The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 4, August 2025
https://doi.org/10.33022/ijcs.v14i4.4965

Enhanced Detection of IoT-Based DoS Attacks Using A Hybrid ANN-RF Classification Model

Solomon B. Ndaba[1], Topside E. Mathonsi[2], and Deon Du Plessis[3]
ndabasbd@gmail.com[1], mathonsite@tut.ac.za[2], danieldp@uj.ac.za[3]
[1,2] Tshwane University of Technology, Pretoria, South Africa
[3] University of Johannesburg, Johannesburg, South Africa

Article Information

Received : 31 Jul 2025
Revised : 11 Aug 2025
Accepted : 30 Aug 2025

Keywords

IoT, DoS Attack, ANN-RF

Abstract

Denial of Service (DoS) attacks pose a significant threat to the integrity and availability of Internet of Things (IoT) networks, where interconnected devices are increasingly targeted due to their vulnerabilities. These attacks overwhelm systems with excessive traffic, disrupting legitimate services and potentially compromising sensitive data. Traditional detection methods often rely on predefined signatures, which struggle to keep pace with the evolving tactics employed by attackers. This study introduces a novel hybrid detection algorithm that integrates Artificial Neural Networks (ANN) and Random Forest (RF) classifiers, termed ANN-RF, to enhance the detection of DoS attacks in IoT environments. The ANN-RF model was evaluated based on critical performance metrics, including detection accuracy, False Positive Rate (FPR), and latency. Experimental results obtained through MATLAB demonstrate that the ANN-RF model achieves a detection accuracy of 93% and a low FPR of 5% when detecting 30 attacks, significantly outperforming standalone ANN and RF models, which recorded accuracies of 82% and 87%, and FPRs of 15% and 10%, respectively. Additionally, the ANN-RF model consistently maintains high detection accuracy, reducing false alarms and enhancing reliability as the number of attacks increases. Thus, the proposed ANN-RF model has strong potential to enhance real-time security in IoT networks by offering a scalable, accurate, and adaptive solution for DoS attack detection, with practical applications across domains such as smart homes, healthcare, and industrial control systems.

A. Introduction

The Internet of Things (IoT) is a computing paradigm that enables interconnected devices to communicate and share data through the Internet, creating a network of physical objects embedded with sensors, software, and other technologies [1, 2]. According to Syed et al. [3], IoT provides extensive resource pools for managing large amounts of data. These devices are commonly utilized in various domains such as healthcare, smart cities, and industrial automation, raising significant security concerns.

Numerous cyber-attacks target the IoT platform, with the Denial of Service (DoS) attack being recognized as a common threat to IoT devices [4, 5]. A DoS attack is a type of cyber-attack that disrupts services by inundating a machine or network with excessive requests, overwhelming systems, and impeding legitimate requests from being processed [6, 7]. One of the main drivers behind the rise in DoS attacks on IoT platforms is data extortion. Due to the significant security risks posed by DoS attacks in IoT, they are considered a major vulnerability. These attacks have the potential to compromise information from millions of devices and redirect data traffic to the attacker [8, 9]. DoS attacks pose a significant threat to IoT devices by impacting their processing ability, bandwidth, and network systems [10-12]. IoT data faces security risks from hackers, with the most common form of attack being the DoS attack as illustrated in Figure 1.

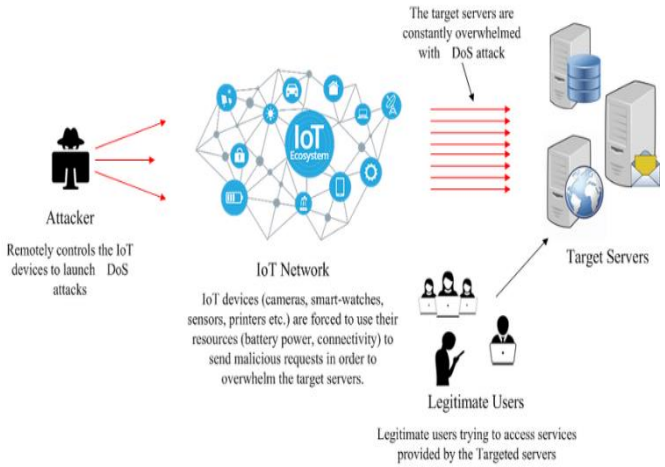

Figure 1. A DoS attack scenario in IoT networks [13].

These attacks are particularly concerning for the availability of IoT services due to the introduction of new vulnerabilities brought about by the nature of IoT, including device heterogeneity and resource constraints [14, 15]. In response to this challenge, Machine Learning (ML) has emerged as a promising avenue for enhancing DoS attack detection [16, 17]. Algorithms such as Support Vector Machines (SVM) and Deep Learning have shown potential in discerning subtle patterns indicative of an impending attack. However, these methods are not without their drawbacks. Studies have identified significant issues with accuracy and False Positive Rates (FPR), leading to inefficient resource allocation and unnecessary service disruptions.

To address these shortcomings, this research introduces a novel solution: the integration of an Artificial Neural Network (ANN) with a Random Forest (RF) classifier, termed ANN-RF. This innovative approach harnesses the complementary strengths of ANNs in recognizing intricate patterns and RFs in handling complex, high-dimensional data. By combining these techniques, ANN-RF aims to bolster DoS attack detection and mitigation capabilities, offering improved accuracy and reduced FPR.

The ANN-RF model operates by first utilising the ANN to extract and analyse intricate features from network traffic data. Subsequently, these features are fed into the RF classifier, which excels in discerning patterns within large and diverse datasets. Through this integrated approach, ANN-RF endeavours to enhance the resilience of network defenses against sophisticated DoS attacks, minimising service disruptions and optimising resource allocation in the face of cyber threats.

Despite the advantages of machine learning techniques, the ongoing threat of DoS attacks continues to pose a significant challenge to IoT security, often overwhelming systems with excessive traffic [18]. Traditional detection methods, which rely heavily on predefined attack signatures, are increasingly unable to keep pace with the dynamic and evolving tactics used by attackers [19]. This scenario emphasizes the need for adaptive defense mechanisms that can effectively counter such sophisticated threats.

In recent years, machine learning models such as SVM and Deep Learning algorithms have been explored for their potential in identifying subtle, often imperceptible, attack patterns characteristic of imminent DoS attacks [20, 21]. However, these approaches are not without limitations. Accuracy concerns and high FPR significantly hinder their practical application, leading to inefficient resource use and potentially compromising system performance under attack.

To overcome these challenges, this study introduces a novel approach that integrates ANN with a RF classifier, collectively referred to as the ANN-RF model. The ANN is well-suited for detecting complex, intricate patterns within network traffic, while the RF classifier excels at handling large and varied datasets, making it ideal for high-dimensional data analysis. In the ANN-RF framework, the ANN is employed to extract key features from network traffic data, which are subsequently fed into the RF classifier for enhanced pattern recognition.

By combining these strengths, the ANN-RF model promises to increase the accuracy of DoS attack detection and, crucially, reduce the FPR. This integrated approach not only bolsters network defenses against advanced and evolving threats but also enables more efficient resource allocation, minimising service disruptions caused by cyberattacks. The result is a more robust and adaptive defense mechanism that can keep pace with the increasingly sophisticated tactics used by attackers in the IoT environment.

The principal contributions of this paper are as follows:

1. Development of a Hybrid ANN-RF Detection Model: This paper introduces an innovative hybrid machine learning algorithm that combines ANN-RF classifiers, forming the ANN-RF model. This integration significantly enhances DoS attack detection accuracy while reducing FPR compared to traditional standalone models.

2. Improved Detection Performance: The ANN-RF model seeks to significantly enhance detection accuracy while minimizing FPR. By combining the strengths of both ANN and RF classifiers, it aims to provide a more reliable and effective defense mechanism against DoS attacks, surpassing the limitations of individual ANN and RF models.
3. Adaptability to Evolving IoT Security Threats: The ANN-RF model is designed to adapt to the evolving nature of DoS attacks, offering robust protection across diverse IoT environments. It effectively handles high-dimensional, complex data and evolves in response to emerging attack tactics.

The structure of this paper is organized as follows: Section B provides a detailed review of existing methods for detecting DoS attacks in IoT environments, highlighting the strengths and weaknesses of various machine learning approaches. Section C discusses the architecture of the proposed ANN-RF model, including its design and how it integrates ANN with RF classifiers. In Section D, we present the results of simulations, describe the experimental setup, outline the dataset used, and analyze the performance of the ANN-RF model. Finally, Section E concludes with a summary of the findings and suggests potential avenues for further research in enhancing DoS attack detection in IoT networks.

B. Related Works

This section critically examines recent research on DoS attack detection using ML techniques, highlighting the strengths and limitations of existing approaches, and discussing their relevance to the design of the proposed ANN-RF algorithm.

Kumar & Jain [22] proposed a machine learning-based approach using SVM and Decision Trees for the detection of DoS attacks in IoT networks. Their method aimed to strengthen network security by automating the detection process through the analysis of network traffic data. By applying SVM and Decision Trees, the system was able to identify patterns associated with DoS attacks. The simulations demonstrated that both models were effective in detecting known DoS attack signatures. Similarly, the proposed ANN-RF algorithm shares common ground with Kumar and Jain's model, as both approaches use machine learning to analyse traffic patterns and detect anomalies that suggest ongoing attacks. However, one of the key limitations identified in their study is the reduced effectiveness in detecting novel or previously unseen DoS attack variants. This shortfall leads to a higher FPR, where normal traffic is incorrectly classified as malicious. Such misclassification can undermine the reliability of the system, potentially leading to unnecessary security measures and network interruptions. While SVM and Decision Trees show promise in identifying known DoS threats, further improvement is required to handle emerging attack types and minimise false alarms in real-time IoT environments.

Santos et al. [23] proposed and evaluated four machine learning algorithms SVM, Multi-Layer Perceptron (MLP), Decision Tree, and RF for DoS attacks within a Software-Defined Networking (SDN) environment. Their study involved a simulated network setup using the Scapy tool, which generated traffic from a list of valid IP addresses to test the performance of each algorithm. The evaluation

focused on two key metrics: accuracy and processing time. Among the tested models, the Random Forest algorithm achieved the highest accuracy, while the Decision Tree algorithm showed the best performance in terms of processing speed. Similar to the proposed ANN-RF algorithm, their approach uses machine learning to analyse network traffic and detect anomalies that signal possible DoS attacks. Both approaches focus on recognising irregular patterns indicative of malicious behaviour. However, a notable limitation in their study was the reduced effectiveness of these models in detecting new or previously unseen variants of DoS attacks. This limitation often led to the misclassification of normal traffic as malicious, resulting in an increased false positive rate (FPR). Therefore, while their models are effective for known attack patterns, improvements are necessary for addressing evolving threats in dynamic network environments.

Altulaihan et al. [24] proposed introducing a hybrid intrusion detection system that integrates RF and K-Nearest Neighbours (KNN) algorithms to identify DoS attacks within IoT-based smart environments. The system employs supervised machine learning techniques to analyse and classify network traffic data, effectively distinguishing between benign and malicious behaviours. Through simulation, their method exhibited a high detection accuracy, particularly in recognising known DoS attack signatures. This hybrid approach mirrors the objectives of the proposed ANN-RF algorithm, as both aim to leverage machine learning for efficient traffic monitoring and anomaly detection in IoT networks. A key strength of the RF-KNN model lies in its ability to process large volumes of data and improve detection precision through the combined strengths of both algorithms. Nevertheless, Altulaihan et al. acknowledged a major challenge in their system: differentiating legitimate high-traffic events from actual DoS attacks. This issue contributed to an elevated false positive rate, reducing the overall trustworthiness of the system. False alarms result in unnecessary system responses, including service disruptions or the misallocation of security resources.

Mansoor et al. [25] proposed a deep learning-based detection framework employing Convolutional Neural Networks (CNNs) to identify DoS attacks within SDN environments. The model is designed to extract both spatial and temporal features from network traffic data, enabling the recognition of complex behavioural patterns indicative of malicious activity. The CNN architecture demonstrated high precision in simulation-based experiments, particularly in detecting known DoS attack signatures. Similar to the proposed ANN-RF algorithm, their model uses the advanced representation learning capabilities of deep neural networks to enhance classification performance and detection accuracy. A key strength of this approach lies in its ability to learn salient traffic characteristics directly from raw input, reducing the reliance on manual feature engineering. However, a critical limitation identified in their study concerns the model's limited generalisation capability. When evaluated on datasets that differ from the training environment, the CNN model exhibited a decline in detection accuracy and an increase in false positive rates. This performance degradation under real-world conditions underscores the challenges associated with deploying deep learning models in heterogeneous and dynamic network settings.

Fatima et al. [26] proposed a lightweight ensemble-based intrusion detection model that integrates Decision Trees and Logistic Regression for the detection of

DoS attacks in IoT networks. The model was specifically tailored for deployment in resource-constrained environments, such as edge or embedded devices, where computational overhead must be minimised. The ensemble algorithms aimed to strike a balance between detection accuracy and processing efficiency, thereby enabling real-time analysis without overburdening device resources. Experimental results demonstrated that the model effectively identified known DoS attack patterns with low latency and acceptable precision. Comparable to the ANN-RF hybrid algorithm, their ensemble approach used the strengths of multiple algorithms to enhance detection robustness. A key advantage of their method was its reduction in false negatives, thereby improving the system's sensitivity to known threats. Nonetheless, the study revealed a critical limitation in its ability to generalise to novel or previously unseen attack behaviours. The model exhibited moderate false positive rates, particularly under conditions of highly dynamic or variable traffic patterns. This outcome underscores the inherent trade-off between computational simplicity and adaptability.

Rustam et al. [27] proposed RF for DoS attack detection using machine learning algorithms. The study focused on utilizing multiple features to enhance the accuracy and efficiency of DoS attack detection and classification. The research was conducted to address the growing threat of DoS attacks in computer networks. DoS attacks are malicious activities that aim to disrupt the normal functioning of a network by overwhelming it with a high volume of traffic or requests. By developing a machine learning-based classification system with multi-features, the researchers sought to improve the ability to detect and mitigate DoS attacks effectively. The results of the study demonstrated that the proposed approach using machine learning algorithms with multi-features was effective in accurately classifying DoS attacks. By leveraging a diverse set of features, the system achieved higher accuracy rates in identifying and categorizing different types of DoS attacks compared to traditional methods. The proposed ANN-RF algorithm and the RF algorithm exhibit similarities in the realm of machine learning for detecting DoS attacks. They both analyze network traffic patterns to identify abnormal behaviors indicative of ongoing attacks. However, their algorithms struggled to identify new variant DoS attacks effectively. This struggle with new variants of attacks result in the algorithms misclassifying normal traffic as malicious, thereby increasing the rate of FPR.

Aswad et al. [28] proposed a model that combines three deep learning algorithms, namely Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and CNN, to create a bidirectional CNN-BiLSTM for detecting DoS attacks in IoT networks. This model aims to address the security challenges posed by insecure IoT devices and the increasing prevalence of DoS attacks targeting these systems. This model outperformed other classifiers such as CNN, LSTM, and RNN in terms of accuracy and other evaluation metrics. The research utilized the Intrusion Detection Evaluation Dataset 2027 (CICIDS2017) dataset, which contains instances of common attacks, to implement and test the proposed model. The proposed ANN-RF algorithm shares similarities with the proposed deep learning models in terms of utilizing network traffic patterns to detect abnormal behaviors indicative of ongoing DoS attacks. Both approaches aim to analyse data patterns

effectively for attack detection. However, it was noted that their algorithm struggled to identify new variant DoS attacks efficiently.

Najar & Naik [29] proposed an efficient approach, combining Balanced Random Sampling (BRS) and CNN, to detect DoS attacks within SDN environments. Various mitigation techniques, including filtering, rate limiting, and the implementation of iptables rules to block spoofed IPs, were employed to address these threats. Additionally, a monitoring system utilizing rate-limiting was introduced to supervise blocked IP addresses, ensuring the efficient processing of legitimate traffic. The proposed model exhibited high performance in both binary and multi-classification tasks, achieving accuracies exceeding 99.99% for binary classification and 98.64% for multi-classification. Notably, the DoS detection system not only identifies attacks but also dispatches detailed contextual information to a designated email address. Comparative analysis against existing literature, employing Area Under The Curve (AUC) analysis, demonstrated the superiority of their model. Furthermore, the efficiency and effectiveness of the proposed DoS mitigation system were evaluated through experiments across three distinct scenarios: Attack-Free, Attack-No Mitigation, and Attack-Mitigation. These results underscored the robustness of the proposed mitigation system in effectively countering DoS attacks while ensuring the uninterrupted continuity of regular network operations. The proposed ANN-RF algorithm mentioned shares similarities with their algorithm in term of using hybrid machine learning algorithms to detect DoS attacks. However, it was noted that their algorithm struggled to identify new variant DoS attacks efficiently.

C. System Design and Architecture

1. System Architecture

The proposed system architecture, illustrated in Figure 2, is specifically designed to improve the accuracy of DoS attack detection and reduce the FPR in IoT environments. The architecture comprises multiple components, including IoT devices, an Internet cloud, a firewall, a network switch, the proposed hybrid ANN-RF algorithm, an administration system, and a data warehouse. The integration of ANN and RF enables advanced detection capabilities by using their strengths. The ANN component facilitates improved DoS detection by learning complex and non-linear patterns in network traffic, recognising subtle anomalies, adapting to evolving threats, and automating feature extraction processes. Meanwhile, the RF component, as an ensemble learning technique, contributes to detection robustness through its ability to evaluate feature importance, handle imbalanced datasets, and maintain high classification accuracy. To further minimise false detection rates, the system employs methods such as hyperparameter tuning, k-fold cross-validation, ensemble learning strategies, and continuous learning mechanisms. The synergistic interaction between ANN and RF allows the system to achieve enhanced detection accuracy while maintaining a low FPR, thus ensuring reliable and efficient protection against DoS attacks in heterogeneous and dynamic IoT network environments.

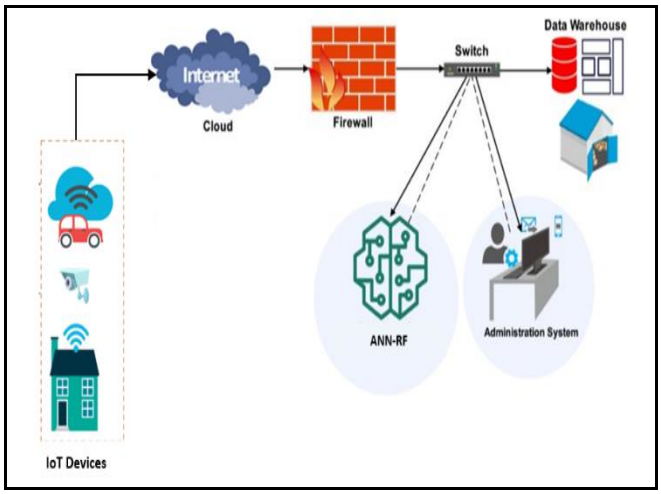

Figure 2. The Proposed DoS Architecture

2. Modelling

The proposed ANN-RF algorithm aims to enhance DoS detection accuracy while minimising FPR in IoT environments. By integrating ANN and RF algorithms, the approach leverages the strengths of these existing solutions to deliver improved detection performance and reliability, addressing critical challenges in securing IoT networks against DoS attacks.

1) Artificial Neural Network

ANN is a computational model inspired by the human brain, consisting to be highly effective in identifying subtle anomalies associated with DoS attacks by analysing complex data patterns [30]. Their inherent ability to adapt to evolving attack strategies through continuous training allows for significant improvements in detection accuracy over time (see Figure 3).

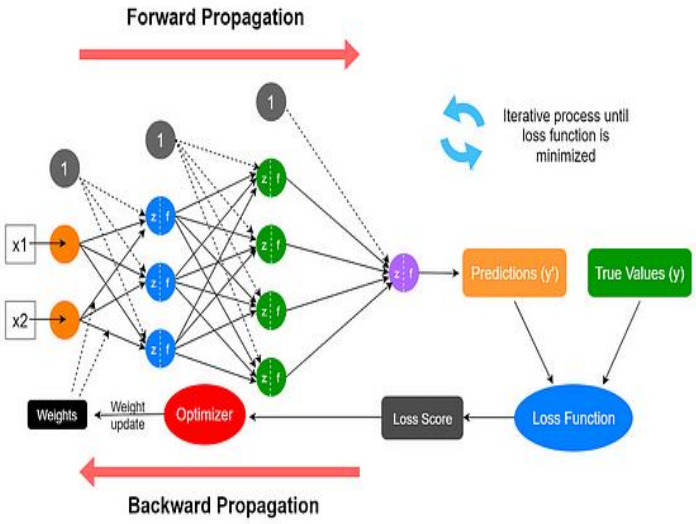

Figure 3. Sequential Process of ANN

This adaptability, coupled with their proficiency in recognising intricate patterns, positions ANNs as a powerful and reliable tool for bolstering IoT network security. By effectively mitigating dynamic and sophisticated threats, ANNs play a critical role in ensuring the resilience and reliability of IoT systems.

The provided equations are integral to optimising DoS detection accuracy in IoT environments. Each equation and its components work collaboratively to enhance the model's ability to identify and respond to potential threats in network traffic, thereby improving the overall security of IoT.

Weighted Sum (Net Input)

This equation calculates the weighted sum of inputs, such as packet size, source IP address, destination IP address to determine the net input z to a neuron. It combines various features of network traffic, forming the basis for the neuron's activation function, which helps identify patterns indicative of DoS attacks. Equation (1) is represented as follows:

$$z = \sum_{i=1}^{n} w_i \cdot x_i + b \quad (1)$$

Where: z: Net input to the neuron, representing the linear combination of inputs, w_i: Weights assigned to each input feature x_i. These weights determine the importance of each feature in contributing to the decision-making process.

x_i: Input features representing characteristics of network traffic (e.g., packet size, source IP, etc.).

Activation Function (ReLU)

The ReLU activation function transforms the net input z to produce an output If z is positive, it is passed through unchanged; if negative, it is set to zero. This non-linear transformation allows the ANN to learn complex patterns in the data, enhancing its ability to detect subtle anomalies related to DoS attacks. Equation (2) is represented as follows:

$$f(z) = max(0, z) \quad (2)$$

Where: f(z) The output of the activation function, which determines whether the neuron should be activated based on the net input z. z: the net input calculated from the weighted sum of inputs. It reflects the combined influence of all input features.

Loss Function (Binary Cross-Entropy)

The binary cross-entropy loss function measures how well the predicted probabilities ŷ align with the true labels y. . Minimizing this loss during training allows the ANN to improve its predictions, thereby enhancing its ability to distinguish between benign and malicious network traffic. Equation (3) is represented as follows:

$$L(y, \hat{y}) = -\frac{1}{N}\sum_{i=1}^{N} 1\, y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)) \quad (3)$$

Where: L: The loss value that quantifies the difference between the true labels and the predicted probabilities. A lower loss indicates better model performance. y: True labels of the data, y_i=1 indicates a DoS attack and y_i=0 indicates normal traffic. ŷ: Predicted probabilities of a DoS attack from the model, ranging between 0 and 1. N: Total number of samples in the dataset. This normalization ensures the loss is averaged over all samples.

Gradient Descent Update Rule

This equation describes the process of updating the weights in the ANN using gradient descent. By iteratively adjusting the weights based on the loss gradient, the model learns to minimise errors in its predictions, leading to improved detection accuracy for DoS attacks. Equation (4) is represented as follows:

$$w_{new} = w_{old} - \eta \nabla L \quad (4)$$

Where: w_new: The updated weight after applying the gradient descent step, reflecting the adjustments made to improve the model's performance. w_old: The current weight before the update, represents the model's state before adjustment. η: The learning rate, which determines the size of the steps taken towards minimising the loss function. A properly tuned learning rate ensures effective convergence. ∇L: The gradient of the loss function concerning the weights, indicating the direction and magnitude of change needed to minimise the loss. It shows how much each weight should be adjusted to reduce the overall loss.

Output Layer Equation for Probability Estimation

This equation models the final output of the ANN, converting the net input z into a probability ŷ_i that indicates the likelihood of a DoS attack. This probabilistic output is crucial for making informed decisions about network traffic classification, enabling timely responses to potential threats. Equation (5) is represented as follows:

$$\hat{y} = \sigma(z) = \frac{1}{1+e^{-z}} \quad (5)$$

Where: ŷ: Predicted probability of a DoS attack occurring, ranging between 0 and 1, allowing for a clear decision boundary for classification. σ(z): The sigmoid activation function applied to the net input z, transforming the raw output into a probability score. e: The base of the natural logarithm, used in the exponential function to shape the output curve, allows for smooth probability transitions.

2) Random Forest

RF is an ensemble learning algorithm that constructs multiple decision trees during training and outputs the mode of their predictions for classification tasks or the average for regression tasks [31]. Each tree in the forest is trained on a random subset of the data, and features are also randomly selected for each split (See Figure 4). This introduces diversity among the trees and enhances the overall model's robustness.

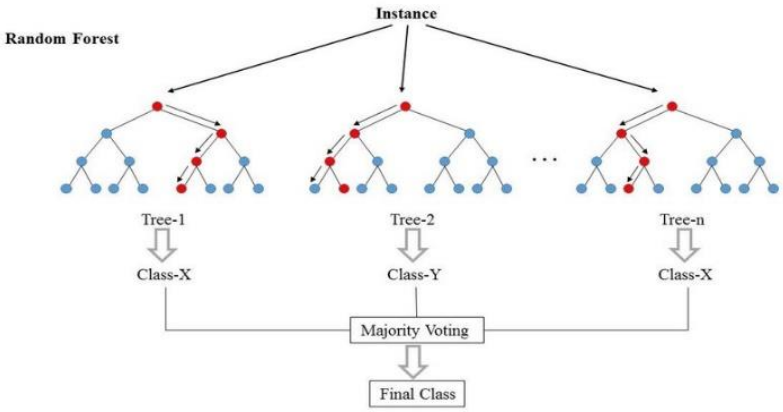

Figure 4. Sequential Process of RF

To minimise FPR, RF uses its ensemble approach, where the final decision is made based on the majority vote from multiple trees. This aggregation helps smooth out individual errors from any single tree, reducing the likelihood that isolated anomalies will incorrectly classify benign instances as attacks. Additionally, RF employs feature importance ranking to focus on the most relevant indicators of DoS attacks, ensuring the model is not misled by noise or irrelevant data. This capability significantly enhances its ability to accurately distinguish between legitimate and malicious traffic.

To minimise FPR in the proposed model using the RF algorithm, we can consider several mathematical formulations that describe the underlying mechanisms of the algorithm. Here are the equations:

Equation for Accuracy

This equation 6 defines accuracy as the ratio of correctly predicted instances (both true positives and true negatives) to the total instances. A higher accuracy indicates better performance, but it can be misleading in cases of class imbalance (e.g., more benign traffic than attacks). Thus, minimising is crucial for improving model performance. Equation (6) is represented as follows:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

Where: TP: True Positives (correctly identified attacks), TN: True Negatives (correctly identified benign instances), FP: FPR (benign instances incorrectly identified as attacks), FN: False Negatives (attacks incorrectly identified as benign).

Precision Formula

Precision measures the ratio of true positive predictions to the total positive predictions (true positives plus FPR). High precision indicates a low FPR, which is vital for applications like intrusion detection systems where misclassifying benign traffic as attacks can lead to unnecessary actions. Equation (7) is represented as follows:

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

Where: TP: True Positive, FP: FPR

F1 Score

The F1 Score is the harmonic mean of Precision and Recall, making it particularly useful in scenarios with imbalanced datasets, where one class (e.g., benign traffic) significantly outweighs the other (e.g., attack traffic). Precision focuses on minimising FPR by ensuring the proposed model is selective about its positive predictions, while Recall emphasises detecting as many true positive cases as possible, thereby minimising False Negatives. By using the harmonic mean, the F1 Score penalises extreme imbalances between Precision and Recall, ensuring the proposed model performs effectively in both aspects and provides a balanced measure of its overall performance. Equation (8) is represented as follows:

$$F1\ Score = 2 . \frac{Precision . Recall}{Precision + Recall} \quad (8)$$

Where: TP: True Positives (correctly identified attacks), FP: FPR (benign instances incorrectly classified as attacks).

Gini Impurity

Gini impurity measures the impurity of a node in a decision tree. Lower values indicate that a node predominantly contains instances of a single class. In RF, minimising impurity while building trees helps reduce the chance of FPR by ensuring that splits create more homogenous groups, thus improving classification accuracy. Equation (9) is represented as follows:

$$Gini = 1 - \sum_{i=1}^{C} (p_i)^2 \quad (9)$$

Where: C: The total number of classes in the dataset (e.g., benign, attack). p_i: The proportion (probability) of instances belonging to class i in the node.

Out-of-Bag (OOB) Error Estimate

OOB error is an internal cross-validation method used in RF to estimate the model's error without needing a separate validation set. By utilising trees that did not include a specific instance in their training, this method helps identify FPR and improve model robustness by refining predictions based on error analysis from multiple trees. Equation (10) is represented as follows:

$$OOB\ Error = \frac{1}{N} \Sigma_{i=1}^{N} \hat{y}_j \neq y_j \quad (10)$$

N: Number of instances in the dataset, y^_j: Predicted class for instance j using trees that did not include j in their training set, y_j: Actual class for instance j.

3) ANN-RF algorithm

ANN and RF were integrated when designing the proposed ANN-RF algorithm to enhance DoS detection accuracy while minimising FPR in IoT environments as outlined in Algorithm 1.

```
1. Step 1: Initialize the Neural Network
2. BEGIN
3. SET learning_rate = η;
4. SET num_epochs = <number_of_epochs>;
5. SET weights = RANDOM_INITIALIZATION();
6. SETactivation_function= <activation_function>;
7. SET loss_function = <loss_function>;
8. Step 2: Training Phase
9.   FOR epoch IN 1 TO num_epochs DO
10.  FOR each_training_sample x DO
11. Step 2.1: Calculate net input
12. SET net_input z = SUM(w[i] * x[i]) + b; -- Equation 1
13.  Step 2.2: Calculate activation output
14. SET activation_output f(z) = MAX(0, z); Equation 2
15.  Step 2.3: Calculate predicted probability
16. SET predicted_probability ŷ = 1 / (1 + EXP(-z)); -- Equation 5
17.  Step 2.4: Calculate loss
18.   SET loss L = -1 / N * SUM(y[i] * LOG(ŷ[i]) + (1 - y[i]) * LOG(1 - ŷ[i])); -- Equation 3
19.  Step 2.5: Compute gradients
20. FOR each_weight w[j] DO
21.  SET gradient ∇L = <calculate_gradient>(); -- Define how to calculate gradient
22.  Step 2.6: Update weights
23.  SET w_new = w_old - η * ∇L; Equation 4
24.  END FOR;
25.  END FOR;
26.    Step 3: Evaluate the Performance of the ANN
27.    SET accuracy = (TP + TN) / (TP + TN + FP + FN); -- Equation 6
28. SET precision = TP / (TP + FP);Equation 7
29.    SET f1_score = 2 * (precision * recall) / (precision + recall); -- Equation 8
30.     Step 4: Initialize Random Forest
31.    SET num_trees = T;
32.    FOR tree_index IN 1 TO num_trees DO
33.  SET sampled_data= RANDOM_BOOTSTRAP_SAMPLING();
34. Step 4.1: Build tree
35. FOR each_node DO
36. SET gini_impurity = 1 - SUM(p[i]^2); -- Equation 3.9
37. IF <node_can_be_split> THEN
38. SPLIT_NODE_ON_FEATURE_IMPORTANCE();
39.  END IF;
40.  END FOR;
41.   END FOR;
42.    Step 5: Evaluate the Random Forest Model
43. SET oob_error = 1 / N * SUM(ŷ_j ≠ y_j); -- Equation 10
44. Analyze performance metrics
45. Step 6: Output Final Predictions and Performance Metrics
46 OUTPUT (predictions, performance_metrics);
47. END;
```

By integrating ANN and RF, the proposed algorithm can intelligently detect DoS attacks, optimise detection accuracy, and minimise FPR, leveraging the

strengths of both models for enhanced performance in identifying and mitigating DoS threats effectively.

D. Simulation Results

This paper introduces the ANN-RF hybrid algorithm as an effective approach for detecting DoS attacks in IoT environments. The algorithm combines the advanced pattern recognition capabilities of ANN with the robust ensemble learning strengths of RF, resulting in enhanced detection accuracy, reduced false FPR, and improved latency performance. By leveraging multi-dimensional network traffic data, the ANN-RF model significantly improves the classification and monitoring of DoS attacks, offering a scalable and reliable solution for real-time threat detection in IoT systems.

The ANN-RF algorithm represents a comprehensive machine learning approach that addresses key challenges in IoT security. It effectively integrates supervised learning techniques with intelligent traffic analysis to identify anomalous behaviours that signal potential DoS threats. The simulation results demonstrate that the ANN-RF model outperforms standalone ANN and RF models across all evaluated metrics. Notably, the hybrid model achieved a detection accuracy of 93%, compared to 87% and 82% for RF and ANN respectively. The ANN-RF model also achieved the lowest FPR at 5%, significantly reducing the risk of false alarms.

In terms of latency, the ANN-RF algorithm consistently exhibited faster processing times, beginning at 15 milliseconds for 10 active devices and rising to only 45 milliseconds at 70 devices. This performance was superior to RF (20–50 ms) and ANN (25–55 ms), demonstrating its suitability for real-time detection scenarios.

Simulations were conducted in MATLAB, and the system was configured to test performance under varying traffic volumes. The simulation setup, aligned with network evaluation standards, used synthetic attack datasets and varied the number of devices from 10 to 70 to assess scalability. The experimental framework was designed to reflect realistic IoT environments, enabling accurate benchmarking of detection performance, FPR, and latency.

Figures 5 to 7 in the results section illustrate the effectiveness of the ANN-RF model across all test parameters. The model consistently maintained high detection accuracy, low FPR, and minimal latency as network traffic increased. These outcomes affirm the model's robustness and adaptability, establishing it as a practical solution for enhancing security in IoT-based systems.

Table 1. Simulation Parameters

Days	Labels
Monday	Benign
Tuesday	BForce,SFTP and SSH
Wednesday	DoS and Hearbleed Attacks slowloris, Slowhttptest, Hulk and GoldenEye
Thursday	Web and Infiltration Attacks Web BForce, XSS and Sql Inject. Infiltration Dropbox Download and Cool disk

Friday	DoS LOIT, Botnet ARES, PortScans (sS,sT,sF,sX,sN,sP,sV,sU, sO,sA,sW,sR,sL and B)

Average DoS Detection Accuracy

Figure 5 depicts the evaluation of Average DoS Detection Accuracy for the ANN-RF hybrid model, the RF algorithm, and the ANN algorithm under varying traffic volumes, represented by the number of active devices. The results reveal significant insights into the performance of these detection mechanisms across different network loads. The ANN-RF hybrid model consistently demonstrated the highest detection accuracy across all tested traffic volumes. Specifically, it achieved an accuracy of 75% at a low traffic volume of 10 devices, which progressively improved to 93% at the highest volume of 70 devices, illustrating its adaptability to increased network load. In comparison, the RF algorithm showed a steady improvement, starting at 70% with 10 devices and reaching 87% at 70 devices. The ANN algorithm, while the least accurate, improved from 65% at 10 devices to 82% at the highest volume. These results, as shown in Figure 5, underscore the superior performance of the ANN-RF hybrid model in detecting DoS attacks, particularly as network traffic intensifies. The model's integration of ANN's advanced pattern recognition with RF's ensemble learning enhances its ability to adapt to evolving attack patterns, providing a robust and scalable solution for improving security in IoT environments.

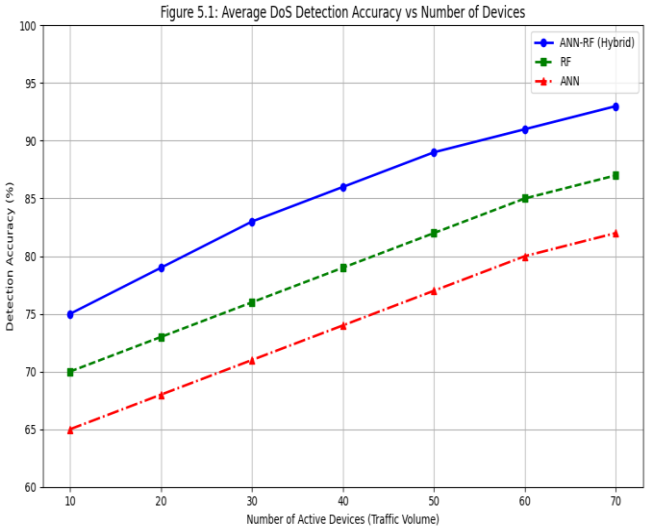

Figure 5. Average DoS detection vs Traffic Volume

False Positive Rate

Figure 6 depicts the performance evaluation of the proposed ANN-RF hybrid algorithm in detecting DoS attacks demonstrates its superiority over traditional models such as the ANN and RF. The ANN-RF model achieved a FPR of 5% when detecting 30 attacks, significantly outperforming the ANN, which had an FPR of 15% while detecting 30 attacks, and the RF, which recorded an FPR of 10% when detecting the same 30 attacks. As the number of attacks detected increased, the ANN-RF model consistently maintained a lower FPR, thereby reducing the

incidence of false alarms and enhancing the reliability of DoS attack detection. In contrast, the ANN and RF models exhibited higher FPR values, indicating a greater likelihood of misclassifying legitimate requests as attacks. This evidence underscores the effectiveness of the ANN-RF hybrid approach in optimising security measures in IoT environments, making it a robust solution for mitigating cyber threats.

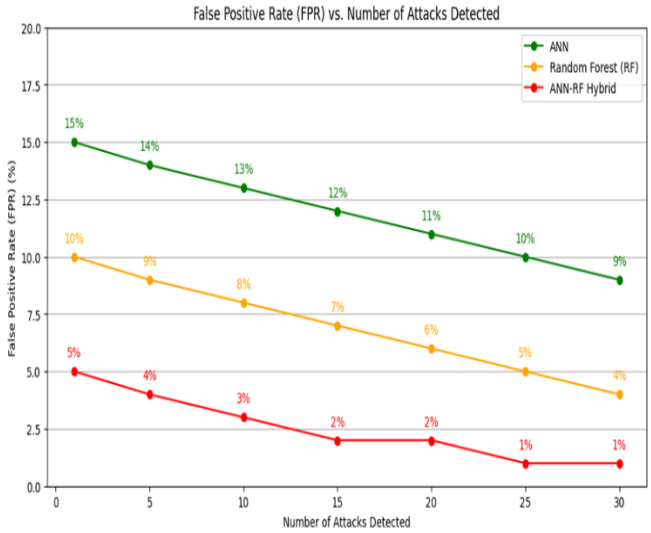

Figure 6. FPR Vs Threshold

Average Latency

Figure 7 depicts the latency analysis of the ANN-RF, RF, and ANN algorithms reveals significant differences in their computational performance as traffic volume increases. The results indicate that the ANN-RF hybrid algorithm consistently exhibits the lowest latency across all tested traffic volumes, starting at 15 milliseconds for 10 active devices and rising to 45 milliseconds for 70 devices. In comparison, the RF algorithm demonstrates moderate latency, beginning at 20 milliseconds with 10 devices and reaching 50 milliseconds at the highest volume. The ANN algorithm, on the other hand, has the highest latency values, starting at 25 milliseconds and increasing to 55 milliseconds as traffic volume increases, as shown in Figure 7. These findings underscore the ANN-RF algorithm's efficiency in handling higher traffic loads while maintaining responsiveness, making it particularly suitable for real-time applications in IoT environments.

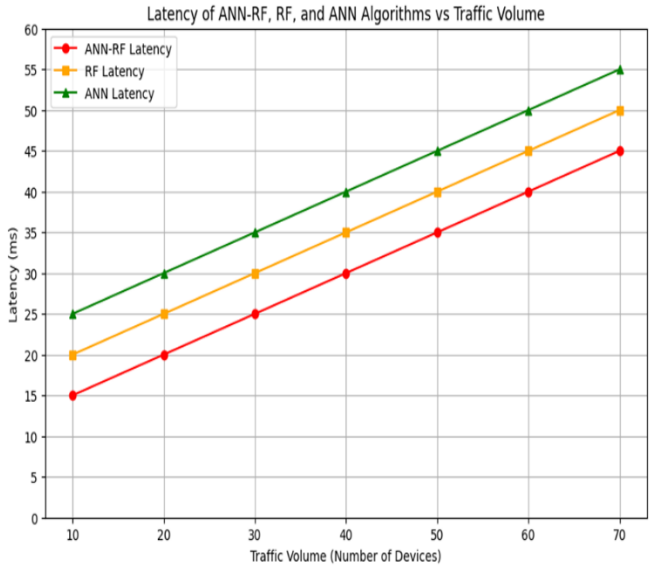

Figure 7. Latency Comparison vs. Traffic Volume

E. Conclusion And Future Work

This paper presented the ANN-RF hybrid algorithm as an effective solution for enhancing the detection of DoS attacks in IoT. By integrating ANN and RF classifiers, the model leverages the pattern recognition capabilities of ANN with the robustness and ensemble learning strengths of RF. The simulation results, conducted using MATLAB, demonstrated that the ANN-RF model significantly outperforms standalone ANN and RF models in terms of detection accuracy, false positive rate (FPR), and latency. Specifically, the hybrid model achieved a maximum detection accuracy of 93%, reduced FPR to 5%, and exhibited the lowest latency across increasing traffic volumes. These findings underscore the model's ability to adapt to network load variations and evolving attack patterns, offering a robust and scalable approach to improving IoT security in areas such as smart homes, healthcare, and industrial control systems.

Future work will focus on further enhancing the ANN-RF model by incorporating additional datasets, including real-world traffic and zero-day attack scenarios, to improve its generalisability. Moreover, the integration of advanced data preprocessing techniques and feature engineering methods will be explored to further reduce false positives. Additional efforts will be made to implement the model in real-time IoT environments using edge computing frameworks, enabling faster threat detection with minimal computational overhead. Finally, comparative studies with emerging deep learning architectures, such as transformer-based models and federated learning frameworks, will be conducted to evaluate the scalability and performance of the ANN-RF approach in large-scale, distributed IoT systems.

F. Acknowledgment

The authors express their sincere gratitude to the reviewers for their insightful comments and constructive feedback, which significantly improved the quality of this paper and supported its successful completion.

G. References

[1] Akpakwu, G.A., et al., Congestion control in constrained application protocol for the Internet of Things: State-of-the-art, challenges, and future directions. IEEE Access, 2025. 13: p. 33733-33767.

[2] Akpakwu, G.A., and Mathonsi, T.E., Markov model-based congestion control for the internet of things. Edelweiss Applied Science and Technology, 2025. 9(7): p. 1187–1204..

[3] Syed, A.S., et al., IoT in smart cities: A survey of technologies, practices and challenges. Smart Cities, 2021. 4(2): p. 429-475.

[4] Mihoub, A., et al., Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Computers & Electrical Engineering, 2022. 98: p. 107716.

[5] Tsiknas, K., et al., Cyber threats to industrial IoT: a survey on attacks and countermeasures. IoT, 2021. 2(1): p. 163-186.

[6] Stuma, V.S. and Mathonsi, T.E., A security algorithm to prevent denial of service attacks in the internet of things devices. 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET), Sydney, Australia, 2024: p. 1-6.

[7] Alabdulatif, A., N.N. Thilakarathne, and M. Aashiq, Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System. Computers, Materials & Continua, 2024. 80(3).

[8] Bukhowah, R., A. Aljughaiman, and M.H. Rahman, Detection of dos attacks for IoT in information-centric networks using machine learning: Opportunities, challenges, and future research directions. Electronics, 2024. 13(6): p. 1031.

[9] Aslan, Ö., et al., A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 2023. 12(6): p. 1333.

[10] Mishra, N. and S. Pandya, Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 2021. 9: p. 59353-59377.

[11] Silas, W.A., L. Nderu, and D. Ndirangu, A distributed framework for distributed denial-of-service attack detection in internet of things environments using deep learning. International Journal of Web Engineering and Technology, 2024. 19(1): p. 67-87.

[12] Baloyi, C., et al., Machine Learning-Based Security Algorithms for Detecting and Preventing DDoS Attacks on the IoT: State-of-the-Art, Challenges, and Future Directions. The Indonesian Journal of Computer Science, 2025. 14(3).

[13] Shah, Z., et al., Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors, 2022. 22(3): p. 1094.

[14] Srivastava, A., et al., Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. International Journal of Communication Systems, 2020. 33(12): p. e4443.

[15] Siwakoti, Y.R., et al., Advances in IoT security: Vulnerabilities, enabled criminal services, attacks, and countermeasures. IEEE Internet of Things Journal, 2023. 10(13): p. 11224-11239.

[16] Asharf, J., et al., A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics, 2020. 9(7): p. 1177.
[17] Alashhab, A.A., et al., Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model. IEEE access, 2024. 12: p. 51630-51649.
[18] Tayyab, M., B. Belaton, and M. Anbar, ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review. IEEE Access, 2020. 8: p. 170529-170547.
[19] Ghadi, Y.Y., et al., Enhancing smart grid cybersecurity: a comprehensive analysis of attacks, defenses, and innovative AI-blockchain solutions. 2023.
[20] Khaleel, Y.L., et al., Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods. Journal of Intelligent Systems, 2024. 33(1): p. 20240153.
[21] Gurram, M.R., Meta-Learning-Based Model Stacking Framework for Hardware Trojan Detection in FPGA Systems. 2024.
[22] Kumari, P. and A.K. Jain, A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security, 2023. 127: p. 103096.
[23] Santos, R., et al., Machine learning algorithms to detect DDoS attacks in SDN. Concurrency and Computation: Practice and Experience, 2020. 32(16): p. e5402.
[24] Altulaihan, E., M.A. Almaiah, and A. Aljughaiman, Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. Sensors, 2024. 24(2): p. 713.
[25] Mansoor, A., et al., Deep learning-based approach for detecting DDoS attack on software-defined networking controller. Systems, 2023. 11(6): p. 296.
[26] Fatima, M., et al., Towards Ensemble Feature Selection for Lightweight Intrusion Detection in Resource-Constrained IoT Devices. Future Internet, 2024. 16(10).
[27] Rustam, F., et al., Denial of service attack classification using machine learning with multi-features. Electronics, 2022. 11(22): p. 3817.
[28] Aswad, F.M., et al., Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks. Journal of Intelligent Systems, 2023. 32(1): p. 20220155.
[29] Najar, A.A. and S.M. Naik, Cyber-secure SDN: A CNN-based approach for efficient detection and mitigation of DDoS attacks. Computers & Security, 2024. 139: p. 103716.
[30] Gopi, R., et al., Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. Multimedia Tools and Applications, 2022. 81(19): p. 26739-26757.
[31] Salman, H.A., A. Kalakech, and A. Steiti, Random forest algorithm overview. Babylonian Journal of Machine Learning, 2024. 2024: p. 69-79.