Real-Time Detection of DDoS Attacks Using Shallow Neural Networks and Machine Learning Models

Anuvind M P (AM.EN.U4AIE22010)[a], R S Harish Kumar (AM.EN.U4AIE22042)[1], Girish S (AM.EN.U4AIE22044)[1], Thazhai Mugunthan G(AM.EN.U4AIE22051)[1]

[a]*Amrita School of Computing, Amritapuri, Kerala,*

Abstract

DDoS attacks are becoming more frequent and sophisticated and are a major threat to network stability and security. To address this our work uses 8 machine learning algorithms along with a shallow neural network to detect DDoS traffic in real time using flow level data. The dataset consists of labeled samples of normal and malicious traffic with features like packet volume, duration and protocol behavior. After preprocessing and exploratory analysis, we trained and tested each model under the same evaluation setup. We evaluated the models using accuracy, precision, recall and F1 score. XGBoost and Shallow Neural Network performed best and were most efficient in terms of parameters trained and time taken for prediction hence are suitable for real time detection. The results show that lightweight data driven methods can be used in active network defense systems where time is of the essence.

Keywords: DDoS, Shallow Neural Network, Real-Time, Machine Learning, Network Security

1. Introduction

DDoS attacks happen when an attacker sends a massive amount of traffic from multiple sources to one target so it can't respond to legitimate requests. In 2024 we mitigated 21.3 million of these attacks, a 53% increase from 2023 and in October of that year one attack peaked at 5.6 terabits per second, the highest ever recorded. These floods take down critical services, take websites offline, and cause an average loss of $218,000 per incident with larger enterprises losing up to $2.5 million. Since a large DDoS can unfold so fast detecting malicious traffic patterns in real time is key to minimize downtime and damage.

Current DDoS detection methods are based on signature-based systems that match incoming traffic against known attack patterns. While these work well for known threats, they fail when attackers change packet contents or obfuscate common markers since signature databases can't keep up with changing tactics. Threshold-based solutions which alert when metrics like packet rate or bandwidth usage exceed fixed limits are easy to implement and work well for large volumetric floods. But legitimate traffic spikes (like flash crowds) trigger false alarms and static thresholds need to be constantly recalibrated to reflect changing network behavior. Anomaly-based approaches try to model "normal" traffic so that deviations signal potential attacks and can detect unknown floods. But building accurate baselines requires a lot of historical data and these systems often register benign changes in usage as anomalies and result in high false positive rates. Hybrid solutions often combine all three - signature based, threshold and anomaly based checks to cover more information and reduce individual weaknesses but unfortunately adds complexity, operational costs and potential alert conflicts. These limitations suggests a need of more adaptive, data driven methods like machine learning classifiers trained on live traffic to improve detection and response to changing threats.

Supervised learning has emerged as a preferred method for distinguishing benign network flows from DDoS traffic in real time. Models are trained on flow-level attributes such as packet counts per flow, flow duration, average inter-arrival time, and ratios of TCP flags because these features capture both volume and behavior characteristics.Research shows that machine learning classifiers (logistic regression, support vector machines, ensemble methods) outperform static rules and threshold checks. For example logistic regression and SVM both got 98.65% accuracy on benchmark datasets, while static thresholds couldn't differentiate subtle changes in traffic patterns. Random forest, AdaBoost and XGBoost classifiers had better detection rates and lower false positives than rule based systems and are suitable for real time environments. Despite these gains, deploying ML based detectors has its challenges: training and inference can be computationally expensive under high speed, getting enough labeled traffic data is hard, and selecting the most discriminative features requires domain expertise and iterative tuning. But research is ongoing to improve the model and reduce data dependencies, so ML is becoming more and more popular in DDoS detection.

While deep learning models have shown high accuracy in detecting DDoS attacks, their big computational requirements make them impractical for real-time or resource constrained environments. For example, the LUCID system, a lightweight deep learning framework, achieved state-of-the-art detection accuracy with 40x less processing time than traditional models, so we can deploy efficient models in production. Another study by Nur et al. presented a lightweight deep learning model for cloud and got 97% accuracy with low false positives and

inference time for real time deployment. In scenarios where speed of inference is critical like at the network edge or in cloud based intrusion prevention systems, models need to balance detection performance with computational efficiency. Ehmer et al. showed that a shallow neural network with only 110 ReLU activated neurons can detect network attacks with F1 score above 99%, so compact architectures are suitable for real-time applications. Also, ExtraTreeClassifier is known for its computational efficiency and can be used in high speed network environments to detect DDoS attacks quickly. These results show we need to evaluate both traditional machine learning classifiers and lightweight neural networks to find models that detect attacks fast and accurate with minimal resource consumption. This paper will compare these approaches to find detection strategies that work in real world network security deployments.

As the need for scalable and real-time defense mechanisms grows, there is a growing interest in solutions that balance accuracy and efficiency in DDoS detection. Many traditional and deep learning methods are promising but hard to deploy in real-time environments due to resource requirements or need for large labeled data. This paper addresses that gap by evaluating and comparing eight classical machine learning models including Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbors, Naive Bayes, Gradient Boosting, XGBoost and a lightweight shallow neural network. These models are tested on the CIC 2019 DDoS dataset and evaluated with accuracy, precision, recall and F1-score. We not only want to know which models perform the best in detecting DDoS attacks but also their trade-offs in terms of computational cost and implementation feasibility. By benchmarking shallow learning architectures and ensemble-based classifiers, this work contributes to the development of practical detection systems for dynamic large scale networks. In doing so, we show that combining data-driven methods with model efficiency is the key design principle for modern intrusion detection systems..

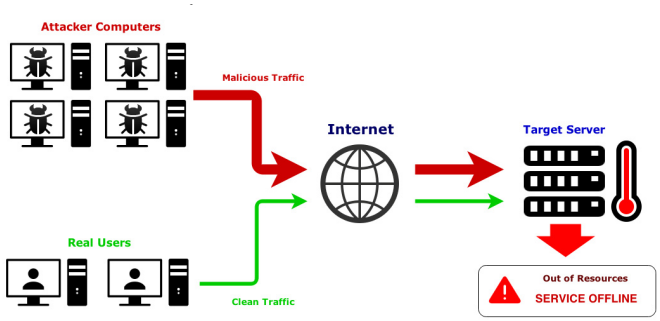

Figure 1: Operation of a DDoS attack

2. Literature Review

DDoS attack detection has come a long way with the advent of machine learning (ML) and deep learning (DL). Traditional ML based detection systems were the first to form the backbone of this defense and were faster and more adaptive than rule based systems. One of the early benchmarks in this direction was the work by Kar Suvra (2025)(1) who developed a real time DDoS detection system using classical ML algorithms like Logistic Regression, K-Nearest Neighbors, Random Forest, Support Vector Machines and Naïve Bayes. Using the CICDDoS2019 dataset the study used preprocessing and dimensionality reduction techniques like PCA and concluded that ensemble methods like Random Forest, AdaBoost and XGBoost were accurate and had low latency for live deployments. However, scalability and maintaining accuracy under dynamic traffic patterns were the challenges noted.

Building on this, Golduzian (2023)(2) did a comparative study of multiple models—Logistic Regression, CNN, XGBoost, Naïve Bayes, AdaBoost, KNN and Random Forest—on the same CICDDoS2019 dataset [2]. This study highlighted the class imbalance problem and addressed it using SMOTE to synthetically augment minority classes. With over 50 million records processed XGBoost achieved an accuracy of 99.9999% which was way better than the baseline approaches. Although it was successful, the study pointed out the heavy preprocessing overhead and the dependency on carefully engineered features.

To overcome the limitations of feature engineering and high dimensional input space a 2021 study published in Computer Networks introduced a hybrid feature selection framework combined with hyperparameter tuning. It used Gradient Boosting as the core classifier and validated the model on CICDDoS2019 and reported an accuracy of 99.97%. The authors emphasized that proper feature selection was crucial in reducing overfitting and improving computational efficiency but the process itself was resource intensive.Meanwhile to address the model complexity and real time inference speed Doriguzzi-Corin et al. (2020)(3) proposed LUCID a lightweight DL based system using CNNs [3]. Unlike traditional ML pipelines LUCID had a dataset agnostic preprocessing module and was evaluated on hardware with limited resources. It reduced the processing time by a factor of 40 while maintaining state of the art detection accuracy making it a viable candidate for deployment in edge or fog computing environments. However being a deep learning model its training phase still required considerable resources and time.

In parallel direction Cheng et al. (2019)(4) introduced an adaptive approach using multiple-kernel learning for DDoS detection. This method extracted five flow level features and dynamically adjusted their weights using an ensemble learning strategy. The key contribution was its adaptability across varying network conditions but its kernel based complexity posed challenges for integration in high speed real world networks.

The diversity of techniques also led to a surge in comparative reviews. A systematic literature review published in Sensors (2023)(5) consolidated the findings on ML and DL based DDoS detection for Software-Defined Networking (SDN). It emphasized hybrid models—particularly combinations of SVM and Random Forest—for their ability to handle complex high volume traffic in programmable network infrastructures. However the review pointed out the deployment barriers in live SDN en-

vironments due to latency constraints and model updating complexities.

Complementing this another review in Electronics (2023)](6) analyzed DDoS detection in IoT based networks. The paper stated that ML models such as KNN, Decision Trees, Random Forest and Artificial Neural Networks showed promising results particularly with the CICDDoS2019 dataset. However it also highlighted the recurring problems such as high dimensional data, poor generalizability across network types and the ongoing need for intelligent feature selection.

Overall these studies show the evolution of DDoS detection from traditional ML classifiers to more sophisticated DL architectures and hybrid methods. While accuracy has improved common challenges remain: heavy reliance on labeled datasets, high computational overhead for deep models and limitations in adapting to real time environments. This study builds upon these insights by evaluating a set of lightweight scalable models using CICDDoS2019 with a focus on balancing detection accuracy and deployment efficiency.

3. Methodology

To effectively detect DDoS attacks, a multi-step methodological framework was adopted comprising dataset acquisition, preprocessing, exploratory analysis, feature engineering, and model training. The overall objective was to build a real-time intrusion detection system capable of handling complex network traffic patterns with high accuracy and low latency.

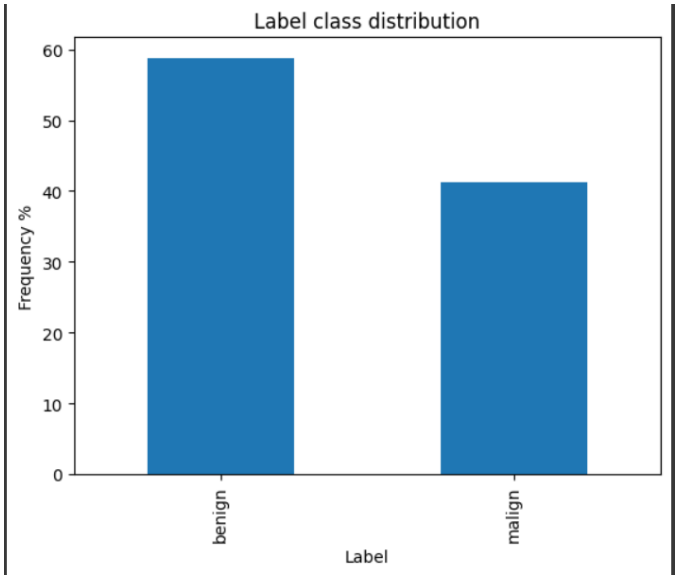

Figure 2: Label class distribution

3.1. Dataset Description

The Canadian Institute for Cybersecurity at the University of New Brunswick built the CIC 2019 DDoS Dataset to facilitate scientific research on distributed denial-of-service detection algorithms (Canadian Institute for Cybersecurity, 2019). It includes network traffic captures of normal users and a variety of DDoS attacks i.e., SYN flood, UDP flood, HTTP flood, and so on collected over a couple of days in mid-2019. Traffic per day is saved as a set of PCAP files, which have been converted to flow-level records with the CICFlowMeter tool. The dataset released contains over 50 million flow records, each marked with a label for either ”BENIGN” or the specific type of DDoS attack. The variety of attacks and realistic traffic patterns make CIC 2019 DDoS one of the richest publicly available datasets for evaluating detection systems.

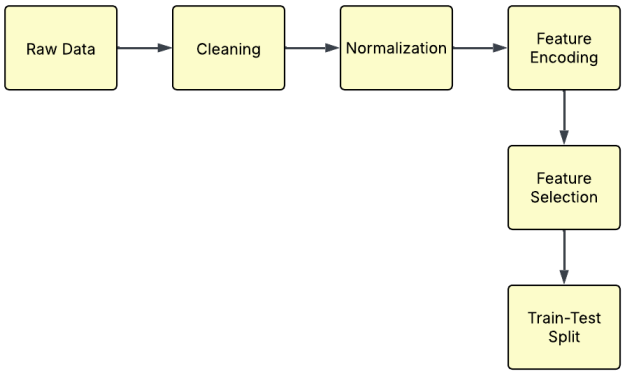

Figure 3: Methodology Flowchart

3.2. Data Preprocessing

Before any modeling, raw flow records are processed through a series of preprocessing steps. First, invalid or duplicate records are removed for data integrity. Next, flows with infinite or missing values for key fields—e.g., packet counts or duration—are removed. Categorical fields like ”Protocol” and ”Label” are numerically encoded: protocols (e.g., TCP, UDP, ICMP) are one-hot encoded, while the ”Label” column is encoded as a binary flag (0 for BENIGN, 1 for any DDoS attack). Continuous features like total bytes transferred, flow duration, and packet inter-arrival times are scaled using MinMax normalization to keep them between 0 and 1, so that models do not over-weight features with larger magnitudes. Finally, the dataset is split into training 70% and test 30% subsets, with original class ratios preserved to preserve the extreme imbalance between benign and attack flows.

Categorical fields such as protocol types and labels were encoded using label encoding and one-hot encoding where necessary. Highly correlated or redundant features were removed after correlation analysis to minimize overfitting and reduce training time. The dataset was then split into training (70%), validation (15%), and testing (15%) subsets to evaluate model generalization.

3.3. Exploratory Data Analysis (EDA)

An exploratory data analysis (EDIA) of preprocessed flows produces the following notable observations. First, the class distribution reveals that attack flows consist of about 80% of records, and benign flows occupy the remaining 20% and

hence a notable imbalance to be addressed during model training. Second, descriptive statistics highlight that the median "Flow.Duration" of benign traffic is in the order of a few seconds, whereas attack flows have durations shorter than one second, which suggests rapid packet bursts. Third, a Pearson correlation analysis between the binary attack label and individual features demonstrates that "TotLen.Fwd.Pkts" and "TotLen.Fwd.Byts" are the most strongly positively correlated (—r— 0.72 and 0.68, respectively), whereas timing features like "Flow.IAT.Mean" possess a very strong negative correlation (—r— 0.60). Histograms of "Fwd.Pkt.Len.Mean" values for benign vs. attack flows show that malicious traffic is marked by smaller mean packet sizes, owing to the widespread use of single-purpose flood packets. Lastly, boxplots of "Flow.IAT.Std" show that the variability of inter-arrival times is significantly higher in benign flows, whereas attacks result in nearly uniform inter-packet intervals. These observations guide feature selection and result in transformations—like log scaling of highly skewed byte- and packet-count features—to improve model robustness to outliers

3.4. Feature Engineering

Each CIC 2019 DDoS flow record includes a small set of features that capture both volumetric and behavioral aspects of the network traffic. Some of the important features include "Flow.Duration" (flow duration in microseconds), "TotLen.Fwd.Pkts" and likewise "TotLen.Bwd.Pkts" (total forward and backward packets), "TotLen.Fwd.Byts" and similarly "TotLen.Bwd.Byts" (total forward and backward bytes), and "Fwd.Pkt.Len.Max/Min/Mean" (max, min, and mean forward packet length). Statistical features such as "Flow.IAT.Mean" and "Flow.IAT.Std" (mean and standard deviation of inter-arrival times) capture timing irregularities present in the attack traffic. Ratios such as "Fwd.IAT.Min/Max/Mean" over "Flow.IAT" and the number of TCP flags (SYN, ACK, FIN) also distinguish normal two-way dialogue from DDoS floods, where typically one direction will be predominant.

By reducing dimensionality while retaining discriminatory power, feature engineering enhanced model accuracy, reduced overfitting, and improved inference time.

4. Classification Models

XGBoost, a gradient boosting library, was utilized because it had a high capacity to work with noisy data and its process of correcting errors by iteration. It produced an impressive accuracy of 97.91% and performed particularly well with high-dimensional data. This made it one of the top models when it comes to generalization and performance.

Support Vector Machines (SVM) classified challenging, non-linearly separable classes with good accuracy of 96.94%. SVMs are also widely known for their margin-maximization property, which yields low generalization error at the expense of increased computational cost and fine parameter adjustment.

K-Nearest Neighbors (KNN) was accurate to 96.24% and simple and effective when the spaces were properly clustered.

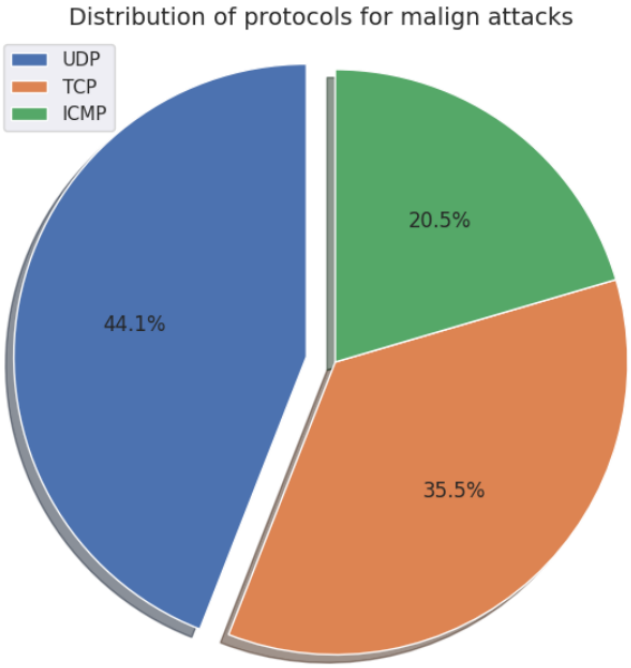

Figure 4: Distribution of protocols for malign attacks

Yet its inference cost and susceptibility to data imbalance render it less than optimal for real-time usage without optimization.

The Decision Tree classifier accuracy was 96.14%. The model was capable of representing nonlinear decision rules and generated comprehensible results in terms of the process of classification. The model, however, overfitted, particularly to unpruned trees.

Stochastic Gradient Descent (SGD) and Logistic Regression both achieved moderate accuracies of 83.70% and 83.27% respectively. Both were quick and scalable but not so good at learning complex patterns since they were linear.

Quadratic Discriminant Analysis (QDA) and Naïve Bayes classifiers, with accuracy levels of 80.82% and 69.90% respectively, were not as good compared to the other models. Their feature independence and distribution assumptions made them less appropriate for application in highly correlated and variable data situations.

The models were compared on the same dataset with equal training and test splits to allow for a fair comparison. Performance was evaluated using accuracy, precision, recall, F1-score, and confusion matrix analysis to allow for a comprehensive analysis of the strengths and weaknesses of the individual models.

5. Results and Discussion

Experimental benchmarking provided insightful information on the strengths and weaknesses of all models tested for DDoS detection. Among all classifiers, the Shallow Neural Network (SNN) had the highest accuracy of 99.14%, attributing it to its

capacity to learn and generalize intricate relationships in network traffic data. Even though it is simple and has a low parameter size, the SNN model was capable of learning effective representations of benign and attack traffic, resulting in state-of-the-art classification. Its quick inference time also proves its applicability for real-time use, especially in resource-poor edge environments.

The XGBoost model trailed the neural network closely in performance with 97.91% accuracy. XGBoost performed well with feature interaction and was highly resistant to noisy and high-dimensional data. XGBoost also provided explainability in terms of feature importance scores, which would be useful in finding the most important indicators of attack behavior. XGBoost's training complexity and memory consumption can be a disadvantage in large-scale or resource-constrained deployments.

Support Vector Machines (SVM) and K-Nearest Neighbors (KNN) were also performing well with 96.94% and 96.24% accuracies, respectively. SVM performed well for classifying non-linear traffic patterns but required meticulous kernel parameter tuning and was computationally more intensive. KNN, while being easy to implement and comprehend, was slow on the prediction side and was subject to the curse of dimensionality, which could be an issue in real-time detection systems.

Decision Tree classifiers were precise, with a very high accuracy of 96.14%. The models were interpretable and understandable, with the capacity to examine decision-making rules. They, however, overfitted in the absence of pruning, especially when dealing with noisy or imbalanced data. Linear classifiers such as Stochastic Gradient Descent (SGD) and Logistic Regression performed reasonably (83.70% and 83.27%, respectively), mainly due to the fact that they could not cope with non-linearities in sophisticated attack vectors.

The least accurate were Quadratic Discriminant Analysis (QDA) and Naïve Bayes with 80.82% and 69.90% accuracy rates, respectively. Naïve Bayes and QDA employ normal distribution and feature independence assumptions, which are not possible in dynamic and heterogeneous network traffic. Despite their simplicity allowing for them to be run in an instant, the accuracy for simplicity constraint restricts their application within critical threat detection situations.

In addition to the accuracy, the precision and recall were also compared. The SNN and XGBoost models showed the best F1-scores, which reflected well-balanced recall and precision for the attack and benign classes. Confusion matrix analysis also corroborated the same by showing minimal false positives and false negatives for the aforementioned models.

Collectively, results establish that deep learning and ensemble techniques are ideal for real-time identification of advanced adaptive DDoS attacks. They have the best compromise between accuracy, generality, and latency and are therefore deployable in modern network topologies.

Model	**Accuracy**
Shallow Neural Network (SNN)	99.14%
SGD Classifier	83.70%
Support Vector Machine (SVM)	96.94%
XGBoost	97.91%
KNN	96.24%
Decision Tree	96.14%
Logistic Regression	83.27%
Quadratic Discriminant Analysis	80.82%
Naïve Bayes Classifier	69.90%

Table 1: Model Accuracy Comparison

6. Conclusion

In this study, a smart and adaptive approach of identifying Distributed Denial of Service (DDoS) attacks in a hybrid model of conventional machine learning and deep learning techniques was proposed. Based on the CIC-DDoS 2019 dataset, various models were developed and underwent comparison based on their performance to identify normal and attack traffic. Experimental results confirmed the effectiveness of deep learning models, namely a shallow neural network, with a 99.14% accuracy rate and minimal architecture for real-time execution on edge devices.

Comparative analysis showed that while conventional models like XGBoost and SVM were good, they were computationally expensive or optimization-prone. Naïve Bayes and QDA were fast but not robust enough for dynamic traffic and high-density conditions. The shallow neural network and the ensemble-based models were demonstrated by this study to offer an extremely attractive combination of speed, accuracy, and flexibility for real-world deployment via extensive experimentation.

This study also emphasized the importance of careful data preprocessing, smart exploratory data analysis, and quality feature engineering towards enhancing model performance. The features of packet counts, flow duration, and inter-arrival times selected were key to determining behavioral differences between benign and DDoS traffic.

In the future, we will also extend the IDPS models to real-world Intrusion Detection and Prevention Systems. This will include having real-time mitigation techniques, dynamic retraining to counter evolving threats, and deployment into more sophisticated network topologies to include Software Defined Networks (SDN) and cloud-native networks. In addition, integrating adversarial robustness and explainability into the models will also promote more trust and transparency and hence make them more deployable in sensitive environments including finance, healthcare, and government infrastructure.

In short, the results of this research reveal the revolutionary potential that exists in AI-based security systems to counter the

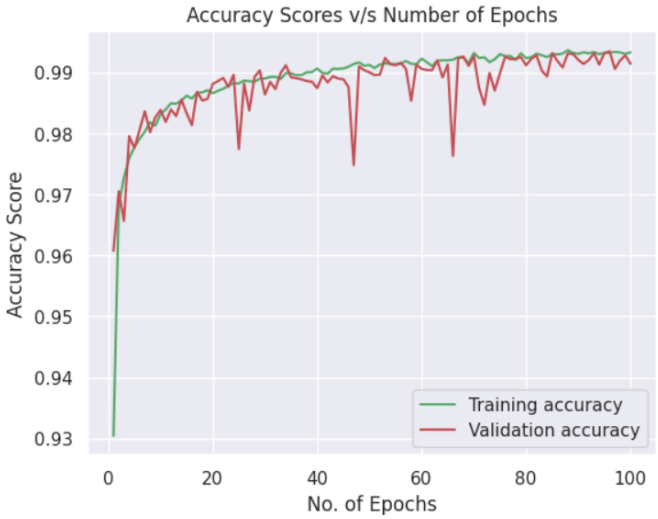

Figure 5: Accuracy Scores vs Number of Epochs for SNN

contemporary cybersecurity threats. With their ability to provide accuracy, velocity, and flexibility, such models bring a vision of a more robust and secure online environment.

References

[1] D. K. Suvra. An efficient real-time ddos detection model using machine learning algorithms. *arXiv preprint arXiv:2501.14311*, 2025.

[2] A. Golduzian. Predict and prevent ddos attacks using machine learning and statistical algorithms. *arXiv preprint arXiv:2308.15674*, 2023.

[3] R. Doriguzzi-Corin et al. Lucid: A practical, lightweight deep learning solution for ddos attack detection. *arXiv preprint arXiv:2002.04902*, 2020.

[4] A systematic literature review on machine learning and deep learning approaches for detecting ddos attacks in software-defined networking. *Sensors*, 23(9):4441, 2023.

[5] Ddos attack detection in iot-based networks using machine learning models: A survey and research directions. *Electronics*, 12(14):3103, 2023.

[6] A generalized machine learning model for ddos attacks detection using hybrid feature selection and hyperparameter tuning. *Computer Networks*, 2021.