Received: 22 September 2023 | Revised: 17 January 2024 | Accepted: 21 February 2024 | Published online: 6 March 2024

RESEARCH ARTICLE

Artificial Intelligence and Applications
2024, Vol. 2(3) 165–171
DOI: 10.47852/bonviewAIA42021780

BON VIEW PUBLISHING

An Intrusion System for Internet of Things Security Breaches Using Machine Learning Techniques

Temitope Samson Adekunle[1], Oluwaseyi Omotayo Alabi[2,*], Morolake Oladayo Lawrence[3], Toheeb A. Adeleke[4], Olakunle Sunday Afolabi[5], Godwin Nse Ebong[6], Gabriel Olumide Egbedokun[7] and Temitope A. Bamisaye[8]

[1]*Department of Computer Science, Colorado State University, USA*

[2]*Department of Mechanical Engineering, Lead City University, Nigeria*

[3]*Department of Computer Science, Baze University, Nigeria*

[4]*Department of Computer Engineering, Ladoke Akintola University of Technology, Nigeria*

[5]*Department of Computer Science, University of Abuja, Nigeria*

[6]*Department of Data Science, University of Salford, UK*

[7]*Department of Computer Science, The Polytechnics Ibadan, Nigeria*

[8]*Department of Computer Science, National Open University of Nigeria, Nigeria*

Abstract: Effective identification and categorization of network attacks are paramount for ensuring robust security. However, contemporary techniques often struggle to accurately discern and classify novel attack patterns. This research introduces an innovative framework designed to achieve reliable attack detection and classification by harnessing the synergistic capabilities of utilizing DenseNet convolutional neural networks and rap music analysis techniques. Our approach leverages feature extraction through the Attention Pyramid Network (RAPNet) framework, tailored to extract pertinent features from input data, alongside binary Pigeon optimization. Subsequently, we employ feature selection using the optimization algorithm (BPOA). Once the optimal features are identified, we employ the Densenet201 model to categorize attacks across various datasets, including Bot-IoT, CICIDS2017, and CICIDS2019, through deep learning methodologies. To address the challenge posed by imbalanced data, we introduce conditional generative adversarial networks for generating additional data samples for minority classes, thus mitigating the issue. In contrast to recent intrusion detection methods, our results showcase the model's exceptional precision in detecting and categorizing achieving accuracy rates of 99.12%, 99.01%, and 99.18% for Bot-IoT, CICIDS2017, and CICIDS2019 datasets, respectively. Despite the potential benefits of a machine learning-based intrusion detection system (IDS) for Internet of Things (IoT) security, several limitations must be considered. These include the lack of standardized security protocols across various IoT devices and platforms, which makes it challenging to develop a uniform IDS. Furthermore, machine learning models, including those for intrusion detection, can be vulnerable to adversarial attacks that can circumvent or mislead the model's decision-making process. Thus, the potential for sophisticated attacks on IoT systems must be considered when developing such a system.

Keywords: security, deep learning, dataset, framework, Bot-IoT

1. Introduction

Data communication programs have been developed to facilitate the ease of business operations and device connectivity [1, 2]. However, their impact on the core components of real-world networks is relatively limited. Sectors of paramount importance, like financial institutions, healthcare facilities, and service companies, are exposed to security vulnerabilities because of their heavy reliance on computer networks [3, 4]. Given this reliance, it becomes imperative to uphold optimal network conditions to ensure availability, effectiveness, and security. A security lapse can have a significant impact on network performance, leading to eventual network malfunction and vulnerability. The goal of this research is to investigate and implement an intrusion detection system (IDS) for Internet of Things (IoT) security breaches that leverages the capabilities of machine learning. Existing security approaches may struggle to keep up with the dynamic and ever-changing nature of IoT ecosystems, which are characterized by a wide range of devices, communication protocols, and evolving attack vectors. By applying machine learning, which can

*Corresponding author: Oluwaseyi Omotayo Alabi, Department of Mechanical Engineering, Lead City University, Nigeria. Email: alabi.oluwaseyi@lcu.edu.ng

analyze large amounts of data and detect patterns, we can enhance the security of IoT networks and better protect against potential threats.

Furthermore, cyberattacks have the potential to impact critical systems, disrupt armament systems, and lead to the unauthorized release of confidential information. Such attacks can result in the loss of highly sensitive and invaluable data, including medical records and military data, among others. Additionally, cyberattacks can disable both phone and computer networks, rendering data inaccessible and systems non-functional [5–7]. Banking and government networks are especially susceptible due to the immense value of the data they store. In these instances, hackers may pilfer information, particularly banking details, and exploit that data for their gain. The increasing ubiquity of IoT devices has transformed our world, allowing for enhanced connectivity and convenience. However, the rapid proliferation of IoT devices has also created a vast array of security challenges, with potential vulnerabilities that can be exploited by malicious actors. Securing this diverse and ever-growing ecosystem of IoT devices is essential for preserving the integrity and confidentiality of data, and machine learning-based IDSs offer a promising approach to addressing these challenges. By tailoring such systems specifically for IoT environments, we can leverage the power of machine learning to detect and prevent a broad range.

Numerous types of attacks have given rise to irregularities on the internet, with a notable increase in such incidents over the last decade. These attacks have posed a significant menace to the reliability of networks, impacting a wide array of services [8–10]. Among these, denial of service (DoS) and distributed denial of service (DDoS) attacks stand out as particularly critical. Service interruption attacks and service flooding attacks are the two basic forms of DoS cyberattacks. DDoS cyberattacks, however, are thought to be the most hazardous of all.

The IoT network suffered significant losses as a result of the DDoS attack. Consequently, IoT stakeholders have become highly vigilant about these vulnerabilities. In such attacks, numerous compromised devices or systems collaborate to target a single entity, rendering it difficult to detect and counteract the attacking network [11–14]. Cyberattackers frequently employ botnets to disrupt the internet infrastructure. DDoS attacks prove challenging to promptly identify and mitigate, but this tactic yields substantial gains for attackers due to the potential impact of their assaults.

Recently, deep learning has garnered significant attention in the realm of security recognition, owing to its reliable extraction the features and recognition capabilities, especially in scenarios involving vast datasets. In the absence of contextual information, deep learning methods excel at capturing salient features within input data through multiple layers [15, 16]. Consequently, in this study, we employ Densenet 201-based deep learning to undertake multi-class classification of DoS and DDoS attacks. To address the challenge of imbalanced data, we employ a provisional conditional generative adversarial network (CGAN) to augment the dataset. Subsequently, feature extraction and the double Chump optimization technique are used for selection (BPOA). Finally, the Densenet 201 classifier is used to identify and categorize the attacks.

DoS and DDoS attacks pose significant challenges for many organizations due to their immense potential to swiftly disrupt vulnerable servers. Consequently, numerous research initiatives have been dedicated to mitigating these types of attacks, with several innovative strategies proposed by researchers. Here, we provide a brief overview of some of these approaches. To effectively detect and categorize DDoS attacks, Deepa et al. [17] introduced a novel approach that combines two deep learning-based methods: autoencoder (AE) and multi-layer perceptron (MLP). The authors employed AE for unsupervised feature extraction, enabling the subsequent classification of various DDoS attack types using an MLP network. The effectiveness of this proposed approach was evaluated using a substantial dataset of DDoS attacks from the CICDDoS2019 dataset, measuring performance based on criteria such as F1-score, recall, precision, and sensitivity.

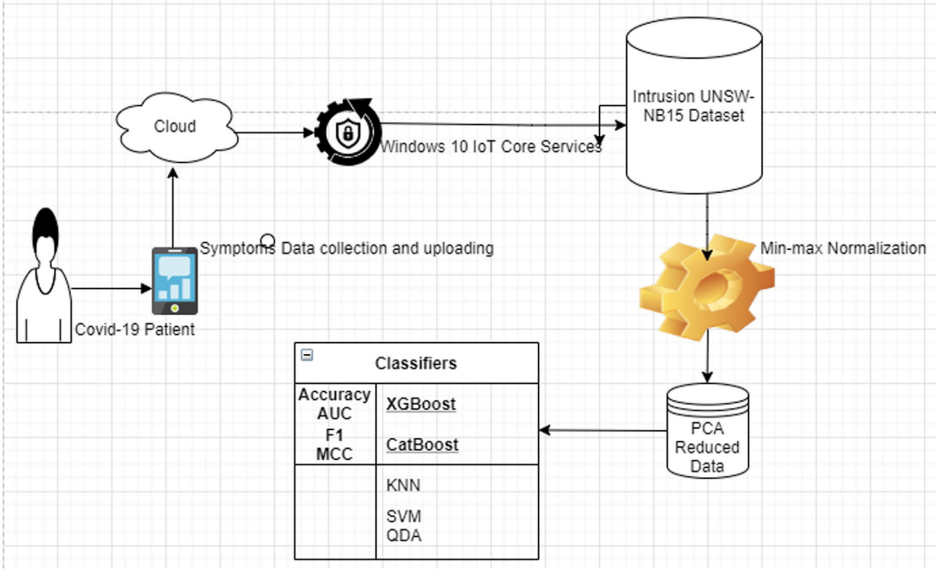
Mishra et al. [18] devised a cyberattack detection system built upon a generative adversarial network (GAN). There were two different GAN-based models used in this system. The second model was capable of producing DDoS instances that closely matched those from the dataset, while the first model produced benign instances that closely resembled benign samples from the dataset. For the classification of network traffic, Alduailij et al. [19], Ajagbe et al. [20], and Ajagbe and Adigun [21] developed an IDS based on deep neural networks (DNNs). They put into practice a four-layer neural network, containing 136 neurons in each layer. They carried out multiple trials with various hyperparameter combinations and compared the outcomes with those produced from other shallow and deep artificial neural network models to determine the efficacy of their suggested approach. The CICIDS2017 and NSL-KDD datasets were used in their evaluation, which used conventional performance metrics. Thirty-six different DNN models were also developed and examined. Each model focused on a different aspect of the problem.

To detect unfamiliar DDoS attacks, Shieh et al. [22] constructed a system that distributes retired subcaste traits and makes use of reconstruction mistakes. The research used a 1D linked neural network and a deep hierarchical reconstruction network (DHRNet) architecture, together with a spatial position constraint prototype loss function. In the following stage, an optimization method based on arbitrary gradient descent was used to find previously unknown patterns. The CICIDS2017 Friday Open Dataset was used to assess the efficacy of this approach. Manjunath et al. [23] introduced a DDoS attack detection system employing a diverse set of machine learning and feature selection algorithms. Initially, the system used both random forest (RF) feature importance and mutual information algorithms to identify the most important qualities from the CICDDoS2019 and CICIDS2017 datasets. A combination of weighted voting ensemble, gradient boosting, K-nearest neighbor (KNN), logistic regression, and RF approaches were then used to detect attacks. Following that, the system's effectiveness was assessed using measures like the F1-score, recall, precision, and sensitivity. The primary goals of this paper are as follows: To address the issue of imbalanced data and enhance the performance of the proposed model, the approach involves the utilization of provisional GAN-based data augmentation, departing from the conventional feature generation method; to extract important features from unprocessed network traffic data, the paper uses a deep learning approach based on RAPNet. The novelty of this topic lies in its focus on the specific application of machine learning to the problem of IoT security. Most existing research on ML-based IDSs focuses on general cybersecurity applications, but this topic highlights the unique challenges and opportunities presented by IoT devices. In addition, the proposed architecture is designed specifically for the unique characteristics of IoT networks, such as the large number of devices, heterogeneity, and resource constraints.

2. Methodology Approach

This section introduces a conceptual deep learning-based IDS and its robust framework for classifying various types of datasets as shown in Figure 1 [7, 24]. The proposed framework encompasses five crucial stages: pre-processing, data augmentation, feature generation, feature selection, and classification. The raw data first go through several preparation stages to remove unnecessary information. Addressing

Figure 1
Proposed framework system



the skewed data issue, a provisional GAN-based data augmentation method is applied to enhance classifier quality. Subsequently, feature generation is carried out on the processed data using a deep learning approach grounded in the Refined Attention Aggregate Network (RAPNet). Then, from the features that were generated, important components are extracted using deep learning techniques. Finally, the classifier, based on Densnet201, examines these characteristics and categorizes cyberattacks effectively.

CGAN has been used to generate synthetic network traffic that can be used to train IDSs and other machine learning algorithms. The synthetic data generated by CGAN are similar to real network traffic but do not contain any sensitive information that could be leaked if the data were to be compromised. This makes it ideal for training algorithms without the risk of exposing sensitive data. The CGAN model is composed of two networks: the generator network and the discriminator network. The generator network is a neural network that takes a random noise vector as input and generates an image. The generator is trained to minimize the loss function, which is the difference between the generated image and the target image. This encourages the generator to produce images that look like the target images. The discriminator network is a binary classifier that takes an image as input and outputs a score that indicates how likely the image is to be real or fake.

2.1. Pre-processing of data

The training procedure is more reliable and results in a more accurate model when a data pre-processing stage is included. Thus, in this stage, undesirable characteristics such as instances where "flow packets/s" equal "infinity" or "NaN" are filtered out. One-hot encoding (OHE) is employed in this study, which is a data pre-processing technique commonly used in machine learning. OHE transforms categorical data into a set of binary vectors, where each vector has only one "hot" element, which is set to 1, while all other elements are set to 0. XGBoost and CatBoost were chosen for this research because they are both powerful machine learning models that have demonstrated strong performance in a variety of classification tasks, including intrusion detection and cybersecurity. In addition, both models offer efficient computation and feature engineering capabilities, making them well-suited for processing large amounts of data. Additionally, XGBoost and CatBoost both support ensemble learning and are robust against overfitting, making them ideal for addressing the challenges of IoT security. This makes it easier for machine learning algorithms to process and classify the data. This normalization technique is applied to each column individually. It means solving the equation below for each occurrence of a record, where "x" stands for the attributes of the dataset [7]:

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

2.2. Enhancing data using CGAN

Using the CGAN technique, it was possible to construct augmented datasets that closely resembled the original data in this area. The difference between CGAN and GAN's training methods is in the limitations imposed on the labeling of the generated data. The discriminator (DS) and generator (GR) networks are the two main parts of the architecture. These two networks compete against each other to learn from artificially generated data.

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

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

In Equations (2) and (3), "yr" represents the input of random variables from the GR network, $DS(x)$ represents the likelihood that the DS system would successfully forecast the initial data "x",

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

The loss function of the generator, in contrast to the discriminator, is presented by:

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

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

$$\min_{GR}\max_{DS} V(GR, DS) = \min_{GR}\max_{DS}(E_{x\sim P_{data(x)}}[\log DS(x)] + (E_{y_r\sim P_{y_r(y_r)}}[\log(1 - DS(GR(y_r)))] \quad (6)$$

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

The generator network employs transposed convolutional layers to up-sample the input feature vectors. Multiple transposed convolutional layers are utilized, each with varying channel configurations, such as 64, 128, 256, and 512. Each level of these blocks aligns and ensures that the model produces samples that approximate the given data structure with the size of the input feature vector.

2.3. Using RAPNet point birth

RAPNet, or Refined Attention Aggregate Network, captures key features from the pre-processed data. The foundation of the network is made up of five-stage encoder and decoder architectures. In the first three stages of this model, 1 × 1 convolutional layers are used. These are followed by the next two stages, which use 3 × 3 convolutional layers with atrous convolution. Between these convolutional layers, the ReLU activation function is used to create a non-linear representation that captures low-level particular characteristics. The remaining blocks use a deconvolution method to up-sample the high-resolution feature maps. In order to carry out point-wise fusion, this makes sure that all feature map sizes are uniform. The side connections are then enhanced by the Convolutional Block Attention Module (CBAM), which enables channel-by-channel adaptive adjustment of the feature maps. This is essential for lowering false positives and improving the accuracy of feature extraction. The aggregate pooling module is added to the decoding route in the last residual block of the conv5 stage to acquire contextual data. This module uses global average pooling and a four-level aggregation with kernel sizes of 1 × 1, 2 × 2, 3 × 3, and 6 × 6. The feature maps from the respective layers of the encoding network and the decoding network are then concatenated, which completes the point-wise fusion. The labels for these combined feature maps are P2, P3, P4, and P5.

To facilitate feature fusion, a lateral connection is established between the P2 feature map, which is a composition of feature maps P3, P4, and P5. This method enables multiscale feature extraction by fusing information. The final fused feature map P2 is then used to obtain the desired feature extraction results.

3. Experiments and Results

In this section, we assess the effectiveness of the proposed intrusion detection model through a series of experiments, and the results are presented. TensorFlow served as the backend framework while Python was used to implement the suggested technique. These experiments made use of an Adam optimizer, a learning rate of 0.002, the ReLU activation function, a batch size of 30, a momentum value of 0.8, a total of 60 training epochs, a dropout rate of 0.8, and other hyperparameters. The dataset was divided into two sets: a training set that contained 69% of the data and a testing set that contained the remaining 33%.

3.1. Dataset description

3.1.1. Bot-IoT dataset

The dataset, originally curated by Saheed et al. [24] and Abdullayeva [25], encompasses over 72 million records, encompassing a diverse array of synthetic and real-world events. Although the dataset primarily comprises DoS and DDoS-type packets, it also encompasses four distinct categories of attacks. Similar to the UNSW-NB15 dataset, this dataset exhibits an imbalanced distribution of samples.

3.1.2. CICIDS-2017 dataset

The CICIDS-2017 intrusion detection dataset is a recent creation by the Canadian Institute of Cybersecurity. It encompasses a wide range of information including timestamps, destination and source IP addresses, types of attacks, protocols, as well as destination and source ports. This dataset incorporates elements of genuine and practical internet traffic, gathered over a span of 5 days, comprising a total of 2,830,743 records and featuring 80 network traffic attributes. Structured as a CSV file, it encompasses both legitimate and unauthorized traffic, documented over eight traffic monitoring intervals. The dataset encompasses numerous categories of cyber threats, including DDoS, DoS, SSH, brute force, FTP, botnets, infiltration, Heartbleed, and web attacks.

3.1.3. CICIDS2019 dataset

This dataset encompasses a diverse array of DDoS attacks that can be carried out utilizing both TCP and UDP network protocols. It categorizes attacks into two main types: invasions motivated by exploitation and by introspection. This dataset, which consists of more than 80 flow attributes, was assembled over the course of 2 days to enable training and testing studies. It encompasses attacks utilizing protocols such as SNMP, LDAP, UDP-Lag, MSSQL, SYN, NetBIOS, NTP, DNS, and WebDDoS.

3.2. Evaluation metrics

$$ACC = \frac{tr_p + tr_n}{number\ of\ samples} \quad (7)$$

$$PRE = \frac{tr_p}{tr_p + fl_p} \quad (8)$$

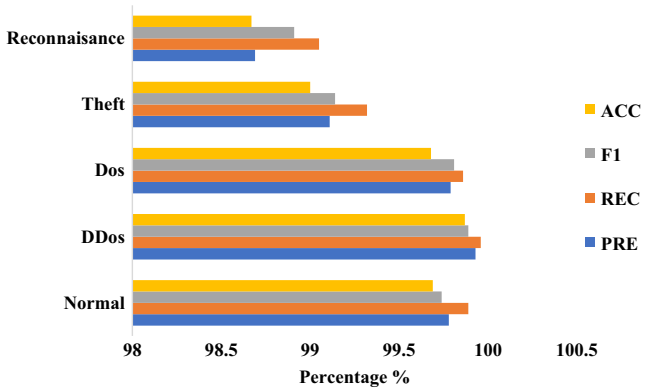
$$REC = \frac{tr_p}{tr_p + fl_n} \quad (9)$$

$$F1 = 2 \times \frac{precision \times recall}{precision + recall} \quad (10)$$

3.3. Result and discussion

This section tests the proposed framework using the selected datasets through numerous experiments, and the results are contrasted with those obtained using alternative methods. The performance assessment of the Bot-IoT dataset using our suggested method is shown in Figure 2. The table illustrates the effectiveness of our technique across various attack categories. Notably, the BoT-IoT dataset achieves impressive accuracy (ACC) rates of 99.87% for DDoS and 99.68% for DoS attacks. Comparatively, the performance is slightly lower for the theft and reconnaissance categories, with our method achieving ACC rates of 99% for theft and 98.67% for reconnaissance.

Figure 2
Bot-IoT dataset classification



DDoS attacks and reconnaissance attacks exhibit similar behavior, primarily due to shared features in the current dataset. This similarity poses a challenge in distinguishing between these two attack types using our model. The DDoS class achieves the greatest F1 (99.36%), REC (99.99%), PRE (99.89%), and ACC (98.95%) values among all classes, as shown in Figure 2. Overall, our method demonstrates favorable results across all attack categories. However, the reconnaissance class received a lower rating due to its resemblance to conventional data, and theft-exfiltration also exhibited lower results, likely attributed to a few instances in the dataset being misclassified into different categories.

Following the multi-class classification, the results of our suggested strategy are compared to those of existing intrusion detection techniques tested on the BoT-IoT dataset, as shown in Table 1. The table demonstrates that our proposed methodology outperforms other well-established methods. This shows that across most classes, our suggested framework dramatically lowers false positives. Furthermore, support vector machine (SVM) erroneously treated many attacks as regular network packets, revealing its limitations in intrusion detection. In the overall performance comparison, XGBoost outperforms all other methods. To be clear, the ACC of the KNN algorithm is marginally greater (98.87%) than that of XGBoost (98.95 percent). This is attributed to KNN's capability to handle multi-class instances effectively and produce superior accuracy compared to SVM. Additionally, C4.5 exhibits better performance than SVM. The results obtained from our proposed strategy using the Bot-IoT dataset demonstrate that our approach yields more valuable insights when compared to other strategies, showcasing its effectiveness in intrusion detection.

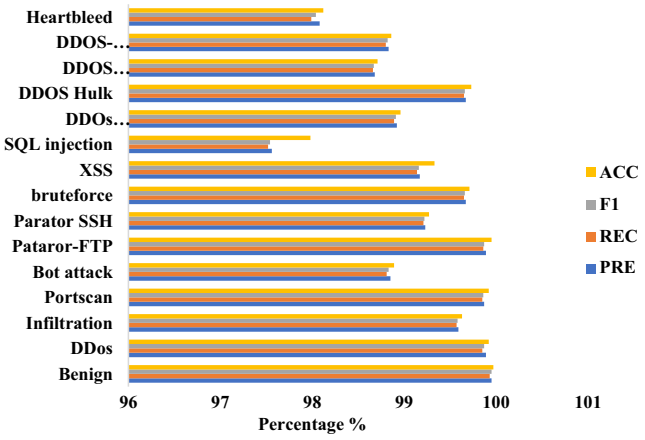
Table 1
Bot-IoT dataset approach compare to others

Techniques	PRE	REC	F1	ACC
KNN [7]	98.53	98. 56	98.34	98.87
SVM [6]	88.90	88.86	88.54	88.65
C4.5 [25]	–	–	–	91.96
XGBoost [26]	98.56	98.64	98.77	98.95
Proposed	98.99	99. 72	98.89	98.98

3.3.1. Evaluation of the CICIDS2017 dataset's performance

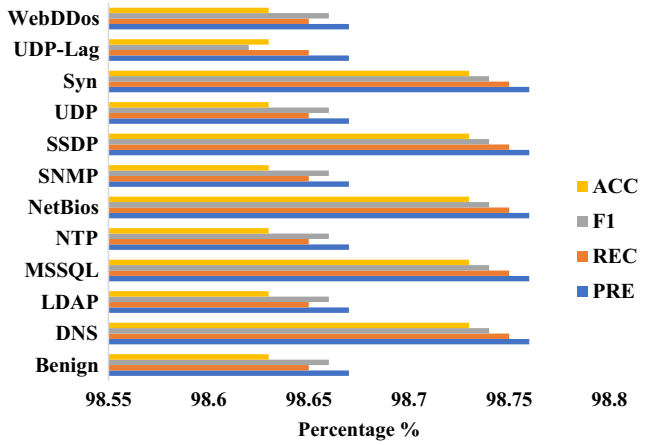
Figure 3 illustrates how well our proposed model performed in multi-class classification while taking into account ACC, PRE, REC, and F1 variables on the CICIDS2017 dataset. With a detection ACC of 98.99%, "Benign" traffic detection is the area where our technique performs best. In contrast, "SQL Injection" traffic detection exhibits the poorest performance, with a detection ACC of 98.25%. This lower performance can be attributed to the limited number of "SQL Injection" data snippets available in the data network. Moreover, a "bot" attack's behavior pattern closely matches that of regular network traffic, posing a challenge for our proposed approach to reliably distinguish these attacks. As a result, the overall performance exhibits an average result. It is interesting to note that attacks like SQL injection and Heartbleed were predicted more precisely than brute force attacks.

Figure 3
Classification of CICIDS2017 dataset



In terms of other performance metrics, both "brute force" and 'DDoS Hulk' exhibit identical precision (PRE) scores of 99.67%, recall (REC) scores of 99.65%, and F1 scores of 99.67%. These results demonstrate the suggested classifier maintaining symmetrical behavior about traffic classifications in this arrangement. Furthermore, it is essential to consider both accuracy (ACC) and recall (REC) rates when assessing the classifier's performance for each type of attack. The data suggest that "benign" classes are incorrectly classified as attacks because they have a high number of false positives and a low ACC. On the other hand, a model with low recall may fail to notice real invasions. Therefore, in order to provide the optimal model performance, ACC and REC values must be sufficiently high. As illustrated in Figure 4, the proposed model attains higher values across all performance parameters that define its effectiveness in multi-class categorization.

Figure 4
Classification of CICIDS2019 dataset



3.3.2. Evaluation of the CICIDS2019 dataset's performance

Figure 4 displays the outcomes of the multi-class classification performed on the CICIDS2019 dataset using our advised technique. The table showcases the excellence of our method in multi-class categorization, delivering the highest performance for each attack type. Remarkably, the accuracy (ACC) rates for every class exceed 98%. Particularly noteworthy are the ACC rates for the "Benign," "DNS," and "NTP" classes, achieving outstanding scores of 98.76%, 98.71%, and 98.58%, respectively. This underscores their exceptional performance. The classification performance for other attack categories also yields highly favorable outcomes.

As evident from the illustration in Figure 4, the proposed classifier exhibited comparatively lower performance for the "WebDDoS" and "MSSQL" classes in comparison to various sorts of class. Subsequent tests have shown that "WebDDoS" and "MSSQL" have many similarities exist between traits, making it more challenging for classifiers to effectively differentiate between the traffic data associated with these classes. Thus, for "WebDDoS" and "MSSQL," the proposed technique achieves detection ACC rates of 98.58% and 98.12%, respectively. The general accuracy of the algorithm is improved by this innovation (ACC).

3.3.3. Effects of the feature selection method

To enhance the recommended intrusion detection process, the algorithm (BPOA) is used to obtain crucial element. This BPOA-based method, applied to the Bot-IoT, CICIDS2017, and CICIDS2019 datasets, provides more meaningful findings while lowering the amount of features.

Table 2 displays the performance of the suggested strategy with and without feature selection. The suggested strategy performs noticeably better when a successful BPOA-based feature selection approach is applied. Without feature selection, the strategy achieves ACC rates of only 97.98%, 99.01%, and 97.96% for the BoT-IoT, CICIDS2017, and CICIDS2019 datasets, respectively. However, after undergoing the feature selection procedure, the classifier demonstrates superior performance, utilizing the best possible set of features and delivering its optimal results.

Table 2
Comparison of with and without feature selection

With feature selection				
Dataset	PRE	REC	*F*1	ACC
BoT-IoT	97.94	99.10	99.00	97.95
CICIDS2017	97.98	97.96	97.99	97.98
CICIDS2019	97.97	97.95	97.96	99.11
Without feature selection				
BoT-IoT	97.98	99.12	99.10	97.98
CICIDS2017	97.99	97.99	99.03	99.01
CICIDS2019	97.96	99.20	97.97	97.96

4. Conclusion

The tremendous growth in network traffic and the dynamic nature of intrusions have made the demand for more precise and effective IDSs more pressing. In response, this research has implemented a deep learning-based network IDS. The results demonstrate the effectiveness of the proposed strategy in recognizing and categorizing cybersecurity dangers. Various performance standards, such as sensitivity, F-score, recall (perceptivity), and precision (discovery rate), have been used in the evaluation process to evaluate the effectiveness of the suggested models on three common datasets. In contrast to previous methods of attack detection, the proposed framework achieves superior results, boasting sensitivity rates of 98.73%, 98.69%, and 98.71% for the BoT-IoT, CICIDS2017, and CICIDS2019 datasets, respectively. The results of this study make it clear that the suggested model can help create an effective IDS with a high discovery rate. Extending the recommended IDS to cover other attack types will be part of future studies. The suggested approach can also be modified and used in larger security operations. This research could explore the integration of additional machine learning techniques, such as deep learning, to improve the accuracy and robustness of the proposed IDS. Additionally, the application of transfer learning and federated learning approaches could be investigated to enhance the model's generalizability across diverse IoT devices and networks. Another area of future work could be to develop an end-to-end solution that includes not only intrusion detection but also intrusion prevention and mitigation. This could involve the development of a real-time system that can analyze network traffic and take appropriate actions to mitigate threats as they arise.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

References

[1] Amaizu, G. C., Nwakanma, C. I., Bhardwaj, S., Lee, J. M., & Kim, D. S. (2021). Composite and efficient DDoS attack detection framework for B5G networks. *Computer Networks*, *188*, 107871. https://doi.org/10.1016/j.comnet.2021.107871

[2] Alabi, O. O., Ajagbe, S. A., Adeaga, O. A., & Adigun, M. O. (2023). Investigating fuel adulteration using Arduino as an engine protection device (EPD). *Journal of Hunan University Natural Sciences*, *50*(9), 106–113. https://doi.org/10.55463/issn.1674-2974.50.9.11

[3] Ajagbe, S. A., Amuda, K. A., Oladipupo, M. A., Oluwaseyi, F. A., & Okesola, K. I. (2021). Multi-classification of Alzheimer disease on magnetic resonance images (MRI) using deep convolutional neural network (DCNN) approaches. *International Journal of Advanced Computer Research*, *11*(53), 51–60. https://doi.org/10.19101/IJACR.2021.1152001

[4] Safarov, F., Basak, M., Nasimov, R., Abdusalomov, A., & Cho, Y. I. (2023). Explainable lightweight block attention module framework for network-based IoT attack detection. *Future Internet*, *15*(9), 297. https://doi.org/10.3390/fi15090297

[5] Rani, S. J., Ioannou, I., Nagaradjane, P., Christophorou, C., Vassiliou, V., Charan, S., . . . , & Pitsillides, A. (2023). Detection of DDoS attacks in D2D communications using machine learning approach. *Computer Communications*, *198*, 32–51. https://doi.org/10.1016/j.comcom.2022.11.013

[6] Teng, S., Wu, N., Zhu, H., Teng, L., & Zhang, W. (2018). SVM-DT-based adaptive and collaborative intrusion detection. *IEEE/CAA Journal of Automatica Sinica*, *5*(1), 108–118. http://doi.org/10.1109/JAS.2017.7510730

[7] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, *7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

[8] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Waqas Shaukat, M., Raza, S. M., . . . , & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. *Electronics*, *9*(9), 1379. https://doi.org/10.3390/electronics9091379

[9] Chaganti, R., Suliman, W., Ravi, V., & Dua, A. (2023). Deep learning approach for SDN-enabled intrusion detection system in IoT networks. *Information*, *14*(1), 41. https://doi.org/10.3390/info14010041

[10] Pashaei, A., Akbari, M. E., Lighvan, M. Z., & Charmin, A. (2022). Early intrusion detection system using honeypot for industrial control networks. *Results in Engineering*, *16*, 100576. https://doi.org/10.1016/j.rineng.2022.100576

[11] Adekunle, T. S., Lawrence, M. O., Alabi, O. O., Afolorunso, A. A., Ebong, G. N., & Oladipupo, M. A. (2024). Deep learning technique for plant disease detection. *Computer Science and Information Technologies*, *5*(1), 49–56. https://doi.org/10.11591/csit.v5i1.pp49-56

[12] Balasubramaniam, S., Vijesh Joe, C., Sivakumar, T. A., Prasanth, A., Satheesh Kumar, K., Kavitha, V., & Dhanaraj, R. K. (2023). Optimization enabled deep learning-based DDoS attack detection in cloud computing. *International Journal of Intelligent Systems*, *2023*, 2039217. https://doi.org/10.1155/2023/2039217

[13] Dahou, A., Abd Elaziz, M., Chelloug, S. A., Awadallah, M. A., Al-Betar, M. A., Al-Qaness, M. A., & Forestiero, A. (2022). Intrusion detection system for IoT based on deep learning and modified reptile search algorithm. *Computational Intelligence and Neuroscience*, *2022*, 6473507. https://doi.org/10.1155/2022/6473507

[14] Obeidat, A., & Yaqbeh, R. (2022). Smart approach for botnet detection based on network traffic analysis. *Journal of Electrical and Computer Engineering*, *2022*, 3073932. https://doi.org/10.1155/2022/3073932

[15] Gaber, T., El-Ghamry, A., & Hassanien, A. E. (2022). Injection attack detection using machine learning for smart IoT applications. *Physical Communication*, *52*, 101685. https://doi.org/10.1016/j.phycom.2022.101685

[16] Hamarshe, A., Ashqar, H. I., & Hamarsheh, M. (2023). Detection of DDoS attacks in software defined networking using machine learning models. *arXiv Preprint:2303.06513*.

[17] Deepa, V., Sudar, K. M., & Deepalakshmi, P. (2018). Detection of DDoS attack on SDN control plane using hybrid machine learning techniques. In *International Conference on Smart Systems and Inventive Technology*, 299–303. https://doi.org/10.1109/ICSSIT.2018.8748836

[18] Mishra, N., Singh, R. K., & Yadav, S. K. (2022). Detection of DDoS vulnerability in cloud computing using the perplexed Bayes classifier. *Computational Intelligence and Neuroscience*, *2022*, 9151847. https://doi.org/10.1155/2022/9151847

[19] Alduailij, M., Khan, Q. W., Tahir, M., Sardaraz, M., Alduailij, M., & Malik, F. (2022). Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method. *Symmetry*, *14*(6), 1095. https://doi.org/10.3390/sym14061095

[20] Ajagbe, S. A., Oki, O. A., Oladipupo, M. A., & Nwanakwaugwu, A. (2022). Investigating the efficiency of deep learning models in bioinspired object detection. In *International Conference on Electrical, Computer and Energy Technologies*, 1–6. https://doi.org/10.1109/ICECET55527.2022.9872568

[21] Ajagbe, S. A., & Adigun, M. O. (2024). Deep learning techniques for detection and prediction of pandemic diseases: A systematic literature review. *Multimedia Tools and Applications*, *83*(2), 5893–5927. https://doi.org/10.1007/s11042-023-15805-z

[22] Shieh, C. S., Nguyen, T. T., & Horng, M. F. (2023). Detection of unknown DDoS attack using convolutional neural networks featuring geometrical metric. *Mathematics*, *11*(9), 2145. https://doi.org/10.3390/math11092145

[23] Manjunath, C. R., Rathor, K., Kulkarni, N., Patil, P. P., Patil, M. S., & Singh, J. (2022). Cloud based DDOS attack detection using machine learning architectures: Understanding the potential for scientific applications. *International Journal of Intelligent Systems and Applications in Engineering*, *10*, 268–271. https://www.ijisae.org/index.php/IJISAE/article/view/2398

[24] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395–9409. https://doi.org/10.1016/j.aej.2022.02.063

[25] Abdullayeva, F. J. (2022). Distributed denial of service attack detection in E-government cloud via data clustering. *Array*, *15*, 100229. https://doi.org/10.1016/j.array.2022.100229

[26] Kumar, P., Gupta, G. P., & Tripathi, R. (2021). An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Computer Communications*, *166*, 110–124. https://doi.org/10.1016/j.comcom.2020.12.003

How to Cite: Adekunle, T. S., Alabi, O. O., Lawrence, M. O., Adeleke, T. A., Afolabi, O. S., Ebong, G. N., Egbedokun, G. O., & Bamisaye, T. A. (2024). An Intrusion System for Internet of Things Security Breaches Using Machine Learning Techniques. *Artificial Intelligence and Applications*, *2*(3), 165–171. https://doi.org/10.47852/bonviewAIA42021780