Vol. 4, No. 2, pp 1 - 17, 2023
DOI: 10.55969/paradigmplus.v4n2a1

PARADIGM Plus

A Framework for Robust Attack Detection and Classification using Rap-Densenet

Temitope Samson Adekunle [1], Toheeb Adetoyese Adeleke [2], Olakunle Sunday Afolabi [3], Oluwaseyi Omotayo Alabi [4,✉], Adekunle Olugbenga Ejidokun [5], Godwin Nse Ebong [6], and Temitope A. Bamisaye[7]

[1]*Colorado State University, Fort Collins, United States*
temitope.adekunle@colostate.edu
[2]*Ladoke Akintola University of Technology, Ogbomoso, Nigeria*
taadeleke50@student.lautech.edu.ng
[3]*University of Abuja, Abuja, Nigeria*
afolabi.olakunle2019@uniabuja.edu.ng
[4]*First Technical University, Ibadan, Nigeria*
engrseyialabi@gmail.com
[5]*Dominion University, Ibadan, Nigeria.*
g.ejidokun@dominionuniversity.edu.ng
[6]*University of Salford, Salford, United Kingdom.*
g.n.ebong@edu.salford.ac.uk,
[6]*National Open University of Nigeria, Abuja, Nigeria.*
bamisaye9999@gmail.com

Abstract

Network attacks must be effectively identified and categorized to guarantee strong security. However, current techniques frequently have trouble correctly identifying and categorizing new attack patterns. This study presents a novel framework for reliable attack detection and classification that makes use of the complementary strengths of rap music analysis methods and DenseNet convolutional neural networks. This study employs feature extraction based on the Attention Pyramid Network (RAPNet) framework that has been proposed to extract features from the input data, and Pigeon in binary. Afterward, feature selection based on Optimization Algorithm (BPOA) is performed. Following the selection of the ideal characteristics, Densenet201, the attacks in Bot-IoT, CICIDS2017, and other systems are categorized using deep learning as well as CICIDS2019 datasets. Additionally, the Conditional Generic Adversarial extra data samples are provided for minority classes using the Convergent Gap Analysis Network (CGAN), so the imbalanced data issue should be addressed. In contrast to the recent intrusion. The outcomes show that the model is capable of precisely detecting and accurately categorizing DoS and DDoS attacks with rates of 98.63%, 98.68%, and BoT-IoT, CICIDS2017, and CICIDS2019 all scored 98.78%.

Keywords: Attack detection · Classification RAP-DenseNet · Deep learning

Received: 2 June 2023 · Accepted: 25 July 2023 · Published: 2 August 2023.

1 Introduction

Systems for computer networks have been put in place to grease device connections and carry out essential commercial operations. On the primary functions of reality's connection systems, nonetheless, this has a lesser impact. Crucial diligence like banking, healthcare institutions, and service providers are vulnerable to insecurity pitfalls because of their substantial and pivotal reliance on computer networks [1, 2, 3]. Due to this dependence, maintaining ideal networks is necessary to maintain availability, effectiveness, and safety. A security breach can significantly impact network performance, leading to insecurity and eventual network incompatibility.

Also, cyberattacks may affect knockouts, issues in armament systems, and nonpublic information releases. They might beget the loss of incredibly sensitive and priceless data, similar to sanitarium lines, military records, etc. Likewise, they can disable phone and computer networks, making data unapproachable or rendering systems unworkable [4, 5]. Banking and government networks are particularly vulnerable because of the tremendous value of the data they contain. The hackers steal the information (especially other people's banking details) and profit from that information.

There have been many different kinds of attacks that have resulted in internet abnormalities. Similar attacks have been more common over the past ten years, posing a severe threat to the stability of networks due to the revision of multitudinous services [6, 7]. Denial of service (DoS) and distributed denial of service (DDoS) attacks rank among the most important. DoS attacks can be divided into two groups.: service outages and service flooding. The most hazardous assaults are DDoS attacks.

The IoT network has endured severe losses due to the DDoS attack. Thus, IoT druggies accordingly paid great attention to the vulnerabilities. multitudinous bias or systems work together to attack a single target, making it challenging to detect and disable the attacking bias [8, 9, 10]. Cyber bushwhackers constantly use a botnet to intrude with internet structure. DDoS attacks are delicate to identify and help in real-time, yet this approach has enormous mileage because attacks can have significant goods.

Lately, deep literacy has attracted important interest in attack discovery due to its effective print birth and literacy capacities, specifically in settings with massive datasets. Without contextual information, deep literacy ways ultimately capture significant characteristics from the input data using multitudinous layers [11, 12]. Thus, in this paper, Densenet 201 grounded deep literacy is enforced to perform multi-class brackets on DoS and DDoS attacks. To break the imbalanced data issue, a tentative Generative Adversarial Network (CGAN) is enforced to perform data addition. subsequently, the point birth and selection are performed using a Refined Attention Aggregate Network (RAPNet) and double Chump optimization algorithm (BPOA). Eventually, the attacks are detected and classified using the Densnet- 201 classifier. The following are this paper's primary objectives: to fix the problem of unbalanced data and boost the effectiveness of the suggested model, tentative Generative Adversarial Network (tentative GAN) grounded data addition is employed, rather than depending on the traditional point birth system, a deep literacy approach grounded on RAPNet is espoused to prize the essential attributes from the raw network business data.

There are five sections in this study. The study's preface is presented in Section 1, and affiliated work is described in Section 2. The exploration's methodology is explained in Section 3, and the study's findings are bandied in Section 4. Finally, Section 5 delivered our conclusion.

2 Literature Review

DoS and DDoS assaults are severe trouble to numerous associations because of their tremendous capability to bring down vulnerable waiters in a short period. As a result, many exploration plans have focused on stopping DoS and DDoS attacks. A number of creative experimenters have suggested defenses against DoS and DDoS attacks. Below is a concise explanation of some of them. To effectively recognize and classify DDoS attacks, Wei et.al., [13] incorporate two deep literacy-grounded

ways called bus Encoder (AE)-Multi-layer Perceptron (MLP). To perform point birth without mortal backing, AE was enforced by the authors. Using the uprooted features, colorful kinds of DDoS attacks were classified by MLP network. To assess the effectiveness of the suggested approach, large DDoS attack samples from the CICDDoS2019 dataset were used employed in terms of f1-score, recall, perfection, and delicacy criteria.

Shroff et.at., [14] created a generative inimical network (GAN) grounded dependable sensor for relating cyber-attacks. In this system, two distinct GAN-grounded models were enforced. The first creator produced benign cases that nearly recalled benign samples from the dataset and the alternate creator was able of producing DDoS cases that nearly recalled those from the dataset. also, the author built a model based on deep neural networks (DNNs) that can differentiate between benign exemplifications and DDoS scenarios in the dataset with various similarity values. For classifying network business, a Deep Neural Network (DNN) grounded IDS was created by [15, 16, 17]. They enforced a four-subcaste network, and each subcaste contains 136 neurons. To dissect the effectiveness of the suggested approach, multitudinous trials were carried out with colorful hyperparameter combinations, and the results were compared with other shallow and deep ANN models. They used CICIDS2017 and NSL-KDD datasets with standard performance criteria for this assessment. They also created and tested 36 indispensable DNN model combinations, each producing different issues.

To identify unknown DDoS attacks, Shieh et.al., [18] created a system that employs reconstruction error and distributes retired subcaste features. The deep hierarchical reconstruction nets (DHRNet) structure was used in this exploration to redact it with a 1D connected neural network using spatial position constraint prototype loss function. An arbitrary grade descent approximation grounded one-class SVM (support vector machine) was enforced to identify the unidentified patterns in the ensuing stage. The performance of this approach was assessed using the CICIDS2017 Friday Open Dataset.

Using colorful machine literacy and point selection algorithms, Alduailij et al., [19] offered a DDoS-attack discovery system. originally, the most material attributes from the CICDDoS2019 and CICIDS2017 datasets were named using the random forest (RF) feature importance and mutual information approaches. subsequently, the attack discovery was performed by weighted voting ensemble (WVE), grade boosting (GB), K- Nearest Neighbor (KNN), logistic retrogression (LR), and RF, and the performance was estimated using f1- score, recall, perfection, and delicacy.

3 Methodology Approach

This section presents envisioned deep literacy-grounded intrusion discovery system and its high-position armature to classify colorful types of DoS and DDoS attacks. First of all, Figure 1 shows a suggested armature with five important stages. They are, pre-processing, Data addition, point birth, point selection, and bracket. originally, the raw data is pre-processed in several ways to exclude unwanted data. The imbalanced data issue is also fixed using a tentative generative inimical network (CGAN)- grounded data addition fashion, which improves the quality of the classifier. Subsequently, the point birth is conducted on the stoked data using Refined Attention Aggregate Network (RAP-Net) grounded deep literacy fashion. From the uprooted features, the binary pigeon optimization algorithm (BPOA) is enforced to gain the important aspects. Eventually, Densnet201 grounded the classifier examines these characteristics, and categorizes the cyberattacks.

3.1 Pre-Processing

Including a data pre-processing phase in training results in more reliable training and a more precise model. As a result, during this stage, undesirable characteristics like "flow packets/s" equal to "infinity" or "NaN" are removed. The duplicate rows are then eliminated, including the following ones: Fwd Avg Bytes/Bulk, Bwd Avg Bulk/Rate, Fwd Avg Bulk/Rate, Fwd Avg Packets/Bulk, Bwd Avg Packets/Bulk, Bwd PSH Flags, and Bwd Avg Bytes/Bulk.

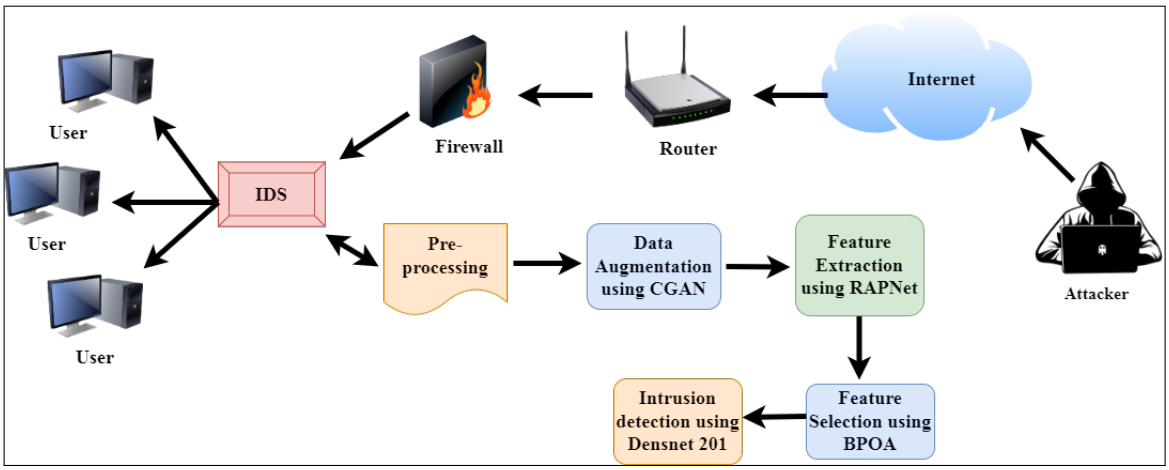

Figure 1: Structure of the System

The main objective of the strategy here is the multi-class categorization of DDoS attacks. This requires the use of encoding. This study uses one hot encoder (OHE) to achieve this. For each label, a new column is created and given a value of 1 or 0, depending on whether the record belongs to that category.

The data are normalized using L2 normalization after the encoding procedure. The L2 standard was applied to each column. In other words, Equation 1, where x stands for each instance of a record, defines the properties of the dataset.

$$||x||_2 = \sqrt{\sum_{i=1}^{n} |x_i|^2} \tag{1}$$

Generally speaking, normalizing the dataset records speeds up training considerably. This normalization resulted in a model that was more accurate because it handled a wide range of dataset attributes consistently.

3.2 Data Augmentation Using CGAN

Using the augmented data sets created in this section, which closely match the original data, by using Conditional Generative Adversarial Network (CGAN) approach. The same training process used by GAN is also used by CGAN but with restrictions on the labeling of the generated samples. There are two sections in this framework. They are generator (GR) and discriminator (DS) networks. These two networks fight for information that is generated artificially.

In Equations 2 and 3, y_r stands for the input of random variables from the GR network, and $DS(x)$ stands for the likelihood that the DS network will successfully predict the initial data x. Integrating and maximizing the aforementioned equations yields the discriminator's total loss function. Since the discriminator's goal is to accurately discriminate between authentic and fake samples presented in Equation 4

$$L(DS(x), 1) = \log(DS(x)) \tag{2}$$

$$L(DS(GR(y_r)), 0) = \log(1 - DS((GR(y_r))) \tag{3}$$

$$L^{(DS)} = \max[\log(DS(x)) + \log(1 - DS((GR(y_r)))] \tag{4}$$

In contrast to the discriminator, the loss function of the generator is presented by Equation 5

$$L^{(GR)} = \min[\log(DS(x)) + \log(1 - DS((GR(y_r)))] \tag{5}$$

The value function $V(GR, DS)$ is specified in Equation 6 based on considering the entire dataset.

$$\begin{aligned} \min\max V(GR, DS) = \min\max(&E_{x\sim P_{data(x)}}[\log(DS(x))]) \\ &+ (E_{y_r\sim P_{y_r(y_r)}}[\log(1 - DS((GR(y_r)))]) \end{aligned} \tag{6}$$

Therefore, $E_{y_r\sim P_{yr(y_r)}}$ stands for the estimated return of all arbitrary inputs $E_{x\sim P_{data(x)}}$ represents the estimated return of original data samples, $P_{y_r(y_r)}$ and stands for data dissemination from the generator and the actual data distribution is represented by $P_{data(x)}$.

Through transposed convolutional layers, the input feature vectors are up-sampled by the generator network. A series of transposed convolutional layers are used with different numbers of channels, including 64, 128, 256, and 512. The blocks at each level correspond to the size of the feature vector input. This model also generates samples with a structure like the given data.

3.3 Point birth Using RAPNet

From the pre-processed data, the effective features are uprooted by the Refined Attention Aggregate Network (RAPNet). Encoder and decoder structures are the foundation of this network, containing five stages. The first three stages of the complication process use 1 × 1 complication layers, and the following two stages use an atrous complication with 3 × 3 complication layers. The ReLU subcaste is used among the two complication layers to produce the non-linear representation, which retrieves low-subcaste specific features. To up-sample the high position point maps in all residual blocks, the deconvolution fashion is employed. Because to conduct the point emulsion operation, all point chart sizes must be the same. After that, the side connection is equipped with the convolutional block attention module (CBAM) to acclimate the point maps subcaste by subcaste. It's used to drop false discovery and increase point birth delicacy. The final residual block of the conv5 stage is subordinated to the aggregate pooling module's operation in the decoding route to acquire environment data. This module employs a four-position aggregate with caddy sizes of 1 × 1, 2 × 2, 3 × 3, and 6 × 6 and employs the global normal pooling operation. subsequently, the point emulsion process is performed by concatenating the point charts of the garbling network's corresponding layers with the decoding network. Eventually, the combined point charts are P2, P3, P4, and P5. To produce the emulsion, point chart P2, which is composed of the point maps P3, P4, and P5, a thick connection is employed in the point aggregate structure. This system allows for the accession of multi-layer fused point maps with rich semantic and spatial data for multiscale structure birth. The point aggregate network has chosen consecution operation rather of element-wise addition for thick and side connections among up sampled point charts. When the final fused point chart P2 is up sampled, the point birth results are produced

3.4 The Binary Pigeon Optimization Algorithm for Feature Selection

In this section, we describe how the BPOA grounded point selection fashion is employed to elect an ideal subset of features from the input data. This fashion contains three essential drivers. They're a compass, chart, and corner. suckers induce a chart for home by interpreting the earth's glamorous forces in the chart and compass. Assume that, in N- dimension hunt space, the ith chump of masses can be represented as Si = (Si, 1, Si, 2... Si, N). Another N-dimensional vector VLi = (VLi, 1, VLi, 2... VLi, N) can be used to indicate a chump's haste, which represents how the chump's position changes. The preliminarily visited position of the chump is denoted by PLi = (PLi, 1, PLi, 2... PLi, N), and the

final optimum position of the chump is denoted by g = (g1, g2... gN). Equations 7 and 8 determine how all suckers fly.

$$VL_i(t_e + 1) = VL_i(t_e) \times e^{-Rt} + rand \times (S_g - S_i(t_e)) \tag{7}$$

$$S_i(t_e + 1) = S_i(t_e) + VL_i(t_e + 1) \tag{8}$$

Here, VL_i and S_i, respectively, represent the pigeon's current velocity and location at a given time. Sg stands for the world's best solution, while rand denotes any number between 0 and 1. The landmark operator assesses each pigeon based on the fitness ratings. Equation 9, in which only 50% of the pigeons are taken into account to calculate the desired location of the center pigeon, is used in all iterations to update the number of pigeons. Every other bird adjusts its terminal at the same moment.

$$TN_p(t_e + 1) = \frac{TN_p(t_e)}{2} \tag{9}$$

Here, TN_p stands for the number of pigeons present at any given time. The target location is found using the Equation 10. Equation 11 is used to update the positions of the other pigeons based on this.

$$S_c(t_e + 1) = \frac{\sum S_i(t_e + 1) \times fitness(S_i(t_e + 1))}{TN_p \sum fitness(S_i(t_e + 1))} \tag{10}$$

$$S_c(t_e + 1) = S_i(t_e) + rand \times (S_c(t_e + 1) \times S_i(t_e)) \tag{11}$$

S_c, in this case, stands for the position of the center pigeon. Instead of using the traditional POA, the BPOA describes the search space as an n-dimensional Boolean lattice, upgrading the solution in the issue space to a continuous numerical location. Additionally, the solution is superior to a hypercube's corner. In order to decide whether to choose or not, a provided variable and a Boolean solution vector are also employed. 1 denotes the parameter selected to include the datasets in this state, while 0 denotes anything else. Based on the aforementioned factors, a fitness function (FsFn) was developed to address this issue and achieve the following balance between the two goals (see Equation 12)

$$F_sF_n = \alpha\Delta_{ER}(C) + \beta\frac{|YS|}{|TF|} \tag{12}$$

Here $\alpha \in [0, 1]$ denotes the error rate's weight of classifications, the total amount of features included in the dataset is denoted by $|TF|$, the size of the subset selected by the method is denoted by $|YS|$, the error rate of a classifier is represented by $\Delta_{ER}(C)$, and the reduction feature's importance is denoted by $\beta = 1 - \alpha$. Instead of the amount of chosen features, the classification performance allows a crucial weight.

4 Experiments and Results

The effectiveness of the suggested intrusion detection model is examined in this section through a number of investigations, and the findings are reported. Windows 10 64-bit with a Core i7 processor running at 2.70 GHz and 16 GB of RAM were the operating systems used for all trials. The suggested method is put into practice using Python with TensorFlow as the backend. The hyperparameters include an Adam optimizer, a learning rate of 0.001, a ReLU activation function, a batch size of 32, a momentum of 0.9 and 50 epochs, and a dropout of 0.9. The dataset is divided into training and testing for 70% and 30%, respectively.

4.1 Dataset Description

4.1.1 Bot-IoT Dataset

The data set was released by Khraisat et al., [20]. It contains more than 72 million recordings and a range of synthetic and real-world events. While DoS and DDoS-type packets make up the majority of the data set, there are four different forms of assault. This set is unbalanced, much like the UNSW-NB15 data set.

4.1.2 CICIDS2017 Dataset

The CICIDS-2017 intrusion detection dataset was recently created by the Canadian Institute of Cybersecurity. The date, destination, source IP addresses, assaults, protocols, destination, and source ports are used to label the CICIDS-2017 dataset. There are elements of real, realistic internet traffic in it. This dataset was compiled over five days and contains 2,830,743 records and 80 network traffic features. The dataset consists of a CSV file with regular and unauthorized traffic and eight traffic surveillance periods. The many categories in this dataset include DDoS, DoS, SSH, brute force, FTP, botnets, infiltration, Heartbleed, and web attacks.

4.1.3 CICIDS2019 Dataset

This dataset includes a variety of DDoS assaults that can be executed using the TCP and UDP network protocols. This dataset classifies attacks using exploitation- and reflection-based invasions. The dataset contains more than 80 flow attributes. The dataset was gathered over the course of two days for training and testing analysis. The dataset includes attacks using SNMP, LDAP, UDP-Lag, MSSQL, SYN, NetBIOS, NTP, DNS, and WebDDos.

4.2 Evaluation Metrics

In Equations 13 to 16, $F1$, REC, PRE, and ACC represent the f1-score, recall, precision, and accuracy, respectively. Moreover, fl_n denotes the false negatives, fl_p denotes the false positives, tr_n denotes the true negatives, and tr_p denotes the true positives.

$$ACC = \frac{tr_p + tr_n}{numberOfSamples} \tag{13}$$

$$PRE = \frac{tr_p}{tr_p + fl_p} \tag{14}$$

$$REC = \frac{tr_p}{tr_p + fl_n} \tag{15}$$

$$F1 = 2 \times \frac{precision \times recall}{precision + recall} \tag{16}$$

4.3 Result and Discussion

In this part, the suggested framework is tested on the chosen datasets (Bot-IoT, CICIDS2017, and CICIDS2019) through many experiments, and the findings are compared to other techniques.

4.3.1 Analyzing the performance of the BoT-IoT dataset

Table 1 shows the evaluation of Bot-IoT Performance on a Dataset. The table demonstrates how well our suggested technique performs across all classes. In the DDoS and DoS categories, the BoT-IoT dataset achieves 99.87% and 99.68% ACC, respectively. In comparison to other courses, the performance for stealing and reconnaissance is a little worse. With our suggested method, only 99% (theft) and 98.67% (reconnaissance) ACC are reached in those classes. DDoS assaults and reconnaissance attacks behave similarly, which is represented in the current feature set. This action makes it harder to distinguish between the two attacks using the model.

Table 1: Multi-class classification on Bot-IoT dataset

Techniques	PRE	REC	F1	ACC
Normal	99.78	99.89	99.74	99.69
DDos	99.93	99.96	99.89	99.87
Dos	99.79	99.86	99.81	99.68
Theft	99.11	99.32	99.14	99
Reconnaisance	98.69	99.05	98.91	98.67

Table 1 is illustrated visually in Figure 2. The F1 (99.89%), REC (99.96%), PRE (99.93%), and ACC (99.87%) values of the DDoS class are greater than those of all other classes, as can be seen from the figure. Overall, all forms of attack have produced favorable effects. However, because it resembled conventional data, the reconnaissance class was given the lowest mark. Because a few occurrences in the dataset were incorrectly assigned to a different class, theft-exfiltration also obtained the lowest results.

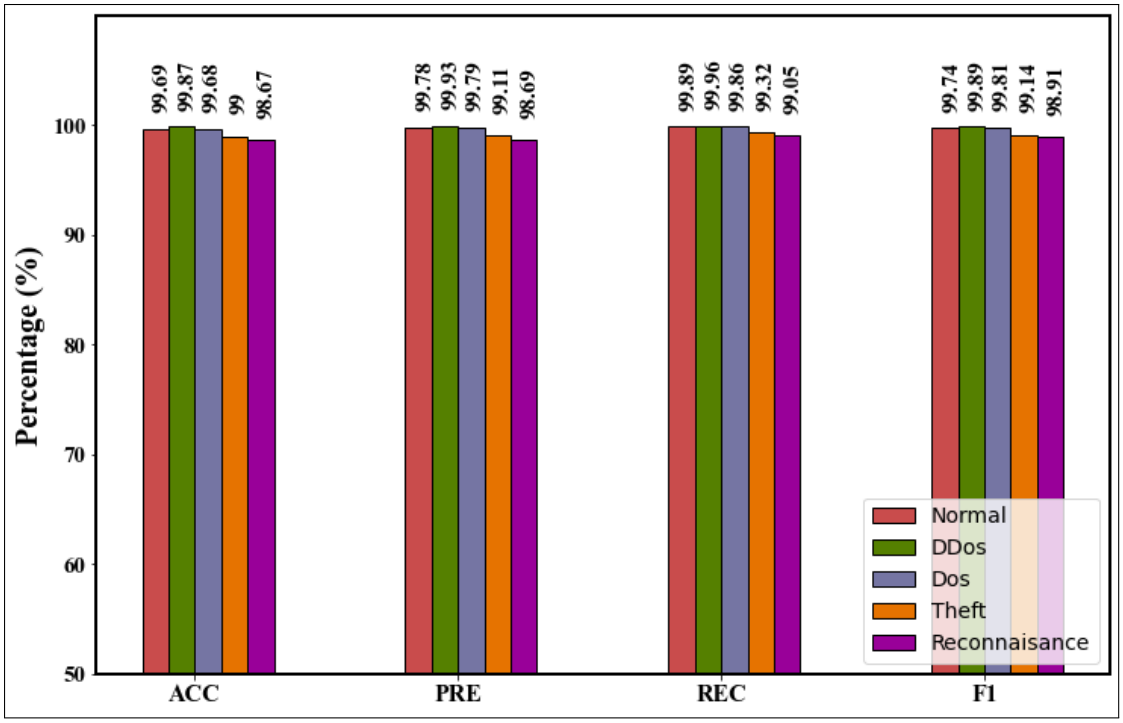

Figure 2: Multi-class classification on Bot-IoT dataset

The findings of the proposed strategy are compared with those of the current intrusion detection methods tested on the BoT-IoT dataset after the multi-class classification, as shown in Table 2. The table demonstrates that the PRE, ACC, F1, and REC of the suggested approach are more significant than those of other existing techniques, indicating that the proposed framework significantly lowers the false positives in the majority of classes. The performance and accuracy of the support vector machine (SVM) may have been higher when compared to all other techniques. because it erroneously categorizes different types of theft assaults. Additionally, a lot of attacks were mistaken for ordinary packets, proving SVM's inability to identify intrusions.

Table 2: Comparison of the proposed approach on BoT-IoT dataset

Techniques	**PRE**	**REC**	**F1**	**ACC**
SVM [26]	89.60	89.35	89.34	89.35
XGBOOST [27]	99.38	99.57	99.47	98.96
KNN [28]	99.04	99.03	99.04	99.03
C4.5 [29]	-	-	-	92.00
Proposed	**99.46**	**99.61**	**99.49**	**99.38**

The overall performance of XGBoost is better than any other method when compared to it. But the ACC of the KNN (k-nearest neighbor) is higher (99.03%) than the XGBoost (98.96%). Due to the fact that it handles multi-class instances with ease and produces superior ACC than SVM. C4.5 performs more efficiently than SVM as well. However, one statistic (ACC) (see Figure 3) alone is insufficient to fully express how well the technique classifies incursions. Not to mention, when compared to other strategies, the outcomes of the suggested strategy obtained using the Bot-IoT dataset reveal that our technique delivers more useful findings.

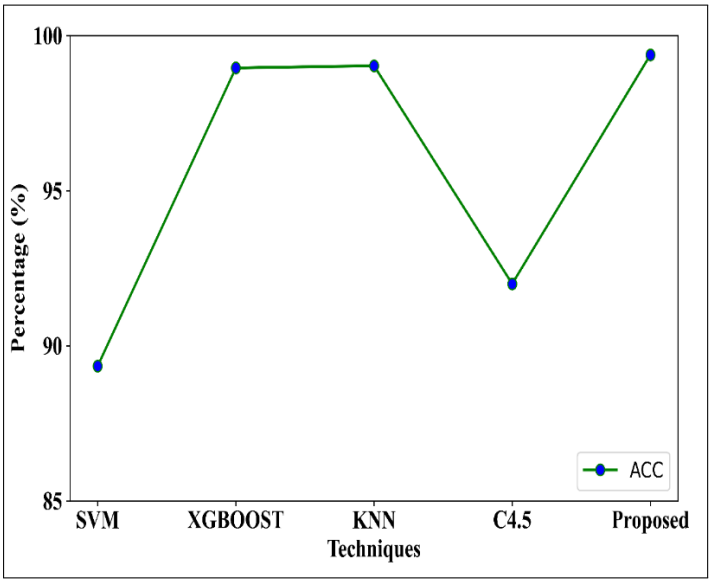

Figure 3: Accuracy comparison of the proposed approach on BoT-IoT dataset

4.3.2 Performance Evaluation on the CICIDS2017 Dataset

Table 3 shows the suggested model's performance in multi-class classification on the CICIDS2017 dataset according to ACC, PRE, REC, and F1. The performance of the suggested method is highest for "Benign" traffic detection (detection ACC of 99.97%) and lowest for "SQL Injection" traffic detection (detection ACC of 97.98%). The classifier performs poorly because there are few "SQL injection" data points in the entire dataset. Additionally, the behavior pattern of a "bot" attack resembles that of normal network traffic, making it more difficult for the suggested approach to reliably identify the attacks. Thus, average performance results. Attacks like Heartbleed and SQL injection were more correctly predicted than brute-force attacks. Table 3 is illustrated visually in Figure 4.

Table 3: Multi-class classification on the CICIDS2017 dataset

Techniques	PRE	REC	F1	ACC
Benign	99.95	99.93	99.95	99.97
DDos	99.89	99.85	99.87	99.92
Infiltration	99.59	99.57	99.58	99.63
portscan	99.87	99.85	99.86	99.92
Bot attack	98.85	98.81	98.83	98.89
Pataror-FTP	99.89	99.86	99.87	99.95
Parator SSH	99.23	99.21	99.22	99.27
bruteforce	99.67	99.65	99.66	99.71
XSS	99.17	99.14	99.16	99.33
SQL injection	97.56	97.52	97.54	97.98
DDOs GoldenEye	98.92	98.89	98.91	98.96
DDOS Hulk	99.67	99.65	99.66	99.73
DDOS slowhttptest	98.68	98.66	98.67	98.71
DDOS-slowloris	98.83	98.8	98.82	98.86
Heartbleed	98.08	97.99	98.04	98.12

'Brute force' and 'DDoS Hulk' both earn identical PRE (99.67%), REC (99.65%), and F1 (99.67%) results in terms of other performance scores. It proved that, in this configuration, the suggested classifier still exhibits symmetric behavior with regard to traffic classifications. Additionally, ACC and REC rates are crucial for evaluating the performance of the classifier for each attack. The statistics show that a class with a low ACC has a high number of false positives. It means that 'benign' classes are erroneously labeled as attacks. A model with low recall may also overlook genuine intrusion. Therefore, ACC and REC values must be sufficiently high to guarantee that the model operates at its best. The proposed model, as shown in Figure 4, gets higher values for all the parameters that define the effectiveness of the strategy for multi-class categorization.

Table 4 contrasts the findings of the proposed methodology with those of existing methods on the CICIDS2017 dataset to demonstrate the usefulness of the suggested strategy. Comparing our proposed strategy to existing approaches, the performance has improved. Recurrent neural networks (RNN) and deep neural networks (DNN) obtain comparable results for F1. Adaboost performs below par when compared to all other methods for classifying DDoS attacks. However, compared to all other methods, this methodology has a higher REC (100%) value. This means that there aren't many false negatives produced by this method.

The Recurrent Neural Network (RNN) (98% ACC) and 1D-CNN (98.96% ACC) approaches, on the other hand, perform better than comparable methods and result in a small amount of missed classification mistakes. It is not, however, greater than the suggested strategy (99.26% ACC). It suggests that the suggested method is better suited for classifying and identifying DDoS attacks.

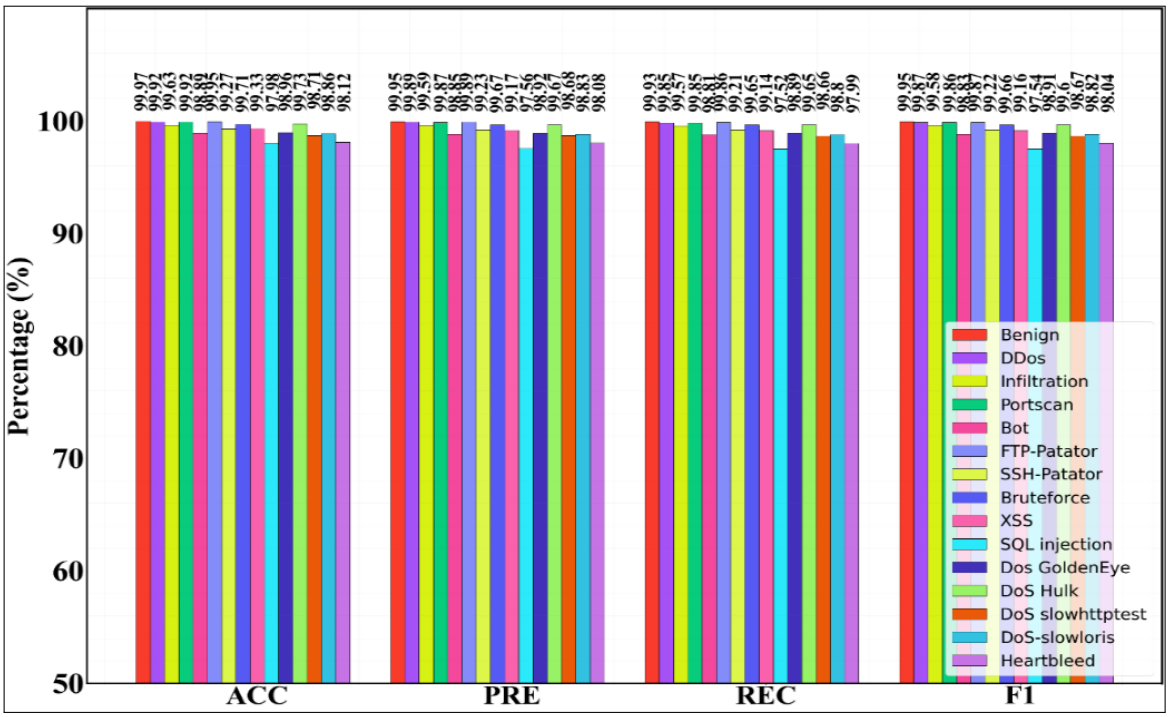

Figure 4: Multi-class classification on the CICIDS2017 dataset

Table 4: Comparison of the proposed approach on BoT-IoT dataset

Techniques	PRE	REC	F1	ACC
Decision tree [30]	97.5	85	90	96.67
DNN [31]	-	-	96	-
1D-CNN [32]	-	-	-	98.96
Adaboost [33]	81.83	100	90.01	81.83
RNN [34]	96	97	96	98
Proposed	**99.19**	**99.15**	**99.17**	**99.26**

4.4 Performance Evaluation on the CICIDS2019 Dataset

Table 5 displays the outcomes of the multi-class classification carried out using the suggested method on the CICIDS2019 dataset. The suggested method, as shown in the table, excels at multi-class categorization and produces the best outcomes for each attack type. For each class, ACC rates are better than 98%. The Benign, DNS, and NTP classes' respective ACC rates are 98. 76%, 98.71%, and 98.58%, highlighting their outstanding achievement. The performance of classification in other assault categories also results in the most significant outcome. Figure 5 shows a graphic representation of Table 5.

The proposed classifier did not perform as well on the "WebDDoS" and "MSSQL" classes as it did on other class types. Testing has revealed that "WebDDoS" and "MSSQL" attributes share a lot of characteristics. In order to effectively classify the traffic data for these classes, the classifiers need more crucial properties. Despite this, because our model uses the efficient BPOA algorithm to choose pertinent attributes, the suggested method's detection ACC for "WebDDoS" and "MSSQL" is 98.58% and 98.12%, respectively. It will lead to an improvement in the classifier's overall ACC.

Table 5: Performance Analysis of the proposed technique on CICIDS2019 dataset (Multi-Class)

Techniques	PRE	REC	F1	ACC
Benign	98. 78	98. 97	98 .78	98. 76
DNS	98. 72	98. 71	98. 72	98. 71
LDAP	98. 37	98. 71	98. 50	98. 63
MSSQL	98. 23	98. 15	98. 13	98. 12
NTP	98. 62	98. 64	98. 63	98. 58
NetBios	98. 63	98. 72	98. 61	98. 50
SNMP	98. 37	98. 40	98. 34	98. 41
SSDP	98. 28	98. 43	98. 31	98. 40
UDP	98. 42	98. 53	98. 45	98. 63
Syn	98. 40	98. 67	98. 48	98. 56
UDP-Lag	98. 20	98. 49	98. 49	98. 62
WebDDos	98. 19	98. 61	98. 39	98. 58

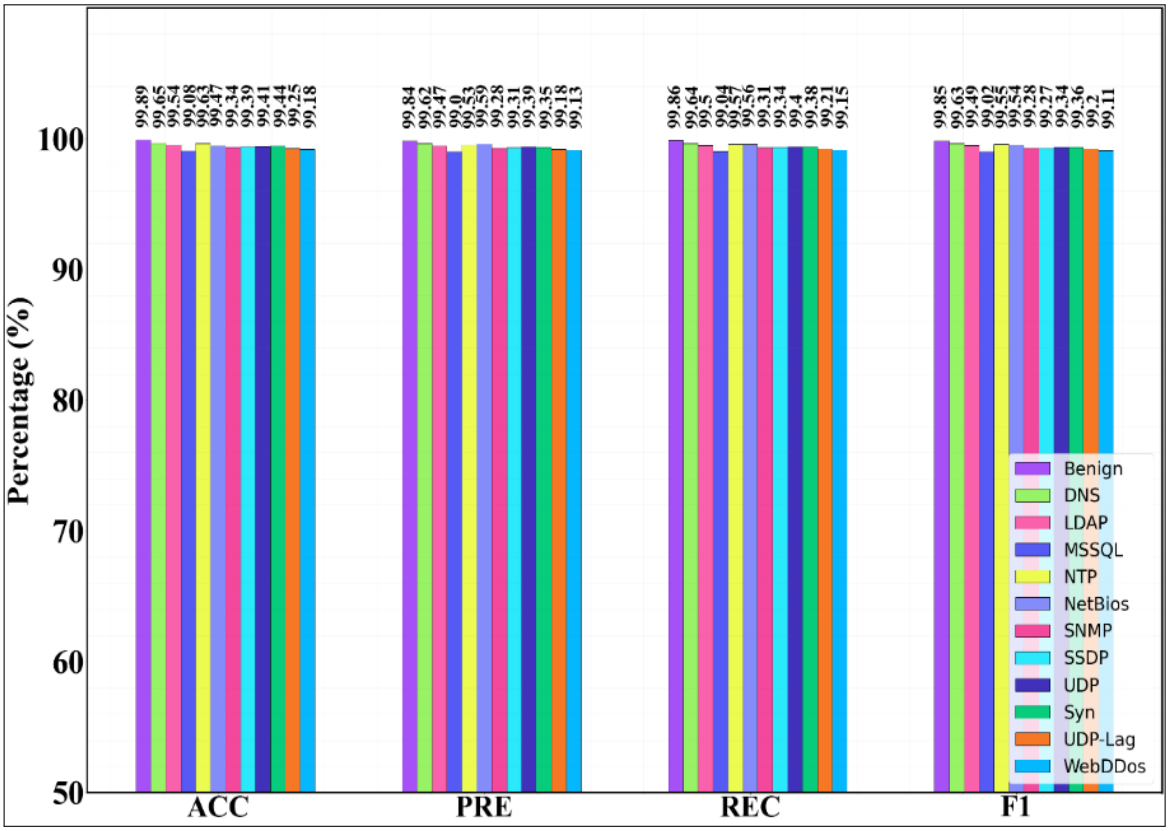

Figure 5: Multi-class classification on the CICIDS2019 dataset

Table 6 and Figure 6 compared to other established intrusion detection systems, evaluate the suggested method. Methods that were already in use were utilized, including the Radial Basis Function Neural Network (RBFNN), Bayes Point Machine (BPM), Explainable Neural Network (XNN), and Convolutional Neural Network (CNN). According to the table, the proposed technique successfully uses the CICIDS2019 dataset to achieve 98.42% F1, 98.39% REC, 98.41% PRE, and 98.29% ACC. Ad-

Table 6: Comparison of proposed strategy using the CICIDS2019 dataset

Techniques	PRE	REC	F1	ACC
BPM [35]	98. 34	96. 89	96. 92	96. 90
RBFNN [36]	98. 21	98. 31	98. 29	98. 24
XNN [37]	98. 10	98. 31	98. 23	98. 29
CNN [38]	98. 42	98. 35	98. 46	98. 38
Proposed	**98. 42**	**98. 39**	**98. 41**	**98. 39**

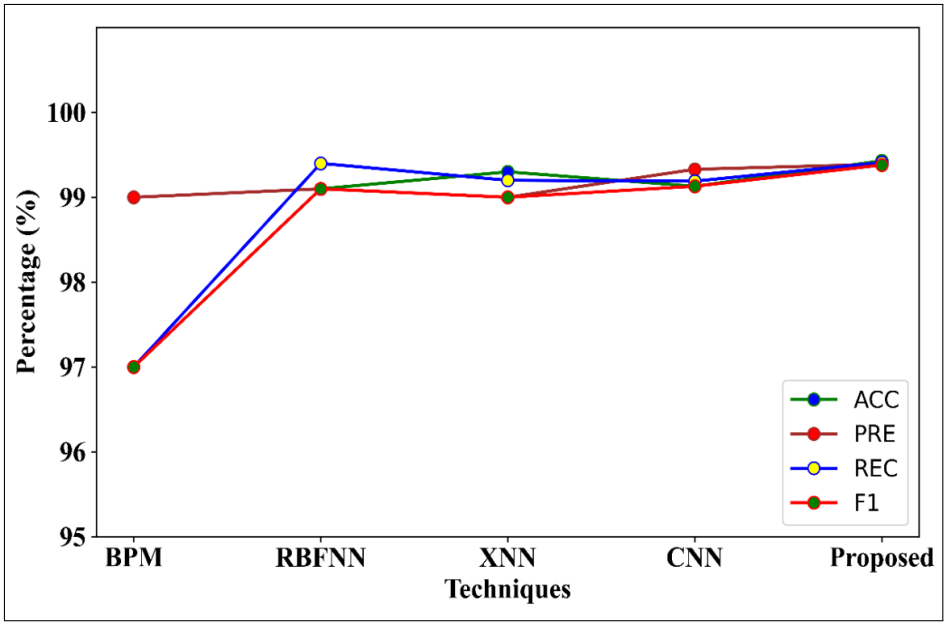

Figure 6: Analysis of proposed strategy with existing techniques on the CICIDS2019 dataset

ditionally, XNN and CNN perform better than BPM. However, all of the approaches produce better outcomes (over 98%) in terms of PRE.

4.4.1 Impact of Feature Selection Approach

A binary POA approach is used to enhance the recommended intrusion detection process by picking the most important elements from the obtained features. The BPOA-based technique offers more information while minimizing the number of features on the Bot-IoT, CICIDS2017, and CICIDS2019 datasets. The performance of the suggested strategy with and without feature selection is shown in Table 7, which demonstrates that the suggested strategy performs better when an effective BPOA-based feature selection approach is used. For the BoT-IoT, CICIDS2017, and CICIDS2019 datasets, respectively, it only achieves 98.63%, 98.76%, and 98.68% ACC without the feature selection method. After the feature selection procedure, the classifier performs better with the best possible collection of features and produces the best results without it.

Table 7: Comparison of proposed strategy using the CICIDS2019 dataset

With Feature selection				
Dataset	PRE	REC	F1	ACC
BoT-IoT	98. 36	98. 71	98. 64	98. 45
CICIDS2017	98. 29	98. 16	98. 53	98. 38
CICIDS2019	98. 40	98. 56	98. 41	98. 56
Without feature selection				
BoT-IoT	98. 43	98. 62	98. 67	98. 63
CICIDS2017	98. 17	98. 42	98. 71	98. 76
CICIDS2019	98. 30	98. 65	98. 64	98. 68

5 Conclusion

The demand for using more precise and effective IDS has grown more critical due to the quick increase in network traffic and the development of intrusions. Therefore, a deep learning-based network intrusion detection is implemented in this research. The results showed how well the suggested strategy performed when it comes to identifying and classifying cybersecurity threats. Different performance Criteria, including delicacy, F- score, recall (perceptivity), and perfection (discovery rate) have been used in the evaluation process to dissect the utility of the suggested models on the three standard datasets. In discrepancy to former attack discovery ways, the proposed frame achieves superior results with 98.63, 98.76, and 98.68 delicacy for BoT- IoT, CICIDS2017, and CICIDS2019 datasets, independently. This outgrowth is attained by the BPOA-grounded point selection system, which improves the data quality. Grounded on the findings of this study, it's determined that the recommended model will help produce a successful Intrusion discovery system with a high discovery rate. future work will number developing the suggested IDS to fete other attack types. Also, the recommended strategy can be altered and used in a significant security operation.

Authors' Information

– **Temitope Samson Adekunle** received the B.Tech. degree in Pure Mathematics from the Federal University of Technology, Minna, Nigeria, the M.Tech. degree in Mathematics (Fluid Dynamics) from the Federal University of Technology, Minna, Nigeria and also MSc degree in Data Science from the University of Salford, Manchester, United Kingdom. He is a Ph.D. student at the Department of Computer Science, Colorado State University, Fort Collins, United State. His major research focus is in the aspect of Artificial Intelligent and Machine Learning, Fluid Dynamics, Mathematics Modeling, Data Engineering, Simulation and Modeling, Big Data Mining.

– **Toheeb Adetoyese Adeleke** received the B.Tech. degree in Computer Engineering at Ladoke Akintola University of Technology, Ogbomoso, Nigeria where he is currently a Master student. His major research focus is in the aspect of Artificial Intelligent, Data Science and Information Security.

– **Olakunle Sunday Afolabi** obtained the B.Tech. degree in Computer Engineering from Ladoke Akintola University of Technology, Ogbomoso, Oyo state, Nigeria, the M.Sc. degree in Information Technology (IT) from NOUN-National Open University of Nigeria, Abuja, Nigeria. He is a Ph.D. student at the Department of Computer Science, University of Abuja, Abuja, Nigeria. His major research focus is in the aspect of Artificial Intelligent and Machine Learning, Simulation and Modeling, Data Mining, Artificial Neural networks, and Information Security.

– **Oluwaseyi Omotayo Alabi** received the B.Eng. and M.Eng. degree in Mechanical Engineering

(Thermo-Fluid) from the Federal University of Technology, Minna, Nigeria, and the University of Ilorin, Nigeria, respectively. He is a Ph.D. student at the Department of Mechanical Engineering, University of Ibadan, Nigeria. He has been engaged in research and teaching for more than two years. His major research focus is in Artificial Intelligent and Machine Learning, Energy, Heat Transfer, Simulation and Modeling, Aerodynamic, and Computational Thermal Fluids.

- **Adekunle Olugbenga Ejidokun** received his bachelor's degree from Ladoke Akintola University of Technology, Nigeria, in 2010. He also obtained a Master's degree from Obafemi Awolowo University, Ile-Ife, Nigeria, at the Department of Computer Science in 2016 and is currently pursuing his Ph.D. at the same university. He is currently a lecturer in the Department of computer sciences at Dominion University, Ibadan. His research interests include information systems, data analytics, data science, and machine learning.

- **Godwin Nse Ebong** is an accomplished professional passionate about technology and innovation. He graduated from Caritas University in Nigeria and the University of Salford, respectively, with a Bachelor of Science in Engineering and a Masters in Data Science, both in the United Kingdom. He is an expert in cloud engineering, data engineering, and data analysis.

- **Temitope A. Bamisaye** received the B.Sc. degree in Communication Technology from the National Open University of Nigeria, Abuja, Nigeria, the M.Sc. degree in Information Technology from the National Open University of Nigeria, Abuja, Nigeria. His major research focus is in the aspect of Artificial Intelligence and Machine Learning, Data Science, Internet of Things, Data Mining, and Information Security.

Authors' Contributions

- **Temitope Samson Adekunle** contributed with the conceptualization, validation and supervision.

- **Toheeb Adetoyese Adeleke** contributed with the conceptualization and methodology.

- **Olakunle Sunday Afolabi** contributed with the resources, software, project administration, and writhing of original draft.

- **Oluwaseyi Omotayo Alabi** contributed with the methodology, editing and review, visualization, and supervision.

- **Adekunle Olugbenga Ejidokun** contributed with the conceptualization, validation and supervision.

- **Godwin Nse Ebong** contributed with the conceptualization and methodology.

- **Temitope A. Bamisaye** contributed with the resources, software, project administration, and writhing of original draft.

Competing Interests

The authors declare that they have no competing interests.

Funding

No funding was received for this project.

References

[1] H. Aydın, Z. Orman, and M. A. Aydın, "A long short-term memory (lstm)-based distributed denial of service (ddos) detection and defense system design in public cloud network environment," *Computers & Security*, vol. 118, p. 102725, 2022.

[2] O. D. Okey, S. S. Maidin, P. Adasme, R. Lopes Rosa, M. Saadi, D. Carrillo Melgarejo, and D. Zegarra Rodríguez, "Boostedenml: Efficient technique for detecting cyberattacks in iot systems using boosted ensemble machine learning," *Sensors*, vol. 22, no. 19, p. 7409, 2022.

[3] S. A. Ajagbe, K. A. Amuda, M. A. Oladipupo, F. A. Oluwaseyi, and K. I. Okesola, "Multi-classification of alzheimer disease on magnetic resonance images (mri) using deep convolutional neural network (dcnn) approaches," *International Journal of Advanced Computer Research*, vol. 11, no. 53, p. 51, 2021.

[4] R. K. Batchu and H. Seetha, "A hybrid detection system for ddos attacks based on deep sparse autoencoder and light gradient boost machine," *Journal of Information & Knowledge Management*, vol. 22, no. 01, p. 2250071, 2023.

[5] J. Li, H. Zhang, Z. Liu, and Y. Liu, "Network intrusion detection via tri-broad learning system based on spatial-temporal granularity," *The Journal of Supercomputing*, vol. 79, no. 8, pp. 9180–9205, 2023.

[6] D. Teixeira, S. Malta, and P. Pinto, "A vote-based architecture to generate classified datasets and improve performance of intrusion detection systems based on supervised learning," *Future Internet*, vol. 14, no. 3, p. 72, 2022.

[7] V. Ravi, R. Chaganti, and M. Alazab, "Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system," *Computers and Electrical Engineering*, vol. 102, p. 108156, 2022.

[8] M. I. Kareem and M. N. Jasim, "Fast and accurate classifying model for denial-of-service attacks by using machine learning," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 3, pp. 1742–1751, 2022.

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

[10] A. Fatani, A. Dahou, M. A. Al-Qaness, S. Lu, and M. A. Elaziz, "Advanced feature extraction and selection approach using deep learning and aquila optimizer for iot intrusion detection system," *Sensors*, vol. 22, no. 1, p. 140, 2021.

[11] M. V. Gaur and R. Kumar, "M-lstm: Multiclass long short-term memory based approach for detection of ddos attacks," *Mathematical Statistician and Engineering Applications*, vol. 71, no. 3s2, pp. 1375–1394, 2022.

[12] J. Halladay, D. Cullen, N. Briner, J. Warren, K. Fye, R. Basnet, J. Bergen, and T. Doleck, "Detection and characterization of ddos attacks using time-based features," *IEEE Access*, vol. 10, pp. 49794–49807, 2022.

[13] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "Ae-mlp: A hybrid deep learning approach for ddos detection and classification," *IEEE Access*, vol. 9, pp. 146810–146821, 2021.

[14] J. Shroff, R. Walambe, S. K. Singh, and K. Kotecha, "Enhanced security against volumetric ddos attacks using adversarial machine learning," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–10, 2022.

[15] H. Azzaoui, A. Z. E. Boukhamla, D. Arroyo, and A. Bensayah, "Developing new deep-learning model to enhance network intrusion classification," *Evolving Systems*, vol. 13, no. 1, pp. 17–25, 2022.

[16] S. A. Ajagbe, O. A. Oki, M. A. Oladipupo, and A. Nwanakwaugwum, "Investigating the efficiency of deep learning models in bioinspired object detection," in *2022 International conference on electrical, computer and energy technologies* (*ICECET*), pp. 1–6, IEEE, 2022.

[17] S. A. Ajagbe and M. O. Adigun, "Deep learning techniques for detection and prediction of pandemic diseases: a systematic literature review," *Multimedia Tools and Applications*, pp. 1–35, 2023.

[18] C.-S. Shieh, T.-T. Nguyen, C.-Y. Chen, and M.-F. Horng, "Detection of unknown ddos attack using reconstruct error and one-class svm featuring stochastic gradient descent," *Mathematics*, vol. 11, no. 1, p. 108, 2022.

[19] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-learning-based ddos attack detection using mutual information and random forest feature importance method," *Symmetry*, vol. 14, no. 6, p. 1095, 2022.

[20] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks," *Electronics*, vol. 8, no. 11, p. 1210, 2019.