;
Computation equation of seagull attack location:

$$P_s(t) = D_s(t) \times x \times y \times z + P_{best}(t) \tag{17}$$

CICIDS 2017 dataset					
Classes	$Accu_y$	$Prec_n$	$Recal$	F_{score}	AUC_{score}
70% TRAS					
Normal	98.41	99.27	98.41	98.84	98.84
Anomaly	99.28	98.43	99.28	98.85	98.84
Average	98.84	98.85	98.84	98.85	98.84
30% TESS					
Normal	98.25	99.28	98.25	98.77	98.77
Anomaly	99.28	98.25	99.28	98.76	98.77
Average	98.77	98.77	98.77	98.76	98.77

Table 4. Detection outcome of ABOADL-IDS technique on the CICIDS2015 dataset.

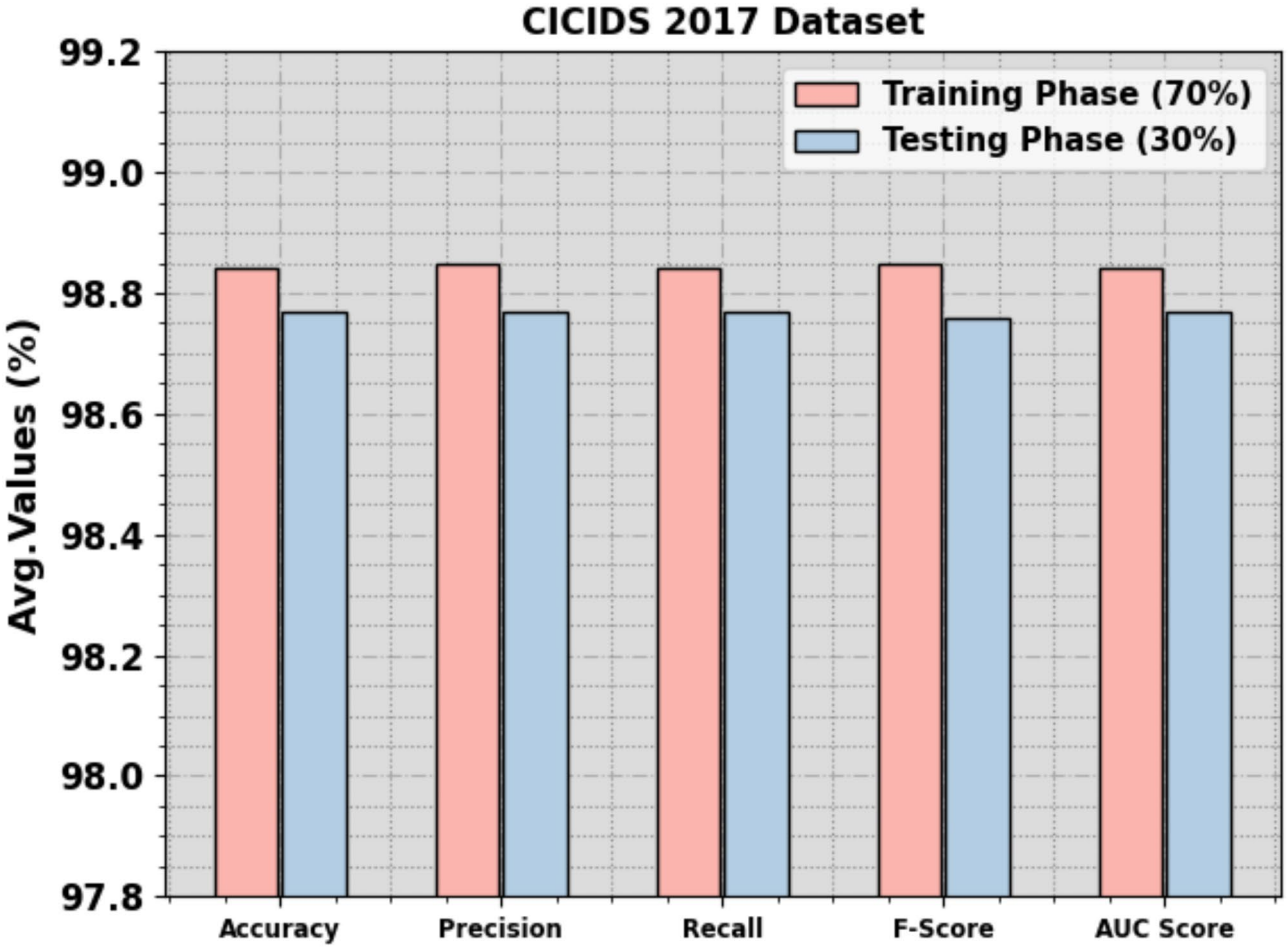

Fig. 10. Average of ABOADL-IDS technique on CICIDS2015 dataset.

The fitness function (FF) is a critical feature of the SGO technique. The encrypted solution is organized to calculate the best solution for candidate results. The accuracy values are the main state developed to project an FF.

$$Fitness = \max(P) \tag{18}$$

$$P = \frac{TP}{TP + FP} \tag{19}$$

FP and TP represent the positive values of false and true.

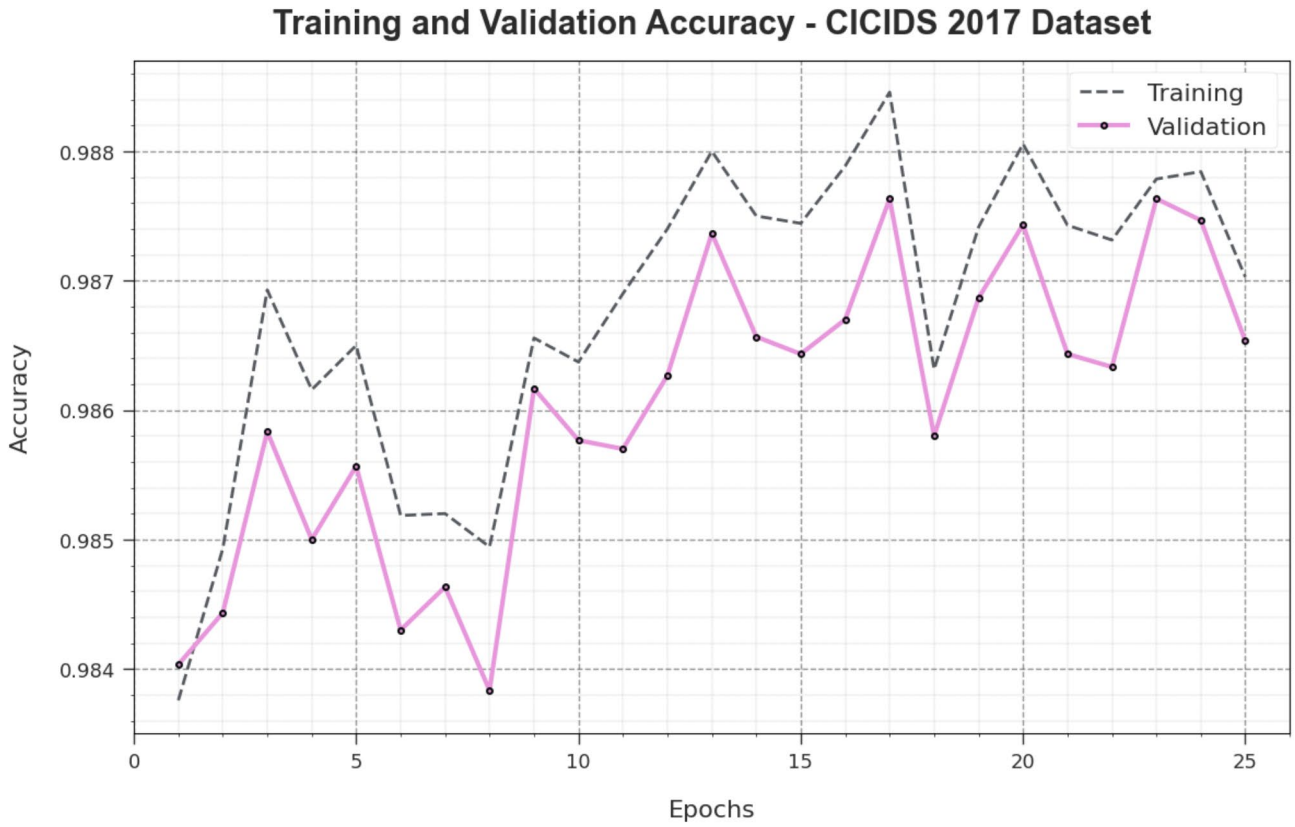

Fig. 11. $Accu_y$ curve of ABOADL-IDS technique on CICIDS2015 dataset

Results and discussion

This section examines the ABOADL-IDS methodology's recognition of intrusion results on dual databases: the NSLKDD2015 and CICIDS2015 datasets. Table 1 provides a comprehensive description of the NSLKDD2015 database.

Figure 5 illustrates the classifier study of the ABOADL-IDS approach in the NSLKDD2015 database. Figure 5a and b establishes the confusion matrices obtainable by the ABOADL-IDS approach on 70% of TRAS:30% of TESS. The simulation value indicated that the ABOADL-IDS method has exactly predicted and classified all two classes. In the same way, Fig. 5c displays the PR study of the ABOADL-IDS technique. The outcome value specified that the ABOADL-IDS method could reach greater PR analysis on 2 class labels. Yet, Fig. 5d determines the ROC performance of the ABOADL-IDS technique. The outcome signified that the ABOADL-IDS model had caused the abilities of simulated results with developed values of ROC in 2 classes.

The detection simulated result of the ABOADL-IDS approach on the NSLKDD 2015 dataset is revealed in Table 2; Fig. 6. The experimentation simulation displays that the ABOADL-IDS method accomplishes effective standard and anomaly classification. With a 70% TRAS, the ABOADL-IDS technique presents an average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 99.28%, 99.25%, 99.28%, 99.27%, and 99.28%, respectively. Also, with a 30% TESS, the ABOADL-IDS technique presents an average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 99.27%, 99.25%, 99.27%, 99.26%, and 99.27%, respectively.

To assess the performance of the ABOADL-IDS approach on the NSLKDD2015 dataset, the curves of TRAS and TESS $accu_y$ are definite, as revealed in Fig. 7. The TES and TRA $accu_y$ curves display the performance of the ABOADL-IDS model over many epochs. The figure provides facts about the task of learning and generalized skills of the ABOADL-IDS method. With an increase in epoch counts, it is experimental that the TES and TRA $accu_y$ curves get enhanced. It is shown that the ABOADL-IDS techniques get higher TES accuracy, which makes them able to categorize the designs in both data sets.

Figure 8 establishes the ample TES and TRA loss values of the ABOADL-IDS method on the NSLKDD2015 dataset over epochs. The TRA loss shows that the model loss obtained decreased over epochs. Initially, the loss value acquired decreases as the model alters the weight to decline the error of prediction on the TES and TRA data. The loss curves exhibit the level where the method fits the TRA data. Both data losses are slowly condensed, which signifies that the ABOADL-IDS technique proficiently absorbs the patterns revealed in the TRA and TES data. It is also experimental that the ABOADL-IDS technique adapts the parameters to decline the modification amid the prediction and new TRA label.

Table 3 exemplifies the detailed explanation of the CICIDS2015 database.

Figure 9 shows the classifier simulated analysis of the ABOADL-IDS methodology under the CICIDS2015 dataset. Figure 9a and b exemplifies the confusion matrices increased by the ABOADL-IDS methodology on

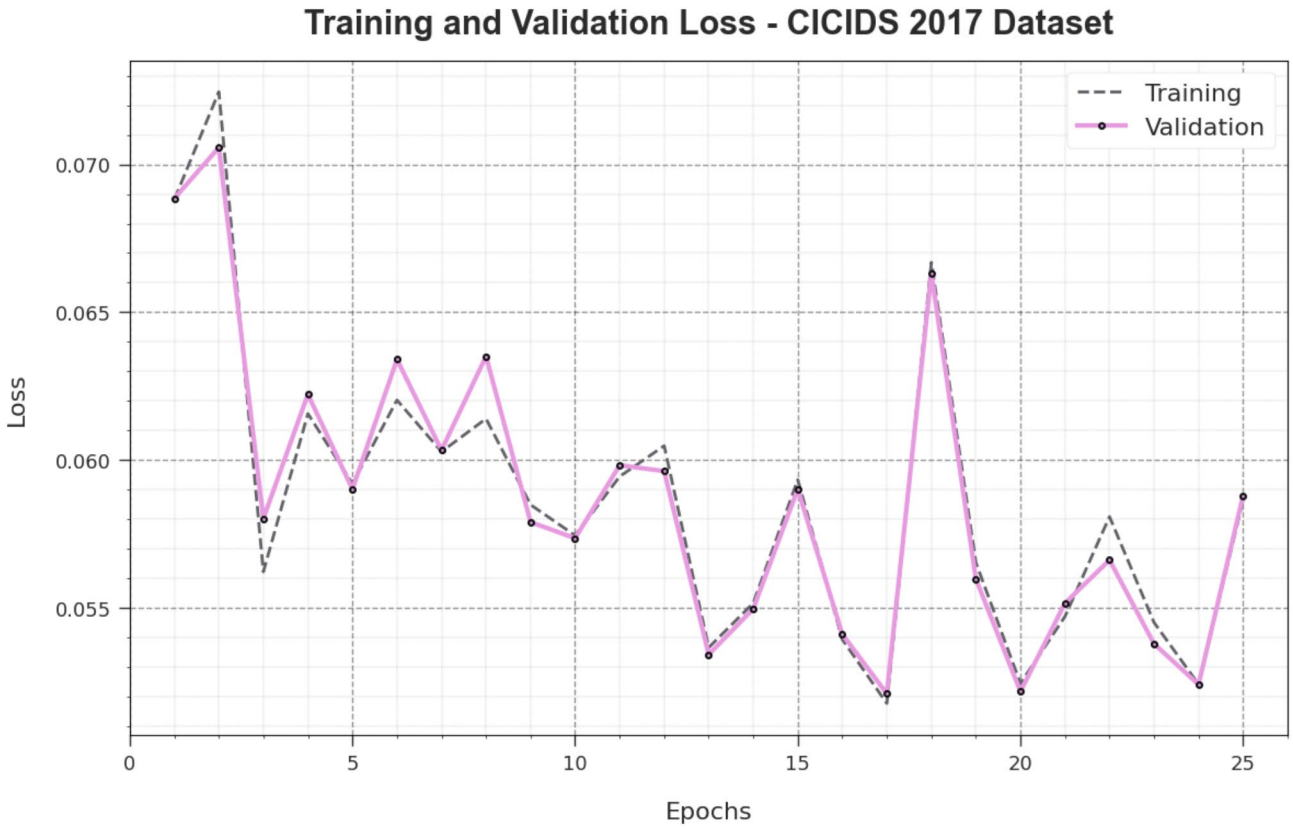

Fig. 12. Loss curve of ABOADL-IDS technique on CICIDS2015 dataset.

Models	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
ABOADL IDS	99.28	99.25	99.28	99.27
XAIIDS-CPS	98.87	98.95	98.87	98.91
FU-RIA	98.14	97.57	96.93	98.26
AERF	97.62	97.35	97.79	97.30
ForestPA	96.72	96.97	97.32	98.13
WI-SARD	96.64	97.58	97.29	98.65
G-SAE	97.63	95.97	98.39	98.19
LIBSVM	96.57	96.96	96.83	97.92

Table 5. Comparative analysis of ABOADL-IDS approach with existing models[11].

70% TRAS and 30% TESS. The simulation value indicated that the ABOADL-IDS model is well-known and that each 2-class label is classified precisely. Also, Fig. 9c determines the PR outcome of the ABOADL-IDS model. The result showed that the ABOADL-IDS model has better PR performance in 2 class labels. But, Fig. 9d describes the ROC study of the ABOADL-IDS technique. The experimental value described that the ABOADL-IDS technique generates excellent resultants with improved values of ROC in 2 classes.

The detection analysis of the ABOADL-IDS method on the CICIDS2015 dataset is exposed in Table 4; Fig. 10. The simulated result demonstrates that the ABOADL-IDS method gets effectual anomaly and normal classification. With a 70% TRAS, the ABOADL-IDS technique provides an average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 98.84%, 98.85%, 98.84%, 98.85%, and 98.84% correspondingly. Also, with a 30% TESS, the ABOADL-IDS technique provides an average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 98.77%, 98.77%, 98.77%, 98.76%, and 98.77% individually.

To calculate the execution of the ABOADL-IDS model on the CICIDS2015 database, TES and TRA $accu_y$ curves are well-said, as exposed in Fig. 11. The TES and TRA $accu_y$ curves show the concert of the ABOADL-IDS approach over some epochs. The figure provides meaningful facts about the tasks of learning and generalizer capacities of the ABOADL-IDS approach. With a rise in epoch counts, it is experimental that the TES and TRA $accu_y$ curves become higher. The ABOADL-IDS approach is perceived to have enhanced TES accuracy in classifying the designs in both data.

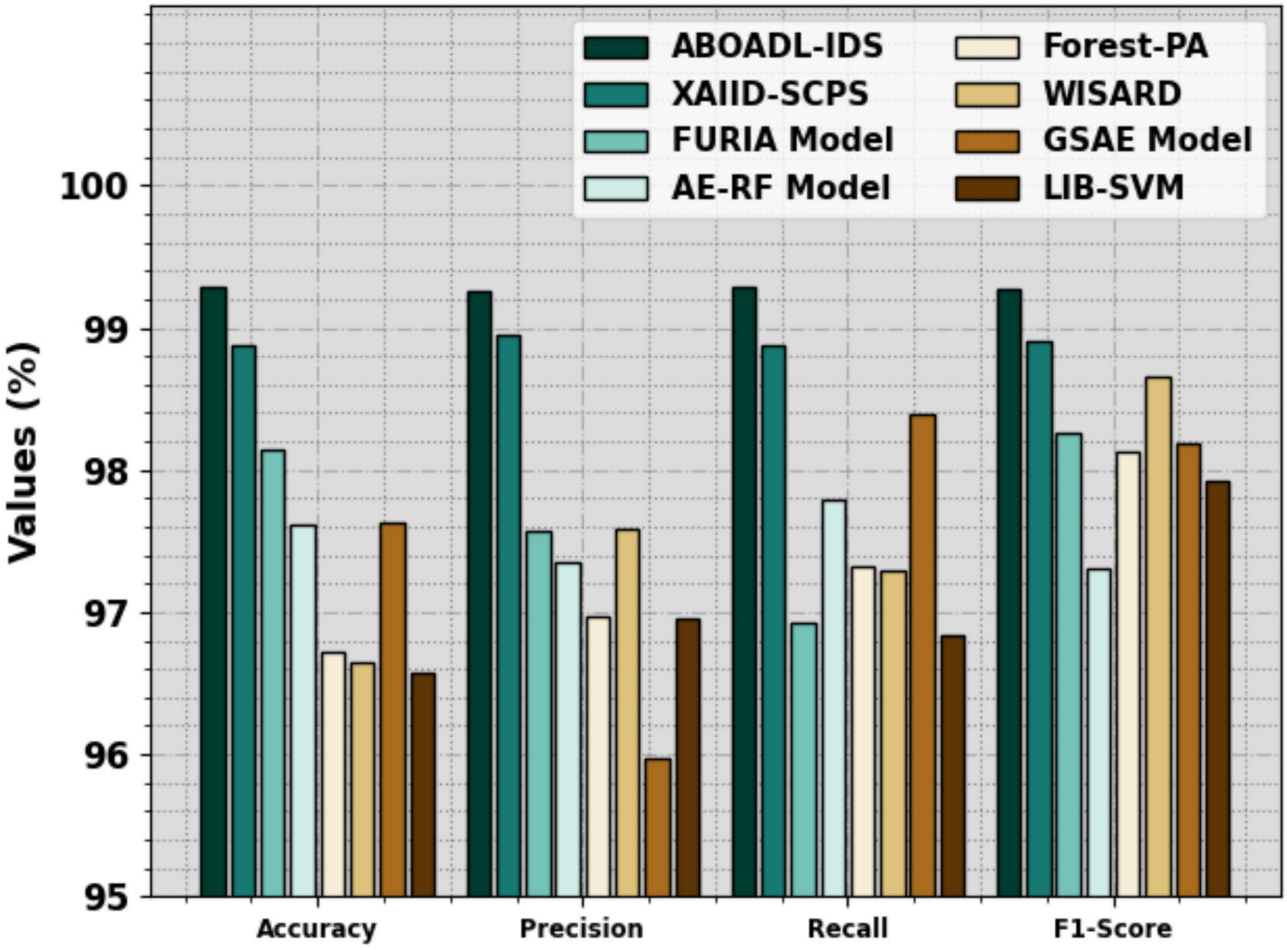

Fig. 13. Comparative outcome of ABOADL-IDS approach with existing models.

Figure 12 shows the complete TRA and TES loss values of the ABOADL-IDS approach on the CICIDS2015 dataset over epochs. The TRA loss demonstrated the method loss is minimized over epochs. Notably, the loss values get condensed as the model alters the weight to reduce the analytical mistakes in the TES and TRA data. The loss curves determine the range where the model fits the TRA. It is seen that both data loss is slowly reduced and represents that the ABOADL-IDS model well acquires the designs revealed in the TES and TRA data. It is also evidenced that the ABOADL-IDS regulates the parameters for reducing the modification amongst the new and forecast TRA classes.

The comparative recognition outcomes of the ABOADL-IDS model with existing techniques are performed in Table 5; Fig. 13[11]. The experimentation result indicates that the ForestPA, WI-SARD, and LIBSVM approaches have worse outcomes, but the AERF and G-SAE models have demonstrated better-increased performance. Concurrently, the XAIIDS-CPS and FU-RIA approaches have obtained considerable results. However, the ABOADL-IDS technique showed promising performance with maximum $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.28%, 99.25%, 99.28%, and 99.27%, respectively. Therefore, the ABOADL IDS technique is effective in achieving recognition results.

Conclusion

This paper presents automatic intrusion recognition using the ABOADL-IDS methodology in the CPS platform. The main intention of the ABOADL-IDS methodology is to utilize the FS with an optimal DL approach for the intrusion detection and identification procedure. It comprises data normalization, ABO-based FS, SDBN-based intrusion recognition, and SGO-based hyperparameter tuning. To select features, the ABOADL-IDS technique utilizes a new ABO approach for FS. Besides, the SDBN approach is used for intrusion detection and classification. To improve the solution of the SDBN model, the SGO method is implemented for the hyperparameter-selection process. The assessment of the ABOADL-IDS technique is accomplished under NSLKDD2015 and CICIDS2015 datasets. The performance validation of the ABOADL-IDS technique illustrated a superior accuracy value of 99.28% over existing models concerning various measures. The limitations of the ABOADL-IDS technique comprise the reliance on predefined datasets, which may not fully represent the diversity of real-world CPS environments and emerging cyber threats. Furthermore, the computational complexity of specific detection models can affect their real-time application, particularly in resource-constrained systems. The study also

assumes a relatively static system setup, which may not be effective in highly dynamic or evolving environments. Moreover, the feature selection process may not capture all relevant patterns, resulting in suboptimal detection accuracy in some cases. Future work should concentrate on developing adaptive models that can continuously learn and update in real time, improving their capability to detect previously unseen attacks. Also, improving model efficiency to balance detection accuracy with computational feasibility will be significant for large-scale implementations. Lastly, integrating privacy-preserving techniques while maintaining high detection performance should be a key focus in future research.

Data availability

The datasets used and analyzed during the current study available from the corresponding author on reasonable request.

Received: 18 June 2024; Accepted: 20 February 2025
Published online: 25 March 2025

References

1. Nour, A. A. et al. Optimizing intrusion detection in industrial cyber-physical systems through transfer learning approaches. *Comput. Electr. Eng.* **111**, 108929 (2023).
2. Alqaralleh, B. A., Aldhaban, F., AlQarallehs, E. A. & Al-Omari, A. H. Optimal machine learning enabled intrusion detection in cyber-physical system environment. *Comput. Mater. Contin.* **72**(3), 4691–4707 (2022).
3. Colelli, R., Magri, F., Panzieri, S. & Pascucci, F. June. Anomaly-based intrusion detection system for cyber-physical system security. In *2021 29th Mediterranean Conference on Control and Automation (MED)* 428–434 (IEEE, 2021).
4. Mboweni, I. V., Ramotsoela, D. T. & Abu-Mahfouz, A. M. Hydraulic data preprocessing for machine learning-based intrusion detection in cyber-physical systems. *Mathematics* **11**(8), 1846 (2023).
5. Panigrahi, R. et al. Intrusion detection in a cyber–physical environment using hybrid Naïve Bayes—Decision table and multi-objective evolutionary feature selection. *Comput. Commun.* **188**, 133–144 (2022).
6. Alqazzaz, A. & Alrashdi, I. An efficient intrusion detection model based on neutrosophic logic for optimal response from the arranged response set. *Int. J. Neutrosophic Sci. IJNS* **23**(3) (2024).
7. Santos, V. F., Albuquerque, C., Passos, D., Quincozes, S. E. & Mossé, D. Assessing machine learning techniques for intrusion detection in cyber-physical systems. *Energies* **16**(16), 6058 (2023).
8. Zainudin, A., Akter, R., Kim, D. S. & Lee, J. M. Towards lightweight intrusion identification in SDN-based industrial cyber-physical systems. In *2022 27th Asia Pacific Conference on Communications (APCC)* 610–614 (IEEE, 2022).
9. Li, W., Wang, Y. & Li, J. A blockchain-enabled collaborative intrusion detection framework for SDN-assisted cyber-physical systems. *Int. J. Inf. Secur.* 1–12 (2023).
10. Dutta, A. K., Negi, R. & Shukla, S. K. Robust multivariate anomaly-based intrusion detection system for cyber-physical systems. In *Cyber Security Cryptography and Machine Learning: 5th International Symposium, CSCML 2021, Be'er Sheva, Israel, July 8–9, 2021, Proceedings 5* pp. 86–93 (Springer International Publishing, 2021).
11. Almuqren, L. et al. Explainable artificial intelligence enabled intrusion detection technique for secure cyber-physical systems. *Appl. Sci.* **13**(5), 3081 (2023).
12. Althobaiti, M. M., Kumar, K. P. M., Gupta, D., Kumar, S. & Mansour, R. F. An intelligent cognitive computing based intrusion detection for industrial cyber-physical systems. *Measurement* **186**, 110145 (2021).
13. Mittal, H. et al. A new intrusion detection method for cyber–physical system in emerging industrial IoT. *Comput. Commun.* **190**, 24–35 (2022).
14. Khan, I. A. et al. A privacy-conserving framework based intrusion detection method for detecting and recognizing malicious behaviours in cyber-physical power networks. *Appl. Intell.* 1–16 (2021).
15. Kukkala, V. K., Thiruloga, S. V. & Pasricha, S. Real-time intrusion detection in automotive cyber-physical systems with recurrent autoencoders. In *Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems* 317–347 (Springer International Publishing, 2023).
16. Alohali, M. A. et al. Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cogn. Neurodyn.* **16**(5), 1045–1057 (2022).
17. Eltanbouly, S. S. Multimodal intrusion detection system for cyber physical systems. Master's thesis (2021).
18. Safavat, S. & Rawat, D. B. Asynchronous federated learning for intrusion detection in vehicular cyber-physical systems. In *IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* 1–6 (IEEE, 2023).
19. Shi, B. et al. Prediction of recurrent spontaneous abortion using evolutionary machine learning with joint self-adaptive sime mould algorithm. *Comput. Biol. Med.* **148**, 105885 (2022).
20. Ji, R., Selwal, A., Kumar, N. & Padha, D. Cascading bagging and boosting ensemble methods for intrusion detection in cyber-physical systems. *Secur. Priv.* **8**(1), e497 (2025).
21. Arumugam, S. R., Paul, P. M., Issac, B. J. J. & Ananth, J. P. Hybrid deep architecture for intrusion detection in cyber-physical system: An optimization-based approach. *Int. J. Adapt. Control Signal Process.* **38**(9), 3016–3039 (2024).
22. Chen, M. R., Yang, L. Q., Zeng, G. Q., Lu, K. D. & Huang, Y. Y. IFA-EO: An improved firefly algorithm hybridized with extremal optimization for continuous unconstrained optimization problems. *Soft. Comput.* **27**(6), 2943–2964 (2023).
23. Abinash, S., Srivatsan, N., Hemachandran, S. K. & Priyanga, S. HGCNN-LSTM: A data-driven approach for cyberattack detection in cyber-physical systems. *SN Comput. Sci.* **6**(1), 69 (2025).
24. Feng, Y., Xu, Y., Hu, Q., Krishnamoorthy, S. & Tang, Z. Predicting vacant parking space availability zone-wisely: A hybrid deep learning approach. *Complex. Intell. Syst.* **8**(5), 4145–4161 (2022).
25. Al Mazroa, A., Albogamy, F. R., Ishak, M. K. & Mostafa, S. M. Boosting cyberattack detection using binary metaheuristics with deep learning on cyber-physical system environment. *IEEE Access* (2025).
26. Rahim, S. A. & Manoharan, A. Fractional artificial Protozoa optimization enabled deep learning for intrusion detection and mitigation in cyber-physical systems. *IEEE Access* (2024).
27. Chen, C. et al. Hybrid 3DMA for multi-user MIMO-VLC. *J. Opt. Commun. Netw.* **14**(10), 780–791 (2022).
28. Markkandeyan, S. et al. Novel hybrid deep learning based cyber security threat detection model with optimization algorithm. *Cyber Secur. Appl.* **3**, 100075 (2025).
29. Gurumoorthy, S., Kokku, A. K., Falkowski-Gilski, P. & Divakarachari, P. B. Effective air quality prediction using reinforced swarm optimization and bi-directional gated recurrent unit. *Sustainability* **15**(14), 11454 (2023).
30. Gulić, M. & Žuškin, M. Enhancing metaheuristic optimization: A novel nature-inspired hybrid approach incorporating selected pseudorandom number generators. *Algorithms* **16**(9), 413 (2023).
31. Ibrahim, A. et al. Wind speed ensemble forecasting based on deep learning using adaptive dynamic optimization algorithm. *IEEE Access* **9**, 125787–125804 (2021).

32. Li, T. H. S. et al. Deep belief network–based learning algorithm for humanoid robot in a pitching game. *IEEE Access* **7**, 165659–165670 (2019).
33. Xue, J., Liu, X., Xu, H. & Zhang, D. Research on the seagull optimization algorithm-based convolutional neural network rolling bearing fault diagnosis method. *Eng. Res. Express* **5**(3), 035050 (2023).

Acknowledgements
This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00337489, Development of data drift management technology to over comeperformance degradation of AI analysis models).

Author contributions
E.L.L.: Conceptualization, Methodology, formal analysis, writing—original draft preparation; S.N.S.V.S.C.R.: Conceptualization, Methodology, data curation; V.D.: Methodology, software, validation, investigation; G.J.M.: software, formal analysis, data curation, investigation; S.C.: validation, investigation, visualization, supervision; S.A.: validation, visualization, supervision, writing-review and editing; C.Y.: data curation, resources, supervision, project administration, funding acquisition.

Declarations

Competing interests
The authors declare no competing interests.

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

Additional information
Correspondence and requests for materials should be addressed to S.A. or C.Y.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.