JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 09 Issue 02
2025

Research Article
https://doi.org/10.56979/902/2025

Machine Learning-Based Cyber Threat Detection Using DDoS Traffic

Osama Javid[1], Muhammad Yasir Shabir[1,*], Zahid Mehmood[1], Afshan Ahmed[1], Shafina Bibi[1], and Tayyab Arshad[1]

[1]Faculty of Computing and Engineering, Department of CS&IT, University of Kotli AJK, 11100, Kotli, AJK, Pakistan.
[*]Corresponding Author: Muhammad Yasir Shabir. Email: yasir.shabir14@gmail.com

Received: May 2, 2025 **Accepted:** July 30, 2025

Abstract: The increasing complexity of cyberattacks, particularly Distributed Denial of Service (DDoS) attacks, poses a serious threat to modern digital infrastructure. The signature-based traditional intrusion detection systems (IDS) have been in most cases unable to identify zero-day and evolving threats. In order to combat this obstacle, the proposed study features a model of machine learning-based cyber threat detection, namely, DDoS detection based on a realistic subset of the CIC-IDS-2017 dataset. This data set of labeled network traffic flows that comprise benign and DDoS activity data. It uses a thorough data preprocessing pipeline, which includes missing value imputation, feature scaling, and ANOVA F-test based statistical feature selection. Three monitored classifiers, Logistic Regression, Random Forest and a Deep Neural Network (DNN) are trained and tested on the picked features. To test the developed models, common measures of performance relevance, accuracy, precision, recall, F1-score and AUC Curve, are used. As shown by experimental results, Random Forest model performs better than the rest, coming up with 99.13% percent accuracy and AUC score of 0.991, showing a high capability and generalization. The results on the DNN and Logistic Regression are well demonstrating the efficacy of the proposed approach. This study demonstrates the applied benefit of machine learning on the topic of Cyber threat detection, and has built a repeatable baseline on which new study may be derived. Some of the extensions that can be suggested are multi-class attack detection, real-time deployment, integration of explainability tools to have transparency in the models.

Keywords: Cyber Threat Detection; DDoS Attack Classification; Machine Learning

1. Introduction

In the same hyper-connected world, the growth of digital infrastructures networks (cloud platforms, IoT system, and 5G networks) has dramatically enlarged the access points of malicious actors [1]. These smart cities, intelligent healthcare, industrial IoT, and autonomous systems have combined to heighten anxieties of cyber resilience, where malefactors target the weaknesses of the systems, services, and devices [2]. DdoS attacks are just one type of these attacks that can be among the most disruptive as they aim to disrupt the availability of a system and compromise the services provided in sectors that include finance and emergency response [3].

Since the standard signature-based IDSs are dependent on known threat models, they tend not to recognize new and zero-day attacks. To address this shortcoming, recent literature has shifted towards machine learning (ML)-based anomaly detection that can be used to automatically detect abnormal traffic patterns without needing the signatures of attacks in advance [4]. These systems can dynamically follow any new network behavior and are also applicable in scenarios that possess changing traffic patterns and malicious approaches. Nonetheless, a main issue concerns the adequate establishment and verification of ML-based models of IDS on realistic large-scale data sets. One such widely adopted benchmark in this area is the CIC-IDS 2017 dataset created by the Canadian Institute for Cybersecurity [5]. It emulates

enterprise-level traffic and combines normal operation behavior and labeled attacks such as DDoS, port scanning, access and brute-force, among others.

As part of the study, we propose a reproducible cyber threat detection system using this slice of DDoS data [6, 7]. This study use an effective preprocessing pipeline that includes missing and infinite values replacement, features normalization, and ANOVA F-test statistic-based top predictors section. Then train and test three ML models Logistic Regression (LR), Random Forest (RF), and a custom DNN and compare their performance in terms of the accuracy, precision, recall, F1-score, and ROC-AUC. We apply the DDoS-specific anomaly detection pipeline to a portion of CIC-IDS-2017 as well as design and implement this pipeline. We use rigorous statistical preprocessing and feature selection procedures to compare three different types of classifiers, one being a model based on Deep Learning (DL). Using DDoS attack flows in particular, the present work shows how highly optimized ML pipelines may be used as lightweight real-time cyber threat detectors and potentially deployed to smart city networks, edge computing frameworks, and critical infrastructure.

2. Literature Review

ML and AI tools have become an important driver of new trends in cyber threat detection, and recent research has extensively studied their application performance across application areas. Thwaini et al. (2022) compared the methods of anomaly detection in network traffic using ML, and the unsupervised Isolation Forest was compared with the supervised Neural Network (NN). Their findings showed that supervised models are both more sensitive and robust at identifying complex malicious patterns by promoting the need to integrate DL with ensemble methods to further improve detection process [8]. In the same breadth, Authors [9] have developed a real-time ML and big data-driven framework to detect threats in cybersecurity. Their work emphasizes that ML will be used to detect abnormal behavior with a high level of accuracy and large data processing will enhance the responsiveness of the systems that are crucial problems related to such concepts as false positives and scalability [9].

The authors [10] addressed malware threat detection with the help of various ML classifiers such as RF and Multilayer Perceptron applied to a heterogeneous dataset augmented with the application of dimensionality reduction measures, such as PCA and LDA. The results of the study verified that integrating ML techniques and heterogeneous datasets could produce high levels of detection accuracy greater than 99% [10]. Similarly, Gaddah and El-Geder (2024) created an IDS based on supervised ML models like the Decision Tree (DT) and Support Vector Classifier that performed quite well in the case of real intrusion classification in a network scenario [11]. Ravikumar et al. (2024) also tested several ML algorithms through both the network and behavioral data with a focus on feature selection and model tuning to enable the automation of threat detection and generation of actionable information [12].

The growth of Internet of Things (IoT) and Industrial IoT (IIoT) environments has brought forth new capabilities and limitations to the threat detection models and has brought the development the lightweight, privacy-aware models. The contribution of Ferrag et al. (2024) is the Security BERT cyber-attack detection model with privacy preservation, which is an implementation of the BERT transformer structure. A high accuracy of 98.2% on the Edge-IIoT set dataset makes Security BERT a fine-grained model on the leading edge 16-bit floating-point sets with the performance of 98.2 percent, surpassing other DL and traditional ML models and possessing a modest size that fit well in sparse IoT devices [13]. Encrypted MANET data transfer [21] and secure e-learning authentication [22] were used to protect email and data transmission.

In the context of security monitoring, Shelke and Hamalainen (2024) gave a complete survey with a highlighted multidimensional approach to detecting cyber threats that involved DNNs, ensemble learning, and behavioral encoding like User and Entity Behavior Analytics (UEBA). They emphasize the importance of collaborative defense tools and situational awareness (going beyond Security Operations Centers (SOC) based on SIEM solutions such as Splunk [14]. To counter the changing nature of cyber threats, Sharma (2024) discussed AI-enhanced cyber threat detection and response systems and reviewed the use of supervised, unsupervised, and reinforcement learning in them. The paper highlights issues regarding the quality of data, adversarial attacks, and ethics issues and recommends interdisciplinary cooperation and nonstop innovation as critical ways of staying abreast of the developing threats [15].

Hassanin et al. (2024) added a new pre-trained Large Language Model (m, PLLM-CS), which can be used with satellite networks and focused on their security. As a value added processor, PLLM-CS achieved a high accuracy on the UNSW NB15 data set in capturing and representing the semantic content of raw network traffic as transformed through the model into inputs that are semantically enriched and thereby suited to being integrated into Transformer architecture models, reflecting high accuracy performance of 100% compared to other existing deep-learning models including BiLSTM and CNN [16].

Kumar et al. (2024) addressed the data integrity and model explainability issues in artificial intelligence (AI)-powered cyber threat detection and included the explainable artificial intelligence (XAI) frameworks and blockchain technology. They came up with an integrated Clique Proof-of-Authority block chain technique which is used to validate multi cloud data safely and their parallel stacked LSTM model which is further augmented with a multi-head attention-based technique that offers increased precision and interpretation especially in smart healthcare situations [17]. Finally, Dhanushkodi and Thejas (2024) have provided a wide survey of the role of AI in cybersecurity application and indicated how transformer-based models are becoming more salient, federated learning, and blockchain as enabling technologies in the real execution of scalable, real-time and privacy-preserving detection of threats in many industrial fields such as industry 5.0, IoT and self-driving cars. Despite these achievements, they indicate remaining issues related to data volume services, real time processing, and the privacy aspect, where interdisciplinary research needs to continue in order to take full advantage of the power of AI in the context of cybersecurity [18].

3. Proposed Methodology

The our methodology of determining the network traffic as benign or DDoS based on a structured pipeline consists of 6 primary stages as shown in the Figure 1 of the framework. To begin with, the raw data contained in the CIC-IDS 2017 dataset is subjected to a data preprocessing step which deals with missing data and performs label encoding. During the second process, the features will be extracted making use of the feature scaling technique applying Standard-Scaler (SS) and feature selection by applying the ANOVA F-test (SelectKBest) creating only the most pertinent features in the process. The cleaned data is subsequently divided to 80% training and 20% testing categories. Three different ML models, LR, RF, and DNN are trained on the data that was used as training. The performance of these models is assessed with the help of such metrics as Accuracy, Precision, Recall, F1-score, and ROC-AUC, as well as the confusion matrix and receiver operating characteristics curve.

3.1. Dataset Selection

We use the CIC-IDS-2017 publicly available [19-[20] dataset. This particular subset can capture the realistic DDoS attack traffic, as well as, regular traffic of an enterprise-like setting. The data set has 80+ traffic flow characteristics per connection which consist of packet lengths, inter-arrival times, flag counts, and protocol level statistics.

3.2. Data Preprocessing

Various preprocessing processes are done before training the models to make sure the quality of data provided as well as to enhance performance of the model:

- Label Encoding: The Label column is changed into a numeric and the ones containing normal are labeled 0, and the ones containing DDoS are labeled 1.
- Missing and Infinite Values Management: All infinite values will be converted to NaN and, in turn, NaNs will be filled with zero or dropped depending on the situation.

3.3. Feature Extraction

In feature extraction, Two major methods are used under feature extraction to form or maximize the input data so that the model can be trained. First, feature scaling is carried out which converts all the features to a known scale with the mean being zero and variance being one so that a single feature does not overwhelm other ones because of its scale. This is followed by a feature selection procedure that would be implemented by (SelectKBest) method of ANOVA F-score as the statistic test that would lower the dimensionality and reduce constitutionality by choosing the most statistically significant 10 features. The classification models are consequently trained using these identified features that are used as input.

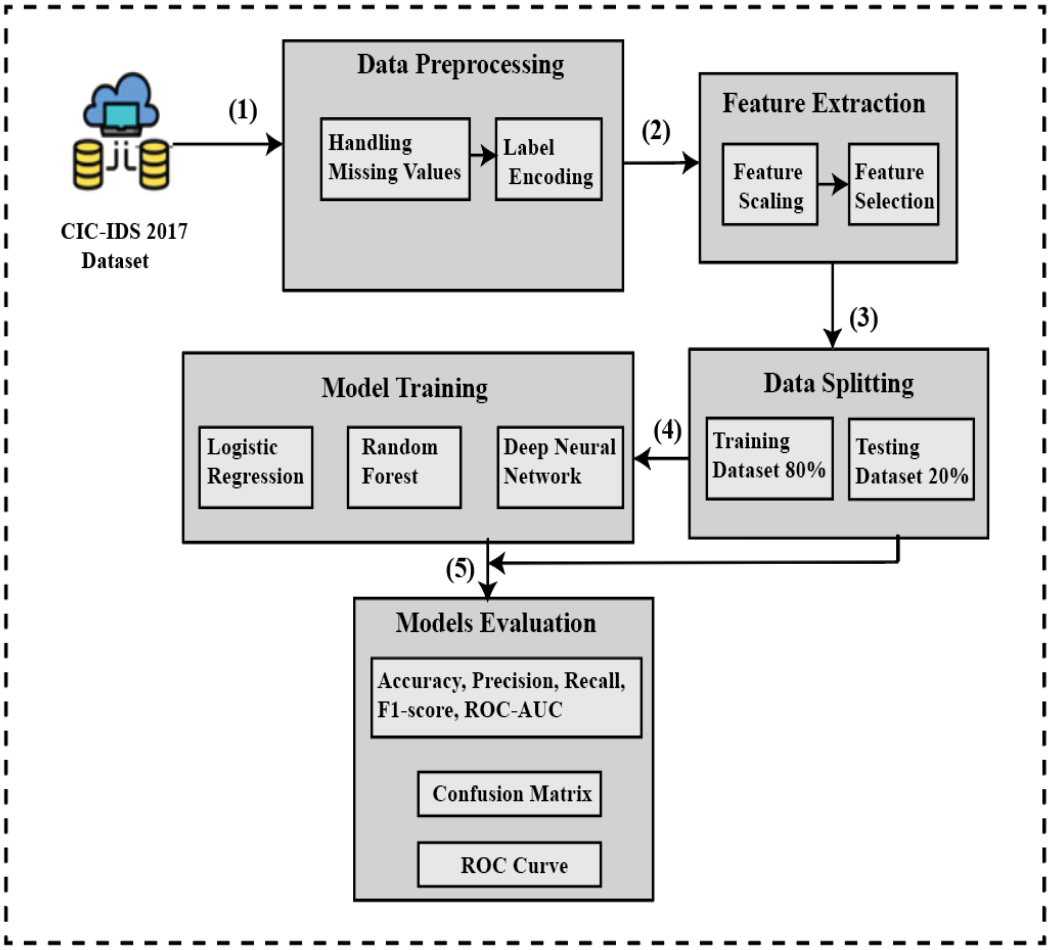

Figure 1. Proposed framework for classifying network traffic as benign or DDoS.

3.4. Model Implementation

During the implementation of the model, three classification algorithms will be used and assessed to identify DDoS traffic. LR is a reference model whose decision boundary is linear and provides a minimal benchmark that helps to compare performances. RF, an ensemble algorithm uses pluralistic decision trees through random feature selection and bootstrapped sampling to boost the accuracy levels of predictions, and hence, incurs minimum over-fitting. DNN is compared to a feed-forward sequential model developed in Keras back end, which utilizes the chosen features as the input layer, followed by two hidden layers involving the ReLU activation functions and an output layer that had sigmoid activation, suited to characterizing binary classifications. All the models are trained with 80 percent of the data and tested with 20 percent of the data to determine their capability in with regards to classifying network traffic into benign and DDoS.

3.5. Evaluation Metrics

For assessing the performance of the proposed classification models, some standard measures are used. Accuracy is the percentage of the total correctly classified instances. Precision quantifies the model capacity to deal with the actual DDoS attacks in cases compared to total predictions by the model to be an attack, whereas Recall is used to measure the effectiveness of the model in pinpointing the recorded DDoS incidences. F1-Score is a balanced metric that calculates harmonic mean of Precision and Recall, which is very advantageous whenever trade-off is present between them. Finally, the ROC-AUC Score estimates the general accuracy of the model in differentiating between the benign and DDoS classes by determining the area under the Receiver Operating Characteristic (ROC) diagram. All these metrics will provide a complete picture of the performance of the detection of every model.

4. Experimental Results

This section includes the experimental study of the suggested model of detecting DDoS attacks using the CIC-IDS-2017 dataset based on ML. Three models of classification LR, RF, and DNN were used

and tested. To compare the models fairly and thoroughly, each model was evaluated on several standard measures of performance, such as Accuracy, Precision, Recall, F1-Score and ROC-AUC. The findings indicate the efficacy of each model in correctly detecting DDoS traffic with the emphasis being put both on the detection accuracy and robustness.

4.1. Experimental Setup

The proposed models were trained and tested on the CIC-IDS-2017 dataset. Preprocessing was then done to deal with the missing and infinite values using the given dataset and further there was binary label encoding i.e. 0 was interpreted as benign traffic and 1 represented DDoS traffic. All the feature values were put on standard scales by feature scaling and applying Standard-Scaler. The Select KBest algorithm with ANOVA F-statistics was used to carry out dimensionality reduction to determine the most related features. The most important 10 features which are statistically significant consist of Bwd Packet Length Mean, Bwd Pkts/s, PSH Flag Count, Average Forward Segment Size, and Minimum Packet Length, among others. The data was further divided into the training and testing sets of 80 and 20 percent respectively to make sure that the model is evaluated well. The same input feature space was shared across all models to enable them to be fairly compared based on their performances.

4.2. Classifier Description

This research applies to three classifiers to test the performance of DDoS detection. LR is a linear L2-regularized, classifier that gives interpretable coefficients and trains fast; using the default settings of scikit-learn, it becomes an acceptable baseline model. RF is another algorithm of the ensemble consisting of 100 trees conditionally (based on training the trees by entropy criterion). It takes advantage of both bootstrapped sampling and random feature selection to make it robust and not over-fitted. DNN is a fully connected feed forward neural model which has been created on TensorFlow and Keras. The structure of the network is an input layer of 10 (corresponding to the chosen features), the two hidden layers of 64 and 32 neurons (activation functions with ReLU) and an output layer with 10 activation functions (ReLU). The output layer has one neuron whose activation is a sigmoid activation in binary classification. Its training is performed based on the Binary Cross-Entropy loss function with the Adam optimizer.

4.3. Qualitative Results

Table 1 shows a comparative study of the three classifiers namely LR, RF and DNN and tested in the test section of the CIC-IDS-2017 DDoS subset with the help of various performance measures. RF model performed better than the others in all the evaluation metrics with the highest percentile of accuracy 99.13%, F1-score 99.13%, and ROC AUC 0.991. The combination of both bagging and feature randomness allowed it to have good generalization qualities and be resistant to over-fitting nature. DNN also stood up to the sequential performance with 98.65 accuracy and 98.62 F1-score, just after RF. Such an outcome reflects the capability of the DNN to learn nonlinear and complicated patterns but consumed more computational resources and needed more training time. LR, as a simple linear model, showed rather decent results serving as a baseline, showing the accuracy of 97.61% and F1-score of 97.40. However, what points to its less successful performance in finding minute differences in the data is its relatively lower recall when differentiating more subtle patterns of DDoS.

Table 1. Performance of Models on the CIC-IDS-2017 DDoS Dataset

AUC - ROC	F1-Score (%)	Recall (%)	Precision (%)	Accuracy (%)	Classifier
0.976	97.40	96.93	97.89	97.61	LR
0.991	99.13	99.00	99.27	99.13	RF
0.986	98.62	98.51	98.74	98.65	DNN

4.4. Confusion Matrix Analysis

To give even more insight into the classification performance of all three classifiers, Figure 2, 3, 4 shows the confusion matrices of each of them, i.e., RF, DNN, and LR. According to the RF confusion matrix, a close to perfect classification is observed, where most of the considered predictions occur along the diagonal with only a very limited number that are miss-classifications which makes the RF strong in

its capacity to classify the benign and DDoS traffic correctly. DNN confusion matrix shows an outstanding performance as well with a very low false positive, false negative demonstrating the balanced nature of the model and high sensitivity and precision. Conversely, the LR confusion matrix has more false negative compared to RF and DNN thereby having the slightest sensitivity and recall. This indicates that although LR works well as a baseline it can present more hidden patterns of attack. In general, the confusion matrix analysis proves the idea that ensemble-based and DL models, in particular RF and DNN, are more resourceful and reliable in detecting DDoS attacks, especially after training on selected features of the CIC-IDS-2017 data.

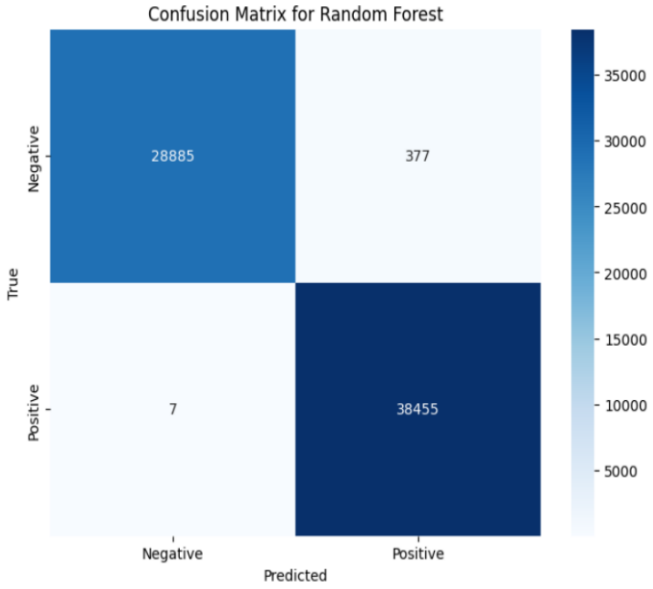

Figure 2. Confusion matrix of RF model for DDoS detection.

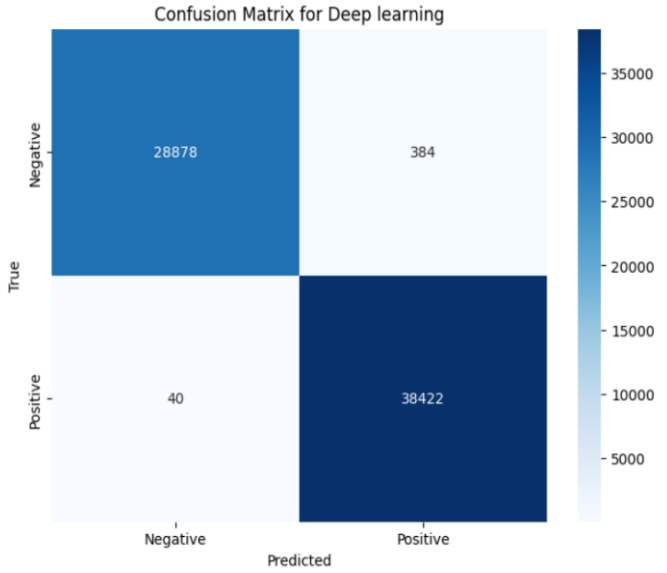

Figure 3. Confusion matrix of DNN model for DDoS detection.

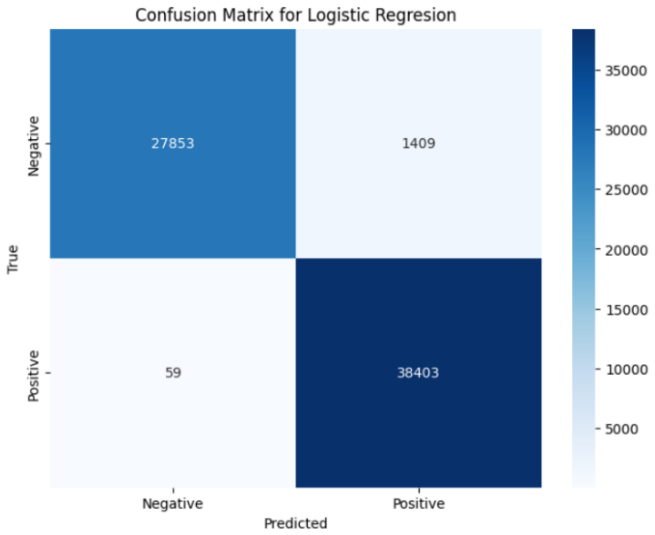

Figure 4. Confusion matrix of LR model for DDoS detection.

4.5. ROC Curve Visualization

Figure 5 plots the ROC curves of the LR and RF classifiers, which discerns the benign, as well as DDoS traffic. Using RF model, the model performed close to perfect classification with an AUC score of 1.00, and such a model is actually very good with lowest false positive rate at all levels of threshold. The LR model is also robust with an AUC of 0.99, but it is lower in increase in comparison with the RF since its curve is flatter and, therefore, is an indicator of a slightly lower though still high sensitivity and specificity. The sharp increase of both the curves to the top-left position in the chart proves the robustness of detection by the models, and RF performs better as a whole.

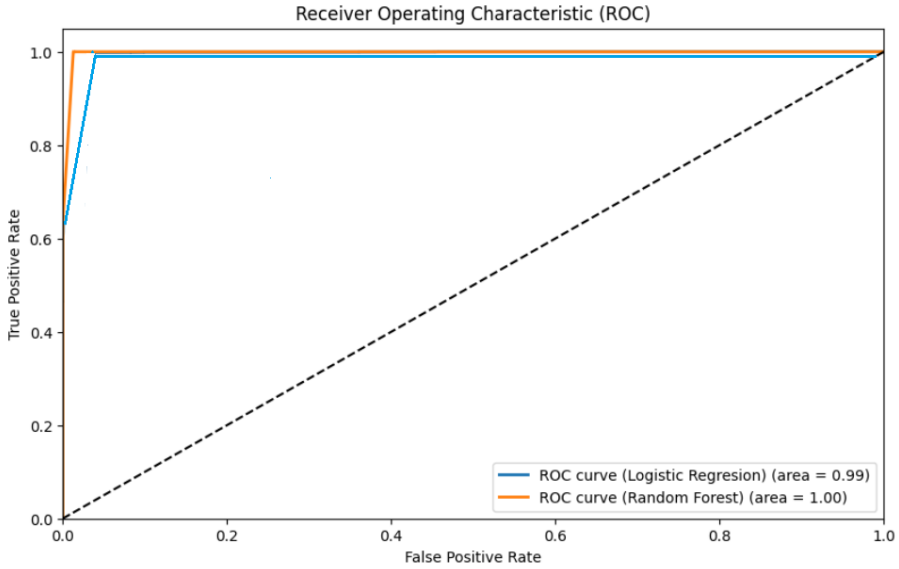

Figure 5. ROC curves of LR and RF classifiers.

4.6. Comparison of Results

To evaluate the performance of the proposed models adequately, a comparative was carried out using major evaluation metrics, related to accuracy, precision, recall, and F1-score. Figure 6 shows a bar chart of the comparison of the performance of the three classifiers: LR, RF, DNN, on the CIC-IDS-2017 DDoS subset. RF classifier clearly performed best with respect to the metrics, because on all of them, it yielded higher scores than most of the other models, including the highest accuracy (99.13%), precision (99.27%), recall (99.00%), and F1-score (99.13%), as illustrated in the figure. It implies that RF has a high performance in identifying the DDoS attack with fewer false positives and false negatives.

DNN also produced impressive results with an accuracy of 98.65 with 98.62 F1-score, slightly behind RF but far ahead of LR. In the meantime, the LR, which has already demonstrated its current good

performance with the accuracy of 97.61%, demonstrated receiving comparatively low values of recall (96.93%). This fact may imply the presence of a slightly increased percentage of the missed DDoS cases. Such comparative study points out to the dominance between ensembles and deep based learning techniques on the traditional linear models when applied on complex, high dimensional intrusion detection datasets.

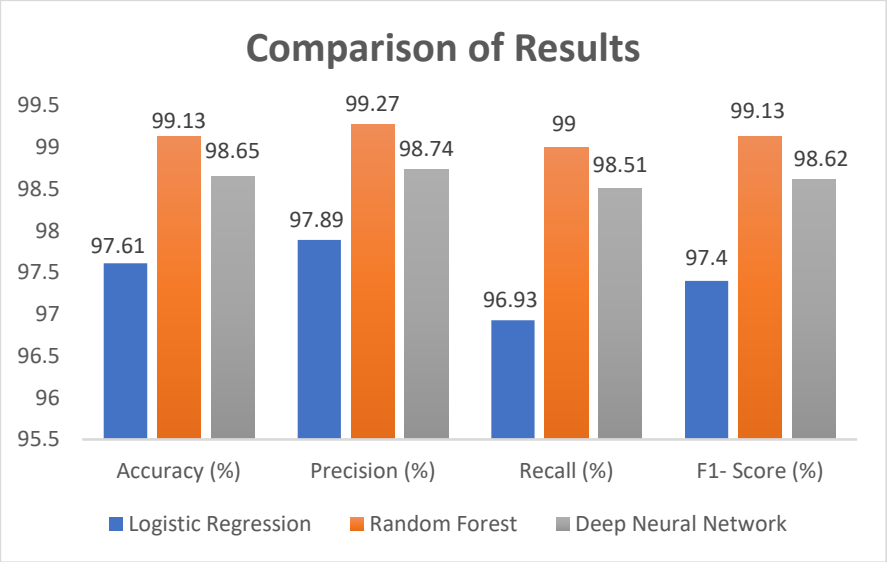

Figure 6. Performance comparison of classifiers.

5. Discussion

The experiment findings provided in the above section illustrate that the three classifiers, namely LR, RF, and DNN, perform at high levels in the prepared data set related to detecting DDoS attacks based on CIC-IDS-2017 collection. Nonetheless, the range with which they perform, generalize and have a place in the real world depends on several factors as we shall see below. In all the assessment metrics, the RF classifier was better than the LR and DNN was, with the former having an accuracy of 99.13 percent and ROC-AUC of 0.991. This can be assisted with the current research confirming the stability of the ensemble-based classifications in detecting intrusions. It is so successful because: Employment of numerous decision trees, which minimize the variance and avoid over-training. The possibility to work with nonlinear interactions with features typical of network traffic data. An inherent feature selection, which is going to be another addition to our preprocessing pipeline with SelectKBest. The false positive and false negative rates of the model in confusion matrix confirm its applicability in production facilities where missing attacks (false negatives) of attacks or generation of too many false alerts (false positives) may result in operational inefficiencies.

DNN also gave good results with an accuracy of 98.65 percent and 0.986 ROC-AUC. It showed: Great learning flexibility presented by complicated data patterns. A well-balanced precision and recall, the strength of which on imbalanced binary classification. Nevertheless, the DNN was more demanding, it needed a more thoughtful adjustment of the parameters, and it took longer to prepare. It can, in the absence of architectural improvements (i.e., dropout, batch normalization), even run the risk of over-fitting to the small/homogeneous subsets. Therefore, though the DNN is promising, real-time or resource-constrained applications would need further engineering before applying DNN. Overall, the performance of simple LR model was rather high (97.61% of accuracy). Its F1-score (97.40 %) and ROC-AUC (0.976) confirm that it is an efficient lightweight baseline classifier. It has: Rapid training and small computation complexity. Incremental interpretable of the coefficients of feature, which helps in explainable threat detection. Nonetheless, the linear decision boundary of this machine reduces its chances of detecting complex or nonlinear relations that are not uncommon in the case of attack patterns. This can be detected in the slightly falser negatives in its confusion matrix.

The findings tend to imply an economy of this type; performance, model complexity, and deployment restriction: RF is suitable where high accuracy is required in the deployment and there is not

much fiddling that is required. DNN would fit into future pipeline of deep leaning with streaming real-time data and adaptive learning but with necessary computing resources. LR is appropriate in edge or IoT-based settings where it is desirable to have a simple and fast interpretable model with only marginal improvements over accuracy. The excellence of all models after data quality and preprocessing also proves the significance of high quality of data. The use of missing value imputation, feature normalization and selection techniques played a key role in the low error rates irrespective of the type of model used.

6. Conclusions

This study proposed a ML–based framework for cyber threat detection, specifically targeting DDoS attacks using the CIC-IDS-2017 dataset. We applied a reproducible pipeline consisting of data cleaning, feature selection, normalization and classification. The accuracy, precision, recall, F1-score, and ROC-AUC were considered to compare three models of supervised learning LR, RF, and DNN. RF has recorded higher accuracy (99.13%) and AUC (0.991) among them indicating its strengths in detecting both threats in a binary way. As much as the models proposed performed well, there is much room to beat them later. Applying the same idea to multi-class classification to deal with multiple types of attacks would result in a wider IDS. Also, generalization can be confirmed by incorporating real-time detection improving model interpretability, as well as an analysis of performance on various benchmark datasets. These would aid in bringing the viable implementation of intelligent, scalable and adaptive types of threat detection systems in dynamic and high-risk network scenarios.

References

1. Almalki, Faris A., Saeed H. Alsamhi, and Marios C. Angelides. "Internet of X-enabled intelligent unmanned aerial vehicles security for hyper-connected societies." Security and Privacy in Cyberspace. Singapore: Springer Nature Singapore, 2022. 75-100.
2. Singh, Pushpendra Pal, and Rakesh Kumar Dixit. "Smart Cities with 5G and Edge Computing in 2030." The Role of Network Security and 5G Communication in Smart Cities and Industrial Transformation. Bentham Science Publishers, 2025. 41-79.
3. Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer networks 2004. 44.5 643-666.
4. PM, Vishnu Priya, and S. Soumya. "Advancements in anomaly detection techniques in network traffic: The role of artificial intelligence and machine learning." Journal of Scientific Research and Technology 2024. 38-48.
5. Cantone, Marco, Claudio Marrocco, and Alessandro Bria. "Machine learning in network intrusion detection: A cross-dataset generalization study." IEEE Access 2024.
6. Niboucha, Redouane, et al. "Zero-touch security management for mMTC network slices: DDoS attack detection and mitigation." IEEE Internet of Things Journal 10.9 2022. 7800-7812.
7. Mahdi, Suadad S., and Alharith A. Abdullah. "Statistical slice-level analysis for online detection of distributed denial-of-service (DDoS) attacks in network slicing environments." Journal of High-Speed Networks 2025. 31.2 145-158.
8. Thwaini, Mohammed Hussein. "Anomaly detection in network traffic using machine learning for early threat detection." Data and Metadata 1 2022. 34-34.
9. Ofoegbu, Kingsley David Onyewuchi, et al. "Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach." Computer Science & IT Research Journal 2024. 4.3.
10. Rahman, Faiaz, et al. "Cyber Threat Detection Using Machine Learning Algorithms on Heterogeneous MiniVHS-22 Dataset." 2022 25th International Conference on Computer and Information Technology (ICCIT). IEEE, 2022.
11. Gaddah, Firas Wajdi, and Suad F. El-Geder. "Cyber Threat Detection Using Machine Learning." 2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA). IEEE, 2024.
12. Ch, Ravikumar, et al. "Exploring machine learning algorithms for robust cyber threat detection and classification: A comprehensive evaluation." 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS). IEEE, 2024.
13. Ferrag, Mohamed Amine, et al. "Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices." IEEe Access 2024. 12 23733-23750.
14. Shelke, Palvi, and Timo Hämäläinen. "Analysing multidimensional strategies for cyber threat detection in security monitoring." Proceedings of the European Conference on Cyber Warfare and Security. No. 1. Academic Conferences International Ltd, 2024.
15. Sharma, Sumit KR. "AI-Enhanced Cyber Threat Detection and Response Systems." Shodh Sagar Journal of Artificial Intelligence and Machine Learning 2024 1.2 43-48.
16. Hassanin, Mohammed, et al. "PLLM-CS: Pre-trained Large Language Model (LLM) for cyber threat detection in satellite networks." Ad Hoc Networks 2025. 166 103645.
17. Kumar, Prabhat, et al. "Blockchain and explainable AI for enhanced decision making in cyber threat detection." Software: Practice and Experience 2024. 54.8 1337-1360.
18. Kavitha, D., and S. Thejas. "Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation." IEEE Access 2024.
19. Sharafaldin, I., A. H. Lashkari, and A. A. Ghorbani. "Toward generating a new intrusion detection dataset and intrusion traffic characterization." Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, Jan. 2018.
20. Chethan H N. Network Intrusion Dataset (CICIDS 2018). Kaggle, 2023. https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset (accessed Aug. 15, 2025).
21. Kausar, Samina, et al. "Secure and efficient data transfer using spreading and assimilation in MANET." Software: Practice and Experience 50.11 (2020): 2095-2109.
22. Kausar, Samina, et al. "Fog-assisted secure data exchange for examination and testing in E-learning system." Mobile Networks and Applications 28.2 (2023): 673-689.