ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20221128071759
Original scientific paper

Intelligent Intrusion Detection System using Enhanced Arithmetic Optimization Algorithm with Deep Learning Model

S. KAVITHA*, N. UMA MAHESWARI, R. VENKATESH

Abstract: The widespread use of interoperability and interconnectivity of computing systems is becoming indispensable for enhancing our day-to-day actions. The susceptibilities deem cyber-security systems necessary for assuming communication interchanges. Secure transmission needs security measures for combating the threats and required developments to security measures that counter evolving security risks. Though firewalls were devised to secure networks, in real-time they cannot detect intrusions. Hence, destructive cyber-attacks put forward severe security complexities, requiring reliable and adaptable intrusion detection systems (IDS) that could monitor unauthorized access, policy violations, and malicious activity practically. Conventional machine learning (ML) techniques were revealed for identifying data patterns and detecting cyber-attacks IDSs successfully. Currently, deep learning (DL) methods are useful for designing accurate and effective IDS methods. In this aspect, this study develops an intelligent IDS using enhanced arithmetic optimization algorithm with deep learning (IIDS-EAOADL) method. The presented IIDS-EAOADL model performs data standardization process to normalize the input data. Besides, equilibrium optimizer based feature selection (EOFS) approach is developed to elect an optimal subset of features. For intrusion detection, deep wavelet autoencoder (DWAE) classifier is applied. Since the proper tuning of parameters of the DWNN is highly important, EAOA algorithm is used to tune them. For assuring the simulation results of the IIDS-EAOADL technique, a widespread simulation analysis takes place using a benchmark dataset. The experimentation outcomes demonstrate the improvements of the IIDS-EAOADL model over other existing techniques

Keywords: arithmetic optimization algorithm; deep learning; feature selection; intrusion detection; security

1 INTRODUCTION

The usage of Internet applications and services is gradually increasing in number of applications like e-commerce and e-learning, which escalates concerns regarding privacy and security. With this usage, breaching cybersecurity using additional and recently established hacking and phishing tools has simultaneously improved for violating the Integrity, Confidentiality, and Availability (CIA) principles. Malicious software (malware) refers to a code that allows to bypass access controls, steal data, or compromise or harm an Internet of Things (IoT) system, a software system, or a computer network [1]. For this reason, dissimilar protection approaches like anti-malware, firewalls, and encryption tools were employed to prevent cyberattacks, whereas digital forensics technique has been utilized to examine the attacks. The emergence of new cyberattacks and zero-day attacks makes the defence against them considerable security problems in the extensive network [2]. An Intrusion Detection System (IDS) can be referred to software application or device that is regarded as a defensive wall. The basic function of the IDS is to monitor the behaviour and activity of network traffic for identifying malicious and abnormal activities and generate reports and alerts of these behaviours. Fig. 1 depicts the architecture of IDS.

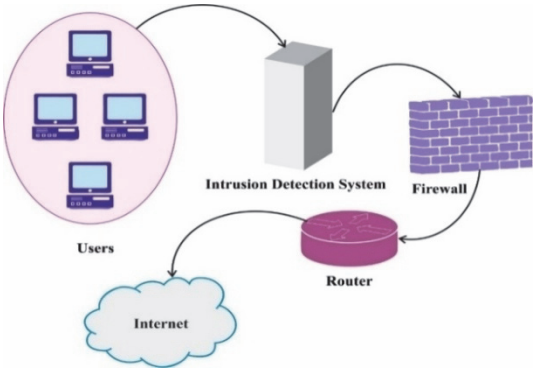

Figure 1 Framework of Intrusion Detection Systems

The IDS would be referred as software or hardware system that works in an automatic manner which helps to monitor the actions which are carried out within the system. It is widely applied with respect to security method and IDS alert is used for system administrators to produce a log based on attack while it predicts the occurrence of any event in host or a network. The IDS can be implemented inside a network on the basis of required action. It is used for detecting the attacks based on maximum patterns and procedures that have distinct signature. Thus, prediction of IDS improves the number of rules. However, presence of massive rules does not refer the input data to be related with alternate procedures. Hence, more amounts of rules tend to machine overhead. Rather than using a typical IDS, an intelligent and robust IDS is required because different systems have the capacity of hiding suspicious network traffic [3]. The classification of IDS depends on different conditions namely the data source and the response and detection models. Network-and Host-based models are the most important classes of IDS based on the data source, whereas signature-and anomaly based models are the major technologies based on the detection technique [4]. IDS handles an enormous quantity of data in the network traffic where data contains irrelevant, noisy, and redundant features that affect the performance of IDS and consume further resources. Consequently, dimension reduction was required for enhancing the efficacy of IDS [5].

With adequate computing power and massive quantity of information gathered from interconnected devices [6], DL model has been taken into account to improve the security of IoT with respect to user behaviors analysis, intrusion detection, privacy preserving, and vulnerabilities [7]. DL technique and particularly CNN is used to identify, learn, and extract complicated patterns and features directly from raw IoT information thereby enhancing the utility of the devices to effectively potential possible attacks and threats in the IoT platform [8]. Furthermore, DL model is very effective in automated feature extraction instead of dependent on conventional machine learning

(ML) method that demands handcrafted statistical features. Over the last few years, researcher workers had proposed different approaches for IDSs [9]. Various ML approaches have been developed for security problems. Additionally, DL model is utilized in IoT environments like generative adversarial networks (GAN) to improve the device utility and secure user private information [10]. Feature selection techniques have proven great performance in IDS with different classifications. Recently, metaheuristics optimization algorithm has been devised for many challenging issues, involving feature selection.

This study develops an intelligent IDS using enhanced arithmetic optimization algorithm with deep learning (IIDS-EAOADL) method. The presented IIDS-EAOADL method performs data standardization process to normalize the input data. Besides, equilibrium optimizer based feature selection (EOFS) approach is developed to elect an optimal subset of features. For intrusion detection, deep wavelet autoencoder (DWAE) classifier is applied. Since the proper tuning of parameters of the DWNN is highly important, EAOA algorithm is used to tune them. For assuring the simulation results of the IIDS-EAOADL technique, a widespread simulation analysis takes place using benchmark dataset.

2 RELATED WORKS

In [11], an artificial neural network (ANN) can be used for the detection of abnormal action in a medical IoT mechanism. The detection precision is based on the features that were granted to the ANN. The crucial and challenging problem of network traffic is choosing the significant and discriminatory features as it has a substantial effect on the learning procedure. In this presented technique, the butterfly optimized approach is a metaheuristic optimized technique used for selecting the best features for the learning procedure in an ANN. Fatani et al. [12] introduce a potential AI-related system for IDS in IoT systems. The metaheuristics (MH) algorithms and deep learning advancements are used by the authors that ensure effectiveness in resolving complicated engineering complexities. Moreover, feature extracting technique utilizing CNN is devised by the authors for extracting appropriate features. In addition, the authors advanced an innovative feature selecting approach utilizing an innovative variant of the transient search optimization (TSO) technique, termed TSODE, and leverage the operatives of differential evolution (DE) method.

Alzaqebah et al. [13] present an altered bio-inspired approach, which is the GWO that improves the efficiency of the IDS in identifying normal as well as anomalous traffic in the networks. The key developments include the smart initializing stage that integrates the filter and wrapper techniques for assuring the informative features that are added in initial iterations. Moreover, to tune the parameters of ELM, the authors approved the Extreme Learning Machine (ELM), modified GWO, and high-speed classification method. Fatani et al. [14] projected creative feature selecting and extracting algorithms for the IDS by making use of the benefits of the swarm intelligence (SI) approaches. Additionally feature extracting system based on the CNN is devised by the author. Then an alternative feature selection (FS) method utilizing the recently advanced Aquila optimizer (AQU) and SI algorithm.

In [15], an IDS can be presented that uses ML and data mining ideas for detecting network intrusion paradigms. In the presented technique, an ANN was utilized as a learning technique. The meta-heuristic algorithm including the swarm-related method can be employed for minimizing ID errors. To reduce ID error rate, the Grasshopper Optimization Algorithm (GOA) was utilized for more accurate and better learning of ANNs. The role of the GOAMLP method was to reduce the ID error in the NN through selection of valuable variables like weight and bias. In [16], an innovative IDS can be modelled that uses the butterfly optimization algorithm (BOA), for executing FS. And to assess the ability of the features which is chosen for predicting assaults, a multi-layer perceptron (MLP) classifier was employed. With a view to enhancing the MLP method, not just the gradient descent (GD) training approach along with 2 meta-heuristic techniques, GA, and PSO were employed for optimizing the classifier structure. In [17], a wrapper FS method for IDS is devised. This technique will make use of the pigeon inspired optimizer for using the selective procedure. A novel technique to binarize a continual pigeon inspired optimizer was modelled and made a comparison with the conventional way of binarizing continual SI methods.

3 THE PROPOSED MODEL

In this study, a new IIDS-EAOADL algorithm was presented for intrusion detection process. To attain this, the presented IIDS-EAOADL model performs data standardization process to normalize the input data. Next, a novel EOFS technique is developed to elect an optimal subset of features. Followed by, the EAOA with DWAE classifier is applied to recognize and classify intrusions. Fig. 2 demonstrates the block diagram of the IIDS-EAOADL approach.

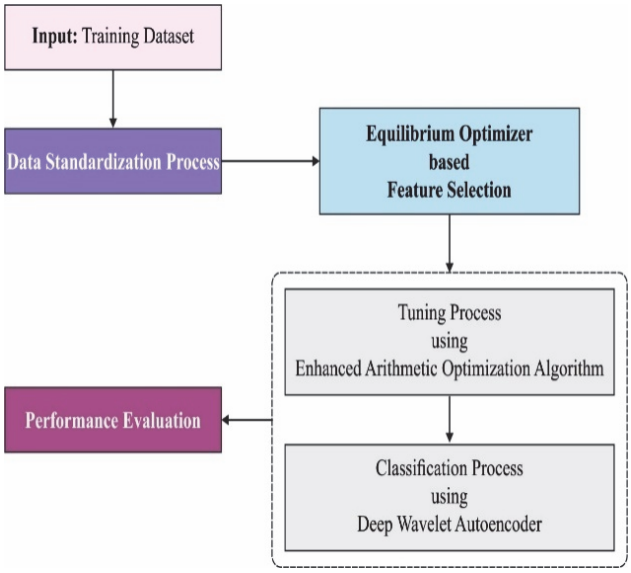

Figure 2 Block diagram of IIDS-EAOADL approach

3.1 Feature Selection Using EOFS Model

In this study, a novel EOFS technique is formulated to elect an optimal subset of features. The EO algorithm is a

metaheuristic technique stimulated by the law of physics that is used to evaluate the equilibrium state [18]. Similar to other optimization techniques, the EO algorithm originated from initial population of the particles. The following equation demonstrates the initial population of the EOA with *n* particles.

$$P_z^{'} = P_{\text{Min}} + \Re_z \left(P_{\text{Max}} - P_{\text{Min}} \right), z = 1, 2, 3, ..., n \tag{1}$$

where $P_z^{'}$ indicates the primary concentration of particle z, P_{Max} represents maximal number of dimensions, P_{Min} signifies minimal number of dimensions, n depicts overall amount of particles, and $\Re_z$ implies random value lies in [0, 1]. For finding the equilibrium state of particle, all the particles in the population are estimated to define the objective function. Next, the concentration updating approach is carried out according to the equilibrium pool that comprises 4 optimum candidate particles and it is mathematically expressed as follows.

$$P_{\text{New}} = P_r + \frac{g_R}{\gamma}\left(1 - f\right) + \left(P - P_r\right) \cdot f \tag{2}$$

Now, P denotes present concentration vector, P_r shows random concentration vector, generation rate is represented by g_R, the exponential term is indicated by f, and the random vector is characterized by γ which is fixed to [0, 1].

Furthermore, the exponential term f and generation rate g_R are evaluated as follows.

$$g_R = \begin{cases} 0.5 R_1 \left(P_r - \gamma P \right) f, \text{ if } R_2 \geq g_p \\ 0, \text{ if } R_2 < g_p \end{cases} \tag{3}$$

$$f = C_1 \, si \, gn\left(\lambda - 0.5\right) \cdot \left(e^{-\gamma \left(1 - \left(t / t_{\text{Max}}\right)\right) C_2 \left(t / t_{\text{Max}}\right)} - 1 \right)$$

Here, R_1 and R_2 indicate the random values within [0, 1], λ represents the random vector amongst zero and one, C_1 and C_2 are constants set to 2 and 1, correspondingly. Likewise, the generation probability g_R is fixed to 0.5; t and t_{Max} depicts existing and overall iterations, correspondingly.

Next, every concentration vector of the particle was restored based on the contribution. The first term demonstrates the random concentration vector gained from the creation of equilibrium pool. The final two terms examine the concentration difference and are responsible for precise exploration and exploitation. Therefore, EO algorithm accomplishes optimum solution from the search space.

The fitness function (FF) of the EO-FS technique will consider the classifier accuracy and the selected features count. It optimizes the classifier accuracy and reduces the set sizes of features which are chosen. Thus, the subsequent FF can be employed for evaluating separate solutions, as given in Eq. (4).

$$Fitness = \alpha \cdot ErrorRate + \left(1 - \alpha\right) \cdot \frac{\#SF}{\#All\_F} \tag{4}$$

where as *ErrorRate* denotes the classifier error rate utilizing the features which are selected. *ErrorRate* can be the complement of the classifier accuracy, *#SF* refers to the selected attributes count and *#All_F* was the total count of features in the original data. α can be employed to control the significance of subset length and classification quality. In these experiments, α indicates set to 0.9.

3.2 Intrusion Detection Using DWAE Model

To identify and categorize intrusions, the DWAE model is applied. The standard autoencoder (AE) features robustness, strong inference ability, and unsupervised feature learning capability [19]. The property of WT has time-frequency localization and focal features. As a result, it is necessary to integrate wavelet transform and typical AE to resolve the real time problems. This study presents a novel type of unsupervised neural network named "DWAE" that could catch non-stationary vibration signals and characterize complicated data. The WAE applied the wavelet function as activation function in conventional state, which defined diverse resolutions.

$$X = \varsigma\left(\hat{\kappa}' Y + b'\right) \tag{5}$$

In Eq. (5), $\hat{X}$ shows the outcomes of the recreated vector, κ signifies kernel vector, b' designates bias value, and $\in$ indicates an error value added in the process of BP. Training instances $y = \left[y_1, y_2, ..., y_n\right]^A$ the output of hidden unit represents *i*.

$$g_j\left(out\right) = \varphi \frac{\left(\sum_{i-1}^{n} v_{ij} y_l - e_i\right)}{b_i} \tag{6}$$

where as: φ indicates the wavelet activation function.

$y_l\left(r = 1, 2, ..., n\right)$ shows the *l*-th dimension input of training instance,

$v_{ij}\left(r = 1, 2, ..., g\right)$ refers to the weight connecting between 1the hidden unit *i* and input unit.

b_i and e_i represents $v_{ij}\left(r = 1, 2, ..., g\right)$ transmitted the scale and shift factors of wavelet activation function for the hidden unit *i*.

$$\varphi\left(a\right) = \cos\left(5a\right) \exp\left(\frac{a^2}{2}\right) \tag{7}$$

$$g_i\left(out\right) = \varphi_{be}\left(i\right) = \cos\left(5 \times \frac{\left(\sum_{i-1}^{n} v_{ij} y_l - e_i\right)}{b_i}\right) 2 \times \times \left(\left(-\frac{1}{2}\frac{\left(\sum_{i-1}^{n} v_{ij} y_l - e_i\right)}{b_i}\right) 2\right) \tag{8}$$

Like typical AE, we select the output layer activation function as sigmoid function. Next, the output of deep WAE is evaluated as follows:

$$\hat{y} = \mathrm{sig}m\left(\sum_{i-1}^{q} v_{ri}\left(\cos 5\times\frac{\left(\sum_{i-1}^{n} v_{ij}y_l - e_i\right)}{b_i}\right)\right) \times\exp\left(-\frac{1}{2}\frac{\left(\sum_{i-1}^{n} v_{ij}y_l - e_i\right)}{b_i}\right)2\Bigg) \tag{9}$$

Now, $\hat{y}$ indicates i the recreated dimension output of training instances, and v_{ri} shows the weight connecting between hidden r and i.

3.3 Parameter Tuning Using EAOA

Since the proper tuning of parameters of the DWNN is highly important, EAOA algorithm is used to tune them [20]. The elementary AOA operation includes initialization, exploration, and exploitation.

(a) Initialization. Candidate solution (XA) is randomly produced. The present population is characterized as the matrix XA. The dimension is represented as DM. The number of individuals can be signified as NP. The optimally accomplished solution was the better solution for all the iterations.

$$XA = \begin{Bmatrix} xa_{1,1} & \cdots & xa_{1,DM-1} & xa_{1,DM} \\ xa_{2,1} & \cdots & xa_{2,DM-1} & xa_{2,DM} \\ \vdots & \cdots & \vdots & \vdots \\ xa_{NP,1} & \cdots & xa_{NP,DM-1} & xa_{NP,DM} \end{Bmatrix} \tag{10}$$

The search phrase was selected as an exploitation or exploration stage using MOA function as follows.

$$MOA(iter) = \min iter + iter\times\left(\frac{\max iter - min\,iter}{Miter}\right) \tag{11}$$

In Eq. (11), Miter denotes the maximal amount of iterations. The present iteration is represented as iter. The maximum and minimum MOA values were max$iter$ and min$iter$, correspondingly. max$iter$ and min$iter$ are variables that are defined as specific values in advance of start of AOA. maxiter and miniter are fixed as 0.2 and 1, correspondingly.

At last, the better solution for the existing iteration is the ideal solution. The present optimum fitness is compared with the prior optimum fitness, and the lowest value was used to define the final optimum solution. The EAOA technique is derived from the use of chaotic concepts with the AOA. Chaotic mapping refers to multi-variate non-linear functions that are used for nonlinear deterministic prediction of time sequences dataset to population, thus enhancing the global searching ability of AOA. In this work, circle chaotic mapping is utilized in the AOA to enhance the initialization population.

The circle map is formulated below:

$$x_{k+1} = x + b - (P - 2\pi)\sin(2\pi x)\,mod\,(1) \tag{12}$$

where $b = 0.2$, and $P = 0.5$ refers to the control variable.

The EAOA algorithm will derive an FF for achieving enhanced classifier outcomes. It sets a positive value for indicating superior performance of the candidate solutions. In this article, the reduction of the classifier will be regarded as the FF, as shown in Eq. (13).

$$fitness(x_i) = ClassifierErrorRate(x_i) = \\ = \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples}\cdot 100 \tag{13}$$

4 RESULTS AND DISCUSSION

In this section, the experimental validation of the IIDS-EAOADL method is tested using the NSLKDD dataset. The presented IIDS-EAOADL model has chosen a set of 19 features from the existing 42 features as shown in Tab. 1.

Table 1 Dataset details

Class	No. of Samples
Normal	77053
DoS	53385
Probe	14078
R2L	3882
U2R	119
Total Number of Samples	148517

The parameter setting is given as follows: Population size: 10, HCMR: 0.99, PAR: 0.33, fw/bw: 0.01. It has 148517 number of samples which falls under two categories namely normal and anomaly.

Fig. 3 exemplifies the set of confusion matrices formed by the IIDS-EAOADL model. On entire dataset, the IIDS-EAOADL method has categorized 76251 instances into normal class, 52541 instances into DoS class, 13621 instances into Probe, 3405 instances into R2L, and 0 instances under U2R. Also, on 70% of TR data, the IIDS-EAOADL approach has categorized 53359 instances into normal class, 36882 instances into DoS class, 9414 instances into Probe, 2377 instances into R2L, and 0 instances under U2R. In addition, on 30% of TS data, the IIDS-EAOADL technique has categorized 22892 instances into normal class, 15659 instances into DoS class, 4207 instances into Probe, 1028 instances into R2L, and 0 instances under U2R.

Tab. 2 provides overall IDS outcomes of the IIDS-EAOADL model. Fig. 4 demonstrates brief IDS results of the IIDS-EAOADL method on entire dataset. The figure highlighted that the IIDS-EAOADL approach has reached enhanced performance in every class label. For example, on normal class, the IIDS-EAOADL method has obtained $accu_y$ of 98.82%, $prec_n$ of 98.78%, $reca_l$ of 98.96%, F_{measure} of 98.87%, and MCC of 97.64%. Simultaneously, on probe class, the IIDS-EAOADL algorithm has gained $accu_y$ of 99.21%, $prec_n$ of 94.97%, $reca_l$ of 96.75%, F_{measure} of 95.85%, and MCC of 95.42%. Concurrently, on R2L class, the IIDS-EAOADL method has obtained $accu_y$ of 99.34%, $prec_n$ of 87.11%, $reca_l$ of 87.71%, F_{measure} of 87.41%, and MCC of 87.07%.

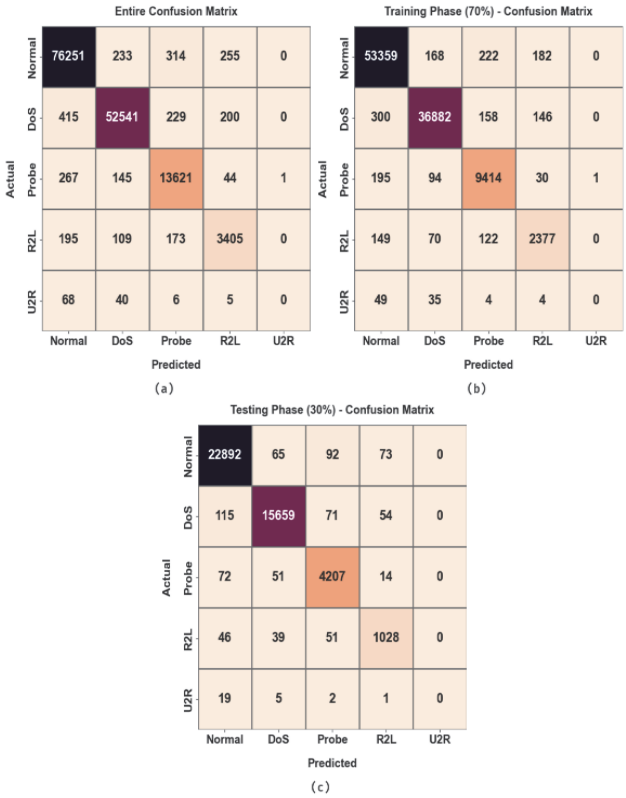

Figure 3 Confusion matrices of IIDS-EAOADL approach (a) Entire dataset, (b) 70% of TR data, and (c) 30% of TS data

Table 2 Result analysis of IIDS-EAOADL algorithm with distinct class labels and measures

Labels	*Accuracy*	*Precision*	*Recall*	$F_{measure}$	*MCC*
Entire Dataset					
Normal	98.82	98.78	98.96	98.87	97.64
DoS	99.08	99.01	98.42	98.71	97.99
Probe	99.21	94.97	96.75	95.85	95.42
R2L	99.34	87.11	87.71	87.41	87.07
U2R	99.92	00.00	00.00	00.00	-0.01
Average	99.27	75.97	76.37	76.17	75.62
Training Phase (70%)					
Normal	98.78	98.72	98.94	98.83	97.56
DoS	99.07	99.01	98.39	98.70	97.97
Probe	99.21	94.90	96.71	95.80	95.36
R2L	99.32	86.78	87.45	87.12	86.77
U2R	99.91	00.00	00.00	00.00	-0.01
Average	99.26	75.88	76.30	76.09	75.53
Testing Phase (30%)					
Normal	98.92	98.91	99.01	98.96	97.83
DoS	99.10	98.99	98.49	98.74	98.04
Probe	99.21	95.12	96.85	95.97	95.54
R2L	99.38	87.86	88.32	88.09	87.77
U2R	99.94	00.00	00.00	00.00	00.00
Average	99.31	76.18	76.53	76.35	75.84

Fig. 5 establishes the detailed IDS results of the IIDS-EAOADL approach on 70% of TR data. The figure emphasized the IIDS-EAOADL methodology has reached enhanced performance in all classes. For example, on normal class, the IIDS-EAOADL approach has reached $accu_y$ of 98.78%, $prec_n$ of 98.72%, $reca_l$ of 98.94%, F_{measure} of 98.83%, and *MCC* of 97.56%. Concurrently, on probe class, the IIDS-EAOADL method has achieved $accu_y$ of 99.21%, $prec_n$ of 94.90%, $reca_l$ of 96.71%, F_{measure} of 95.80%, and *MCC* of 95.36%. Parallelly, on R2L class, the IIDS-EAOADL approach has attained $accu_y$ of 99.32%, $prec_n$ of 86.78%, $reca_l$ of 87.45%, F_{measure} of 87.12%, and *MCC* of 86.77%.

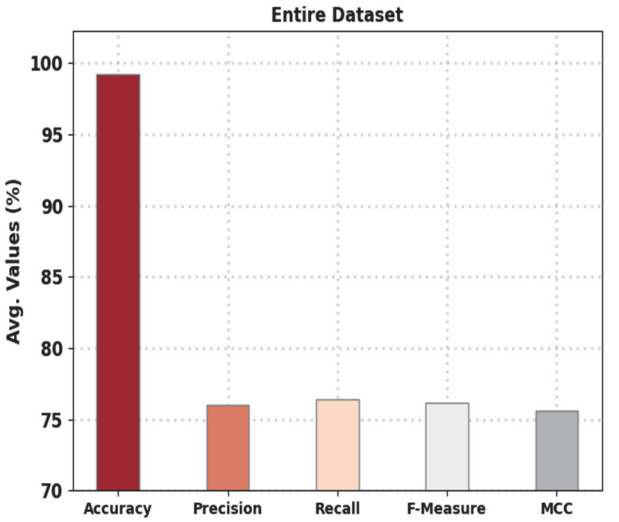

Figure 4 Average analysis of IIDS-EAOADL algorithm under entire dataset

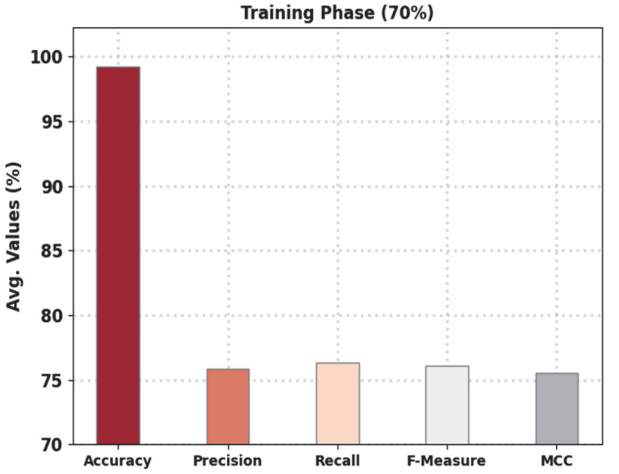

Figure 5 Average analysis of IIDS-EAOADL algorithm under 70% of TR data

Fig. 6 portrays the comparative IDS results of the IIDS-EAOADL algorithm on 30% of TS data. The figure pointed that the IIDS-EAOADL methodology has reached enhanced performance under all classes. For example, on normal class, the IIDS-EAOADL approach has attained $accu_y$ of 98.92%, $prec_n$ of 98.91%, $reca_l$ of 99.01%, F_{measure} of 98.96%, and *MCC* of 97.83%. At the same time, on probe class, the IIDS-EAOADL approach has acquired $accu_y$ of 99.21%, $prec_n$ of 95.12%, $reca_l$ of 96.85%, F_{measure} of 95.97%, and *MCC* of 95.54%. Simultaneously, on R2L class, the IIDS-EAOADL method has attained $accu_y$ of 99.38%, $prec_n$ of 87.86%, $reca_l$ of 88.32%, F_{measure} of 88.09%, and *MCC* of 87.77%.

The training accuracy (TRA) and validation accuracy (VLA) achieved by the IIDS-EAOADL approach under test dataset is shown in Fig. 7. The experimental outcome denotes the IIDS-EAOADL approach has acquired maximal values of TRA and VLA. Seemingly the VLA is greater than TRA.

The training loss (TRL) and validation loss (VLL) obtained by the IIDS-EAOADL technique under test dataset are displayed in Fig. 8. The experimental result highlighted the IIDS-EAOADL algorithm has exhibited minimal values of TRL and VLL. Particularly, the VLL is lesser than TRL.

A clear precision-recall inspection of the IIDS-EAOADL method under test dataset is depicted in Fig. 9. The figure represented the IIDS-EAOADL methodology has resulted in enhanced values of precision-recall values in every class label.

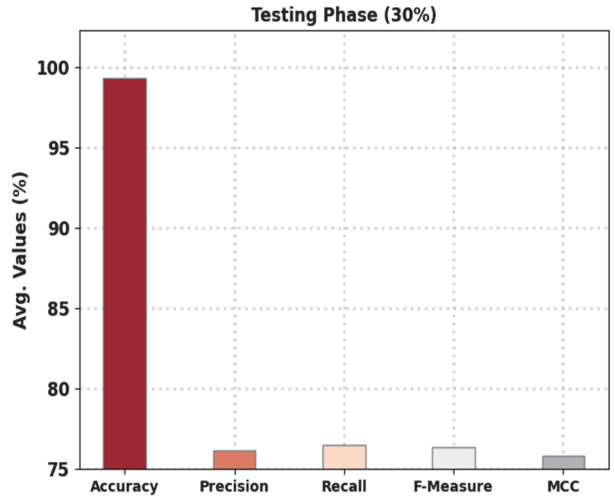

Figure 6 Average analysis of IIDS-EAOADL algorithm under 30% of TS data

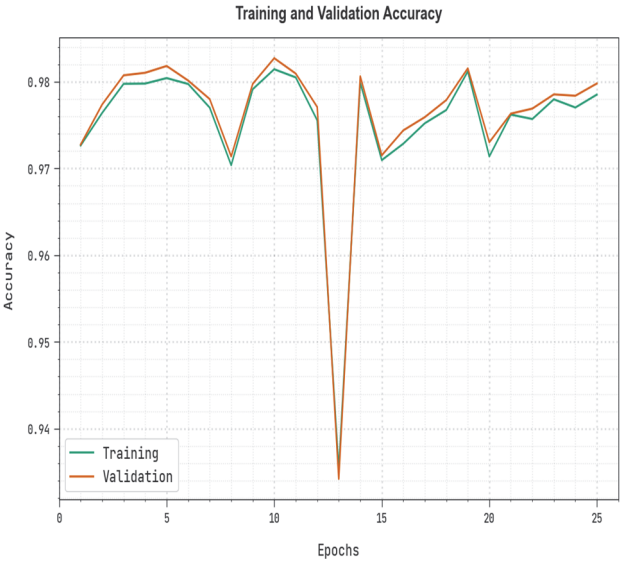

Figure 7 TRA and VLA analysis of IIDS-EAOADL algorithm

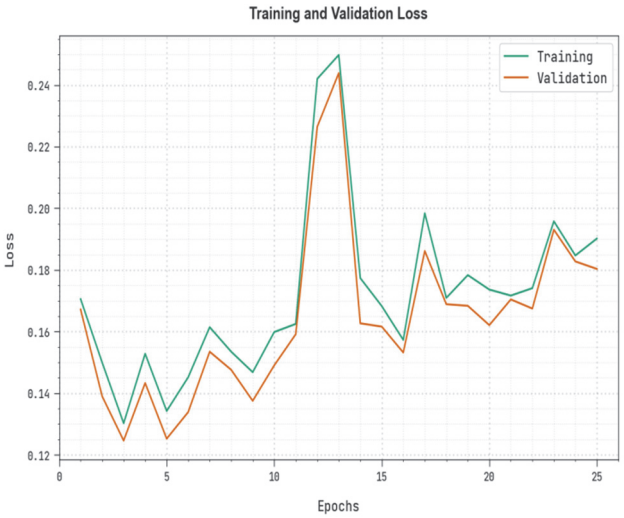

Figure 8 TRL and VLL analysis of IIDS-EAOADL algorithm

A brief ROC study of the IIDS-EAOADL approach in test dataset is portrayed in Fig. 10. The outcomes pointed that the IIDS-EAOADL method has displayed its capability in classifying different classes.

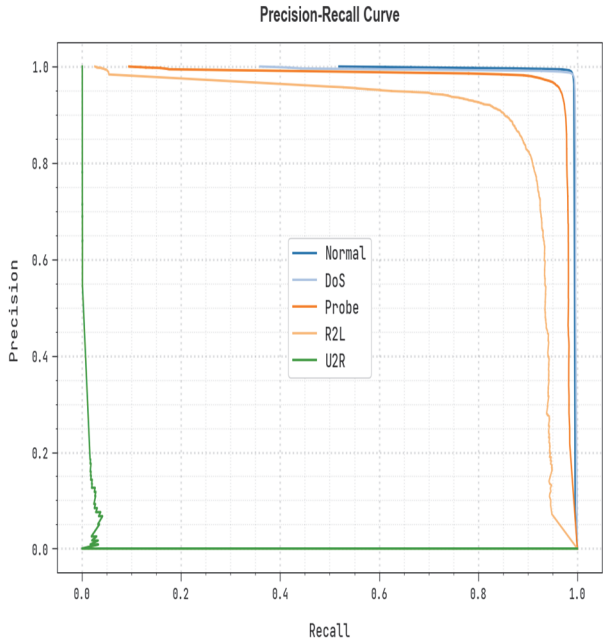

Figure 9 Precision-recall analysis of IIDS-EAOADL algorithm

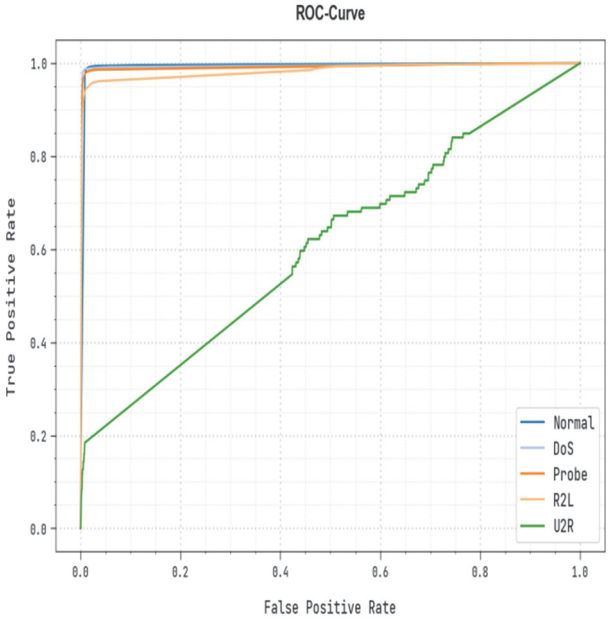

Figure 10 ROC curve analysis of IIDS-EAOADL algorithm

Tab. 3 presents a comparative analysis of the IIDS-EAOADL method with recent models [12]. A detailed $accu_y$ examination of the IIDS-EAOADL model with other IDS models is given in Fig. 11. These results denoted the MFO, TSO, and GWO techniques have exhibited ineffectual outcome with reduced $accu_y$ values of 95.90%, 96.41%, and 96.51% respectively. Followed by, the BAT algorithm has attained slightly improvised $accu_y$ $accu_y$ of 98.35%. In line with, the MVO and TSODE techniques have resulted in reasonable $accu_y$ of 99.20% and 99.16% respectively. But the IIDS-EAOADL model has accomplished maximum $accu_y$ of 99.31%.

Table 3 Comparative analysis of IIDS-EAOADL approach with existing methodologies

Methods	*Accuracy*	Running Time / sec
IIDS-EAOADL	99.31	0.860
MVO Algorithm	99.20	6.400
GWO Algorithm	96.51	1.117
MFO Algorithm	95.90	3.617
BAT Algorithm	98.35	6.483
TSODE Algorithm	99.16	8.450
TSO Algorithm	96.41	2.550

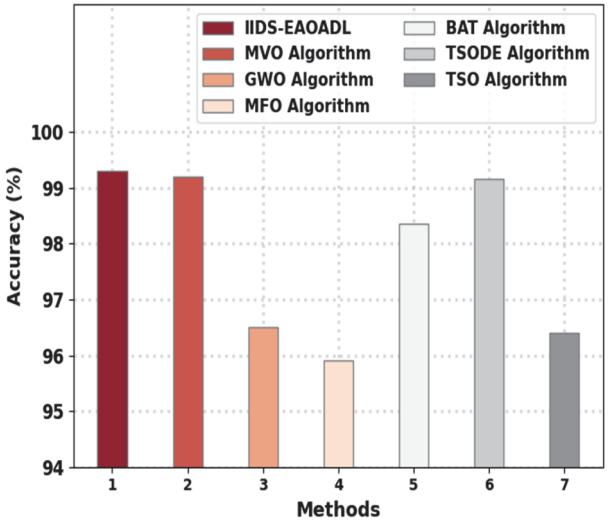

Figure 11 Accuracy analysis of IIDS-EAOADL approach with existing methodologies

A comprehensive RT review of the IIDS-EAOADL approach with other IDS methods is given in Fig. 12. These results denote that the MVO, TSODE, and BAT approaches have exhibited ineffectual outcome with higher RT of 6.4 s, 6.483 s, and 8.450 s correspondingly.

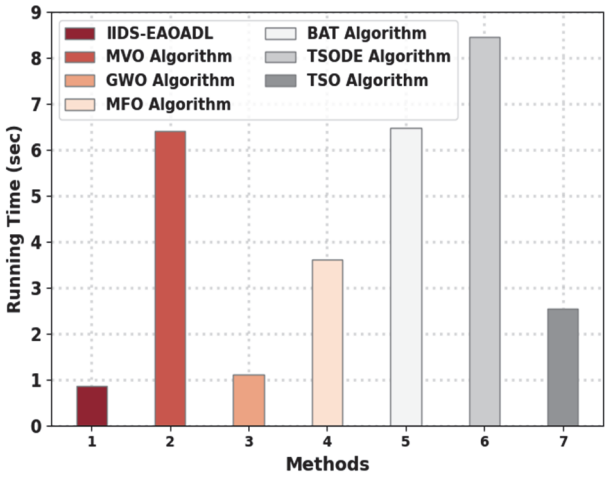

Figure 12 RT analysis of IIDS-EAOADL approach with existing methodologies

Then, the MFO and TSO algorithms have gained slightly decreased RT of 3.617 s and 2.550 s correspondingly. In this context, the GWO method has resulted in reasonable RT of 1.117 s. But the IIDS-EAOADL technique has exhibited minimal RT of 0.860 s. These results affirmed the betterment of the IIDS-EAOADL model over other models.

5 CONCLUSION

In this study, a new IIDS-EAOADL approach was presented for intrusion detection process. To attain this, the presented IIDS-EAOADL model performs data standardization process to normalize the input data. Next, a novel EOFS technique is developed to elect an optimal subset of features. Followed by, the DWAE classifier is applied to recognize and classify intrusions. Since the proper tuning of parameters of the DWNN is highly important, EAOA algorithm is used to tune them. For assuring the simulation results of the IIDS-EAOADL technique, a widespread simulation analysis takes place using benchmark dataset. The experimentation results demonstrate the improvements of the IIDS-EAOADL method over other existing techniques. Thus, the presented IIDS-EAOADL technique can be utilized for maximum detection efficiency. In future, hybrid DL methods will be applied to further boost the overall intrusion classification outcomes. Also, the proposed work can be further improved by the use of data reduplication techniques. In addition, data encryption technique can also be employed for secure data transmission in cloud environment.

6 REFERENCES

[1] Almomani, O. (2021). A hybrid model using bio-inspired metaheuristic algorithms for network intrusion detection system. *Computers, Materials & Continua*, *68*(1), 409-429. https://doi.org/10.32604/cmc.2021.016113

[2] Dahou, A., Abd Elaziz, M., Chelloug, S. A., Awadallah, M. A., Al-Betar, M. A., Al-qaness, M. A., & Forestiero, A. (2022). Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm. *Computational Intelligence and Neuroscience*. https://doi.org/10.1155/2022/6473507

[3] Hakkoymaz, V. (2020). Classifying Database Users for Intrusion Prediction and Detection in Data Security. *Tehnički vjesnik*, *27*(6), 1857-1862. https://doi.org/10.17559/TV-20190710100638

[4] Premkumar, M., Sundararajan, T. V. P., & Mohanbabu, G. (2022). Dynamic Defense Mechanism for DoS Attacks in Wireless Environments Using Hybrid Intrusion Detection System and Statistical Approaches. *Tehnički vjesnik*, *29*(3), 965-970. https://doi.org/10.17559/TV-20210604113859

[5] Khare, N., Devan, P., Chowdhary, C. L., Bhattacharya, S., Singh, G., Singh, S., & Yoon, B. (2020). Smo-dnn: Spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. *Electronics*, *9*(4), 692. https://doi.org/10.3390/electronics9040692

[6] Malibari, A. A., Alotaibi, S. S., Alshahrani, R., Dhahbi, S., Alabdan, R., Al-wesabi, F. N., & Hilal, A. M. (2022). A novel metaheuristics with deep learning enabled intrusion detection system for secured smart environment. *Sustainable Energy Technologies and Assessments*, *52*. https://doi.org/10.1016/j.seta.2022.102312

[7] Lateef, A. A. A., Al-Janabi, S. T. F., & Al-Khateeb, B. (2020). Hybrid intrusion detection system based on deep learning. 2020 *IEEE International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI)*, 1-5. https://doi.org 10.1109/ICDABI51230.2020.9325669

[8] Kareem, S. S., Mostafa, R. R., Hashim, F. A., & El-Bakry, H. M. (2022). An effective feature selection model using hybrid metaheuristic algorithms for iot intrusion detection. *Sensors*, 22(4). https://doi.org/10.3390/s22041396

[9] Rai, A. (2020).Optimizing a new intrusion detection system using ensemble methods and deep neural network. *IEEE 4th International Conference on Trends in Electronics and Informatics (ICOEI).* 527-532. https://doi.org/10.1109/ICOEI48184.2020.9143028

[10] Almomani, O. (2020). A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms. *Symmetry*, *12*(6). https://doi.org/10.3390/sym12061046

[11] Li, Y., Ghoreishi, S. M., & Issakhov, A. (2021). Improving the Accuracy of Network Intrusion Detection System in Medical IoT Systems through Butterfly Optimization Algorithm. *Wireless Pers Commun*, 126, 1999-2017. https://doi.org/10.1007/s11277-021-08756-x

[12] Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M. A., & Lu, S. (2021). IoT intrusion detection system using deep learning and enhanced transient search optimization. *IEEE Access*, *9*, 123448-123464. https://doi.org/10.1109/ACCESS.2021.3109081

[13] Alzaqebah, A., Aljarah, I., Al-Kadi, O., & Damaševičius, R. (2022). A Modified Grey Wolf Optimization Algorithm for an Intrusion Detection System. *Mathematics*, *10*(6). https://doi.org/10.3390/math10060999

[14] Fatani, A., Dahou, A., Al-Qaness, M. A., Lu, S., & Elaziz, M. A. (2021). Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system. *Sensors*, *22*(1). https://doi.org/10.3390/s22010140

[15] Moghanian, S., Saravi, F. B., Javidi, G., & Sheybani, E. O. (2020). GOAMLP: Network intrusion detection with multilayer perceptron and grasshopper optimization algorithm. *IEEE Access*, *8*, 215202-215213. https://doi.org/10.1109/ACCESS.2020.3040740

[16] Mahboob, A. S. & Moghaddam, M. R. O. (2020). An anomaly-based intrusion detection system using butterfly optimization algorithm. *IEEE. 6th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS*). 1-6. https://doi.org/10.1109/ICSPIS51611.2020.9349537

[17] Alazzam, H., Sharieh, A., & Sabri, K. E. (2020). A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. *Expert System with Applications*, 148. https://doi.org/10.1016/j.eswa.2020.113249

[18] Wang, J., Yang, B., Li, D., Zeng, C., Chen, Y., Guo, Z., Zhang, X., Tan, T., Shu, H., & Yu, T. (2021). Photovoltaic cell parameter estimation based on improved equilibrium optimizer algorithm. *Energy Conversion and Management*, 236(3). https://doi.org/10.1016/j.enconman.2021.114051

[19] Balamurugan, T. (2021). Deep Wavelet Autoencoder Based Brain Tumor Detection Analysis Using Deep Neural Network. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(11), 639-645.

[20] Khatir, S., Tiachacht, S., Le Thanh, C., Ghandourah, E., Mirjalili, S., & Wahab, M. A. (2021). An improved Artificial Neural Network using Arithmetic Optimization Algorithm for damage assessment in FGM composite plates. *Composite Structures*, *273*. https://doi.org/10.1016/j.compstruct.2021.114287

Contact information:

S. KAVITHA, Assistant Professor
(Corresponding author)
Department of Computer Science and Engineering,
Velammal College of Engineering and Technology,
Madurai, India
E-mail: kavithacsephd@gmail.com

N. UMA MAHESWARI, Professor
Department of Computer Science and Engineering,
P.S.N.A. College of Engineering and Technology,
Dindigul, India

R. VENKATESH, Professor
Department of Information Technology,
P.S.N.A. College of Engineering and Technology, Dindigul, India