Vol.67: e24231010, 2024
https://doi.org/10.1590/1678-4324-2024231010
ISSN 1678-4324 Online Edition

BABT
Brazilian Archives of Biology and Technology

Article - Engineering, Technology and Techniques

Modeling of Intrusion Detection System Using Double Adaptive Weighting Arithmetic Optimization Algorithm with Deep Learning on Internet of Things Environment

Vinoth Kumar Kalimuthu[1*]
https://orcid.org/0000-0002-8920-4936

Rajakani Velumani[2]
https://orchid.org/0009-0006-4767-0329

[1] Vivekanandha College of Engineering for Women (Autonomous), Department of ECE, Thiruchengode, India; [2]Anjalai Ammal Mahalingam Engineering College, Department of ECE, Thiruvarur, India.

Editor-in-Chief: Alexandre Rasi Aoki
Associate Editor: Fabio Alessandro Guerra

Received: 02-Oct-2023; Accepted: 17-Nov-2023; Corrected: 05-Aug-2024

*Correspondence: vinodkumaran87@gmail.com; (V.K.K.).

This document has an erratum: https://doi.org/10.1590/1678-4324-errata-2024999904

HIGHLIGHTS

- Developing IDS DAWAOA-DL approach in the IoT environment.
- CNN-GRU technique is used for the intrusion detection task.
- A series of simulations were performed on the BoT-IoT dataset.

Abstract: The Internet of Things (IoT) has experienced rapid development in area-specific applications, including smart transportation systems, healthcare, industries, and smart agriculture, to enhance socio-economic development over the past few years. This IoT system includes different actuators, interconnected sensors, and network-enabled devices that exchange various data through private networks and the Internet infrastructure. The intrusion detection system (IDS) is deployed with preventive security mechanisms, namely access control and authentication. The usual behaviors of the mechanism distinguish malicious and normal activities based on specific patterns or rules of IDSs. Therefore, this article focuses on developing IDS using Double Adaptive Weighting Arithmetic Optimization Algorithm with Deep Learning (DAWAOA-DL) approach in the IoT environment. The DAWAOA-DL methodology's objective is to recognise and classify intrusions in the IoT platform accurately. To execute this, the presented DAWAOA-DL approach involves the design of the DAWAOA technique for the feature selection procedure. Next, the convolutional neural network-gated recurrent unit (CNN-GRU) technique is used for the intrusion detection task. Finally, the Adam optimizer is exploited as a hyperparameter optimizer of the CNN-GRU methodology. A series of simulations were performed on the BoT-IoT dataset to exhibit the effectual detection performance of the DAWAOA-DL method. A widespread experimental validation demonstrated the betterment of the DAWAOA-DL method over other recent models under several metrics.

Keywords: Internet of Things; Security; Hybrid deep learning; Intrusion detection; Feature selection.

INTRODUCTION

A network of interconnected devices or gadgets is known as the Internet of Things (IoT). Such gadgets can determine without any interference from humans [1]. The development of different technology domains, such as embedded computing, automatic identification, tracking, 5G networks, wireless communications, sensors, and distributed services, has raised the use of advanced objects in everyday actions through the Internet [2]. The IoT is the combination of intelligent objects that can communicate and interact with the Internet [3]. This new paradigm had a prominent role in the ICT business in the future. In the IoT, a thing can be anything; for example, a farm animal with transponders that can be given an IP address and the capability of transferring data through a network [4], an individual with a blood pressure observation implant, a car entrenched sensors that alert the driver if the tire pressure becomes low.

With the outset of the internet and the fast growth of ubiquitous technologies, different types of attacks or cybercrime have increased worldwide [5]. Even though many cyber security experts keep developing defence methods, invaders often find valuable resources by launching adaptable, automatic, and cultured assaults. These invaders cause chaos to businesses, individuals, and governments. Five million cyber attacks are carried out every day through computers [6]. Thus, because of the intrinsic potentiality of the Intrusion Detection System (IDS) to find assaults in real time, the method has gained popularity [7]. The IDS is a complicated domain that detects cyber-attacks like policy violations or hostile actions on networks by analyzing the data to be sent in the data packets. The data packets are transformed into vectors of continual and categorical parameters like flags, size, and addresses, among other things, that indicate the existence of network links [8]. This vector is compared to preregistered vectors linked with assaults, namely signature-based ID or normal traffic. To find intrusions, the vector can be used as input to machine learning (ML) classification methods or statistical techniques [9]. But, with the complex growth of the network environment and wide-ranging application of IoT terminal equipment, it becomes hard to explore the security vulnerability in the network, and the techniques of network attack are hard to forecast [10]. Many prevailing ID technologies need help to fulfil the demands.

This article focuses on developing IDS using Double Adaptive Weighting Arithmetic Optimization Algorithm with Deep Learning (DAWAOA-DL) technique in the IoT environment. The presented DAWAOA-DL technique involves the design of the DAWAOA technique for the feature selection procedure. Next, the intrusion detection task uses the convolutional neural network-gated recurrent unit (CNN-GRU) approach. Finally, the Adam optimizer is exploited as a hyperparameter optimizer of the CNN-GRU methodology. A series of simulations were performed on the BoT-IoT dataset to exhibit the effectual detection performance of the DAWAOA-DL technique.

RELATED WORK

Shah and coauthors [11] modeled an AI-related mechanism with two objectives. Initially, it identifies the malicious users who attempt to compromise the IoT platform with dual classifier problems. Also, to provide tamper-proof storage for storing non-malicious IoT datasets,blockchain (BC) technology is leveraged. DL methods can be utilized to categorize non-malicious and malicious smart contracts. [12],modelled3 DL methods for classifying the intrusions: a CNN, an LSTM, and a hybrid CNN, including the LSTM method. The complexities of the network data were minimized dimensionality, and to enhance the presented mechanism, the PSO has been utilized for choosing related attributes from the network dataset. Thamilarasu and Chawla [13] developed an intellectual IDS for the IoT environment. To be specific, the author leveraged a DL method for finding attacks in IoT networks. The detection solution facilitates interoperability between different network transmission protocols utilized in IoT and provides security. The author assessed the presented detection structure with the use of real-network traces to offer a proof of concept.

Al-Amiedyand coauthors [14] devised and applied the IoT features extraction CNN named IoTFECNN includes a hybrid layer for better IoT AD. In [15], a new AD-related IDS for IoT systems was developed. Initially, a CNN approachwas utilized for framing a multiclass classification model. This method was applied with the help of CNNs in 3D, 1D, and 2D. TL has been applied for executing multiclass and binary classification using the CNN multiclass pre-trained method. This technique makes use of IoT-23 datasets, BoT-IoT, and MQTT-IoT-IDS2020. Alalhareth and coauthors [16] devise a secure automated two-level IDS (SATIDS) that uses an enhanced version of LSTM based on artificial RNN and the minimum redundancy maximum relevance (MRMR) feature selecting approach for enhancing the IDS performances. SATIDS intends to find traffic anomalies with higher precision and minimise the time. The method usesInSDN and ToN-IoT datasets.

Javeed and coauthors [17] presented an SDN-based DL-driven structure for finding threats in an IoT platform. The Cuda-bidirectional long short-term memory (Cu-BLSTM) and Cu- DNNGRU classifiers are applied for the potential identification of threats. The up-to-date, openly available CICIDS2018 dataset is presented to train the hybrid model. Mamdouhand coauthors [18] modelled intelligent IDS utilizing a CNN, viz., HetIoT-CNN IDS, a DL-related CNN for the HetIoT. The presented IDS mitigates and finds different DDoS attacks successfully in the HetIoT structure. Multi-class (8- and 13-classes) and binary classification can evaluate this particular structure.

THE PROPOSED MODEL

In this article, we have developed a novel DAWAOA-DL-based intrusion detection approach in the IoT environment. The intention of the DAWAOA-DL technique lies in the accurate recognition and classification of intrusions in the IoT platform. To execute this, the presented DAWAOA-DL algorithm comprises data preprocessing, DAWAOA-based feature subset selection, CNN-GRU based detection, and Adam optimizer based hyperparameter tuning. Figure 1 shows the working flow of the DAWAOA-DL algorithm.

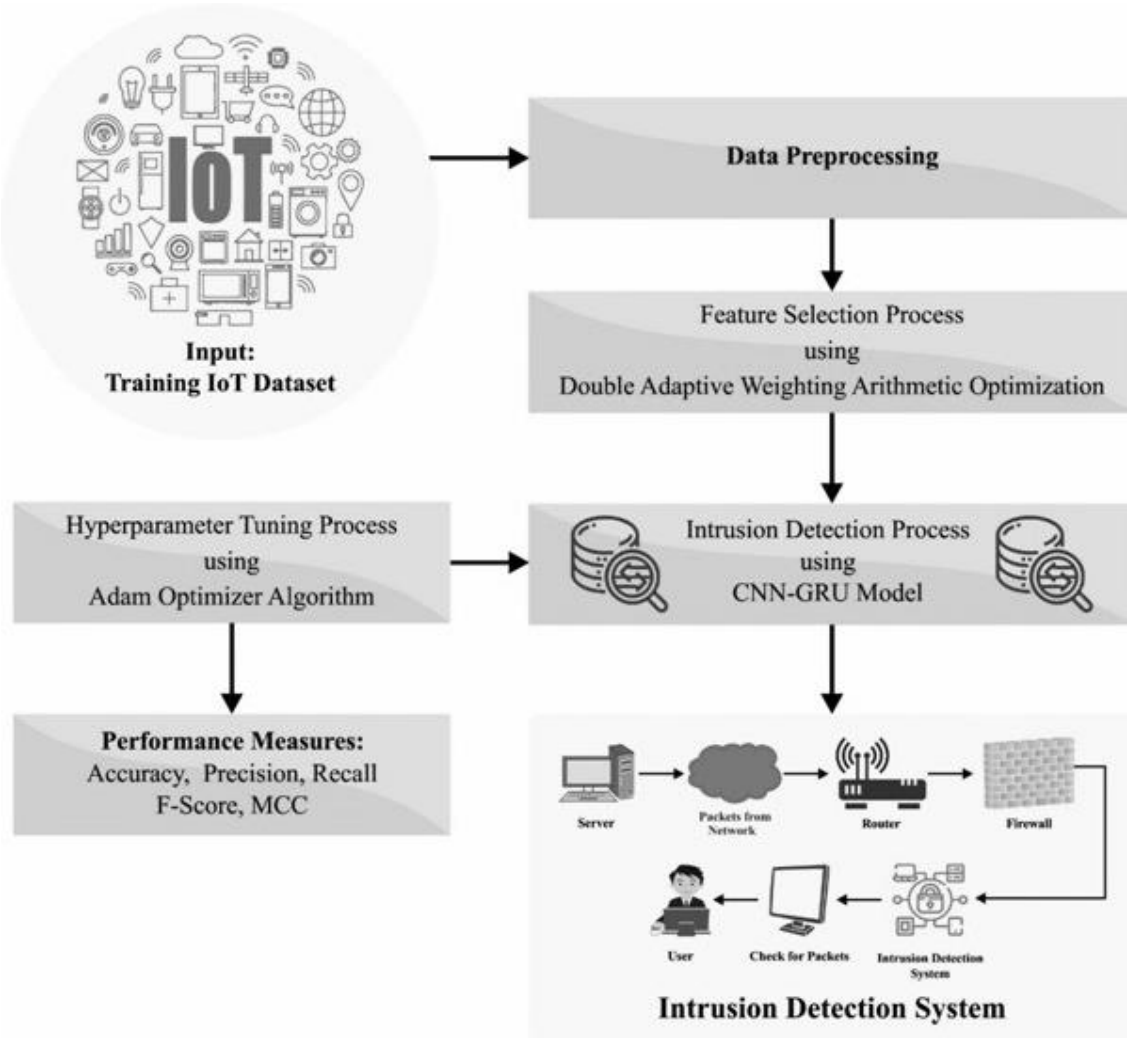


Figure 1. Working flow of DAWAOA-DL algorithm

Data Pre-processing

At first, the dataset feature was preprocessed by the Linear Scaling Normalization (LSN) [19]. By normalizing the dataset's features, the problem of large number ranges being dominatedcan be prevented, which assists to make accurate predictions.

$$y_i' = \frac{y_i - y_{min}}{y_{max} - y_{min}} \quad (1)$$

Where $\min$ and $\max$ correspondingly denote minimal and maximal values of features. y_{min}, the actual value of the input datasetis y_{Yi}, the normalized value scaled as per the range.

Feature Selection using DAWAOA Technique

The DAWAOA technique is used to elect an optimal feature set. The proposed AOA has somewhat upgraded the solution's accuracy and stability. But the AOA easily get trapped into the local optima and slower converges[20]. The study presents that the DAWAOA depends on two approaches to resolve the problems. In this work, the perturbation produced by the basic function is added to MOP and MOA, and double adaptive weight is includedin the location updating equation. This allows the model to implement a satisfactory global search, prevent a fall into the local optimal solution, and increase the convergence rate and the accuracy of the attained solution.

The AOA has two major components, MOP andMOA, considerablyimpacting the development and exploration ability. When the amount of iterations rises, the original MOA rises, and the original MOP reduces. In the presented method, random perturbations produced by the simple function were proposed for improving the two variables. This could reduce the probability of getting trapped in local optima, increase the convergence capability, and balance the exploration and exploitation performance.

Furthermore, the MOP and MOA parameters are multiplied with the g and h coefficients correspondingly to enhance the parameter using the random fluctuation produced by the primary function:

$$MOP(t)=\left(1-\frac{t^{\frac{1}{\alpha}}}{T^{\frac{1}{\alpha}}}\right)\times g \tag{2}$$

$$MOA(t)=\left(\min+(\max-\min)\times\frac{t^{\frac{1}{3}}}{T^{\frac{1}{3}}}\right)\times h \tag{3}$$

$$g=|m_1\times\operatorname{acos}(m_3)| \tag{4}$$

$$h=|m_2\times\operatorname{acos}(m_3)| \tag{5}$$

The coefficient values g and h are evaluated by Eqs. (4) and (5); m_1 and m_2 denotes the constant parameters, m_1 is fixed as 1.2, m_2 is fixed as 0.65, and m_3 shows the random integer within $[0,1]$.

In this work, the locally developed and globally explored location updating equation was critical in the search for optimum solution. But some solutions might get trapped in the local optima due to the limited search region. A dual adaptive weighting approachhas been proposed. The weight curve decreased gradually based on the level where the algorithm easily fall into local optima. In the DAWAOA technique, adaptive weight w_1 is applied once the AOA implements subtraction and division operators, and adaptive weight w_2 is applied once it implements addition and multiplication operators. This prevents local optimum stagnation while enhancing local search ability and the solution's accurateness. The location updating formula for the two phases is shown below.

$$x_{i,j}(t+1)=\begin{cases}w_1\times best(x_j)\div(MOP+\varepsilon)\times V_j & r2\le 0.5\\ w_2\times best(x_j)\times MOP\times V_j & r2>0.5\end{cases} \tag{6}$$

$$x_{i,j}(t+1)=\begin{cases}w_1\times best(x_j)-MOP\times V_j & r3\le 0.5\\ w_2\times best(x_j)+MOP\times V_j & r3>0.5\end{cases} \tag{7}$$

$$w_1=\left(1-\frac{t}{T}\right)^{1-\tan\left(\pi\times(rand-0.5)\right)\times\frac{S}{T}} \tag{8}$$

$$w_2=\left(2-\frac{2t}{T}\right)^{1-\tan(\pi\times(rand-0.5))\times\frac{S}{T}} \tag{9}$$

The w_1 andw_2 weight values are given by Eqs. (8) and (9), where the present and maximal amount of iterations are represented as t and T, correspondingly; rand indicates a randomly generated value within [0,1]. The pseudocode of DAWAOA is demonstrated in Algorithm 1.

Algorithm 1: *Pseudocode of the DAWAOA*

Initialization parameter and population position $X_i(i = 1,2 \ldots N)$
While $(t < T)$
MOP $(t)=\left(1-\frac{t^{\frac{1}{\alpha}}}{T^{\frac{1}{\alpha}}}\right)\times g$,MOA(t)$=\left(\min+(\max-\min)\times\frac{t^{1/3}}{T^{1/3}}\right)\times h$
For i=1: N
For j$= 1: N$
If r1>MOA
If r2 > 0.5 (exploration stage)

$$x_j,i(t+1)=w_1\times best(x_j)\div(MOP+\varepsilon)\times V_j$$

Else

$$x_{i,j}(t+1)=w_2\times best(x_j)\times MOP\times V_j$$

End if
If $r3 > 0.5$ (development stage)

$$x_{i,j}(t+1)=w_1\times best(x_j)-MOP\times V_j$$

Else

$$xi,j(t+1)=w_2\times best(\chi_{j)}+MOP\times y_j$$

End if
End if
End for
End for
End while

Return to the optimum solution

In the DAWAOA methodology, the objectives are compiled into one objective equationso that a current weight recognized every objective importance [21]. Here, a fitness function was adoptedwhichintegrates both objectives of FS as follows.

$$Fitness(X)=\alpha\cdot E(X)+\beta^*\left(1-\frac{|R|}{|N|}\right) \quad (10)$$

Where (X) denotes classifier error rate through the features chosen in X subset, $Fitness(X)$ shows fitness value of the subset $X, E|R|$ and $|N|$refers to the amount of selected and original attributes in the data correspondingly, α and βrefers to weights of classifier error and reduction ratio, $\alpha \in [0,1]$ and $\beta = (1-\alpha)$applied.

Intrusion Detection using Optimal CNN-GRU Model

For intrusion detection and classification process, the CNN-GRU model is utilized. Many excellent evolution models were produced with regard to RNN, namely GRU and LSTM [22]. This model resolves the problem of LTD with the memory unit and avoids gradient explosion using gating mechanism. UnlikeLSTM, GRU combines input and forget gates into update gate, as well as combines the hidden and cell states so that there are fewer parameters and the training is very fast. Thus, the GRU was selected for feature extraction. The activation of j^{th}hidden units is evaluated using the following equation:

$$\begin{cases} r_j=\sigma([W_r x]_j+[U_r h_{(t-1)}]_j) \\ z_j=\sigma([W_Z x]_j+[U_Z h_{(t-1)}]_j) \\ \tilde{h}_j^{(t)}=f([Wx]_j+r_j[Uh_{(t-1)}]) \\ h_j^{(t)}=z_j h_j^{(r-1)}+(1-z_j)\tilde{h}_j^{(t)} \end{cases} \quad (11)$$

In Eq. (11),z_j represents the update gate, f indicates the $\tanh$ functionr_j refers to the reset gate,σ is a sigmoid logical function;$h_{(r-7)}$ indicates input and hidden states of prior state, correspondingly,h_j shows actual activation of the unit, $[.]_j$ represents the j^{th}component of vector and, x and W_r and U_r denotes weight matrix. The reset gate defines how to integrate new input dataset with prior memory.

The CNN-GRU was split into two parts (prediction and training). We created six-layer DNN architecture: the last two were FC layer, the initial two CNN layers, and middle two were GRU layers.

For the next convolutional layer, $0$is no longer filled at the edge to reduce redundancy of eigenvalue, and $a(N-2)\times(N-2)\times60$ eigenmaps were finally attained. The amount of input features for all the time steps was 4, and the data format was converted. The hidden state value of time step of these layers is returned for output series, and the output series of initial GRU layer was inputted to the next GRU layer. The cross-entropy loss function was introduced into the NN for selecting the better performance model.

$$L=\frac{1}{N}\sum_{i=1}^{N}\sum_{k=1}^{K}\gamma_j^k * \log\hat{y}_i^k \quad (12)$$

In Eq. (12), $\hat{y}_i^k$ denotes the prediction possibility of observation sample i^{th} belongs to class k.N means the amount of samples, K indicates the amount of categories, y_j^{k} shows sign function (1 or 0) if true type of i^{th} sample was equivalent to k equals 1, or else 0. Figure 2 demonstrates the framework of GRU model.

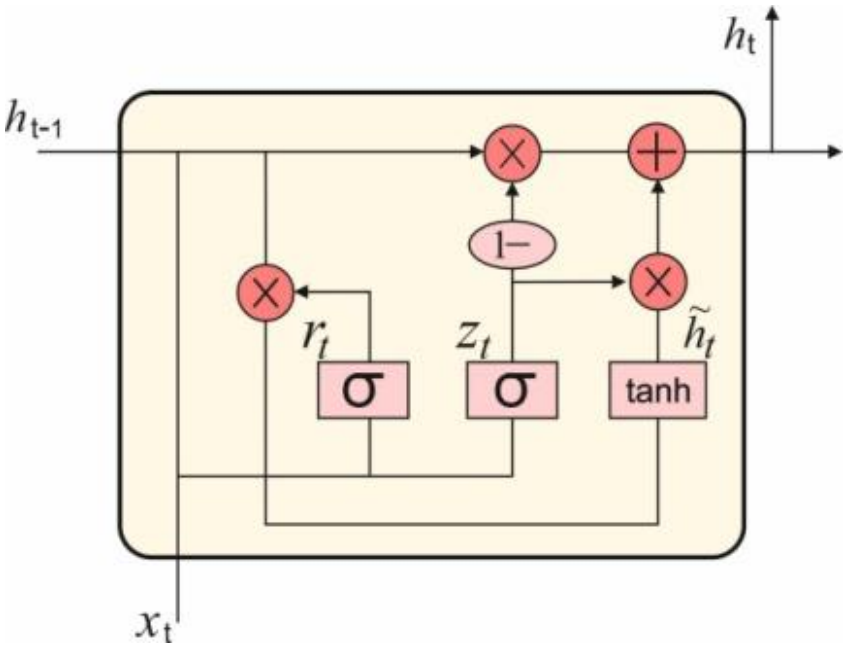


Figure 2. Structure of GRU

The Adam optimiser is used to adjust the hyperparameter values of the CNN-GRU model. Adam is a DNN training-specific adaptive learning rate optimization technique initially developed in 2014. It gained a higher attraction from several researcher workers because of its higher performance than RMSprop or SGD [23].

The method exploits adaptive learning rate technique to define the learning rate for all the parameters. Adam's algorithm effectively handles complicated problems, including many records or variables. It needs less memory and is reliable. It is a fusion of the 'RMSP' methods and 'gradient descent with momentum. The momentum process speed up the GDA by considering 'exponentially weighted average' of the gradient. Furthermore, it exploits the benefits of Adagrad to implement well in environments with sparse gradient. However, it struggles with non-convex optimization of NN. Also, it uses the benefits of RMSprop to overcome the shortcomings of Adagrad and to implement well in online settings.

$$w_{t+1}=w_t-\alpha m_t \quad (13)$$

Hence,

$$m_t=\beta m_{t-1}+(1-\beta)\left[\frac{\delta L}{\delta w_t}\right] \quad (14)$$

Where β indicates the moving average parameter. m_{t-1} denotes the aggregate of gradient at t1time, W_t indicates the weight at time t, m_t shows gradients aggregate at t time, W_{t+1} denotes the weights at time $t+1, \partial W_t$ denotes the derivative of the weight at time t, α_t represents the learning rate at time $t, \partial L$ shows the derivative of loss function.

RESULTS AND DISCUSSION

In this study, the experimental outcomes of the DAWAOA-DL method take place on the BoT-IoT database [24, 25]. It comprises normal and attack samples, as shown in Table 1.

Table1. Details of databases

Class	Sub-Category	No. of Records
Normal		2000
Attack	Reconnaissance	2000
	DoS	2000
	DDoS	2000
	Information theft	2000
Total Number of Attacks		10000

Figure 3 shows the classifier outcomes of the DAWAOA-DL method on binary class. Figure 3a shows the confusion matrix presented by the DAWAOA-DL approach on 70% of TRP. The figure denoted that the DAWAOA-DL approach has detected 1403 samples under normal and 5547 samples on attack. Moreover, Figure 3b portrays the confusion matrix rendered by the DAWAOA-DL approach on 30% of TSP. The figure specified that the DAWAOA-DL method had identified 579 samples on normal and 2402 samples on attack.

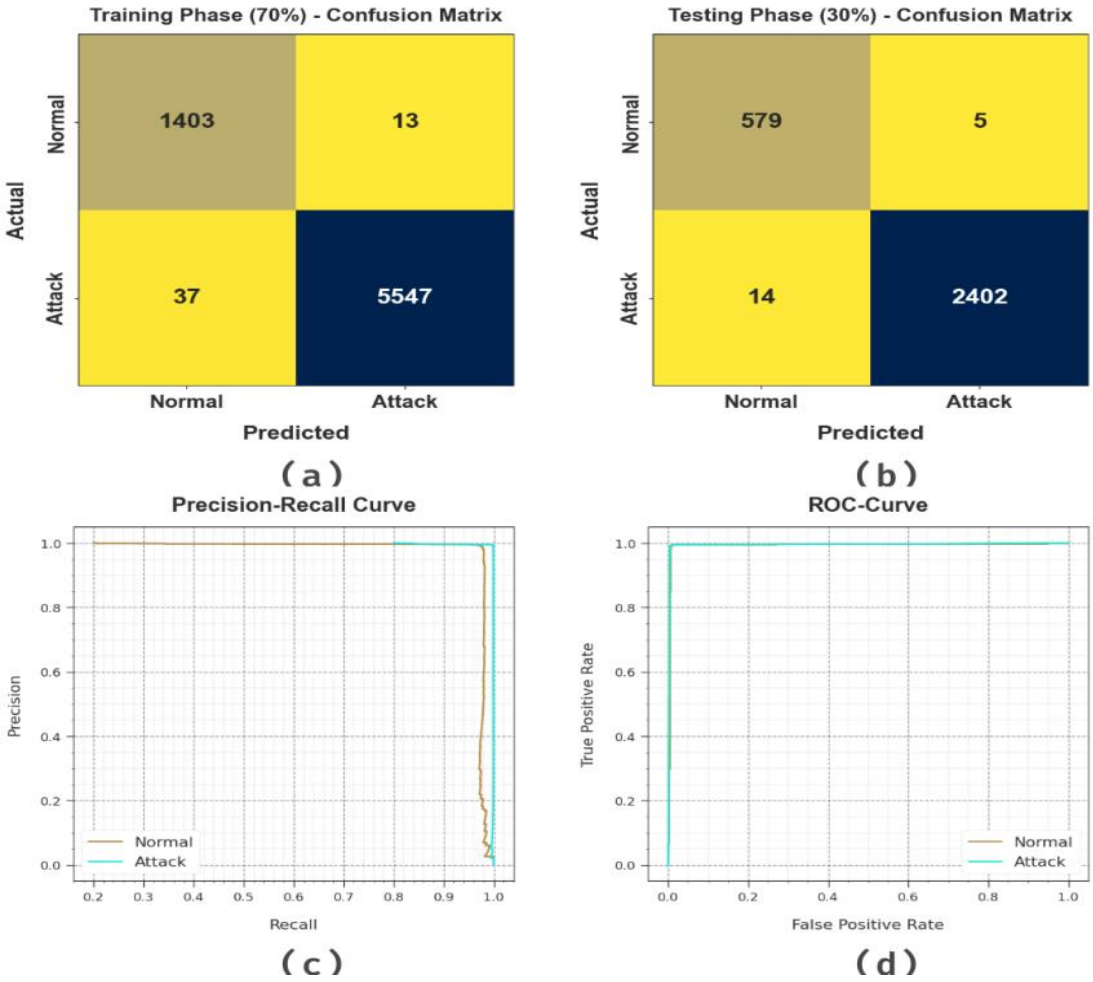


Figure 3. Classifier outcome DAWAOA-DL approach on binary class (a-b) Confusion matrices, (c) PR curve, and (d) ROC curve

Likewise, Figure 3c demonstrates the PR analysis of the DAWAOA-DL methodology. The figure pointed out that the DAWAOA-DL approach has gained maximal PR performance in every class. Eventually, Figure 3d shows the ROC investigation of the DAWAOA-DL model. The figure portrayed that the DAWAOA-DL method has productive results with maximum ROC values on different class labels.

Table 2 and Figure 4 demonstrate the overall binary classification outcomes of the DAWAOA-DL methodology are demonstrated. The results showed that the DAWAOA-DL technique resulted in effectual performance in all classes. For instance, on 70% of TRP, the DAWAOA-DL technique attains average $accu_y$ of 99.21%, $prec_n$ of 98.60%, $reca_l$ of 99.21%, F_{score} of 98.90%, and MCC of 97.81%. Meanwhile, on 30% of TSP, the DAWAOA-DL method gained average $accu_y$ of 99.28%, $prec_n$ of 98.72%, $reca_l$ of 99.28%, F_{score} of 99%, and MCC of 98%.

Table 2. Classifier outcome of DAWAOA-DL method on binary class

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	MCC
		Training Phase (70%)			
Normal	99.08	97.43	99.08	98.25	97.81
Attack	99.34	99.77	99.34	99.55	97.81
Average	99.21	98.60	99.21	98.90	97.81
		Testing Phase (30%)			
Normal	99.14	97.64	99.14	98.39	98.00
Attack	99.42	99.79	99.42	99.61	98.00
Average	99.28	98.72	99.28	99.00	98.00

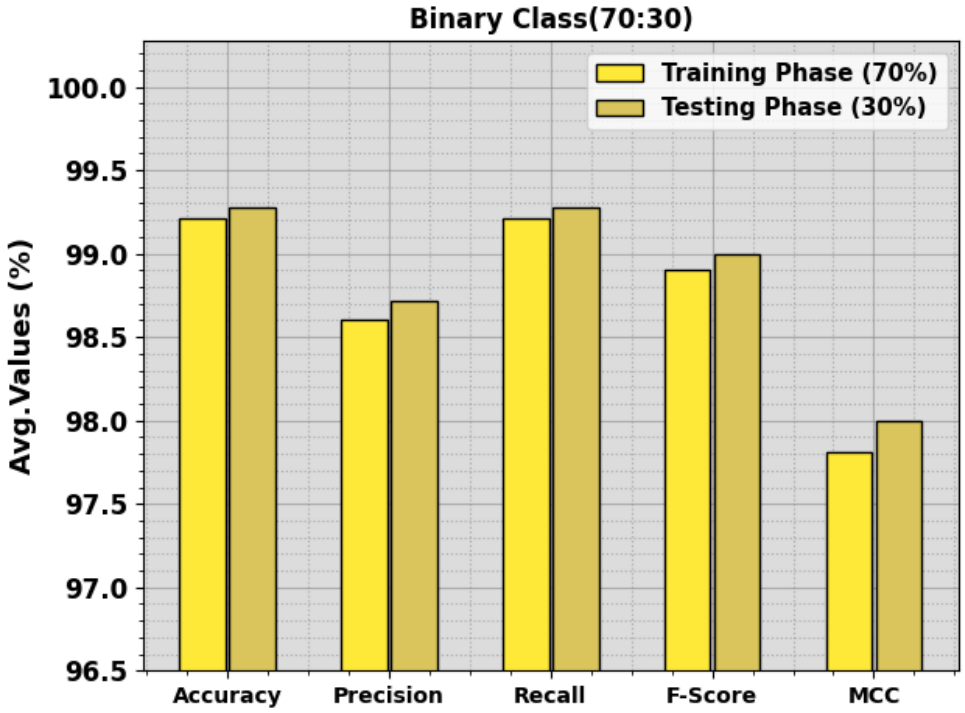


Figure 4. Average outcome of DAWAOA-DL approach on binary class

Table 3. Comparative outcome of DAWAOA-DL method with other approaches

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
DAWAOA-DL	99.28	98.72	99.28	99.00
RNN Model	94.21	95.66	95.82	95.89
LSTM Model	95.86	96.49	94.47	95.57
Ensemble Model	95.95	95.59	94.93	95.64

DeepDCA	97.02	95.2	96.89	96.53
TCNN Model	98.79	96.93	97.03	97.18
FNN Model	94.74	96.59	96.83	96.91

In Table 3 and Figure5, a comparison analysis of the DAWAOA-DL approach with current approaches is made [26]. The results indicate that the DAWAOA-DL algortihm reaches enhanced performance over other methods. At the same time, the FNN, RNN, LSTM, and ensemble models obtain poor performance, while the DeepDCA and TCNN models have reached closer results. It is noticed that the DAWAOA-DL technique attains maximum $accu_y$ of 99.28%, $prec_n$ of 98.72%, $reca_l$ of 99.28%, and F_{score} of 99%. These results show that the DAWAOA-DL technique reaches effectual performance on the intrusion detection in the IoT environment.

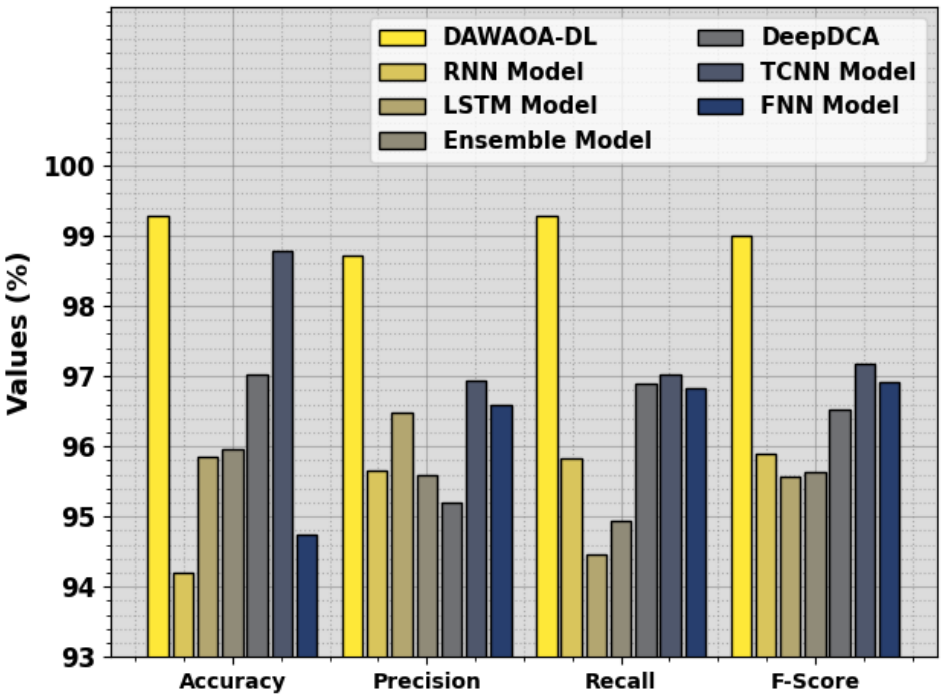


Figure 5. Comparative outcome of DAWAOA-DL approach with other algorithms

CONCLUSION

This article introduced a novel DAWAOA-DL based intrusion detection approachin the IoT environment. The intention of the DAWAOA-DL technique lies in the accurate recognition and classification of intrusions in the IoTenvironment. For execution, the presented DAWAOA-DL technique comprises data preprocessing, DAWAOA based feature subset selection, CNN-GRU based detection, and Adam optimizer based hyperparameter tuning. A series of simulations were performed on the BoT-IoT dataset to exhibit the effectual detection performance of the DAWAOA-DL technique. A widespread result analysis demonstrated the betterment of the DAWAOA-DL approach over other recent models in terms of several metrics. Therefore, the DAWAOA-DL algorithmcan be employed for enhanced intrusion detection results in the IoT environment. In the upcoming years, the performance of the DAWAOA-DL methodcan be boosted by outlier removal process.

Funding: No sponsor or fund available.
Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

1. Balyan AK, Ahuja S, Lilhore UK, Sharma SK, Manoharan P, Algarni AD, et al. A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method. Sensors (Basel). 2022 Aug 10; 22(16):5986. doi: 10.3390/s22165986.
2. Thiruvenkatasamy S, Sivaraj R, Vijayakumar M. Blockchain Assisted Fireworks Optimization with Machine Learning based Intrusion Detection System (IDS). TV-TG. 2024; 31(2): 596-603. doi:10.17559/TV-20230712000798

3. Javed A, Awais M, Shoaib M, Khurshid KS, Othman M. Machine learning and deep learning approaches in IoT. PeerJ Comput Sci. 2023 Feb 6; 9:e1204. doi: 10.7717/peerj-cs.1204.
4. Rihan SDA, Anbar M, Alabsi BA. Approach for Detecting Attacks on IoT Networks Based on Ensemble Feature Selection and Deep Learning Models. Sensors (Basel). 2023 Aug 23; 23(17):7342. doi: 10.3390/s23177342.
5. Ahmed S, Irfan S, Kiran N, Masood N, Anjum N, Ramzan N. Remote Health Monitoring Systems for Elderly People: A Survey. Sensors (Basel). 2023 Aug 10; 23(16):7095. doi: 10.3390/s23167095.
6. Haque S, El-Moussa F, Komninos N, Muttukrishnan R. A Systematic Review of Data-Driven Attack Detection Trends in IoT. Sensors (Basel). 2023 Aug 15; 23(16):7191. doi: 10.3390/s23167191.
7. Thiruppathi M, Vinoth Kumar K. Seagull Optimization-based Feature Selection with Optimal Extreme Learning Machine for Intrusion Detection in Fog Assisted WSN. TV-TG. 2023; 30(5): 1547-1553. doi: 10.17559/TV-20230130000295.
8. Khan BUI, Olanrewaju RF, Anwar F, Mir RN, Najeeb AR. A critical insight into the effectiveness of research methods evolved to secure IoT ecosystem. Int. J. Inf. Comput. Secur. 2019; 11:332–54. doi: 10.1504/IJICS.2019.101908.
9. Luo K. A distributed SDN-based intrusion detection system for IoT using optimized forests. PLoS One. 2023 Aug 30; 18(8):e0290694. doi: 10.1371/journal.pone.0290694.
10. Yazdinejad A, Kazemi M, Parizi RM, Dehghantanha A, Karimipour H. An ensemble deep learning model for cyber threat hunting in industrial internet of things. Digit Commun Netw, 2023; 9(1):101-10. doi: 10.1016/j.dcan.2022.09.008
11. Shah H, Shah D, Jadav NK, Gupta R, Tanwar S, Alfarraj O, et al. Deep Learning-Based Malicious Smart Contract and Intrusion Detection System for IoT Environment. Mathematics, 2023;11(2):418. doi: 10.3390/math11020418.
12. Morales-Molina CD, Hernandez-Suarez A, Sanchez-Perez G, Toscano-Medina LK, Perez-Meana H, Olivares-Mercado J, et al.A Dense Neural Network Approach for Detecting Clone ID Attacks on the RPL Protocol of the IoT. Sensors (Basel). 2021 May 3;21(9):3173. doi: 10.3390/s21093173.
13. Thamilarasu G, Chawla S. Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. Sensors (Basel). 2019 Apr 27;19(9):1977. doi: 10.3390/s19091977.
14. Kavitha S, Uma Maheswari N, Venkatesh R. Intelligent Intrusion Detection System using Enhanced Arithmetic Optimization Algorithm with Deep Learning Model. TV-TG. 2023; 30(4): 1217-24. doi: 10.17559/TV-20221128071759
15. Ullah S, Ahmad J, Khan MA, Alkhammash EH, Hadjouni M, Ghadi YY, et al. A New Intrusion Detection System for the Internet of Things via Deep Convolutional Neural Network and Feature Engineering. Sensors (Basel). 2022 May 10;22(10):3607. doi: 10.3390/s22103607.
16. Premkumar M, Sundararajan TVP, Mohanbabu G. Dynamic Defense Mechanism for DoS Attacks in Wireless Environments Using Hybrid Intrusion Detection System and Statistical Approaches. TV-TG. 2022; 29(3): 965-70. doi: 10.17559/TV-20210604113859
17. Javeed D, Gao T, Khan MT, Ahmad I. A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT). Sensors (Basel). 2021 Jul 18;21(14):4884. doi: 10.3390/s21144884.
18. Mamdouh M, Awad AI, Khalaf AAM, Hamed HFA. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. Comput. Secur. 2021;111:102491. doi: 10.1016/j.cose.2021.102491.
19. Albulayhi K, Smadi AA, Sheldon FT, Abercrombie RK. IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. Sensors (Basel). 2021 Sep 26;21(19):6432. doi: 10.3390/s21196432.
20. Du H, Zhou S, Yan W, Wang S. Study on DNA Storage Encoding Based IAOA under Innovation Constraints. Curr Issues Mol Biol. 2023 Apr 18;45(4):3573-90. doi: 10.3390/cimb45040233.
21. Mafarja M, Thaher T, Al-Betar MA, Too J, Awadallah MA, Abu Doush I, et al. Classification framework for faulty-software using enhanced exploratory whale optimizer-based feature selection scheme and random forest ensemble learning. Appl Intell (Dordr). 2023 Feb 9:1-43. doi: 10.1007/s10489-022-04427-x.
22. Zhao X, Miao C. Spatial-Temporal Changes and Simulation of Land Use in Metropolitan Areas: A Case of the Zhengzhou Metropolitan Area, China. Int J Environ Res Public Health. 2022 Oct 28;19(21):14089. doi: 10.3390/ijerph192114089.
23. Vinoth Kumar K, Thiruppathi M. Oppositional Coyote Optimization based Feature Selection with Deep Learning Model for Intrusion Detection in Fog Assisted Wireless Sensor Network. Acta Montan. Slovaca. 2023; 28(2): 496-508. doi: 10.46544/AMS.v28i2.18.
24. Alabsi BA, Anbar M, Rihan SDA. CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks. Sensors (Basel). 2023 Jul 19;23(14):6507. doi: 10.3390/s23146507.
25. Rajakani V, Vinoth Kumar K. Barnacles Mating Optimizer with Hopfield Neural Network Based Intrusion Detection in Internet of Things Environment. TV-TG. 2023; 30(6): 1821-8. doi: 10.17559/TV-20230414000533.
26. Salman EH, Taher MA, Hammadi YI, Mahmood OA, Muthanna A, Koucheryavy A. An Anomaly Intrusion Detection for High-Density Internet of Things Wireless Communication Network Based Deep Learning Algorithms. Sensors (Basel). 2022 Dec 25;23(1):206. doi: 10.3390/s23010206.

© 2024 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)