Securing IoT Devices Based on Zero Trust Intrusion Detection System Using Deep Learning with Sine Cosine Algorithm

Sergey Bakhvalov[1], Viktor Starostin[2], Rafina Zakieva[3], M Ilayaraja[4] and E. Laxmi Lydia[5,*]

[1] *Candidate of Economic Sciences, Associate Professor of Department of Economics and Management of Elabuga Institute, Kazan Federal University, Kazan, Russia; bakhvalov.s.yu@yandex.ru*

[2] *Candidate of Medical Sciences, Associate Professor of Department of Theories and Principles of Physical Education and Life Safety, North-Eastern Federal University named after M.K. Ammosov, Yakutsk, Russia; resprofsci@gmail.com*

[3] *Doctor of Pedagogical Sciences, Associate Professor of Department of Industrial Electronics, Kazan State Power Engineering University, Kazan, Russia;*

zakievarr@inbox.ru

[4] *School of Computing, Kalasalingam Academy of Research and Education, Krishnankoil, India; ilayaraja.m@klu.ac.in*

[5] *Department of Information Technology, VR Siddhartha Engineering College(A), Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada, India; elaxmi2002@yahoo.com*

Abstract

The rapid growth of Internet of Things (IoT) devices provides distinct challenges in preserving the privacy and security of interconnected systems. As cyber-attacks are more common, evolving a scalable and effective Intrusion Detection System (IDS) based on deep learning (DL) for IoT has become more complex. When handling evolving and dynamic cyberattacks, the present techniques are unable to balance temporal and spatial feature extraction. The lack of diversity in dataset employed for DL-based IDS evaluation also interferes with evolution. Besides, there is a significant trade-off between scalability and performance, mainly when the amount of edge devices in communication upsurges. To tackle these challenges, this research paper presents a horizontal DL method that unites Bidirectional Long-Term Short Memory (BiLSTM) and Convolutional Neural Network (CNN) for efficient intrusion detection. This article introduces a novel Sine Cosine Algorithm with Deep Learning based Zero Trust Intrusion Detection System (SCADL-ZTIDS) method for secure IoT Devices. The foremost intention of the SCADL-ZTIDS technique rests in the effectual and automated classification of zero trust IDS. In the first stage, the SCADL-ZTIDS approach endures a min-max scaler utilizing data pre-processing to convert the actual data into beneficial form. Moreover, the deep neural network (DNN) technique is employed for the identification and classification of intrusions. Furthermore, the sine cosine algorithm (SCA) is utilized for fine-tuning the parameters contained in the DNN method. To describe the heightened performance of the SCADL-ZTIDS approach, a wide range of empirical analyses are implemented on benchmark datasets, and the outcomes are examined under various features. The simulation outcomes highlighted the improved intrusion detection performance of the SCADL-ZTIDS approach over the recent DL techniques.

Keywords

Intrusion Detection System, Zero Trust, IoT Devices, Sine Cosine Algorithm, Deep Learning, Data Pre-Processing

Proceedings of SNSFAIT 2024: International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies, Delhi, India, August 08-09th, 2024

[1*] Corresponding author : , elaxmi2002@yahoo.com –(E. Laxmi Lydia)

[†] These authors contributed equally.

bakhvalov.s.yu@yandex.ru (Sergey Bakhvalov); resprofsci@gmail.com (Viktor Starostin); zakievarr@inbox.ru (Rafina Zakieva), ilayaraja.m@klu.ac.in -(M Ilayaraja)

1. Introduction

The Internet of Things (IoT) transformed digital connectivity by presenting smart communication techniques, resulting in more reliable, dynamic, and efficient network communication [1]. It enables intelligence network processes amongst manual objects using sensors and a communication protocol. Sensors generate a connectivity set-up by connecting the applicants, and the communication protocol controls the flow of data over the network [2]. From this perspective, the idea of zero trust turns out to be critical. Cyber experience in IoT creates chances for different antagonistic pursuits like malware exploits, Denial of Service (DoS) attacks, phishing schemes, IoT botnet infiltrations, routing manipulations, Man-in-the-Middle (MITM) attacks, and tasks associated with cloud securities [3].

The zero-trust method has become progressively more widespread as administrations look to improve their cybersecurity posture in front of developing threats [4]. By pretentious that each customer, application, and network device is untrustworthy till confirmed reliable, the zero-trust approach can assist in reducing the attack footsteps and reduce data breaches by incessantly authenticating and verifying devices, applications, and users in an active environment [5]. The zero-trust concentrated on limiting source access and admitting access on the standard of the minimum privileges necessary to implement the desired task. An operative description of zero trust is whether it be a security approach that needs continuous authentication and verification of all devices, applications, and users' earlier allowing access to resources [6]. Zero trust is a complete security outline and operating policies that execute the zero-trust method over an organization's complete networks, to reduce the threat of data breaches and cyberattacks [7].

The safety of IoT networks besides cyber threats is becoming a paramount study area in modern years [8]. Artificial Intelligence (AI) based methodologies, particularly Federated Learning (FL), have stored significant attention for recommending security resolutions because of their privacy-preserving mechanism and reliability [9]. The FL-based Intrusion Detection System (IDS) functions in a systematic design except for real data interchange among the participant nodes and the central server; as an alternative, this method upgrade is shared among the communication party [10]. FL significantly supports continuous learning methods in which iterative cycles are executed, succeeding that the central server has distributed the universal approach. When training at the confined data nodes, this method upgrades were transferred back to the server.

This article introduces a new Sine Cosine Algorithms with DL based Zero Trust Intrusion Detection System (SCADL-ZTIDS) method for secure IoT Devices. In the first stage, the SCADL-ZTIDS approach endures min-max scaler utilizing data preprocessing to transform the actual data into beneficial forms. Moreover, the deep neural network (DNN) technique is employed for the identification and classification of intrusions. Furthermore, the sine cosine algorithm (SCA) is utilized for fine-tuning the parameters contained in the DNN method. To describe the heightened performance of the SCADL-ZTIDS approach, wide range of empirical analyses are implemented on benchmark datasets, and the results are studied below various features.

2. Related Works

Dhanya and Chitra [11] present a DL method named Autoencoder to encode the IoMT data. The encoding features are provided to an XGBoost Classification whose hyper-parameters are enhanced by utilizing the Genetic Algorithms. XGBoost classification identifies the occurrence of malware in the clamp and IoMT datasets by a precision correspondingly. This lightweight method attains the reduction of dimensionality using Autoencoder and efficiently identifies malware with an enhanced XGBoost classification through limited computing cost and faster convergence. In [12], an improved DL method based on uniting XGBoost and AutoEncoder (AE)

method is presented. At initial, the SHapley Additive exPlanations (SHAPs) FS technique is utilized to choose the proper subset features. Then, the AE is trained on the preceding subsets to study a squeeze representation of the input feature. The latent representation produced by the AE is utilized as input for the XGBoost method, simultaneously, Grid Search Cross Validation (GSCV) is utilized to detect the optimum hyper-parameters for the AE-XGBoost.

Zhu and Liu [13] present a new technique that leverages a single combination of ensemble learning and subspace clustering. This structure incorporates 3 advanced tactics: Iterative Feedback Loop (IFL), Two Level Decision Making (TDM), and Clustering Results as Features (CRFs). This method uses common data for the selection of features and uses 4 sub space clustering methods–, LOF, SUBCLU, PROCLUS, and CLIQUE– to generate further feature sets. 3 base learners – XGB, NB, and LGBM– are utilized in conjunction with a Logistic Regression (LR) Meta learners. To tune our method, the method employs a Particle Swarm Optimizer (PSO) for the optimization of hyper-parameters. Cheng *et al.* [14] present an in vehicle IDS, which incorporates an integration of stream clustering and sparse regularization convolutional AE (SRCAE) to create a deep evolving stream clustering method, like DESC-IDS. Particularly, this technique encodes the constant message as a 2D data frame that is fed into the SRCAE created by the temporal CN (TCN) method. In [15], an optimum secure defense mechanism is presented for DDoS in IoT networks utilizing the feature optimization and intrusion detection system (OSD-IDS). The method proposes an improved ResNet structure for feature extraction that mines many profound features from the traces of given traffic traces. An improved quantum query optimizer (IQQO) method is utilized in FS. The model designs an accurate and fast intrusion detection mechanism, called as hybrid DL method that incorporates CNN and diagonal XG boosting (CNN-DigXG) methods.

3. Methodology

In this article, we have introduced a novel SCADL-ZTIDS method for secure IoT Devices. The foremost intention of the SCADL-ZTIDS technique rests in the effectual and automated classification of zero trust IDS. It contains three distinct processes such as preprocessing, classification, and parameter tuning are demonstrated in Fig. 1.

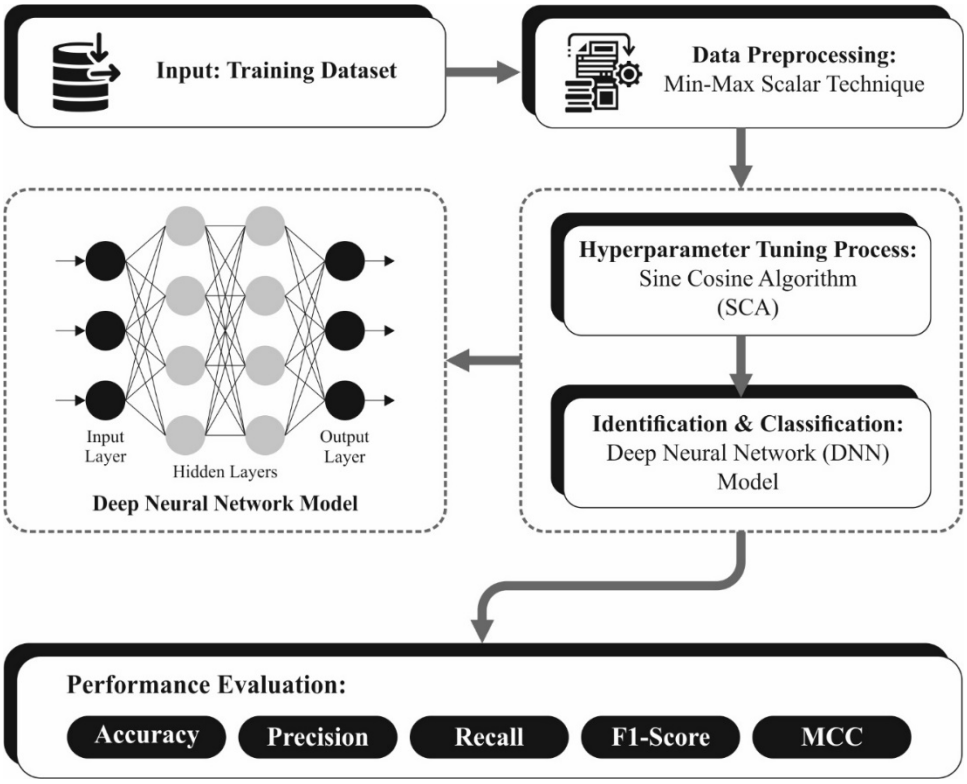

Figure 1: Overall process of SCADL-ZTIDS method

3.1. Min-max Scaler

In the first stage, the SCADL-ZTIDS approach endures min-max scaler utilizing data preprocessing to transform the actual data into beneficial forms. The Min-Max Scaler is a vital data pre-processing method employed to regularize the scope of feature values [16]. By scaling feature to a standard range, usually [0, 1], the Min-Max Scaler certifies that every feature donates evenly to the method, averting any distinct feature from unevenly influencing the outcomes. This normalization is vital to enhance the accuracy and performance of ML techniques in identifying intrusions, as it permits the model to progress input data effectively and consistently, increasing its capability to detect latent security threats in an IoT environment.

3.2. Intrusion Detection using DNN Model

Next, the DNN technique is utilized for the identification and classifier of intrusions. A DNN is a novel kind of artificial neural network (ANN), which contains many layers and authorizes it to obtain data and appeal conclusions from wide databases [17]. DNN excels in speech and image detection tasks, exhibiting their skill to identify compound patterns and deliver specific forecasts. DNN has 3 main layers such as input, output, and hidden layer (HL). The DNN is organized with double HLs to easily acquire the map relation between the output and input data by engaging the weight fitness. Throughout the stage of training, the DNN utilizes JOA to attain its objectives. In the HL, the weight of the nodes was modified. Always, the neural networks are regulating the decision limit of the categorized training data owing to the enlarged amount of training iteration. To get superior identification accuracy and quicker DNN training, dual HLs are generated. The complete quantity of nodes in the HL is defined utilizing Eq. (1).

$$j = \sqrt{M + N} + B \tag{1}$$

The input and output layers have M and N nodes, respectively. The HL has j nodes, which refers to a constant value between 1 and 10, and is signified as B.

In the HL of DNN, an activation function is comprised to allow non-linear fitness capability. Then the sigmoid is applied as an activation function.

$$A - \frac{1}{1 + e^{-p}} \tag{2}$$

P denotes the input data and is activated by the map function K_f.

$$K_f - sigm(\alpha_i P + \gamma_i) \tag{3}$$

The matrix of weight and bias among the layer of output and HL were signified by P and N, correspondingly.

To make sure the interior neuron of a DNN, we intend a supervised $loss\ function$[23–26]. This model utilizes labeled data samples. Particularly, we have a data sample (P, l), which is labeled theoretically for an HL, so we can compute the function of loss.

$$V(W_A, N_A; p, l) = \frac{1}{2s} \sum_{j=1}^{s} \| O_j(W_A, N_A; P) - l_j \|_2^2 \tag{4}$$

W_A and N_A are the sub-sets of biases; the amount of neurons in the HL is represented as S.

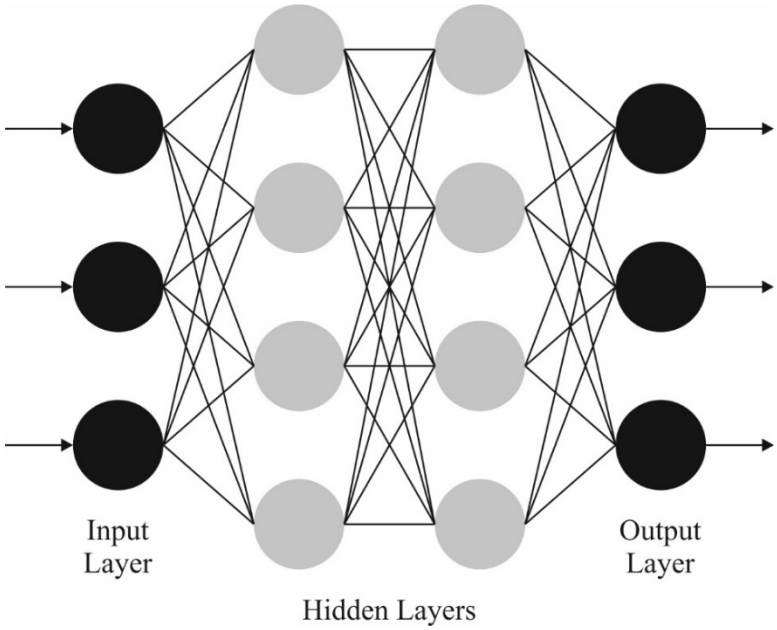

Figure 2: DNN structure

The DNN utilizes cross entropy for both testing and training uses as its loss function. This is the major development in the performance of SoftMax and sigmoid output methods. The formulation of cross entropy loss is expressed in Eq. (11).

$$R_E = \frac{1}{j} \sum_{Q=1}^{m} [\, D_Q \log \widehat{D}_k + (1 - D_Q) \log (1 - \widehat{D}_Q)] \tag{5}$$

Where j denotes the integer of training sample, D_Q and k^{th} expresses the k^{th} output of training and testing sets, respectively. Fig. 2 depicts the infrastructure of DNN.

3.3. Parameter Tuning

Eventually, the SCA is utilized for fine-tuning the parameters contained in the DNN method. The SCA is a population-based optimization algorithm that randomly produces many promising solutions for the optimization problem [18]. It exploits the mathematical equation of Sin-Cos to oscillate away from or towards the optimum solution, highlighting exploration and exploitation to find a global optimum solution in the search range.

Compared to another population-based approach, SCA has shown its maximum effectiveness in reaching global optimal solution. It explores various milestones in the search range when the sin and cos functions produce values below or beyond the one. This can be mathematically formulated as follows:

$$X_i^{t+1} = X_i^t + r_1 \sin(r_2) * \left| r_3 P_i^t - X_i^t \right| \quad (6)$$

$$X_i^{t+1} = X_i^t + r_1 \cos(r_2) * \left| r_3 P_i^t - X_i^t \right| \quad (7)$$

Where, X_i^t and P_i^t are the current and best candidate locations in the i^{th} dimension at t^{th} iterations. r_1, r_2, r_3, and r_4 are the random integers.

$$X_i^{t+1} = \begin{cases} X_i^t + r_1 * \sin(r_2) * \left| r_3 P_i^t - X_i^t \right|, r_4 < 0.5 \\ X_i^t + r_1 * \cos(r_2) * \left| r_3 P_i^t - X_i^t \right|, r_4 \geq 0.5 \end{cases} \quad (8)$$

In Eq. (8), r_1, defines whether the search range stays within or extends beyond the solution space. r_2, define the extent of this deviance from the destination. r_3 presents a random weight to the destination, de-emphasizing $((r_3) < 1)$ or emphasizing $\left((r_3) > 1\right)$ its influence on the distance. Finally, r_4 smoothly alternates between the sin and cos components. During the search process, Eq. (9) dynamically fine-tunes r_1 to balance exploration and exploitation.

$$r_1 = a - t\frac{a}{T} \quad (9)$$

Where T is the optimum iteration counter, t is the existing iteration and a is a constant value.

The SCA is harnessed for optimizing the learning rate of Patch GAN discriminator and the generator. The learning rate considerably influences performance of the model. The algorithm finds the optimum value configuration that increases a performance measure. It modifies the learning rate iteratively through a metaheuristic algorithm that seeks the configuration that leads to effective generation of real images. This ensures that the generator has been instrumental in the overall image quality.

$$x_i(t+1) = x_i(t) + r_1(t) \cdot \sin(\omega t) \cdot |p_{best}(t) - x_i(t)| + r_2(t) \cdot \cos(\omega t) \cdot |g_{best}(t) - x_i(t)| \quad (10)$$

In Eq. (10), $X(t)$ refers to the location of i^{th} particles at t^{th} iteration. $p_{best}(t)$ and $g_{best}(t)$ are the optimum location and the global optimum location of each particle. ω shows the angular frequency. $r(t)$ and $r(t)$ are two random values within [0,1]. Thus, the update of learning rate can be formulated as follows:

$$learning_{rate} = lb + 0.5 \cdot (ub - lb) \cdot \left(1 + \sin(a)\right) \quad (11)$$

In Eq. (11), lb and ub are the lower and upper boundaries of learning rates. The parameter a differs with all the iterations as follows:

$$a = \frac{2\pi t}{\max_{iter}} \quad (12)$$

In Eq. (12), t and $\max_{iter}$ are the existing and the maximal iteration counters. π indicates the mathematical constant pi. The variable a is adjusted according to the t^{th} existing iteration to the $\max_{iter}$. This makes a smooth changing variable that proportionally increases with the iteration count. The 2π term proposes a full cycle, hence the parameter a differs over the full cycle as the process repeats from 1 to $\max_{iter}$.

The SCA obtains a FF to achieve enhanced classifier performances. It defines a positive integer to express the best performances of the candidate solution. In this research, the reduction of the classifier rate of error is examined as the FF, as provided in Eq. (13).

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

4. Result Analysis and Discussion

In this section, the stimulation validation analysis of the SCADL-ZTIDS method is tested using UNSW-NB18 dataset [19], which contains 2500 sample records under five classes are represented in Table 1.

Table 1
Details on Dataset

Type of Attacks	Data Record
Normal	500
Generic	500
Exploits	500
Fuzzers	500
DoS	500
Total Record	**2500**

Fig. 3 depicts the classifier outcomes of the SCADL-ZTIDS model under the test database. Figs. 3a-3b shows the confusion matrix with correct classification and identification of all 5 classes on a 70:30 TRAP/TESP. Fig. 3c represents the analysis of PR, pointing out superior performance over all class labels. Finally, Fig. 3d denoted the analysis of ROC and portrayed efficient outcomes with greater values of ROC for different classes.

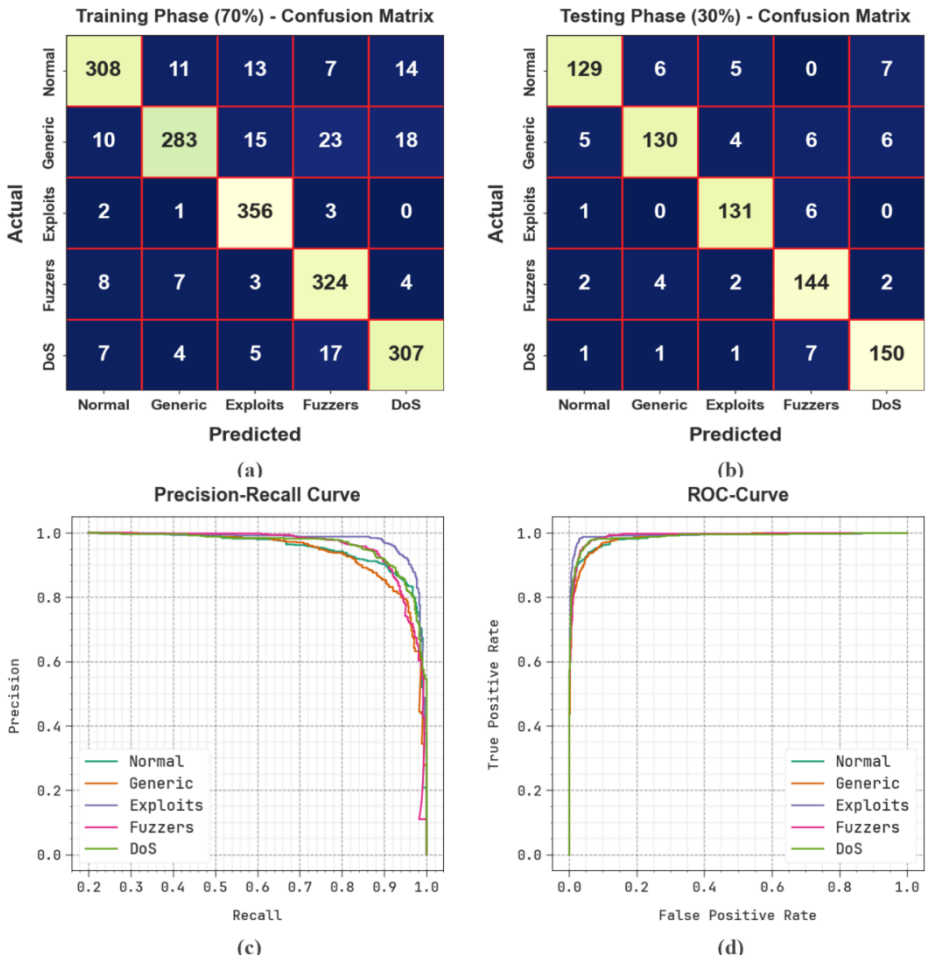

Figure 3: Classifier outcomes of (a-b) Confusion Matrices and (c-d) PR and ROC curves

Table 2 represents the detection results of the SCADL-ZTIDS approach with 70%TRAP and 30%TESP. The results inferred that the SCADL-ZTIDS model has appropriately identified five classes. With 70%TRAP, the SCADL-ZTIDS methodology gains an average $accu_y$, $prec_n$, $reca_l$, $F1_{score}$, and MCC of 96.07%, 90.28%, 90.12%, 90.05%, and 87.72%, respectively. Moreover, with 30%TESP, the SCADL-ZTIDS approach obtains average $accu_y$, $prec_n$, $reca_l$, $F1_{score}$, and MCC of 96.48%, 91.31%, 91.21%, 91.19%, and 89.04%, accordingly.

In Fig. 4, the training and validation accuracy outcomes of the SCADL-ZTIDS method are established. The precision values are calculated for 0-25 epoch counts. This figure underlined that the training and validation accuracy values display a growing trend that informed the capability of the SCADL-ZTIDS technique with enhanced performance across numerous iterations. Moreover, the training accuracy and validation accuracy stay nearer over the epoch counts which specifies less minimum overfitting and shows greater performance of the SCADL-ZTIDS systems, assuring continuous prediction on hidden instances.

Table 2
Detection outcomes of SCADL-ZTIDS approach at70%TRAP and 30%TESP

Class	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$	MCC
			TRAP (70%)		
Normal	95.89	91.94	87.25	89.53	87.02
Generic	94.91	92.48	81.09	86.41	83.57
Exploits	97.60	90.82	98.34	94.43	93.02
Fuzzers	95.89	86.63	93.64	90.00	87.52
DoS	96.06	89.50	90.29	89.90	87.45
Average	**96.07**	**90.28**	**90.12**	**90.05**	**87.72**
			TESP (30%)		
Normal	96.40	93.48	87.76	90.53	88.37
Generic	95.73	92.20	86.09	89.04	86.47
Exploits	97.47	91.61	94.93	93.24	91.70
Fuzzers	96.13	88.34	93.51	90.85	88.46
DoS	96.67	90.91	93.75	92.31	90.20
Average	**96.48**	**91.31**	**91.21**	**91.19**	**89.04**

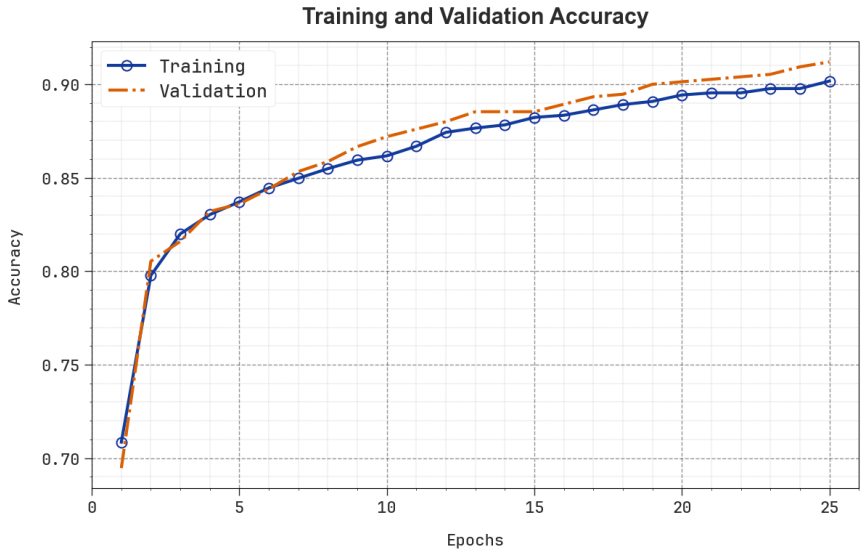

Figure 4: $Accu_y$ curve of the SCADL-ZTIDS approach

In Fig. 5, the training and validation loss graph of the SCADL-ZTIDS approach is presented. The loss values are calculated throughout 0-25 epoch counts. It is portrayed that the training and validation accuracy values demonstrate the lowest trend that reported the capacity of the SCADL-ZTIDS technique to balance a trade-off between generalization and data fitting. The consistent decrease in loss values also promises better performance of the SCADL-ZTIDS methodology and tuning of the prediction outcomes in time.

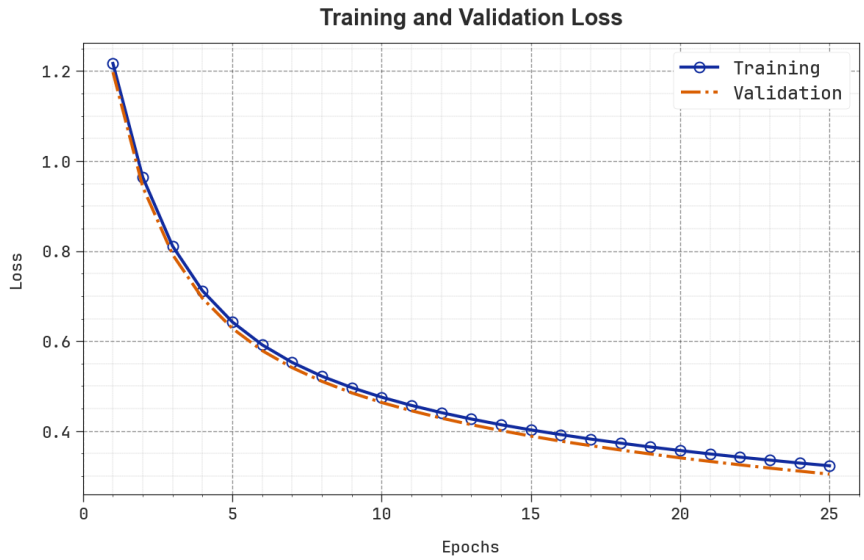

Figure 5: Loss curve of the SCADL-ZTIDS approach

Table 3
Comparative outcome of SCADL-ZTIDS approach with existing models

Research	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$
SCADL-ZTIDS	96.48	91.31	91.21	91.19
Random Forest	95.43	85.89	89.73	83.01
Decision Tree	94.20	81.94	89.13	81.29
CNN Classifier	96.00	82.84	86.71	85.28

MLP Algorithm	84.24	83.60	84.24	82.85
KNN Model	75.62	79.92	75.61	76.58
Densely-ResNet	73.93	80.94	76.68	88.11

In Table 3 and Fig. 6, the performance outcomes of the SCADL-ZTIDS method with the existing technique are provided [20-22]. These outcomes display that the Densely-ResNet approach showed inferior performance with $accu_y$, $prec_n$, $reca_l$, and $F1_{score}$ of 73.93%, 80.94%, 76.68%, and 88.11%, correspondingly. Simultaneously, the KNN methodology has attained marginally improved results with $accu_y$, $prec_n$, $reca_l$, and $F1_{score}$ of 75.62%, 79.92%, 75.61%, and 76.58%, appropriately. Further, the MLP, CNN, and DT techniques have achieved reasonably adjacent performance. In the meantime, the RF approach has caused significant results with$accu_y$, $prec_n$, $reca_l$, and $F1_{score}$ of 95.43%, 85.89%, 89.73%, and 83.01%, proportionately. Then the SCADL-ZTIDS model exceeds the other technique with greater$accu_y$, $prec_n$, $reca_l$, and $F1_{score}$ of 96.48%, 91.31%, 91.21%, and 91.19%, correspondingly [21].

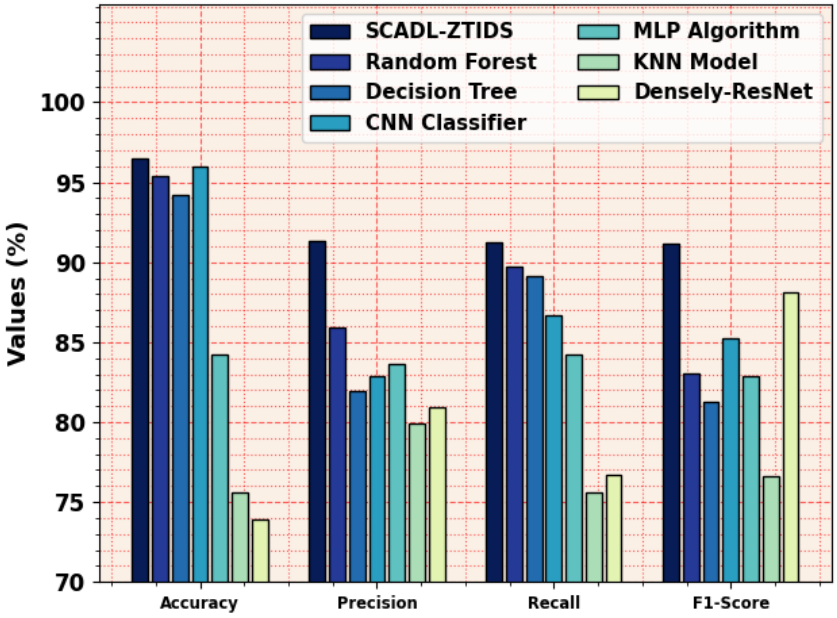

Figure 6: Comparative outcome of SCADL-ZTIDS approach with existing models

5. Conclusion

In this article, we have introduced a novel SCADL-ZTIDS method for secure IoT Devices. The foremost intention of the SCADL-ZTIDS technique rests in the effectual and automated classification of zero trust IDS. In the first stage, the SCADL-ZTIDS approach endures min-max scaler utilizing data pre-processing to convert the actual data into beneficial form. Moreover, the DNN technique is employed for the identification and classification of intrusions. Furthermore, the SCA is utilized for fine-tuning the parameters contained in the DNN method. To describe the heightened performance of the SCADL-ZTIDS approach, wide range of empirical analyses are implemented on benchmark datasets, and the outcomes are examined under various features. The simulation outcomes highlighted the improved intrusion detection performance of the SCADL-ZTIDS approach over the recent DL techniques.

References

[1] J. Simon, N. Kapileswar, P.K. Polasi, M.A. Elaveini, Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm, Computers and Electrical Engineering, 102, (2022) 108190.

[2] G. Parimala , R. Kayalvizhi, An Effective Intrusion Detection System for Securing IoT Using Feature Selection and Deep Learning, 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, (2021) 1-4.

[3] R. Salama, M. Ragab, Blockchain with Explainable Artificial Intelligence Driven Intrusion Detection for Clustered IoT Driven Ubiquitous Computing System, Computer Systems Science & Engineering, 46.3, (2023) 2917-2932.

[4] S. Fraihat, S. Makhadmeh, M. Awad, M.A. Al-Betar , A. Al-Redhaei, Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm, Internet of Things, (2023) 100819.

[5] A.D. Jasim, A survey of intrusion detection using deep learning in internet of things, Iraqi Journal For Computer Scienc., Mathematics, 3.1, (2022) 83-93.

[6] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman , R.M. Mohammad, Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT, Journal of Sensor and Actuator Networks, 12.2, (2023) 29.

[7] B. R, S. Deepajothi, P. G, D. T, P. Karthikeyan , V. S, Survey on Intrusions Detection System using Deep learning in IoT Environment, 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, (2022) 195-199.

[8] M. Ragab, M.F. S. Sabir, Outlier detection with optimal hybrid deep learning enabled intrusion detection system for ubiquitous and smart environment, Sustainable Energy Technologies and Assessments, 52 (2022) 102311.

[9] J. Shareena, A. Ramdas, H. AP, Intrusion detection system for iot botnet attacks using deep learning, SN Computer Science, 2.3, (2021) 1-8.

[10] Y. Zhang, P. Li , X. Wang, Intrusion detection for IoT based on improved genetic algorithm and deep belief network, IEEE Access, 7, (2019) 31711-31722.

[11] L. Dhanya, R. Chitra, A novel autoencoder based feature independent GA optimised XGBoost classifier for IoMT malware detection, Expert Systems with Applications, 237, (2024) 121618.

[12] M.A. Setitra, M. Fan , Z.E.A. Bensalem, An efficient approach to detect distributed denial of service attacks for software defined internet of things combining autoencoder and extreme gradient boosting with feature selection and hyperparameter tuning optimization, Transactions on Emerging Telecommunications Technologies, 34.9, (2023) 4827.

[13] J. Zhu , X. Liu, An integrated intrusion detection framework based on subspace clustering and ensemble learning, Computers and Electrical Engineering, 115, (2024) 109113.

[14] P. Cheng, M. Han, G. Liu, DESC-IDS: Towards an efficient real-time automotive intrusion detection system based on deep evolving stream clustering, Future Generation Computer Systems, 140, (2023) 266-281.

[15] J.S. Prasath, V.I. Shyja, P. Chandrakanth, B.K. Kumar , A. Raja Basha, An optimal secure defense mechanism for DDoS attack in IoT network using feature optimization and intrusion detection system, Journal of Intelligent & Fuzzy Systems, (Preprint), (2024) 1-18.

[16] B. Deepa, K. Ramesh, Epileptic seizure detection using deep learning through min max scaler normalization, Int. J. Health Sci, 6, (2022) 10981-10996.

[17] Z. Zhou, H. Zhang, M. Effatparvar, Improved sports image classification using deep neural network and novel tuna swarm optimization, Scientific Reports, 14.1, (2024) 1-20.

[18] A. Alqushaibi, M.H. Hasan, S.J. Abdulkadir, K.U. Danyaro, M.G. Al-Selwi, E.H. Sumiea, H. Alhussian, Enhanced Colon Cancer Segmentation and Image Synthesis through Advanced Generative Adversarial Networks based-Sine Cosine Algorithm, in IEEE Access, 2024.

[19] https://www.kaggle.com/datasets/dhoogla/unswnb15

[20] I. Katib, M. Ragab, Blockchain-assisted hybrid harris hawks optimization based deep DDoS attack detection in the IoT environment, Mathematics, 11.8 (2023) 1887.
[21] I. Tareq, B.M. Elbagoury, S. El-Regaily , E.S.M. El-Horbaty, Analysis of ton-iot, unw-nb15, and edge-iiot datasets using dl in cybersecurity for iot, Applied Sciences, 12.19, (2022) 9572.
[22] M. Basheri, M. Ragab, Quantum Cat Swarm Optimization Based Clustering with Intrusion Detection Technique for Future Internet of Things Environment, Computer Systems Science & Engineering, 46.3, (2023) 3783-3798.