International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8180
***Article Received:** 26 June 2023 **Revised:** 22 August 2023 **Accepted:** 06 September 2023*

Heuristic Optimization Algorithm with Ensemble Learning Model for Intelligent Intrusion Detection and Classification

[1,*]K. Hemavathi, [2]Dr. R. Latha
[1]Research Scholar, Department of Computer Science,
St. Peter's Institute of Higher Education and Research, Chennai.
hemavathibhavani@gmail.com
[2]Professor and Head, Department of Computer Science,
St. Peter's Institute of Higher Education and Research, Chennai.
latharamavel@gmail.com

Abstract—Intrusion Detection (ID) for network security prevents and detects malicious behaviours or unauthorized activities that occurs in the network. An ID System (IDS) refers to a safety tool that monitors events or network traffic for responding to and identifying illegal access attempts or malevolent activities. IDS had a vital role in network security by finding and alerting security teams or administrators about security breaches or potential intrusions. Machine Learning (ML) methods are utilized for ID by training methods for recognizing behaviours and patterns linked with intrusions. Deep Learning (DL) methods are implemented to learn complicated representations and patterns in network data. DL methods have witnessed promising outcomes in identifying network intrusions by automatically learning discriminatory features from raw network traffic. This article presents a new Teaching and Learning based Optimization with Ensemble Learning Model for Intelligent Intrusion Detection and Classification (TLBOEL-IDC) technique. The presented TLBOEL-IDC method mainly detects and classifies the intrusions in the network. To attain this, the TLBOEL-IDC method primarily preprocesses the input networking data. Besides, the TLBOEL-IDC technique involves the design of an ensemble classifier by the integration of three DL models called Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Bidirectional LSTM (BLSTM). Moreover, the hyperparameter tuning of the DL models takes place using the TLBO approach that improves the overall ID outputs. The simulation assessment of the TLBOEL-IDC approach takes place on a benchmark dataset and the outputs are measured under various factors. The comparative evaluation emphasized the best accomplishment of the TLBOEL-IDC technique over other present models by means of diverse metrics.

Keywords- Network security; Teaching and learning-based optimization; Intrusion detection system; Ensemble learning; Deep learning.

I. INTRODUCTION

With a growing diverse and digital atmosphere, it became highly complex to protect private data utilizing conventional safety solutions. In recent years, several cyberattacks on computer networks have increased [1]. Different techniques for finding abnormal activities of the network with intrusive behaviours that includes changing tendency, obscurity, variety, and entanglement were continuously developing [2]. Lately, the accuracy of ID and preventing measures was considerably improved with the utilization of artificial intelligence-related methodologies. The IDS refers to a mechanism which monitors traffic in a network to identify abnormal or malicious activity and then take preventive actions against intrusion threats [3]. IDS are categorized into two different kinds: HIDS and NIDS. The NIDS can be often positioned or applied at critical network points to ensure that it covers traffic that can be susceptible to attacks, while the HIDS system functions on any gadgets in the networking system that has access to internet. There exist two fundamental methods for identifying intrusions, such as signature-based and anomalies based [4]. Signature-based IDS is to update the sign dataset to the zero-day attack pattern regularly and focus on finding signature patterns of intrusion occurrence.

The anomaly-based IDS compare the trustworthy behavioural pattern with new behaviour depending on regular activity monitoring [5]. Once the manager receives an alert from the IDS, it exploits Intrusion Prevention System (IPS) to avoid outbreaks namely DDoS attacks, Trojan horses, etc. [6]. Anomaly detection has the benefit of identifying unknown attacks instead of depending on the signature profiles of known attacks. For such reasons, a considerable amount of effort has been dedicated to the improvement of anomaly detection IDSs related to DL and ML methods [7]. DL relies on an Artificial Neural Network (ANN), while the ML technique has a relatively simple structure. DL method has outperformed the classical ML technique while engaging with a massive set of data [8]. Furthermore, the ML method requires human intervention for feature extraction to accomplish more effective outcomes.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8180
***Article Received:** 26 June 2023 **Revised:** 22 August 2023 **Accepted:** 06 September 2023*

Manual feature engineering is unrealistic with large-scale and multidimensional data due to the rapid expansion in transmitted traffic [9]. DL approaches could obtain feature representation from datasets without human interference for generating better outcomes. Conventional ML methods are frequently represented as shallow models, due to the simple structure. A deep structure that has several hidden layers is one differentiating feature of the DL model. But due to the complex structure, multi-layer DL models require substantial processing numbers and computation time [10].

This article presents a new Teaching and Learning based Optimization with Ensemble Learning Model for Intelligent Intrusion Detection and Classification (TLBOEL-IDC) technique. The presented TLBOEL-IDC method detects and classifies the intrusions in the network. To attain this, the TLBOEL-IDC method primarily preprocesses the input networking data. Besides, the TLBOEL-IDC technique involves the design of an ensemble classifier by the integration of three DL models called Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Bidirectional LSTM (BLSTM). Moreover, the hyperparameter tuning of the DL models takes place using the TLBO approach that improves the overall ID outputs. The simulation assessment of the TLBOEL-IDC approach takes place on a benchmark dataset and the outputs are measured under various factors.

II. RELATED WORKS

Rao and Suresh Babu [11] devise an Imbalanced GAN (IGAN) to overcome the class imbalance problem by maintaining efficiency and raising the recognition rate of minority classes. For limiting the impact of the maximal or minimal value on the attributes, the initial dataset has been standardized and one-hot encoded utilizing data pre-processing. Rani and Gagandeep [12] present a DNN that uses classifier-level class imbalance solutions to figure out this issue efficiently. By using data conversion and the min-max normalization model, the network data was pre-processed. After, normalized data was given to NN, in which the function of cross-entropy was altered for solving the issue of class imbalance.

Fu et al. [13] present a method for traffic AD called a DL method for Network ID (DLNID) that integrated the Bi-LSTM network and attention mechanism, first deriving sequence features of data traffic using CNN networks, then reallocating weights of all channels using the attention system, and eventually utilizing Bi-LSTM for learning network of sequence features. Mbow e al. [14] devise a hybrid method for managing the imbalance issue. This hybrid model was an integration of oversampling with Tomek link and SMOTE, an under-sampling approach for minimizing noises. Also, this study utilizes two DL methods like CNN and LSTM to offer a better ID mechanism. Al-Essa and Appice [15] inspect the oversampling effect combined to feature selection, to comprehend how feature relevance can vary because of the artificial rare sample creation.

Bedi et al. [16] introduces Siam-IDS that was an IDS dependent on Siamese-NN. The presented method can identify U2R and R2L attacks without making use of conventional class balancing methods like random undersampling and oversampling. The performances of Siam-IDS were compared with prevailing IDS utilizing DL methods like CNN and DNN. Gupta et al. [17] devised LIO-IDS depending on the LSTM method and enhanced One-to-One method to handle infrequent and frequent network intrusions. LIO-IDS can be referred to as a 2 levelled layer Anomaly-based NIDS (A-NIDS) that finds several IDs in the networking with low computational time and high accuracy. LIO-IDS model's first layer finds intrusion from traffic of the network through the LSTM classifiers. Layer 2 utilizes collective approaches for classifying detected intrusions into various attack classes.

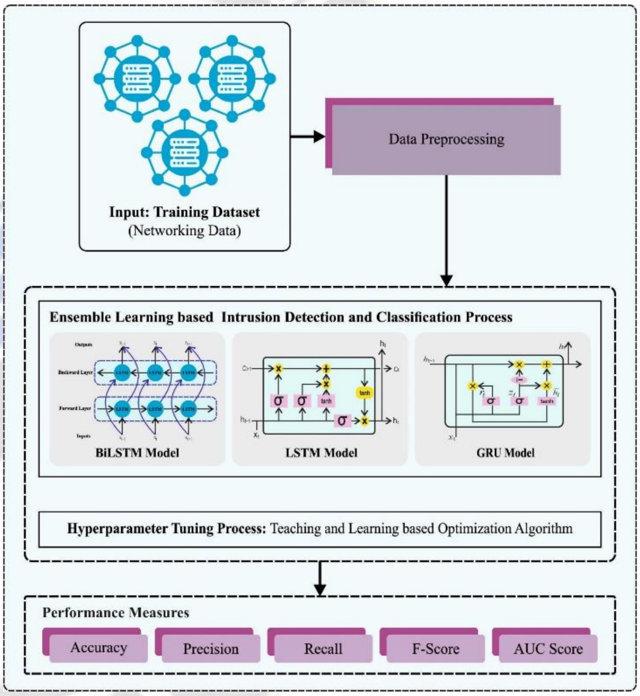

Input: Training Dataset
(Networking Data)
Data Preprocessing
Ensemble Learning based Intrusion Detection and Classification Process
BiLSTM Model
LSTM Model
GRU Model
Hyperparameter Tuning Process: Teaching and Learning based Optimization Algorithm
Performance Measures
Accuracy
Precision
Recall
F-Score
AUC Score

Figure 1. Overall flow of TLBOEL-IDC method

III. THE PROPOSED MODEL

In the current article, an automatic IDS, termed the TLBOEL-IDC technique is introduced. The presented TLBOEL-IDC approach mainly detects and classifies the intrusions in the network. To achieve this, the TLBOEL-IDC technique encompasses three major processes such as data preprocessing, ensemble learning and TLBO based tuning and classification procedure. Fig. 1 illustrates the working flow of the TLBOEL-IDC methodology.

A. Data Preprocessing

Z-score normalization, also termed standardization, is a technique used to rescale numerical data so that it has a standard deviation and mean of 1 and 0. This normalization method transforms the data to a standard distribution, making it easier to compare and analyze variables with different scales. The formula for computing the z-score of the data point is given as follows:

$$z = (x - \mu)/\sigma \tag{1}$$

where: z is the standardized value (z-score), x, μ, and σ indicates the dataset's original data point, mean, and standard deviation. For imbalanced data handling, the Conditional Generative Adversarial Network (CGAN) technique is utilized to stabilizing the instance numbers in the dataset.

B. Ensemble Learning-Based Classification

In this work, the ensemble learning process takes place for the identification of the intrusions in the network. The TLBOEL-IDC approach involves the design of an ensemble classifier by the integration of three DL models namely GRU, LSTM, and BiLSTM. Majority voting is considered the most effective and easier approach to incorporating the predictions created by various approaches [18]. In majority voting, all the class votes can be computed over the input classifier, and the majority class can be selected. The rule for selecting classifiers was to make an ensemble instead of using all the classifiers tested in dissimilar ways. There were 3 kinds of majority voting in that the ensemble could, firstly, elect the class "unanimous vote" where the overall classifiers approve; next, the easy majority where a similar forecast was done; and then, plurality voting. In such cases, majority voting can be used.

Consider a trained set, and a classifier series as $h_1, h_2, \ldots, h_n$, and all the classifiers are attained on a trained set. Thus, after the trained set, the classifiers make a forecast. The classifier h_1 generates the ratio of prediction and classifier as $h_1 : h_2 : h_n$ and $y_1 : y_2 : y_n$. It takes n predictions to the new data point. Then, it takes voting to attain the last prediction. Voting reduces n-class prediction to a single data point as a single class. Hence, major number of voting is used to determine the ultimate voting. The operation mode was utilized to gain the final voting that is expressed as follows:

$$y_f = mode\{h_1(x), h_2(x), \ldots, h_n(x)\} \tag{2}$$

Whereas $h_i(x) = y_i(x)$.

Utilizing majority voting was similar to questioning a group of experts for voting on a particular solution. Once the major number of members provides their vote, the solution is acknowledged. In this model, the probability of making any anticipation errors can be insignificant.

1) Gated Recurrent Units

Conventional RNN architecture suffers from rising and vanishing gradients; this makes optimizing process more complex and prevents the network from learning long-term dependency [19]. Various RNN modifications were introduced to address this issue, the most popular of which is LSTM. Compared to LSTM, GRU have better performance, requires fewer parameters, and is easy to implement.

Where reset (α_t), update (β_t) and output (h) are gates at t time. W_α, W_β, $w_{\hat{h}}$ and W_o designate the weight for the output and input of the models. The output of gates h_t and h_{t-1} are output at t and $t-1$ times, the activation functions $(\sigma,\ \tanh)$, and Input (X) is at t time correspondingly. $\hat{y}_t$ demonstrates the training instance output at time t.

$$\alpha_t = \sigma\left(W_\alpha \cdot \left[\hat{h}_{t-1'} X_t\right]\right) \tag{3}$$

$$\beta_t = \sigma\left(W_\beta \cdot \left[\hat{h}_{t-1'} X_t\right]\right) \tag{4}$$

$$h_t = \tan h\left(W_{\hat{h}} \cdot \left[\alpha_t * \hat{h}_{t-1},\ X_t\right]\right) \tag{5}$$

$$\hat{h}_t = (1 - \beta_t) * \hat{h}_{t-1} + z_t * h_t \tag{6}$$

$$\hat{y}_t = \sigma\left(w_o \cdot \hat{h}_t\right) \tag{7}$$

2) Long Short-Term Memory

The LSTM model proposes a unique configuration called a memory cell which comprises four building blocks: an output, neuron, forget, and input gates with self-recurrent architecture. The capability of cells to access and store data for a long duration. Using the following equations, the hidden state is evaluated by the LSTM model:

$$i = \sigma(x_n U^i + s_{n-1} W^i) \tag{8}$$

$$f = \sigma(x_n U^f + s_{n-1} W^f) \tag{9}$$

$$\mathrm{o} = \sigma(x_n U^o + s_{n-1} W^o) \tag{10}$$

$$g = \tanh(x_n U^g + s_{n-1} W^g) \tag{11}$$

$$c_n = c_{n-1} \circ f + g \circ i \tag{12}$$

$$s_n = \tanh(c_n) \circ \mathrm{o} \tag{13}$$

$$y = soft\max(Vs) \tag{14}$$

Generally, a neural network is implemented namely FFNN along with RNN. An FFNN was an ANN in which the result of any layer does not disturb the entire performances of a similar layer, viz., there are no cycle formed by the links between both units. But FFNN is processed in the network by the output and input layers.

3) Bidirectional LSTMs

The BLSTM model can be a sequence of processing that involves both LSTM models: the initial act and the next one in a forward and backward direction. BLSTM efficiently improve the amount of data obtainable to the network, which gives the model more context. The BLSTM structure comprises hidden, forward and backward layers. In the BLSTM structure, σ denotes the activation functions of the layer, and y and x represents the output and input, correspondingly.

C. Hyperparameter Tuning

To adjust the DL model's tuning values, the TLBO approach was exploited in this work. TLBO model aims to utilize the metaheuristic, population-based, optimization process to simulate the standard learning environment [20]. In fact, while

Article Received: *26 June 2023* ***Revised:*** *22 August 2023* ***Accepted:*** *06 September 2023*

duplicating the classroom atmosphere, the TLBO method selects, from the student class, called learners, the maximum learners as teachers. The learners slowly enhance their knowledge due to the input of teachers. Thus, learners and teachers constitute two fundamental components.

On the other hand, a class of learners was determined as$P$ and $P_G = [X_{1,G}, X_{2,G}, \dots, X_{N_p,G}]$ where G denotes the generation in question, $X_{i,G}$ the individual number vector, and N_p, the population sizes. The dimension of the subject is called D, $X_{i,G} = [x_{1i,G}, x_{2i,G}, \dots, x_{Di,G}]^T$ determines every vector $X_{i,G} (i = 1,2, \dots, N_p)$ as an individual of generation G.

$$P_{i,j}^{0} = P_j{}^{\min} + rand * \left(P_j{}^{\max} - P_j{}^{\min}\right) \qquad (15)$$

Where P^0 denotes the randomly initialized population. In such cases, $P_j{}^{\max}$ and $P_j{}^{\min}$ represent the maximum and minimum values, $rand\ a(0,1)$ ranged uniform distributed random parameter.

In the TLBO model, this definition leads to the observation that no model-specific parameter was needed, which distinguishes the latter from its counterparts, while enabling proper tuning accessibility and less complexity. Moreover, as before mentioned, the population size and the number of generations is the only common controlling parameter required for these certain process. Generally, the TLBO technique includes a Teacher and a Learner Phase. A comprehensive discussion of these particular modes is given below.

Teacher Phase

The aim is to upgrade the learner's knowledge to an amount equivalent to that of teachers. Yet, the practice displays the teacher's role as a knowledge transmitter, the one, rather than concentrating on the performances of the individual learner, work toward in rising the normal results of the learner populace. Moreover, the knowledge-share method can be aided by teacher-learner interaction.

Subsequently, the teacher, nominated as $X_{t,G}$ represents the learner with the optimum fitness amongst the learner's population, in a certain generation G. A teacher phase vector $V_{i,G} = [v_{1i,G}, v_{2i,G}, \dots, v_{Di,G}]^T$ is produced using the following expression:

$$V_{\mathrm{i},G} = X_{i,G} + r_i\left(X_{t,G} - T_F M_G\right) \qquad (16)$$

In Eq. (16), a random number $r_i \in (0,1)$, $i = 1,2,\ N_p$, a mean vector of each individual in the generation populace, M_G, and learning weight, values at either 1 or 2, $T_F = round[1 + rand(O,1)\{2-1\}]$ are added. This formula enables a novel solution to be produced based on the prior optimal solution and the mean of the population.

Then, $G+1$ was represented as the following iteration of generation G, along with new individuals $X_{i,G+1}$ $(i = 1,2, N_p)$ of the population $P_G + 1$, chosen by the subsequent formula:

$$X_{i,G+1} = \begin{cases} X_{i,G}, & if\ f\left(X_{i,G}\right) \le f\left(V_{\iota',G}\right), \\ V_{i,G}, & otherwise \end{cases} \qquad (17)$$

In Eq. (17), $f(\cdot)$ denotes the fitness function. Greedy selection is the process of the abovementioned formula.

Learner Phase

In this stage, learners make interaction among them in addition to their teacher, thereby improving their knowledgebase. A further intellectual learner assists in upgrading the knowledgebase of other learners. Every learner compares their knowledge with another learner in their class. This results in unchanged, additional, or rectified knowledge in the learner's grasp.

Therefore, the specific learner can be detected by the learner phase vector $U_{i,G} = [u_{1i,G}, u_{2i,G}, \dots, u_{Di,G}]^T$, based on the following equation:

$$U_{i,G} = \begin{cases} X_{m,G} + r_m\left(X_{m,G} - X_{n,G}\right) & if\ f\left(X_{m,G}\right) < f\left(X_{n,G}\right), \\ X_{m,G} + r_m\left(X_{m,G} + X_{n,G}\right) & otherwise \end{cases} \qquad (18)$$

If $m \neq n$, then random integer $r_m \in (0,1)$, and two individuals attained from the random selection in the generation populace G, $X_{m,G}$ and $X_{n,G}$, are observed.

Gradually, $G+1$ is represented as the next iteration of the generation G, along with novel individuals $X_{i,G+1}$ $\left(i = 1,2, N_p\right)$ of the population P_{G+1}, chosen by the subsequent formula:

$$X_{i,G+1} = \begin{cases} X_{i,G} & if\ f(X_{i,G}) \le f(U_{i,G}), \\ U_{i,G} & otherwise \end{cases} \qquad (19)$$

In Eq. (19), $f(\cdot)$ denotes the fitness function. Like the teacher phase, this equation also enables greedy selection. Fig. 2 displays the flowchart of TLBO.

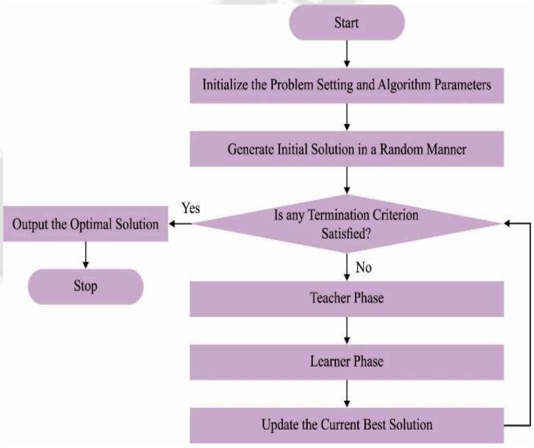

Start
Initialize the Problem Setting and Algorithm Parameters
Generate Initial Solution in a Random Manner
Is any Termination Criterion Satisfied?
Yes
Output the Optimal Solution
Stop
No
Teacher Phase
Learner Phase
Update the Current Best Solution

Figure 2. Flowchart of TLBO

The selection of fitness is a main element in the TLBO methodology. Solution encoding was leveraged to evaluate the progress of the candidate solution. The value of accuracy is the primary conditions applied to build the FF.

$$Fitness = \max(P) \qquad (20)$$

DOI: https://doi.org/10.17762/ijritcc.v11i11s.8180
***Article Received:** 26 June 2023 **Revised:** 22 August 2023 **Accepted:** 06 September 2023*

$$P = \frac{TP}{TP + FP} \qquad (21)$$

From the expression, FP and TP denote the false and the true positive values.

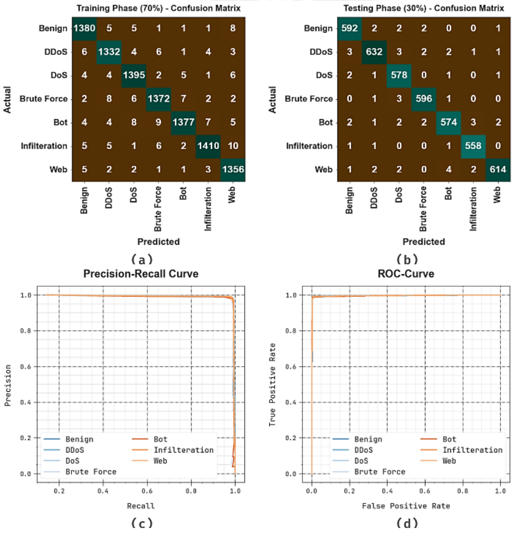
IV. RESULTS AND DISCUSSION

In the current segment, the simulation outputs of the TLBOEL-IDC method are investigated on the dataset namely CSE CICIDS2018 [21] that comprises 13995 instances with 7 classes as provided in Table 1. In addition, CGAN is used to balance the dataset.

TABLE I. DETAILS OF DATABASE

Class	No. of Samples
Benign	2000
DDoS	2000
DoS	2000
Brute Force	2000
Bot	2000
Infiltration	2000
Web	1995
Total Samples	13995

Fig. 3 portrays the classifier outcomes of the TLBOEL-IDC approach under testing dataset. Figs. 3a-3b depicts the confusion matrix presented by the TLBOEL-IDC approach on 70:30 of TRP/TSP. The figure portrayed that the TLBOEL-IDC technique has recognized and categorized all 7 classes precisely. Also, Fig. 3c shows the PR study of the TLBOEL-IDC technique. The figures stated that the TLBOEL-IDC approach portrayed greater PR achievement under 7 classes. Finally, Fig. 3d portrayed the ROC analysis of the TLBOEL-IDC approach. The figure depicted that the TLBOEL-IDC method has greater outcomes with greater values of ROC under 7 classes.



Training Phase (70%) - Confusion Matrix

Actual \ Predicted	Benign	DDoS	DoS	Brute Force	Bot	Infilteration	Web
Benign	1380	5	5	1	1	1	8
DDoS	6	1332	4	6	1	4	3
DoS	4	4	1395	2	5	1	6
Brute Force	2	8	6	1372	7	2	2
Bot	4	4	8	9	1377	7	5
Infilteration	5	5	1	6	2	1410	10
Web	5	2	2	1	1	3	1356

Testing Phase (30%) - Confusion Matrix

Actual \ Predicted	Benign	DDoS	DoS	Brute Force	Bot	Infilteration	Web
Benign	592	2	2	2	0	0	1
DDoS	3	632	3	2	2	1	1
DoS	2	1	578	0	1	0	1
Brute Force	0	1	3	596	1	0	0
Bot	2	1	2	2	574	3	2
Infilteration	1	1	0	0	1	558	0
Web	1	2	2	0	4	2	614

Figure 3. Classification result of (a-b) 70:30 of TRP/TSP, (c) PR-curve, and (d) ROC-curve

In Table 2 and Fig. 4, the ID outputs of the TLBOEL-IDC methodology are reported. The outputs stated that the TLBOEL-IDC technique attains effectual recognition under every class label. On 70% of TRP, the TLBOEL-IDC technique provides average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 99.49%, 98.22%, 98.23%, 98.22%, and 98.97% respectively. Meanwhile, on 30% of TSP, the TLBOEL-IDC technique provides average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 99.63%, 98.69%, 98.71%, 98.69%, and 99.24% respectively.

TABLE II. ID OUTPUT OF TLBOEL-IDC MODEL ON 70:30 OF TRP/TSP

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
Training (70%)					
Benign	99.52	98.15	98.50	98.33	99.10
DDoS	99.47	97.94	98.23	98.09	98.95
DoS	99.51	98.17	98.45	98.31	99.07
Brute Force	99.47	98.21	98.07	98.14	98.89
Bot	99.45	98.78	97.38	98.08	98.59
Infiltration	99.52	98.74	97.98	98.36	98.88
Web	99.51	97.55	98.98	98.26	99.29
Average	**99.49**	**98.22**	**98.23**	**98.22**	**98.97**
Testing (30%)					
Benign	99.62	98.50	98.83	98.67	99.29
DDoS	99.52	98.75	98.14	98.44	98.96
DoS	99.60	97.97	99.14	98.55	99.41
Brute Force	99.74	99.00	99.17	99.09	99.50
Bot	99.50	98.46	97.95	98.20	98.85
Infiltration	99.79	98.94	99.47	99.20	99.65
Web	99.62	99.19	98.24	98.71	99.05
Average	**99.63**	**98.69**	**98.71**	**98.69**	**99.24**

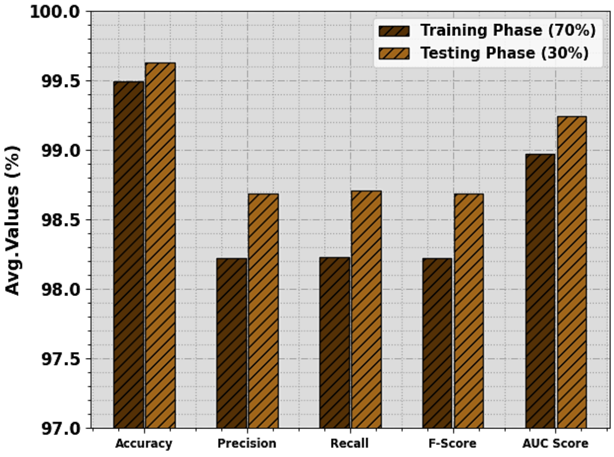


Figure 4. Average output of TLBOEL-IDC model on 70:30 of TRP/TSP

Article Received: 26 June 2023 Revised: 22 August 2023 Accepted: 06 September 2023

Fig. 5 investigates the $accu_y$ of the TLBOEL-IDC methodology in the testing data. The output pointed out the TLBOEL-IDC methodology attains higher $accu_y$ values over optimum epochs. Additionally, the greater validation $accu_y$ over the training $accu_y$ portrayed that the TLBOEL-IDC approach learned effectually on testing data.

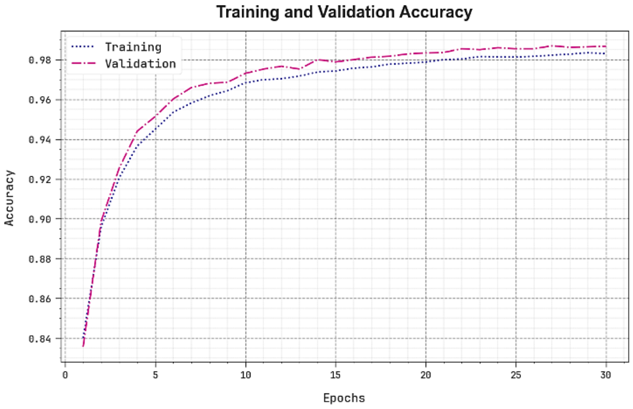


Figure 5. $Accu_y$ curve of the TLBOEL-IDC system

The loss evaluation of the TLBOEL-IDC methodology in the testing data in Fig. 6. The output highlights the TLBOEL-IDC methodology obtains nearer loss values. The TLBOEL-IDC technique learned optimally on a testing data.

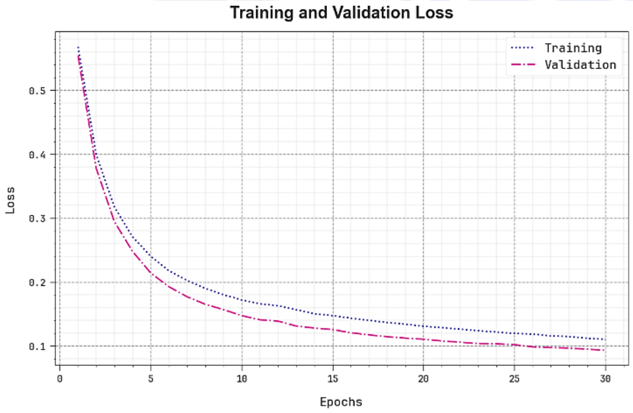


Figure 6. Loss curve of the TLBOEL-IDC system

In Table 3 and Fig. 7, an overall outcome of the TLBOEL-IDC method is portrayed. The results have shown that the AdaBoost model gained worse outcomes than other models [22]. Concurrently, the Extra Tree (ET), Decision Tree (DT), Random Forest (RF), AdaBoost (XGB), and LGBM methods have reported moderately improved performance. However, the TLBOEL-IDC technique surpassed the other existing models with a maximum $accu_y$ of 99.63%, $prec_n$ of 98.69%, $reca_l$ of 98.71%, and F_{score} of 98.69%. These results verified the improvement of the TLBOEL-IDC technique compared to other existing models.

TABLE III. RELATIVE OUTPUT OF TLBOEL-IDC METHOD OVER OTHER APPROACHES

Model	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
TLBOEL-IDC	99.63	98.69	98.71	98.69
DT	98.70	96.67	97.67	97.67
RF	98.40	97.43	95.43	96.43
ET	98.30	97.35	97.35	98.05
XGB	97.80	97.74	97.65	97.80
LGBM	98.80	97.83	96.83	97.83
XGB	98.90	96.97	96.98	96.97

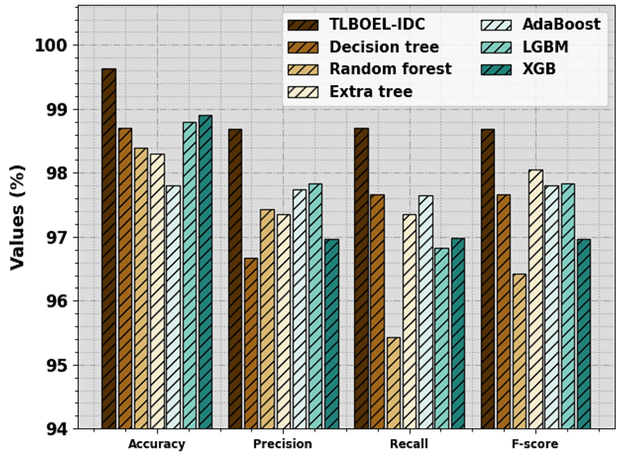


Figure 7. Comparative results of TLBOEL-IDC methods with other methodologies

V. CONCLUSION

In this article, an automated ID model has been introduced, named the TLBOEL-IDC method. The presented TLBOEL-IDC method classifies and detects intrusions in the network. To attain this, the TLBOEL-IDC approach encompasses three major processes such as data preprocessing, ensemble learning-based classification, and TLBO-based hyperparameter tuning. Besides, the TLBOEL-IDC approach involves the design of an ensemble classifier by the integration of three DL models namely GRU, LSTM, and BiLSTM. Moreover, the hyperparameter tuning of the DL models takes place using the TLBO approach, which in turn enhances the overall ID results. The simulation evaluation of the TLBOEL-IDC approach takes place on a benchmark dataset and the outputs are measured under various factors. The comparative evaluation accentuated the best achievement of the TLBOEL-IDC approach over other current methods in terms of different metrics.

REFERENCES

[1] Gupta, N., Jindal, V. and Bedi, P., 2022. CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class

imbalance in network-based intrusion detection systems. Computers & Security, 112, p.102499.

[2] Zhang, H., Huang, L., Wu, C.Q. and Li, Z., 2020. An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset. Computer Networks, 177, p.107315.

[3] Abdelkhalek, A. and Mashaly, M., 2023. Addressing the class imbalance problem in network intrusion detection systems using data resampling and deep learning. The Journal of Supercomputing, pp.1-34.

[4] Thakkar, A. and Lohiya, R., 2023. Attack classification of imbalanced intrusion data for IoT network using ensemble learning-based deep neural network. IEEE Internet of Things Journal.

[5] Arief Hidayat, Kusworo Adi, Bayu Surarso. (2023). Prediction of Various Computational Parameters using Naive Bayes and Felder and Silverman Methods. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 434–443. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2692.

[6] Lin, Y.D., Liu, Z.Q., Hwang, R.H., Nguyen, V.L., Lin, P.C. and Lai, Y.C., 2022. Machine learning with variational AutoEncoder for imbalanced datasets in intrusion detection. IEEE Access, 10, pp.15247-15260.

[7] Panigrahi, R., Borah, S., Bhoi, A.K., Ijaz, M.F., Pramanik, M., Kumar, Y. and Jhaveri, R.H., 2021. A consolidated decision tree-based intrusion detection system for binary and multiclass imbalanced datasets. Mathematics, 9(7), p.751.

[8] Pimsarn, C., Boongoen, T., Iam-On, N., Naik, N. and Yang, L., 2022. Strengthening intrusion detection system for adversarial attacks: improved handling of imbalance classification problem. Complex & Intelligent Systems, 8(6), pp.4863-4880.

[9] Tran, N., Chen, H., Jiang, J., Bhuyan, J. and Ding, J., 2021. Effect of Class Imbalance on the Performance of Machine Learning-based Network Intrusion Detection. International Journal of Performability Engineering, 17(9).

[10] Amalapuram, S.K., Reddy, T.T., Channappayya, S.S. and Tamma, B.R., 2021, October. On handling class imbalance in continual learning based network intrusion detection systems. In The First International Conference on AI-ML-Systems (pp. 1-7).

[11] Seo, J.H. and Kim, Y.H., 2018. Machine-learning approach to optimize smote ratio in class imbalance dataset for intrusion detection. Computational intelligence and neuroscience, 2018.

[12] Raj, R., & Sahoo, D. S. S. . (2021). Detection of Botnet Using Deep Learning Architecture Using Chrome 23 Pattern with IOT. Research Journal of Computer Systems and Engineering, 2(2), 38:44. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/31.

[13] Rao, Y.N. and Suresh Babu, K., 2023. An Imbalanced Generative Adversarial Network-Based Approach for Network Intrusion Detection in an Imbalanced Dataset. Sensors, 23(1), p.550.

[14] Rani, M. and Gagandeep, 2022. Effective network intrusion detection by addressing class imbalance with deep neural networks multimedia tools and applications. Multimedia Tools and Applications, 81(6), pp.8499-8518.

[15] Fu, Y., Du, Y., Cao, Z., Li, Q. and Xiang, W., 2022. A deep learning model for network intrusion detection with imbalanced data. Electronics, 11(6), p.898.

[16] Mbow, M., Koide, H. and Sakurai, K., 2022. Handling class Imbalance problem in Intrusion Detection System based on deep learning. International Journal of Networking and Computing, 12(2), pp.467-492.

[17] Al-Essa, M. and Appice, A., 2021, September. Dealing with imbalanced data in multi-class network intrusion detection systems using xgboost. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases (pp. 5-21). Cham: Springer International Publishing.

[18] Bedi, P., Gupta, N. and Jindal, V., 2021. I-SiamIDS: an improved Siam-IDS for handling class imbalance in network-based intrusion detection systems. Applied Intelligence, 51, pp.1133-1151.

[19] Mr. B. Naga Rajesh. (2019). Effective Morphological Transformation and Sub-pixel Classification of Clustered Images. International Journal of New Practices in Management and Engineering, 8(01), 08 - 14. https://doi.org/10.17762/ijnpme.v8i01.74.

[20] Gupta, N., Jindal, V. and Bedi, P., 2021. LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system. Computer Networks, 192, p.108076.

[21] Alqarni, A.A., 2022. Majority vote-based ensemble approach for distributed denial of service attack detection in cloud computing. Journal of Cyber Security and Mobility, pp.265-278.

[22] Roy, B., Malviya, L., Kumar, R., Mal, S., Kumar, A., Bhowmik, T. and Hu, J.W., 2023. Hybrid Deep Learning Approach for Stress Detection Using Decomposed EEG Signals. Diagnostics, 13(11), p.1936.

[23] Brian Moore, Peter Thomas, Giovanni Rossi, Anna Kowalska, Manuel López. Exploring Natural Language Processing for Decision Science Applications. Kuwait Journal of Machine Learning, 2(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/217.

[24] Berrou, B.K., Al Kalbani, K., Antonijevic, M., Zivkovic, M., Bacanin, N. and Nikolic, B., 2023, January. Training a Logistic Regression Machine Learning Model for Spam Email Detection Using the Teaching-Learning-Based-Optimization Algorithm. In Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022) (Vol. 104, p. 306). Springer Nature.

[25] https://registry.opendata.aws/cse-cic-ids2018/

[26] Ogobuchi Okey, D.; Sarah Maidin, S.; Adasme, P.; Lopes Rosa, R.; Saadi, M.; Carrillo Melgarejo, D.; Zegarra Rodríguez, D. BoostedEnML: Efficient Technique for Detecting Cyberattacks in IoT Systems Using Boosted Ensemble Machine Learning. Sensors 2022, 22, 7409. https:// doi.org/10.3390/s22197409.