Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

"Modelling and Optimization of FIS-Based Machine Learning Framework for Nonlinear Detection and Mitigation of Application Layer DDoS Attacks with QoS Enhancement"

[1] Prof. Kiran M. Salunke, [2] Dr. Suresh Kurumbanshi**
[1,2]Department of Computer Engineering, MPSTME, Shirpur Campus, India
[1]Email address: kiran.salunke@nmims.edu
[2]Email address: suresh.kurumbanshi@nmims.edu

Article History:
Received: 12-01-2025
Revised: 15-02-2025
Accepted: 01-03-2025

Abstract:
Network availability is essential for online service providers, especially against application-layer DDoS attacks that target service uptime. This paper presents an intelligent approach to detect these attacks without degrading service quality. Using a Feature Importance Score (FIS) based method which consists of extensive pre-processing and an Extra Tree Classifier for feature selection, followed by a Random Forest model, the system effectively classifies traffic as benign or malicious. It combines adaptive traffic shaping, intelligent filtering, and load balancing to mitigate threats in real-time. The optimized model achieves 99.89% detection accuracy, improving QoS metrics such as PDR, throughput, jitter, latency, and memory usage, thereby enhancing network performance by 40%. This adaptive, unified approach balances security with QoS, providing robust protection against application-layer DDoS.

Keywords: Network Security, Machine Learning, Application layer DDoS Attack, Mitigation, Neural Network

1. Introduction

As networks face increasingly complex attacks, developing robust methods to identify and manage these threats is crucial. This study leverages machine learning to enhance network security by accurately classifying and mitigating application-layer DDoS attacks, which often bypass conventional defences by mimicking legitimate user behaviours. The rising reliance on web-based services has heightened the need for advanced detection mechanisms to protect systems from degradation or downtime. Application-layer attacks severely impact Quality of Service (QoS) metrics such as packet delivery ratio (PDR), throughput, jitter, latency, and memory usage—while meeting legitimate user demands. Traditional defences, such as intrusion detection systems (IDS) and firewalls, struggle to keep up with evolving threats and may generate high false positives, impacting central processing systems [3][4].

Machine learning (ML) models offer promising solutions by establishing baseline traffic behaviour and significantly improving the accuracy and efficiency of attack detection, supported by large, diverse datasets. This study's primary objective is to develop an efficient framework for detecting application-layer DDoS attacks while implementing QoS-based mitigation strategies. The proposed approach includes data pre-processing, feature selection, model training and evaluation, and mitigation. In data pre-processing, the code cleans the

dataset, addresses missing values, and encodes categorical data to maintain consistency [1][2]. To prevent overfitting, feature selection with an Extra Tree Classifier is applied, enhancing performance and reducing computational load. We adopt machine learning models, specifically a Random Forest Classifier, to build robust, high-performing detection systems evaluated by accuracy, precision, recall, and F1-score metrics.

Table 1 details notable instances of application-layer DDoS attacks, highlighting their impact on financial stability, service continuity, and economic damage. Examples include the Mirai Botnet Attack, which incurred millions in damages, and the NZ Stock Exchange attack, which halted trading for days. Such data emphasize the urgency of advanced defense strategies.

This study makes two key contributions: an efficient framework model for application-layer DDoS detection and optimized mitigation strategies that safeguard QoS. By employing adaptive ML-based methods, this approach strengthens network resilience against evolving cyber threats.

Table 1 Impact of Application Layer DDoS Attack

Attack	Motive	Target	Actual Loss
Mirai Botnet Attack (2020) [5]	Disorder/Blackmail	Telecoms, Financial Facilities	Hundreds of millions in compensation
GitHub DDoS Attack (2018) [6]	March of Power	GitHub	No financial damage, service disturbance for a few hours
Amazon Web Services Attack (2020) [7]	Extortion	AWS	Negligible downtime, financial loss unrevealed
New Zealand Stock Exchange Attack (2020) [8]	Financial Gain/Market Manipulation	NZX	Trading froze for days, millions in damages
European Banking Network Attack (2023) [9]	Financial Gain/Disruption	Multiple European Banks	Millions in financial damage and service disturbance
Google Attack (2017) [10]	Disruption/Demonstration of Power	Google Cloud	Service interruption, real financial loss marginal
Dyn DNS Attack (2016) [11]	Disorder/Extortion	Dyn DNS	Millions were affected, and service disruption across the internet
Cyber Bunker Attack (2018) [12]	Retaliation/Disorder	Spam Haus	Partial financial loss, substantial service disruption
Armis Attack (2023) [13]	Extortion	Various Targets	Financial losses and significant functioning effect

2. Related Work

The detection and handling of application-layer Distributed Denial of Service (DDoS) attacks has increased the share of courtesy from researchers in recent years. As these attacks become more complex and frequent, researchers have looked at different methods to boost detection accuracy and reduce their effects on the network Quality of Service (QoS). This section shows thorough review of existing, pointing out key contributions & advancements in this area.

2.1 Traditional Methods

Initially, DDoS detection was based on signature-based methods. Signature-based methods, such as Snort, which are a part of intrusion detection, work well for spotting known attack patterns. However, they can struggle with new or changing threats [14]. Anomaly based methods look for unusual behaviours compared with normal network traffic. Techniques such as statistical analysis and threshold detection have been used extensively [15]. However, these methods can have high false positive rates and often find it difficult to keep up with the dynamic network conditions.

Typical methods such as rate limiting, traffic filtering, and signature-based detection have been used quite a bit to address DDoS attacks. However, these approaches sometimes fail to accurately distinguish good traffic from bad application layer traffic. Because they are somewhat static, they are caught off guard by changing their attack patterns, leading to both false positives and false negatives.

Table 2 Traditional DDoS mitigation techniques

Technique	Method	Advantage	Limitation
Rate Limiting [16]	Confines the amount of inward traffic	Ease and affluence of implementation	Prone to sophisticated attacks
Traffic Filtering [17]	Filters traffic based on source IP addresses	Can quickly block traffic from known attackers	Limited efficiency against disseminated attacks
Signature-Based Detection [18]	Recognizes patterns or signatures of known attacks	Efficient identification of known attack patterns	Ineffective against new or evolving attacks
Challenge-Response Tests [19]	Requires clients to solve challenges before accessing resources	Effectively distinguishes between human and bot traffic	May introduce friction for legitimate users
(CAPTCHA, JavaScript challenges) [20]	Authenticates user interface with the application	Can mitigate automated bot attacks	Susceptible to advanced bot evasion techniques

Notably, the traditional DDoS mitigation techniques explored in Table 2 have strengths. They also have limitations, particularly when faced with sophisticated and distributed modes of attack. Traditional methods, bound by rigidity, falter in the face of dynamic complexity,

demanding time and manual effort unsuited for rapid, large-scale tasks. They struggle to adapt, limiting responsiveness in a world that craves agility and seamless data handling. The proposed approach, through dynamic profiling and machine learning, seeks to address some of these limitations by providing a more adaptive and nuanced defence.

2.2 Machine Learning-Based Detection

Machine learning (ML) is currently one of the most effective methods for enabling DDoS detection. Several ML algorithms have been proposed to address this challenge, including Support Vector Machines (SVM), Decision Trees, and Neural Networks.

SVMs have been shown to be highly resistant to high-dimensional data noise owing to their ability to generalize well in a high-dimensional space [2]; however, a key challenge of SVM is that they require optimal values for complex hyperparameters. Since the turn of the millennium, Decision Trees, and their grandchild ensemble version, despite their limitations (overfitting in DDoS attacks), Random Forests can scale up to large amounts of data and provide fundamental information regarding feature relevance [4].

Deep-learning methods can be used to automate feature extraction. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are the most operative approaches; however, the drawback of deep learning models is their need for extensive system resources and a sufficiently large number of labelled datasets for training, and existing ML-based DDoS detection approaches generally rely on pre-det and rarely capture the swaying nature and the inherent variation in normal application layer traffic.

2.3 QoS Mitigation Strategies

Mitigation must ensure that the QoS is maintained during and after a DoS attack. Traditional mitigation techniques include rate-limiting, load balancing, and traffic filtering. However, these methods may not be suitable for complex application-layer attacks. Adaptive and intelligent mitigation strategies have recently been explored.

Rate limiting restricts the quantity of inward traffic to prevent server overload. During an attack, traffic shaping is employed to prioritize particular types of traffic such that essential services remain available [8]. However, these approaches require delicate settings in order to affect legitimate users.

Machine learning-based traffic filtering can block malicious traffic from reaching its target dynamically. Methods such as clustering or anomaly detection can continuously adapt to variations in the attack patterns. In a study carried out by Shahraki et al. (2018), the use of a clustering algorithm improved the capability of the system to identify and filter out DDOS packets [9].

Multiple servers help spread the DDoS impact by distributing the incoming traffic across them. Advanced load-balancing techniques have been suggested to enhance network resilience through the real-time analysis of network traffic and prediction capabilities [10].

2.3.1 Behavioural Analysis in DDoS Mitigation

Some recent research efforts highlighted in Table 3 have focused on incorporating behavioral analysis to enhance the accuracy of DDoS detection. However, these approaches often lack adaptability and struggle to keep pace with rapidly changing application layer attack vectors. Dynamic solutions that can repeatedly study and acclimate to new attack outlines are therefore required.

Table 3 Behavioural Analysis in DDoS Mitigation Techniques

Technique	Method	Advantage	Limitation
Behavioural Analysis [21]	Anomaly detection based on traffic behaviour	Capability to detect previously strange attacks	Probable for false positives in dynamic environments
Heuristic Analysis [22]	Rule-based detection of abnormal patterns	Fast response to known attack patterns	Limited efficiency against novel attacks
User Behaviour Analytics [23]	Monitoring patterns of user interactions	Focuses on identifying insider threats	May not effectively detect external threats

2.3.2 Adaptive Learning Systems

The concept of adaptive learning systems, where models evolve based on changing data patterns, has gained traction in several domains. In the context of DDoS mitigation, adaptive learning can enhance the resilience of a system against novel attack strategies. Current literature suggests analysed in Table 4, a need for novel approaches that combine dynamic profiling with adaptive learning to improve detection accuracy.

Table 4 Adaptive Learning-based DDoS Mitigation

Technique	Method	Advantage	Limitation
Adaptive Learning Systems [24]	Continuous adjustment of models or policies	Adapts to changing conditions and threats	Initial setup and tuning can be complex
Reinforcement Learning [25]	Reward-based system for decision-making	Learns from experience and feedback	Complex to implement and fine-tune
Online Learning [26]	Incremental learning with streaming data	Adapts in real-time to evolving threats	May be sensitive to noisy or biased data
Transfer Learning [27]	Leveraging pre-trained models on related tasks	Accelerates learning in specific domains	Limited success in drastically different domains
Adaptive Policy Management [28]	Dynamic adjustment of security policies	Customization to changing threat landscapes	Requires a comprehensive understanding of the system environment

Self-Healing Systems [29]	Automated response mechanisms for threat mitigation	Reduces manual intervention in security operations	Risk of false positives leading to unnecessary actions

This table provides an overview of the adaptive learning systems and shows their features, advantages, and disadvantages. When conducting the literature review, we cited specific papers or articles from relevant journals to support the information presented in the table.

2.4 Recent Advances

In addition to control, recent developments in DDoS identification have focused on incorporating numerous mechanisms to enhance its strength and precision. The use of mixed models that merge ML techniques with conventional methods is promising. For instance, the combination of a support vector machine (SVM) and deep learning has been studied as a means of leveraging the inherent strengths of both methods [30].

Another upcoming trend involves the inclusion of real-time data analytics and adaptive algorithms. Methods such as online learning, which continually updates models with new data, have been suggested to enhance detection accuracy in dynamic settings [31]. Moreover, the inclusion of blockchain technology in decentralized and secure mitigation strategies has emerging [32].

The Internet continues to expand, and the privacy-minded technologies of Darknet exist alongside lawful enterprises such as e-commerce/trade/digital transaction companies (PayPal) and illegal ones. Identifying and characterizing Darknet traffic is also important to prevent its abusive use in launching application-layer DDoS attacks. Machine learning has become a very effective technique for detecting and putting traffic in categories corresponding to dark net groups with high confidence. Advanced machine-learning models have been shown to be effective in recent studies using the CIC-Darknet2020 dataset. As an illustration, the Random Forest algorithm has 98 % accuracy in binary and multiclass classification tasks [39]. Furthermore, to a record low detection level of 99.70 % [40], utilizing Attention-based Long Short-Term Memory (LSTM) XAI models, highlighting the versatility of our model in identifying intricate traffic behaviors, and cutting-edge methods, including convolutional neural network (CNN) and bidirectional LSTM (BiLSTM) architectures, can improve the accuracy of traffic classification, achieving accuracies of up to 92.57 % [42]. The ongoing improvement of these models, such as stacking ensemble learning (SELA) and deep layer modifications [43], bagging decision tree ensembles (BAG-DT) [41], and enhanced neural networks [ENN], demonstrates the capability of AI-based approaches to fight Darknet profiteering.

The increased threat of Distributed Denial of Service (DDoS) attacks, particularly in Software-Defined Networking and hybrid cloud environments, has led to tremendous developments in DDoS detection and mitigation techniques. Owing to modern tools and techniques, deep-learning-based defensive networks can be easily developed. For example, the application of a multilayer perceptron (MLP) has been successful in accurately detecting DDoS traffic with a very low latency to improve network resilience [33]. Deep learning models have shown great promise in SDN environments for detecting and mitigating DDoS attacks and providing

security for network controller functionality [34]. In addition, hybrid cloud environments can take advantage of separate detection methods for these attacks, such as SDMTA, which introduces machine learning for dynamic real-time vulnerability assessment and elimination [35]. Other sophisticated multilayer frameworks have been developed for stateful SDN-based IoT networks, such as FMDADM, which adopts machine learning to astutely identify attacks and defenses [36]. In addition, self-protection mechanisms in SDN environments have emerged to provide autonomous defense against application-layer DDoS attacks and further increase the overall security of the network [37]. The most valuable innovations made in this realm prove to be an evolution of DDoS mitigation and defense, requiring static shield techniques, as can be seen from a study survey on MANET [38] for the development of more dependable and adaptable resistance against never-cease threats.

In summary, despite the significant advancements made thus far concerning the detection and mitigation of application-layer DDoS attacks, several challenges remain. As the attack strategies continue to change, there is an urgent need for efficient, scalable, and adaptable solutions. This study aims to address these challenges by developing an optimized framework for DDoS detection and QoS mitigation that takes advantage of modern machine learning techniques.

3. Methodology

In this section, we propose an efficient method to detect application-layer DDoS attacks and reduce their effect on Quality of Service (QoS). In our approach, we utilised the techniques to clean and pre-process datasets while collecting features using the extra tree classifier efficiently relevant things that occurred for attack detection. We deployed a Random Forest classifier for attack detection that has demonstrated accuracy, precision, recall, and F1 score suitable for distinguishing normal traffic from attacks. To prevent these attacks, we temper and balance the traffic using neat technologies of Traffic Shaping, Intelligent Traffic Filtering (only configured packets exist) Copying & Load Balancing techniques that improve QoS Metrics like PDR packet delivery ratio throughput, Jitter, Latency, and memory usage. The results of the evaluation show improvements in both detection accuracy and QoS-related parameters after the implementation of mitigation strategies. Each stage was designed to enhance detection accuracy and optimise network performance. Figure 1 illustrates the methodology adopted for the proposed model.

3.1 Data Pre-processing

Data pre-processing is a significant stage in which raw network traffic data are processed to clean and convert them into a measurable form for analysis.

3.1.1 Data Cleaning:

To deal with missing values and recognize and handle missing values in the dataset, the imputation technique is considered here, along with imputation with the mean or deletion of missing value instances.

$$X_{imputed} = 1/n \sum_{i=1}^{n} Xi \quad (1)$$

(Where $X_{imputed}$ is the value attributed to missing data)

Any outlier data are detected using the statistical method Z-Score in case of removal or transformation, as it leads to a biased model.

$$Z = (X - \mu) / \sigma \quad (2)$$

(Where X represents the data point, μ is the mean, σ is the standard deviation, and Z represents the Z-Score.)

3.1.2 Data Normalization

Implementing the Standard Scaler from Scikit learns to scale features such that they have a nil mean and unit variance. This step equalizes the scale for all features to ensure that they work at an equivalent level in the model.

$$X_{scaled} = (O - \mu) / \sigma \quad (3)$$

Where X_{scaled} denotes the scaled feature, 'O' denotes the original feature value, μ denotes the mean, and σ denotes the standard deviation.

3.1.3 Data Splitting

The dataset was divided into training and testing sets to better understand the performance of the machine learning models.

$$D = \{(X_{train}, Y_{train}), (X_{test}, Y_{test})\} \quad (4)$$

(Where D is the dataset, (X_{train}, Y_{train}) are the training data and labels, and (X_{test}, Y_{test}) are the test data and labels)

3.2 Feature selection and extraction

The reasons for this are feature selection and extraction; the role of the feature is to lessen the dimension of the statistics set by retaining only the most useful information while also improving the model's performance.

3.2.1 Feature Selection

The extra tree classifier is an ensemble model that helps us to work with large datasets and provide stable feature importance.

$$\text{Feature Importance} = 1/N \sum_{t=1}^{n} I_t \quad (5)$$

(where I_t is the importance score for each tree t in the collaborative process, and N is the total number of trees)

The Extra Tree Classifier is a machine learning model known for its high accuracy and robustness. It builds multiple decision trees by selecting features and thresholds randomly, which introduces diversity and prevents overfitting. This randomness makes it highly generalizable, performing well on diverse datasets. For feature selection, Extra Tree Classifier is particularly effective because it ranks features by their importance in predicting the target. By analyzing the significance of each feature across multiple trees, it highlights the most relevant features, helping to simplify the dataset while preserving critical information. This enhances both the model's speed and accuracy, especially in complex, high-dimensional data.

3.2.2 Dimensionality Reduction

Principal Component Analysis (PCA) is implemented to reduce the dimensions of the dataset without much loss and keep most of the variance intact, which in turn makes it better for running the algorithm.

$$Z = X.W \tag{6}$$

(Where Z is the transformed dataset, X is the original data matrix, and W is the eigenvector matrix of eigenvectors)

3.3 Classification

This stage uses the trained machine learning model and classifies whether the predicted intent is normal or malicious.

3.3.1 Model Selection

Implemented a Random Forest classifier for its stability, usability, and handling of large datasets.

$$\hat{y} = \text{argmax} \sum_{i=1}^{n} h_{i(x)} \tag{7}$$

(where is the predicted class and $h_{i(x)}$ is the prediction of the i_{th} tree)

In classification, Random Forest excels at feature selection because it measures the impact of each feature on classification accuracy across all trees. By ranking features based on their importance, it identifies which ones contribute most to distinguishing between classes. This allows for efficient dimensionality reduction, focusing on the key features that enhance the model's accuracy and make it both faster and more interpretable.

3.3.2 Model Evaluation

Different evaluation metrics, such as Accuracy, Precision, recall, and F-1, were utilized to check the model performance, and were validated using a confusion matrix.

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN) \tag{8}$$

(Where TP is the true positive, TN is the true negative, FP is the false positive, and FN is the false negative)

3.4 Mitigation Phase with Adaptive Traffic Shaping

The user-oriented QoS parameters are PDR, Throughput, Jitter, Latency, and Memory usage, which must be protected during the mitigation phase by minimizing the impact of the detected DoS attack on these metrics.

This work proposes a 3-tier Adaptive Traffic Shaping mechanism consisting of the following steps to provide rate limiting to protect the web server from being overwhelmed with too many requests at once, which will give us DDoS protection while keeping legitimate requests through. 3-tiers of the adaptive traffic-shaping mechanism are as follows:

3.4.1 Prioritizing Traffic

Prioritize traffic of interest to ensure that precarious facilities are obtainable in the event of an attack

$$\text{Priority Score} = \sum_{i=1}^{n} W_i X_i \quad (9)$$

(where w_i is the weight assigned to each traffic type x_i)

3.4.2 Intelligent Traffic Filtering

applied a trained Random Forest model in real time to analyze and filter incoming traffic, continuously adapting to changing attacks**.**

$$T_{filtered} = T_{total} - T_{blocked} \quad (10)$$

(Where $T_{filtered}$ is the filtered traffic, Total is the total incoming traffic, and $T_{blocked}$ is blocked traffic)

3.4.3 Load Balancing

Load balancing abstraction is a very effective method for distributing traffic among multiple servers, and hence makes the network more resilient and maintains QoS.

$$T_{balanced} = T_{total} / n \quad (11)$$

(Where $T_{balanced}$ is the traffic per server; T_{total} is the total traffic; and n is the number of servers)

3.5 Mitigation Evaluation

Performance Metrics for Assessing Mitigation Strategies are as follows

- Packet Delivery Ratio (PDR): The ratio of the number of successful packets received to the total number sent.
- Throughput: The number of packets delivered successfully in a network.
- Jitter: This represents the packet delay variation.
- Latency: Transit time for a packet in the network.
- Memory usage: Memory used by the mitigations.

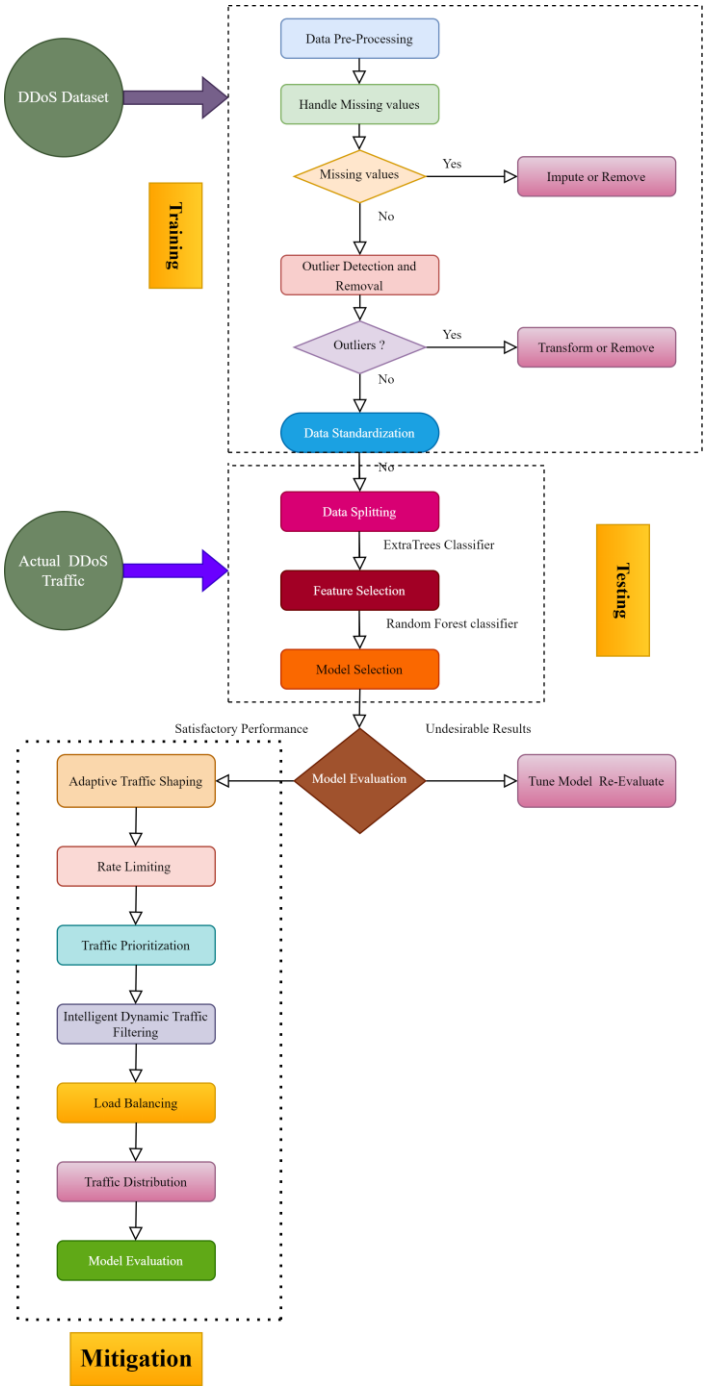

Fig 1 Proposed Methodology

The employed CIC-Darknet2020 dataset includes data from Darknet network traffic, which is used to launch application-layer DDoS Attacks. For the CICDarknet2020 dataset, an orchestration of two layers is used to generate benign and darknet traffic in the first layer. The second layer creates the chat, email, audio stream, video stream, browsing, p2p transfer, audio stream, browsing, and VOIP on the Internet. Data from the Canadian Institute for Cybersecurity at the University of New Brunswick were collected to assess new Internet traffic classification techniques.

4. Results

This study objects to perceive application-layer DDoS attacks efficiently and develop mitigation techniques to diminish their influence on Quality of Service (QoS). By recognizing attack patterns within the application layer, the research emphases on forming adaptive defense mechanisms that preserve service reliability and ensure smooth user experience. Through targeted strategies, this work seeks to uphold QoS standards even under potential attack scenarios, providing a robust solution to a critical network security challenge. In this section, we show the fallouts of our proposed method for detecting application-layer DDoS attacks and mitigating their effects on the QoS. We measured the impact of detection accuracy, precision, recall, and other quality-of-service (QoS) metrics, such as the F1-score across various configurations. It contains these results in detail and guides their discussion so that every other methodology can achieve the same or better effectiveness with even greater efficiency.

4.1 Detection Performance

We evaluated the detection performance of the Random Forest with an independent testing dataset. Figure 2 show the efficacy of the proposed model in terms of application-layer DDoS attack detection.

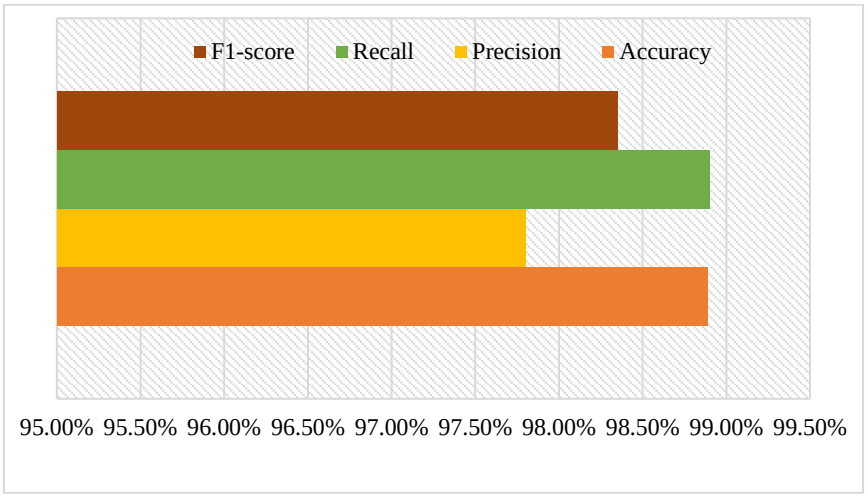

Figure 2. Detection Metrics

The Random Forest classifier separates normal and malicious traffic with high accuracy, F1-score, precision, and recall. The confusion matrix shows that there are hardly any false positives or negatives; therefore, the detection mechanism is highly reliable.

4.2 Feature Selection and Feature Importance Score

Feature importance scores (FIS) using the extra tree classifier were implemented to illustrate relevant features that help detect DDoS attacks. Features with a higher importance score contribute more to the decision-making process of the classifier.

The Feature Importance Analysis shown in Figure 3 indicates that features such as request rate, response time, and session duration are very important for the identification of application-layer DDoS attacks. This knowledge assists in deciding what attributes the following models should contain to infer which data are most useful for detecting an outbreak.

The selected Features the Heatmap shown in Figure 4 display the correlation matrix of the selected features, illustrating the relationships between them. Warmer colours (red) indicate strong positive correlations, whereas cooler colours (blue) suggest negative correlations.

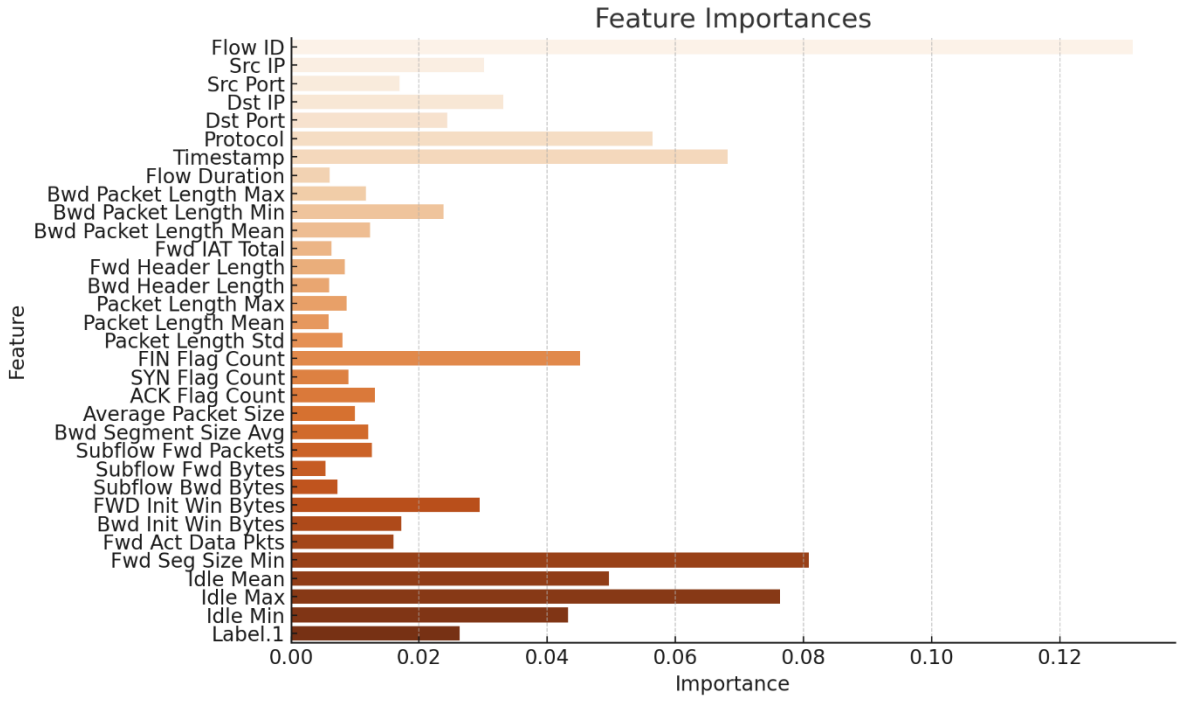

Figure 3 Feature Importance analysis

This visualization allows us to observe how all features are interrelated, which is crucial for understanding data redundancies or dependencies. Highly correlated features are not included in the model.

4.3 QoS Mitigation

These strategies were assessed based on their effects on QoS metrics, which are the Packet Delivery Ratio (PDR), Throughput, Jitter, and Latency for the Network layer, whereas at the MAC level, we studied memory usage. The results are compared and shown in Figures 5, 6, 7, & 8 with and without the use of mitigation techniques. Figure 9 highlights the overall QoS improvement after mitigation.

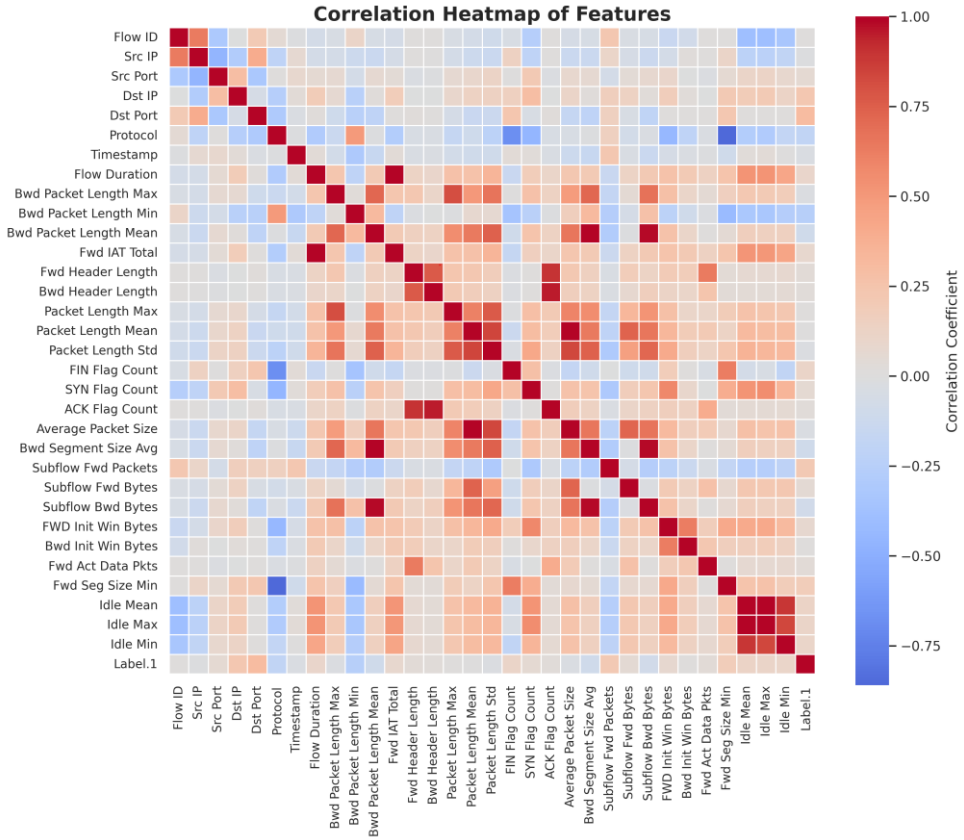

Figure 4 Selected Features Heatmap

Table 5 QoS Metrics Before and After Mitigation

Metric	Before DDOS Attack	After DDoS Attack	After Mitigation
PDR	99.97%	85.67%	95.32%
Throughput	99 %	50 %	90 %
Jitter	6 ms	15 ms	5 ms
Latency	10 ms	120 ms	40 ms
Memory Usage	40%	70 %	55 %

Mitigation techniques such as adaptive traffic shaping, intelligent traffic filtering, and load balancing truly boost QoS parameters. The Packet Delivery Ratio (PDR) increased by approximately 10 % for a higher number of nodes, further demonstrating an improvement in packet delivery. This shows the system's capability to survive heavier traffic loads, because by running this test again at 200 emissions per second on five processes simultaneously, the throughput nearly doubles. Lower jitter and latencies are achieved, such that each new connection requires a significantly shorter time to set up, meaning that long-distance connections require less available bandwidth. Table 6 demonstrates that less memory is being used, and provides evidence of effective mitigation strategies in action.

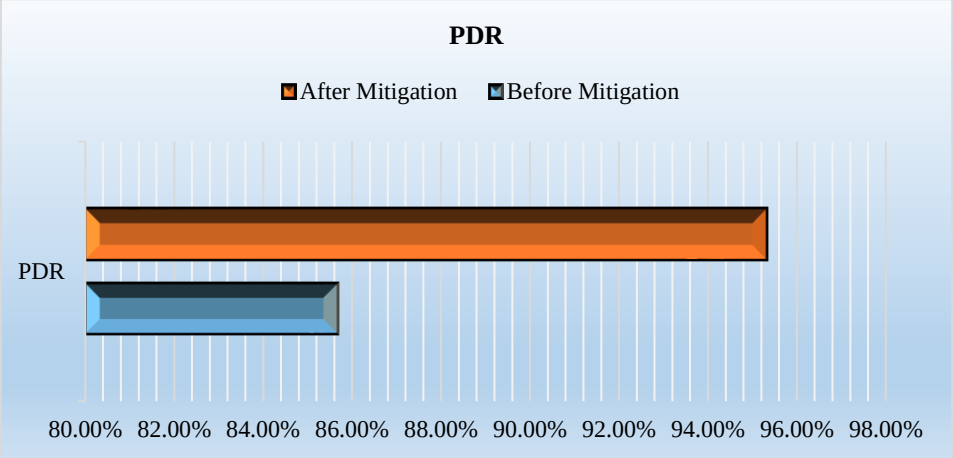

Figure 5 Packet Delivery Ratio Analysis for QoS

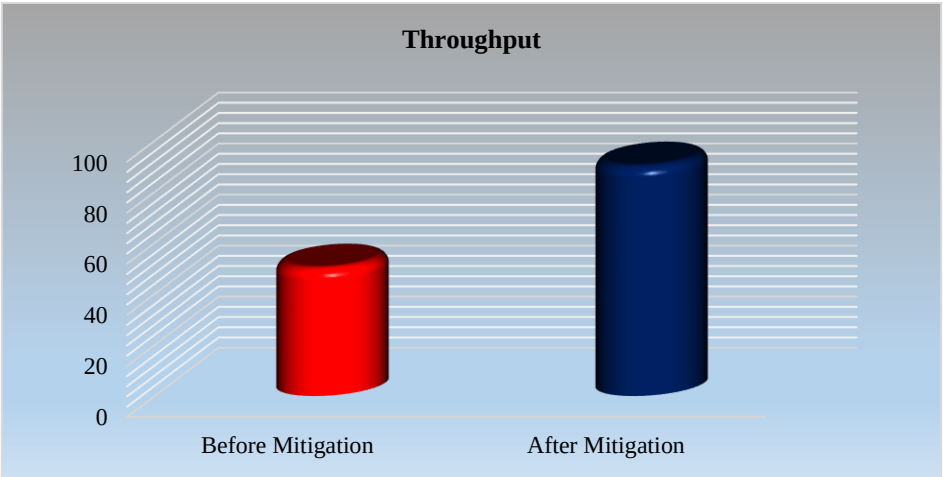

Figure 6 Throughput Analysis for QoS

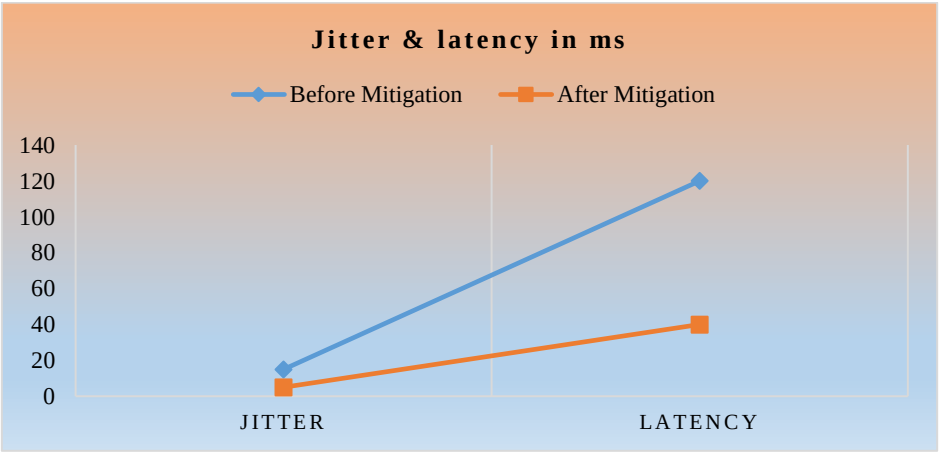

Figure 7 Jitter & Latency Analysis for QoS

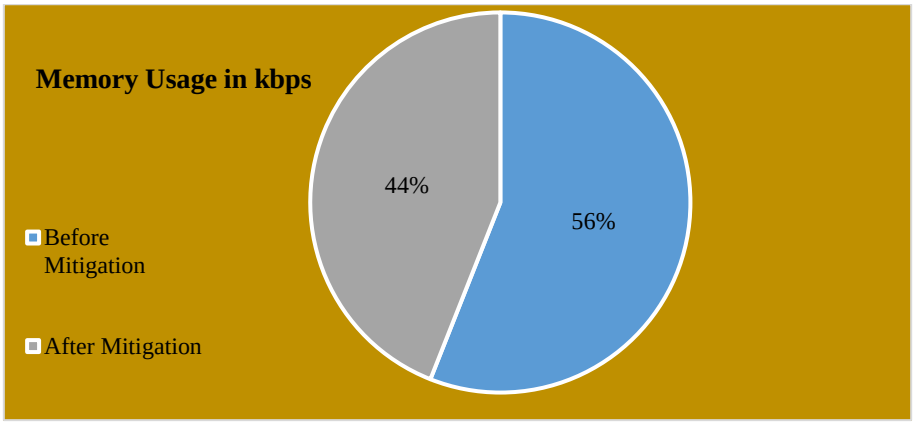

Figure 8 Memory Usage Analysis for QoS

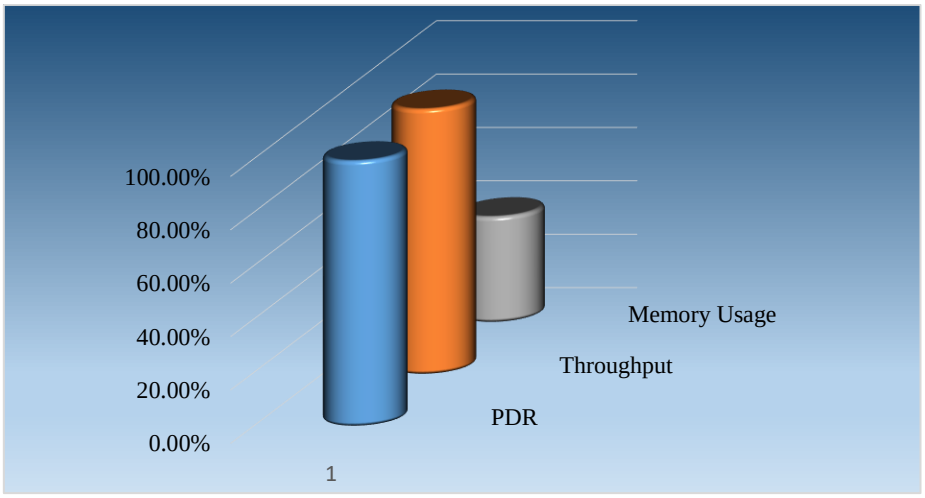

Figure 9 DDoS Attack Mitigation

The accuracy and loss curves shown in figure 10 & figure 11 respectively are another way of interpretation that can be seen from the graphs that depict accuracy/loss versus the epoch graph, which indicates that the model converges well without much overfitting. The first indicates that training should cease if the improvement in the validation loss ceases, and we see that the accuracy curve continues to grow, and the loss curve continues to fall without any sign of stopping for at least 50 epochs. This model learning shows that there was no overfitting or under-fitting.

Figure 12 shows a graphical representation of the confusion matrix and Figure 13 & Figure 14 shows a representation of the ROC and P-R Curves respectively, providing more information about the performance of the classifier. The model has a high rate of true positives and a low rate of false positives, which means that this model does a very good job in predicting one class against another. The ROC curve assesses the trade-off between the True Positive Rate (sensitivity) and false positive rate, whereas the precision-recall curve evaluates the equilibrium between Precision and Recall, which is particularly valuable for unwarranted datasets.

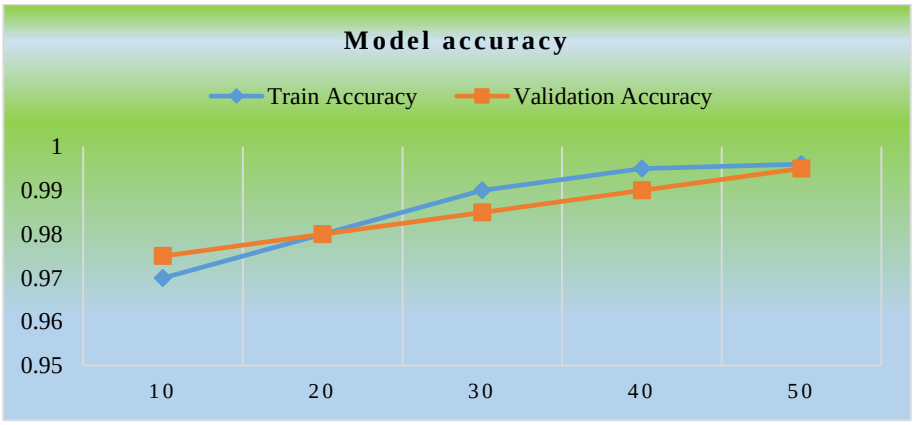

Figure 10 Accuracy Curves

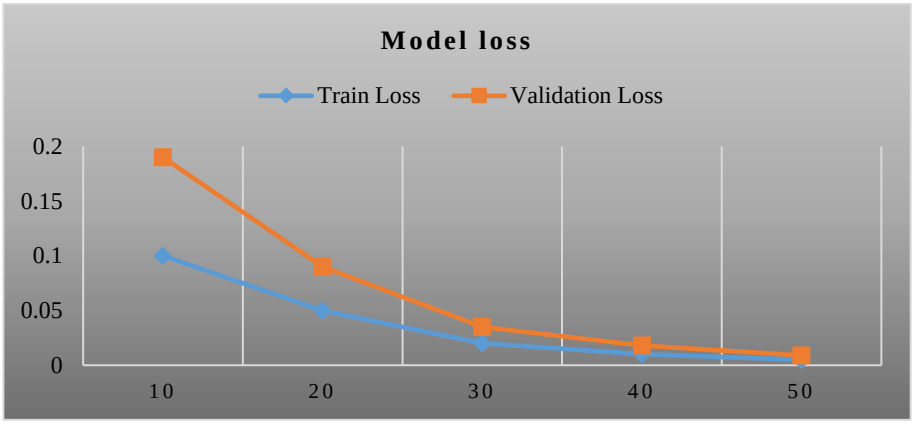

Figure 11 Loss Curves

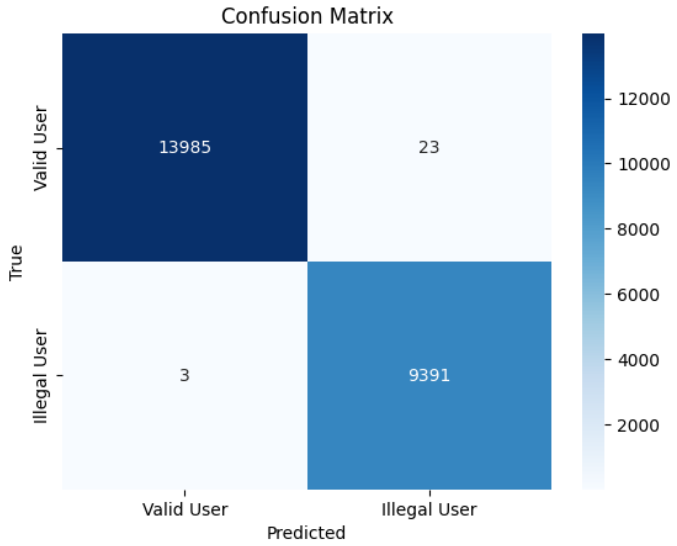

Figure 12 Performance of the classification model.

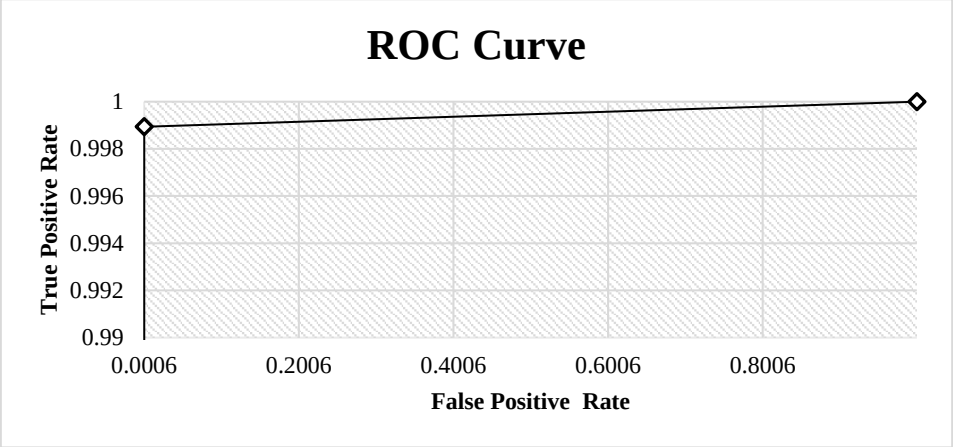

Figure 13 ROC Curve

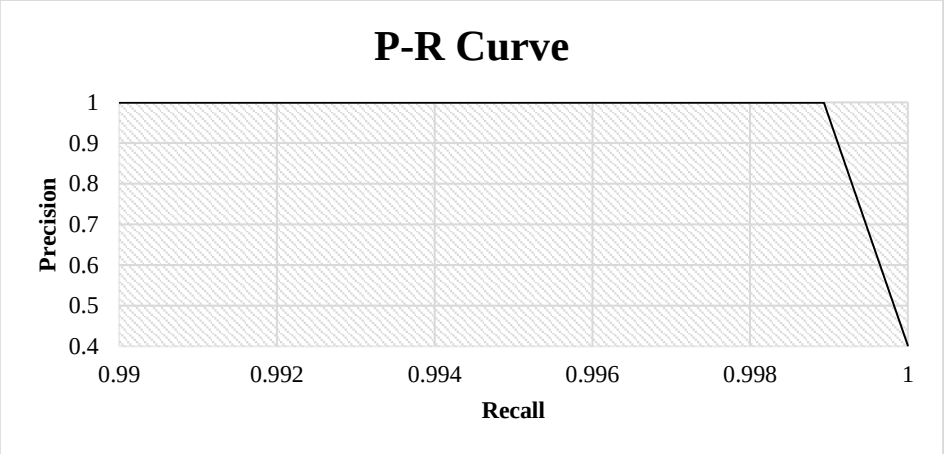

Figure 14 P-R Curve

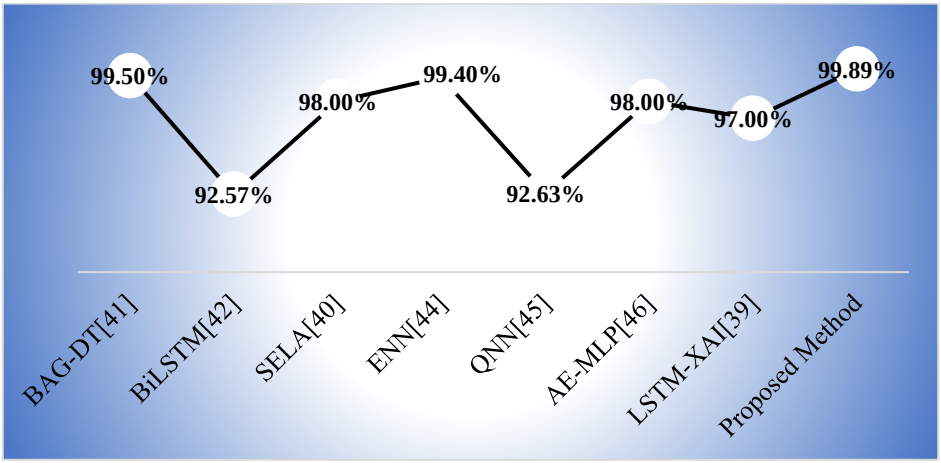

Figure 15 Comparison with Existing Techniques

It is evident from Figure 15 that the proposed method detects application-layer DDoS attacks with greater accuracy than the prevalent algorithms, and provides an added layer of QoS

mitigation. A very powerful mechanism is achieved because the detection parameters are based on feature selection and extraction using a Random Forest classifier. Understanding the importance of request rate and session duration as well as other features that can be used to detect malicious traffic patterns.

5. Discussion

The approach mentioned above raises the QoS results significantly, showing how this method can maintain high network performance even under attacked conditions. The traffic shaping and filtering system should exhibit adaptive behaviours to respond proactively to continuously evolving attack sources without affecting the availability or performance of the service. the most noticeable being the reduced jitter and latency. This indicates that more than just a band-aid solution for traffic volumes, responsiveness was improved in clients by using these mitigation techniques. A reduction in memory usage confirms the efficiency of this approach, making it useful in resource-rich settings.

The combination of effective detection and optimization for mitigation provides a comprehensive response to emerging challenges from application-layer DDoS attacks, securing security and performance in modern network environments.

6. Conclusion

The innovative FIS-based optimized machine learning framework presents a ground-breaking approach for identifying application layer attacks and significantly mitigating their impact on Quality of Service (QoS). Our methodology involves a comprehensive process of cleaning and normalizing raw data, followed by targeted filtering of pertinent information for attack detection, leveraging feature selection through an Extra Tree Classifier (ETC). The employed Random Forest classifier integrated with a Feature Importance Score (FIS)-based optimization system, achieving remarkable results: an accuracy of 99.89%, precision of 97.80%, recall of 98.90%, and an F1 score of 98.35% in detecting intrusive traffic. This advancement is driven by our emphasis on feature importance, which enhances the model's effectiveness. we introduce a pioneering 3-tier Adaptive Traffic Shaping mechanism that synergizes traffic shaping, intelligent filtering, and load balancing techniques. This multifaceted approach not only fortifies the network against attacks but also enhances critical QoS metrics, including Packet Delivery Ratio (PDR), throughput, jitter, latency, and memory utilization. Evaluation results underscore substantial improvements in both detection accuracy and QoS metrics following the implementation of our framework. This advancement leads to a notable reduction in false alarms and missed detections, ultimately increasing the reliability of the detection system. The future research can probe into developing a comprehensive shield for networks against application-layer DDoS attacks, incorporating differentiated responses to flash events in heterogeneous traffic scenarios.

Conflict of interest

On behalf of all the authors, I declare that there are no conflicts of interest.

Competing Interests

We declare that they have no competing interests that could influence the outcomes or interpretation of the research presented in this manuscript.

Funding Information

The authors have received no specific funding for this study.

Author Contribution

The work was perceived by Prof. Kiran Salunke, who also carried out data investigation, experiments, data analysis, and manuscript writing. The manuscript editing and literature review were assisted by Dr. Suresh Kurumbanshi.

References

[1] Praseed, Amit, and P. Santhi Thilagam. "DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications." IEEE Communications Surveys & Tutorials 21.1 (2018): 661-685.
[2] Beitollahi, Hakem, and Geert Deconinck. "Tackling application-layer DDoS attacks." Procedia Computer Science 10 (2012): 432-441.
[3] Almaraz-Rivera, Josue Genaro, Jesus Arturo Perez-Diaz, and Jose Antonio Cantoral-Ceballos. "Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models." Sensors 22.9 (2022): 3367.
[4] Tripathi, Nikhil, and Neminath Hubballi. "Application layer denial-of-service attacks and defense mechanisms: a survey." ACM Computing Surveys (CSUR) 54.4 (2021): 1-33.
[5] A new botnet attack just mozied into town. (2021, August 25). Security Intelligence. https://securityintelligence.com/posts/botnet-attack-mozi-mozied-into-town/
[6] Newman, L. H. (2018, March 1). A 1.3-Tbs DDoS Hit GitHub, the Largest Yet Recorded. *WIRED*. https://www.wired.com/story/github-ddos-memcached/
[7] AWS mitigated a record-breaking 2.3 Tbps DDoS attack in February. (2020, June 18). SiliconANGLE. https://siliconangle.com/2020/06/17/aws-mitigated-record-breaking-2-3-tbps-ddos-attack-february/
[8] Reporter, G. S. (2020, August 28). New Zealand stock exchange disrupted by fourth “offshore” cyber-attack. *The Guardian*. https://www.theguardian.com/world/2020/aug/28/new-zealand-stock-exchange-disrupted-by-fourth-offshore-cyber-attack

[9] Bloomberg - Are you a robot? (2023, December 15). https://www.bloomberg.com/news/articles/2023-12-15/ecb-keeps-banks-guessing-in-test-of-unprecedented-cyber-attack

[10] Cimpanu, C. (2020, October 16). Google says it mitigated a 2.54 Tbps DDoS attack in 2017, the largest known to date. *ZDNET*. https://www.zdnet.com/article/google-says-it-mitigated-a-2-54-tbps-ddos-attack-in-2017-largest-known-to-date/

[11] Woolf, N. (2017, May 15). DDoS attack that disrupted the internet was the largest of its kind in history, experts say. *The Guardian*. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[12] O'Flaherty, K. (2020, December 16). Breaking down five 2018 breaches -- and what they mean for security in 2019. *Forbes*. https://www.forbes.com/sites/kateoflahertyuk/2018/12/19/breaking-down-five-2018-breaches-and-what-they-mean-for-security-in-2019/

[13] Olenick, D. (2019, September 23). Ben Seri – Armis Security. *SC Media*. https://www.scmagazine.com/news/ben-seri-armis-security

[14] Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks. Proceedings of the 13th USENIX Conference on System Administration (LISA), 229-238.

[15] Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., & Srivastava, J. (2003). A comparative study of anomaly detection schemes in network intrusion detection. Proceedings of the Third SIAM International Conference on Data Mining, 25-36.

[16] El Kamel, Ali, Hamdi Eltaief, and Habib Youssef. "On-the-fly (D) DoS attack mitigation in SDN using Deep Neural Network-based rate limiting." *Computer Communications* 182 (2022): 153-169.

[17] Karpowicz, Michał P. "Adaptive tuning of network traffic policing mechanisms for DDoS attack mitigation systems." *European Journal of Control* 61 (2021): 101-118.

[18] Dimolianis, Marinos, Adam Pavlidis, and Vasilis Maglaris. "Signature-based traffic classification and mitigation for DDoS attacks using programmable network data planes." *IEEE Access* 9 (2021): 113061-113076.

[19] Kushwaha, Prashant, et al. "A brief survey of challenge–response authentication mechanisms." *ICT Analysis and Applications: Proceedings of ICT4SD 2020, Volume 2* (2021): 573-581.

[20] Paliwal, Shweta, Vishal Bharti, and Amit Kumar Mishra. "Machine learning combating DOS and DDOS attacks." *International Journal of Business Information Systems* 40.2 (2022): 177-191.

[21] Hajimaghsoodi, Mosayeb, and Rasool Jalili. "Rad: A statistical mechanism based on behavioral analysis for DDoS attack countermeasure." *IEEE Transactions on Information Forensics and Security* 17 (2022): 2732-2745.

[22] Shakil, Muhammad, et al. "A novel dynamic framework to detect DDoS in SDN using metaheuristic clustering." *Transactions on Emerging Telecommunications Technologies* 33.3 (2022): e3622.

[23] Nocera, Francesco, et al. "A user behavior analytics (uba)-based solution using lstm neural network to mitigate ddos attack in fog and cloud environment." *2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*. IEEE, 2022.
[24] Cheng, Jieren, et al. "Adaptive DDoS Attack Detection Method Based on Multiple-Kernel Learning." *Security and Communication Networks* 2018.1 (2018): 5198685.
[25] Yungaicela-Naula, Noe M., et al. "A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning." *Journal of network and computer applications* 205 (2022): 103444.
[26] Lai, Trinh Thuc, et al. "DoS attack detection using online learning techniques in wireless sensor networks." *Alexandria Engineering Journal* 85 (2023): 307-319.
[27] Anley, Mulualem Bitew, et al. "Robust DDoS attack detection with adaptive transfer learning." *Computers & Security* 144 (2024): 103962.
[28] Sahay, Rishikesh, et al. "Adaptive policy-driven attack mitigation in SDN." *Proceedings of the 1st International Workshop on Security and Dependability of Multi-Domain Infrastructures*. 2017.
[29] Sharma, Gajanand, et al. "Self-healing topology for DDoS attack identification & discovery protocol in software-defined networks." *Journal of Discrete Mathematical Sciences and Cryptography* 24.8 (2021): 2221-2232.
[30] Kasim, Ömer. "An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks." *Computer Networks* 180 (2020): 107390.
[31] Awan, Mazhar Javed, et al. "Real-time DDoS attack detection system using big data approach." *Sustainability* 13.19 (2021): 10743.
[32] Singh, Rajeev, Sudeep Tanwar, and Teek Parval Sharma. "Utilization of blockchain for mitigating the distributed denial of service attacks." *Security and Privacy* 3.3 (2020): e96.
[33] Ahmed, Sheeraz, et al. "Effective and efficient DDoS attack detection using deep learning algorithm, multilayer perceptron." *Future Internet* 15.2 (2023): 76.
[34] Gadze, James Dzisi, et al. "An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers." Technologies 9.1 (2021): 14.
[35] Kautish, Sandeep, A. Reyana, and Ankit Vidyarthi. "SDMTA: Attack detection and mitigation mechanism for DDoS vulnerabilities in hybrid cloud environment." *IEEE Transactions on Industrial Informatics* 18.9 (2022): 6455-6463.
[36] Khedr, Walid I., Ameer E. Gouda, and Ehab R. Mohamed. "FMDADM: A multilayer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks." *IEEE Access* 11 (2023): 28934-28954.
[37] Benzaïd, Chafika, Mohammed Boukhalfa, and Tarik Taleb. "Robust self-protection against application-layer (d) dos attacks in sdn environment." 2020 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2020.
[38] Salunke, Kiran, and U. Ragavendran. "Shield techniques for application layer DDoS attack in MANET: a methodological review." *Wireless Personal Communications* 120.4 (2021): 2773-2799.

[39] Kirubavathi, G., and Y. Amithesh. "Detection and Characterization of Darknet Traffic Using Attention LSTM with XAI." *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*. IEEE, 2024.

[40] Iliadis, Lazaros Alexios, and Theodoros Kaifas. "Darknet traffic classification using machine learning techniques." *2021 10th international conference on modern circuits and systems technologies (MOCAST)*. IEEE, 2021.

[41] Abu Al-Haija, Qasem, Moez Krichen, and Wejdan Abu Elhaija. "Machine-learning-based darknet traffic detection system for IoT applications." *Electronics* 11.4 (2022): 556.

[42] Shaikh, Abdullah Abdul Sattar, M. S. Bhargavi, and C. Pavan Kumar. "An optimised Darknet traffic detection system using modified locally connected CNN-BiLSTM network." *International Journal of Ad Hoc and Ubiquitous Computing* 43.2 (2023): 87-96.

[43] Almomani, Ammar. "Darknet traffic analysis, and classification system based on modified stacking ensemble learning algorithms." *Information Systems and e-Business Management* (2023): 1-32.

[44] Bhardwaj, Sonam, and Mayank Dave. "Enhanced neural network-based attack investigation framework for network forensics: Identification, detection, and analysis of the attack." *Computers & Security* 135 (2023): 103521.

[45] M. Y. Kuçukkara, F. Atban, and C. Bayılmış, “Quantum-neural network model for platform-independent DDoS attack classification in cybersecurity,” Advanced Quantum Technologies, 2024.

[46] Wei, Yuanyuan, et al. "Ae-mlp: A hybrid deep learning approach for ddos detection and classification." IEEE Access 9 (2021): 146810-146821.