British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 51-70)
www.abjournals.org

MACHINE LEARNING FOR DETECTING DoS ATTACK: A COMPARATIVE APPROACH

Bright Gazie Akwaronwu[1], Innocent Uche Akwaronwu[2], and Oluwabamise Joseph Adeniyi[3]

[1]Department of Computer Science, Babcock University, Ilishan Remo, Nigeria.
Email: akwaronwu0329@pg.babcock.edu.ng

[2]Department of Industrial and Systems Engineering, The university of Alabama in Huntsville, Alabama, USA.
Email: iua0001@uah.edu

[3]Department of Computer Science, Babcock University, Ilishan Remo, Nigeria.
Email: adeniyi0416@pg.babcock.edu.ng

Cite this article:

Akwaronwu, B. G., Akwaronwu, I. U., Adeniyi, O. J. (2025), Machine Learning for Detecting DoS Attack: A Comparative Approach. British Journal of Computer, Networking and Information Technology 8(2), 51-70. DOI: 10.52589/BJCNIT-I0V0HK0Y

Manuscript History

Received: 11 Apr 2025

Accepted: 14 May 2025

Published: 30 May 2025

Copyright © 2025 The Author(s). This is an Open Access article distributed under the terms of Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0), which permits anyone to share, use, reproduce and redistribute in any medium, provided the original author and source are credited.

ABSTRACT: *Denial-of-Service (DoS) attacks has been a critical challenge in cybersecurity, disrupting the availability of network services and causing significant operational and economic losses. To ascertain the most suitable approaches to mitigate to dilemma, this study compares the effectiveness of some selected machine learning models in identifying denial-of-service (DoS) attacks. Two ensemble learning models, Random Forest (RF) and Extreme Gradient Boosting (XGB), showed remarkable accuracy and dependability. RF performed almost perfectly on criteria including accuracy (99%), precision (99%), and recall (99%). Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) stood out as Deep Learning models, capturing complex patterns with CNN achieving an accuracy of 98% and a perfect AUC score of 1.00. The models utilized the Recursive Feature Elimination (RFE) to select significant features and ensured proper data balancing techniques for robust model training and evaluation, minimizing overfitting and enhancing generalization. The results highlight RF and CNN as the best-performing models, with RF offering interpretability and computational efficiency, while CNN excels in handling unstructured and complex datasets. This study underscores the need for context-driven model selection and suggests exploring hybrid approaches that integrate the strengths of ML and DL for improved DoS attack detection. Future work should aim to enhance scalability and adaptability for real-world cybersecurity applications.*

KEYWORDS: Denial-of-Service (DoS) Attacks, Machine Learning, Random Forest, Convolutional Neural Network, Feature Selection, Cybersecurity, Model Performance Analysis.

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 51-70)
www.abjournals.org

INTRODUCTION

Denial-of-Service (DoS) attacks is a prominent cyber-attack that aims at distorting computer networks, system or service and tend to render these facilities unavailable to its legitimate owners or users(Arroyabe et al., 2024). The core features of cyber systems are the Confidentiality, Integrity and Availability, which forms the CIA Triad in cybersecurity (Osazuwa, 2023; Qadir & Quadri, 2016).

Just as the name sounds, denial of service encompasses an attack that is launched to deny a required service that is progressively in operation. Intruders achieve a successful Denial of service attack by flooding the target system/service from a single source as seen in Figure 1, with multiple requests that are not part of the operations of the service or systems (Islam et al., 2021; Kumar, 2016). These illegitimate flooding overwhelms the operation of the system and interrupt normal operations of the system thereby denying the legitimate user(s) adequate usage or access to the system (Islam et al., 2021).

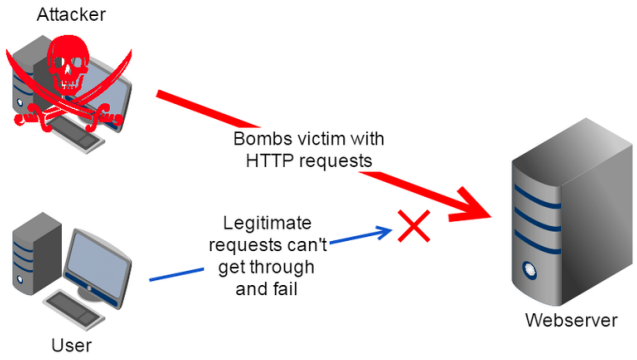

Figure 1: DoS Attack Flow (Suryateja, 2018)

DoS attack has a chronic effect on cyber industry and has been a challenge for many years (Gebreyes, 2020). It effect extend to the exhaustion of network bandwidth, memory, or CPU capacity, leading to a service outage (Eliyan & Di Pietro, 2021; Okeh et al., 2023). The fact that cyber systems progressive function on a feature of network dependency is a significant prospect for DoS attack to strive across the system (Uddin et al., 2024).

The focus of intruders in utilizing DoS attacks are vulnerabilities in server configurations, network protocols and firewalls (Balarezo et al., 2022). When this attack is distributed through multiple channels, it becomes more complex to mitigate and easier to compromise a system (Tuli et al., 2022). This organized form of system attack is called Distributed Denial of Service (DDoS) attack (Eliyan & Di Pietro, 2021; A. Singh & Gupta, 2022).

The progressive growth of DoS attack calls for more adequate and more advanced model suitable for detecting and mitigating the impact of this cyber threat (Sathishkumar et al., 2024). Machine learning (ML) models are viable tools and they are capable of analysing traffic patterns, network behaviour, and anomaly detection in real-time (S. F. Ahmed et al., 2023; Akwaronwu et al., 2025; Sathishkumar et al., 2024; Shargunam & Rajakumar, 2022). Bringing these models together will enhance the speed of identifying the best model suitable for mitigating this attack (Owaid & Hammoodi, 2024; Talafha et al., 2021).

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

Most ML have been utilized in mitigating the impact DoS attacks by analysing network traffic patterns and other pattern indicators (Owaid & Hammoodi, 2024). Models like Random Forest, Logistics Regression and Support Vector Machines (SVM) which are Machine learning models are widely used for classification of anomalies and benign in detecting DoS attacks (Kiranashree et al., 2021). However, these models may not capture all attack patterns (Ahmad et al., 2018; Natarajan et al., 2024; Sarker, 2021b). Deep learning models, such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), enhance accuracy by effectively capturing intricate data patterns. However, they often require significant computational resources (S. F. Ahmed et al., 2023; Alzubaidi et al., 2021; Sarker, 2021a).

This comparative approach is vital in selecting the appropriate technique that is required for various environments, it will also resolve the problem of model complexity, speed, and resource consumption and give an accurate performance measure using the prescribed performance measures to estimate the most preferred approach for prompt and effective detection of DoS attack (Al-Shareeda et al., 2023; Azevedo et al., 2024; Tien et al., 2022).

RELATED WORKS

Denial-of-Service (DoS) attacks pose significant threats to the availability of cyber services (D. Singh & Uma Mageswari, 2025), It overwhelm cyber systems with malicious request that hinders legitimate users from accessing cyber services (Asadi et al., 2024). The use of traditional approaches such as signature-based and rule-based systems, yielded inadequate protection caused by their inability to adapt to complex patterns (Admass et al., 2024; Mahjabin et al., 2017). Subsequently, there are increasingly numbers of Machine Learning approaches, driven by deep learning and machine learning, which offer adequate solutions for identifying complex patterns in real-time (Sarker, 2021a).

A. Mechanisms in DoS Attack Detection

Mechanism in detecting DoS attacks are classified into Machine Learning and traditional approach (N. Ahmed et al., 2024). Application of Machine Learning mechanism has enhanced mitigating cyber-attacks like Denial-of-Service (DoS), brute force, dictionary, and several more (Agrafiotis et al., 2018; Bendovschi, 2015). Mitigating cyberattack with any of these approach depends of the severity of the DoS attack(s) and the urgent requirement of the mitigation (Ainslie et al., 2023).

I. Traditional Machine Learning

Traditional Machine Learning (ML) serves as a fundamental approach for detecting Denial-of-Service (DoS) attacks, utilizing algorithms that analyze historical data to recognize patterns and detect anomalies suggestive of an attack. Methods like Decision Tree, Naïve Bayes, Support Vector Machine (SVM), and logistic regression are good at categorizing network traffic by examining characteristics like protocol type, frequency, and packet size (Hulayyil et al., 2023; Qaid et al., 2021). These models are computationally efficient and suitable for environments with limited resources. However, they may require extensive feature engineering to effectively capture complex or evolving attack patterns.

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

II. Ensemble Learning

The use of ensemble models enhances DoS attack detection by merging multiple learners to build a strong predictive model. By aggregating decisions from various base models, ensemble methods improve generalization to new and complex data while the parameters are finetune to overcome overfitting. XGBoost is remarkable for its efficiency, scalability, and ability to manage "Not a Number" (NaN) or imbalanced data, making it well-suited for real-world network environments (Al-Jarrah et al., 2016; Moustafa et al., 2019). However, ensemble models may require careful hyperparameter tuning to achieve optimal performance.

III. Deep Learning

Deep Learning (DL) models are unique models that offers substantial techniques in DoS attack detection by learning sophisticated patterns from raw network traffic data. Models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Artificial Neural Networks (ANNs) and several more, are linked with advanced modules such as Long Short-Term Memory (LSTM) to enhance the training and learning process units excel in analysing spatial and temporal characteristics of network logs (Mercuri et al., 2023; Şahin et al., 2021). CNNs are proficient at identifying static features, while RNNs capture sequential dependencies, making them effective against sophisticated and evolving DoS attacks. The computational complexity and large training data requirements of DL models aids the accuracy in spite of their restricted use in settings with limited resources (L. Chen et al., 2022).

A primary concern in using ML models for DoS detection is overfitting, which arises when models learn noise in the data rather than generalizable patterns. Balanced sampling techniques, such as downsizing datasets to equalize class distributions, have been effective in addressing this issue (Akwaronwu et al., 2025; Barbierato & Gatti, 2024). Additionally, standardizing input features ensures that models are not biased toward high-magnitude variables, further improving generalization (Barbierato & Gatti, 2024; Mohamed, 2023).

B. Feature Engineering

A basic factor that determines the success of model training and accuracy in machine learning and deep learning is the proper application of feature selection. Data preprocessing embeds feature selection which involves identifying and retaining the most significant features among other features in the dataset. By focusing on the most important attributes, feature selection improves model interpretability, reduces computational complexity, and enhances predictive performance by minimizing noise in the data (Crombé et al., 2022). This approach is particularly useful in cases involving high-dimensional datasets, where an excessive number of features may result in overfitting and reduced model effectiveness. Feature selection techniques are generally classified into three categories: filter methods, which assess features independently of the learning model; wrapper methods, which iteratively choose features based on their influence on model performance; and embedded methods, which incorporate feature selection within the model training process. Two widely used feature selection techniques are Recursive Feature Elimination (RFE) and Principal Component Analysis (PCA), both of which help refine the feature set and maintain a balance between efficiency and accuracy before proceeding to the training phase (Abdelwahab et al., 2022; Alabassi et al., 2022; "Loan Prediction System," 2023).

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 51-70)
www.abjournals.org

I. Recursive Feature Elimination (RFE)

Recursive Feature Elimination (RFE) is a special technique that iteratively identifies the most important features by fitting a model and removing the least significant ones. RFE starts with the entire set of features, rates them according to how much they contribute to the model's performance, and then removes features that do not have much of an impact (C. Chen et al., 2024). This process is repeated until a predetermined number of features that are considered the most pertinent. This approach is very useful training predictive models. RFE provides robust performance by reducing noise and irrelevant data in the feature space (Gaber et al., 2022; He et al., 2023).

II. Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is an unsupervised dimensionality reduction technique that converts the original set of features into a new set of orthogonal components known as principal components. These components are designed to retain the maximum variance within the dataset, with the initial components usually accounting for the majority of the variance (Qureshi et al., 2021). PCA reduces the dimensionality of data while preserving as much information as possible. This makes it ideal for huge datasets that have correlated features. Unlike RFE, PCA does not rely on a predictive model but instead focuses on compressing the data structure, which is particularly useful for enhancing the computational efficiency and generalization of predictive models (Beattie & Esmonde-White, 2021).

C. OSI Models' Rule in Network Traffic Management

The seven layers of the Open Systems Interconnection (OSI) highlighted in Figure 2 has a fundamental role in network operations with each layer fulfilling its own purpose in a connected network framework. The OSI model follows a specific procedure to transport data from one level to another, from the user in the host layer to the physical server in the media layer and back again (Howser, 2020).

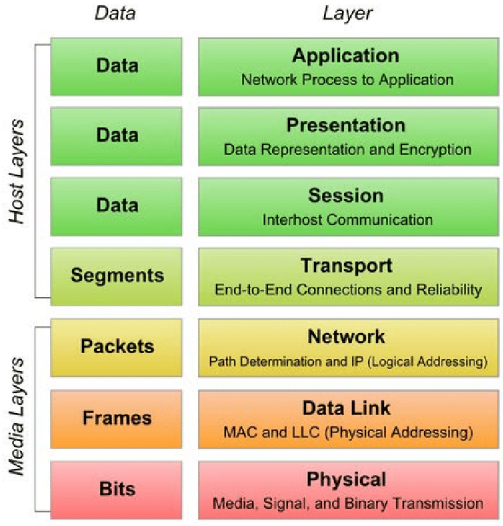

Figure 2: OSI Layer Media and Host Layer (Eduardo Márquez Díaz, 2021)

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

The layers carry protocols that is unique from one layer to the other with makes the traffics unique and responsible for sending/receiving protocol data unit (PDU). These protocols ensure that each layer is assigned their stipulated functions.

D. Research Gaps

Denial-of-Service (DoS) attacks are significant threat to cybersecurity because utilize vulnerability to exploit network infrastructures and flood services with unauthorized requests, making cyber services unavailable to authorized operators. The impact of these attacks is far-reaching, leading to substantial operational disruptions, economic losses, and reputational damage to organizations. Modern DoS attacks are too complex for traditional defenses like firewalls to detect and stop, especially as attackers use more complex techniques like Distributed Denial-of-Service (DDoS) attacks, which spread the attack across several sources (Kumar, 2016; Najafimehr et al., 2023).

While Machine Learning techniques have exhibited promissory performance in detecting DoS attacks by analysing network traffic patterns and anomalies, a key challenge lies in identifying the most effective approach for real-time detection (J. O. et al., 2025). Models such as Random Forest and Support Vector Machines have been widely used, but they may not capture all complex attack patterns and could suffer from limitations in accuracy (Najafimehr et al., 2023; Onuiri et al., 2024). Meanwhile, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) which standouts as deep learning models, offer improved detection capabilities but are often computationally intensive, resulting to complications in model development and deployment (Ersavas et al., 2024).

There is a critical need for a comprehensive comparison of Machine Learning (ML) and Deep Learning (DL) techniques to determine which models are best suited for detecting DoS attacks in various environments (Ali et al., 2023). Factors such as detection accuracy, computational efficiency, real-time applicability and several more are to be considered. This study seeks to provide remedy to this gap by carrying out a comparative analysis of ML and DL models to identify the optimal method for detecting DoS attacks, taking into account the complexities of different network environments, the speed of detection, and resource consumption.

The integration of feature selection techniques like RFE with robust classifiers such as SVM, promise in enhancing the detection of DoS attacks. The adoption of data preprocessing methods, balanced datasets, and careful evaluation through visual metrics (e.g., confusion matrices, ROC curves) is crucial for developing models capable of real-world deployment.

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 51-70)
www.abjournals.org

METHODOLOGY

This research will utilize the principle of machine learning research framework that acquires data, preprocess, train, and evaluate the trained model using standard evaluation metrics. This framework as expanded in figure 3 gives a clarity of the mothodology and highlights the number of models that will be utilized in the proposed system.

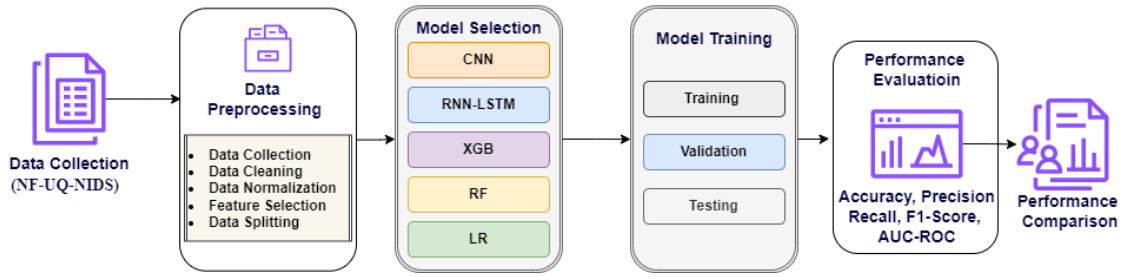

Figure 3: Model Architecture

A. Data Description

The dataset is that will be utilized for this models is "NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems" (NF-UQ-NIDS) (Sarhan et al., 2021), acquired from the university of Queensland with varying DoS attack vectors which include Hulk, Slow-HTTP-Test, attacks-Golden-Eye and several more categorized as parent DoS category with 348962 DoS vectors and 9208048 Benign operations among others.

The dataset contains feature which are; Source and destination IPv4 addresses, layer 4 Source and destination port numbers, layer 3 network protocol, layer 7 protocol, Numbers of bytes sent and received in the flow, Number of packets sent and received in the flow, total duration of the network flow.

B. Data Preprocessing

The data preprocessing encompasses every activity done on the data to prepare it ahead of the training which include cleaning, normalization, feature selection, and splitting and it likes. This is aimed at preparing the data for the training process in the model development phase.

To guarantee high-quality input for model development, data cleaning will find and fix mistakes, inconsistencies, and missing values in the dataset. This process includes handling missing data using imputation techniques, removing duplicate records, and correcting anomalies or outliers that may skew model performance. The next crucial step is data normalization, which scales feature values into a uniform range, usually between 0 and 1. During model training, this makes sure that characteristics with bigger magnitudes don't overpower those with smaller magnitudes.

To find the most pertinent characteristics for the prediction task, less significant features will be progressively removed using Recursive Feature Elimination (RFE) as depicted in Figure 4 and 5. This approach entails training an initial model and allocating weights to features according to their impact on predictive accuracy. Features with the least significance are progressively removed in an iterative process until the most effective subset is determined.

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 51-70)
www.abjournals.org

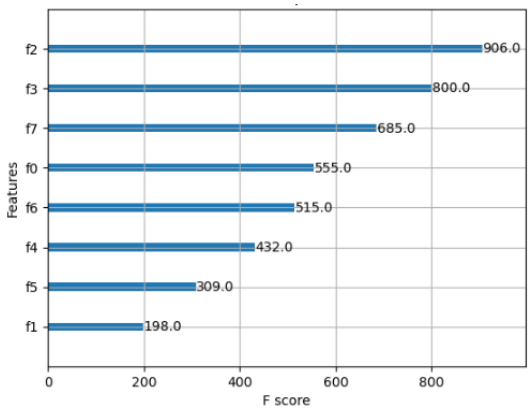

Figure 4: Feature importance scaling

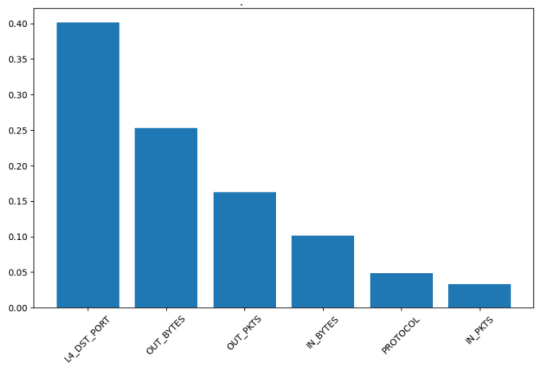

Figure 5: Feature Importance hierarchy

The dataset is generally partitioned into three subsets: training, testing, and validation. The training set consists of 70% of the data, while the remaining 30% is evenly split between testing and validation. This systematic division helps ensure that the model's performance remains objective and accurately represents real-world conditions.

C. Model Building process

The model will utilize Python as the main programming language, while utilizing its extensive libraries like NumPy, Pandas, Scikit-learn, Matplotlib, Seaborn, and Joblib, which are essential for data preprocessing, model training, evaluation, visualization, and deployment. Jupyter Notebook will serve as the primary integrated development environment (IDE) for scripting, documentation, and iterative experimentation due to its user-friendly interface and support for interactive computing. Figure 6 showcases the model that will be used for this training representing the traditional machine learning models, deep learning models and ensemble machine leaning models.

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 51-70)
www.abjournals.org

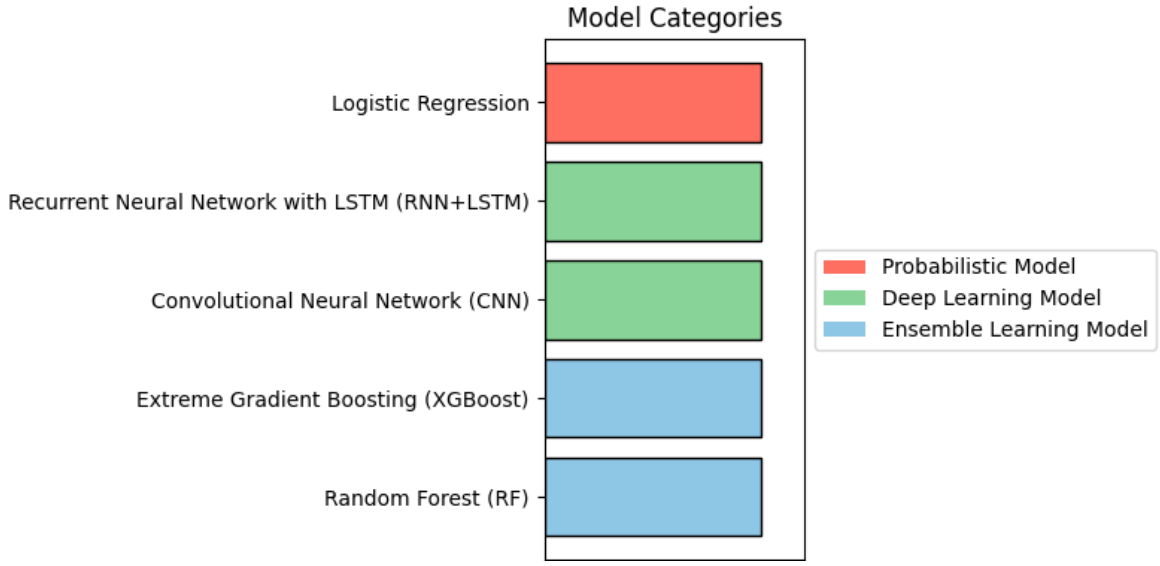

Figure 6: Training Model Categories

Machine Learning models in their various categorise play critical roles in DoS attack detection, they utilize advanced algorithms and techniques to identify and mitigate malicious network activity, with unique strengths and limitations tailored to different computational and environmental needs.

i. Logistic Regression

Logistic Regression models the probability of an input belonging to a particular class (DoS attack or benign) by applying the sigmoid activation function to a linear combination of input features. The prediction probability is given by (1):

$$p = \sigma(z) = \frac{1}{1 + e\text{^}(-z)} \quad (1)$$

$$z = w^T x + b \quad (2)$$

where w representing the weight vector, x the input features, and b the bias term. This probabilistic output enables the model to interpret network traffic data and classify whether a given instance is indicative of a DoS attack.

Training optimization is achieved through the Binary Cross-Entropy loss function, expressed as BCE (3):

$$BCE = -(y * \log(p) + (1 - y) * \log(1 - p)) \quad (3)$$

where y denotes the true label (0 for benign, 1 for DoS attack), and p is the model's predicted probability.
This loss function penalizes incorrect predictions and drives the model toward maximizing classification accuracy. The combination of linear decision boundaries and probabilistic interpretation underpins Logistic Regression's ability to effectively distinguish between benign and malicious traffic patterns in network intrusion detection systems.

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 51-70)
www.abjournals.org

ii. Recurrent Neural Network (RNN) with LSTM

The Long Short-Term Memory (LSTM) network enhances traditional RNNs by addressing the vanishing gradient problem, enabling effective learning over long sequences. The core operation of the LSTM cell is governed by the cell state update equation (4):

$$c_t = f_t * c_{t-1} + i_t * g_t \quad (4)$$

where c_t represents the current memory cell state, f_t is the forget gate output controlling memory retention, i_t is the input gate output regulating new information entry, and g_t denotes the candidate memory update.
This mechanism enables the LSTM to dynamically remember or forget patterns over time, making it well-suited for analyzing sequential network traffic data where temporal patterns of DoS attacks may span across multiple packet flows.

Training optimization is achieved using the Binary Cross-Entropy (BCE) loss function, expressed as (3). the loss function effectively guides the LSTM toward minimizing classification errors, promoting high recall and accuracy in detecting distributed or time-staggered DoS attacks.

iii. Convolutional Neural Network (CNN)

The fundamental convolution operation, expressed as output (2) enables the model to detect suspicious traffic patterns regardless of their position within the input sequence.

$$Output(i) = \sum_{j=0}^{k-1} \big(Input(i+j) \times Filter(j)\big) + Bias \quad (5)$$

This translation invariance property proves particularly valuable for network traffic analysis, where attack signatures may appear at varying temporal positions. The model's hierarchical feature extraction process begins with the first Conv1D layer detecting basic network traffic patterns, while the second Conv1D layer combines these foundational elements into more complex attack signatures. Training optimization is achieved through the Binary Cross-Entropy loss function, defined as BCE (3) to guide the model toward accurate DoS attack detection, contributing to the model's exceptional performance in classifying DoS attacks.

iv. Extreme Gradient Boosting (XGBoost)

XGBoost employs an additive boosting strategy, sequentially improving model performance by training new decision trees to predict residual errors from prior models. The update rule for the ensemble model is defined as (5):

$$F_{m(x)} = F_{(m-1)(x)} + h_{m(x)} \quad (6)$$

where $F_m(x)$ represents the updated model at the m-th boosting iteration and $h_m(x)$ is the newly trained weak learner (decision tree) that corrects previous prediction errors. This incremental approach enables XGBoost to capture complex non-linear relationships in the data, making it highly effective for identifying subtle DoS attack patterns within network

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

traffic features. The overall training objective minimizes both the prediction loss and model complexity, as formulated in (7):

$$Obj = \sum_{i=1}^{n} l(y_i, p_i) + \sum_{k=1}^{k} \Omega(f_k) \qquad (7)$$

where l(yi,pi) denotes the loss between the true label and predicted probability, and Ω(fk) penalizes overly complex trees to prevent overfitting. Through this regularized learning framework, XGBoost achieves a balance between accuracy and generalization, leading to robust detection of DoS attacks.

v. Random Forest (RF)

Random Forest is an ensemble learning method that builds multiple decision trees and aggregates their outputs to improve predictive accuracy and control overfitting. The overall prediction is determined through majority voting among individual tree outputs, defined as (7):

$$RF(x) = majority_{vote}\left(Tree_1(x), Tree_2(x), \ldots, Tree_N(x)\right) \qquad (8)$$

where $Tree_i(x)$ represents the prediction from the i-th tree, and N is the number of trees in the forest.
This ensemble approach enhances the model's robustness by reducing variance and mitigating overfitting, which is critical for maintaining high performance across diverse network traffic patterns.

At the core of each decision tree's construction, the Gini impurity criterion is employed to select the optimal feature splits. The Gini impurity at a node is calculated as (8):

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

where p_i is the proportion of samples belonging to class i at that node.

By minimizing Gini impurity during splits, Random Forest ensures the creation of highly pure subgroups, allowing for effective separation of benign and DoS attack traffic.

D. Evaluation Metrics

The model performance will be rated by utilizing the 5 (five) standard metric for evaluation; accuracy, precision, recall, f1 score and ROC-AUC to provide clarity and readability of the performance of the model.

These metrics will evaluate the proposed model efficiency in detecting brute force attack(s). The accuracy will give the overall correctness of he model, the precision will highlight the measure of false positves that was recorded, the recall will highlight the measure of the false negatives recorded, the F1-measure will balance the precision and recall, while ROC-AUC will evaluate classification performance across different thresholds.

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 51-70)
www.abjournals.org

EXPERIMENTAL RESULTS AND ANALYSIS

This phase presents the analysis of the dataset and the results of various machine learning and deep learning models trained to detect Denial-of-Service (DoS) attacks. The models' performance was assessed using standard evaluation metrics, including Accuracy (Acc), Precision (Pre), Recall (Rec), F1-Score (F1), and Area Under the Curve (AUC). Table 1 and Figure 7 summarizes the performance metrics for the five models analysed: Convolutional Neural Network (CNN), Recurrent Neural Networks (RNNs) with LSTM, Extreme Gradient Boosting (XGB), Random Forest (RF), and Logistic Regression (LR). Each model was tested on both training and test datasets to evaluate its generalization ability. The results provide insights into the strengths and weaknesses of each model, assessing their suitability for real-world applications.

Table 1: Model Performance

Models	Acc	Pre	Rec	F1	AUC
Logistic Regression (LR)	0.91	0.90	0.92	0.91	0.98
Recurrent Neural Networks (RNN) with LSTM	0.96	0.98	0.94	0.96	1.00
Convolutional Neural Network (CNN)	0.98	0.97	0.99	0.98	1.00
Extreme Gradient Boosting (XGB)	0.97	0.97	0.98	0.97	1.00
Random Forest (RF)	0.99	0.99	0.99	0.99	1.00

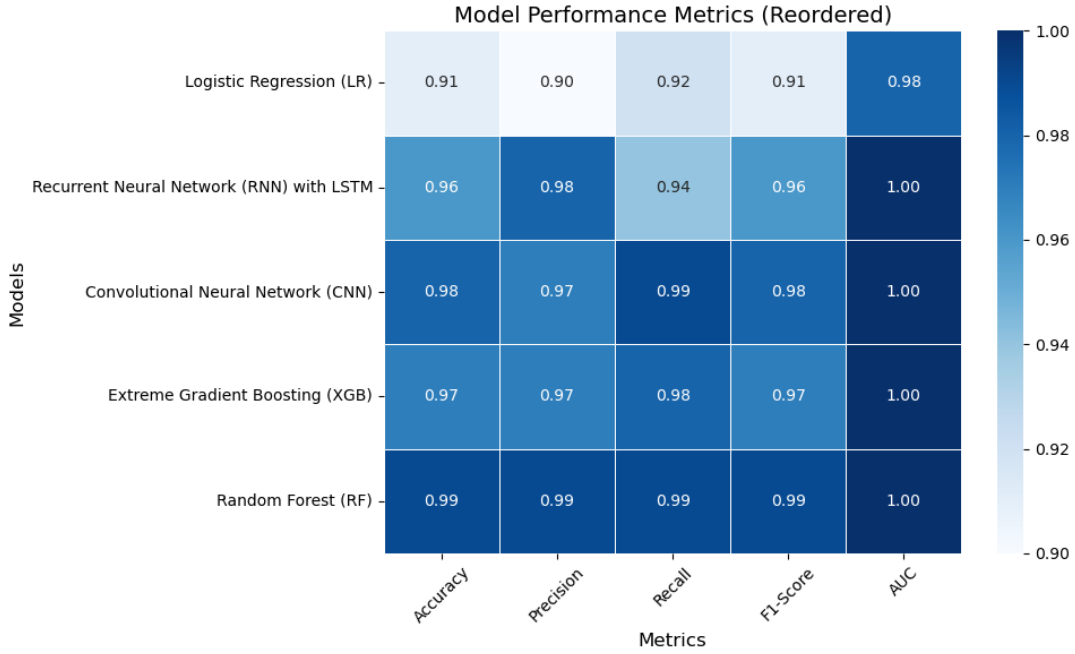

Figure 7: Heatmap of the Models' Performance

A. Models' Results Analysis

The various results yielded outputs that exposed the strength and weakness of the models in detecting Distributed Denial of Service.

Logistic Regression demonstrated the lowest performance among the models, achieving 91% accuracy on both training and test datasets. While it maintains decent recall (0.92), its lower

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

precision (0.90) indicates a tendency to generate more false positives compared to other models. This limitation could lead to higher rates of unnecessary alerts in practical applications. Nevertheless, its AUC score of 0.98 reflects good discriminatory power, making it suitable for lightweight, resource-constrained environments where interpretability and computational efficiency take precedence over high accuracy.

The Recurrent Neural Network (RNN) with LSTM achieved 96% accuracy on both training and test datasets, slightly lower than CNN. It demonstrated strong precision (0.98), indicating that it effectively minimizes false positives. It recorded a recall (0.94) which is slightly lower, suggesting that it may miss some DoS attacks in real-world scenarios. Despite this, the RNN with LSTM attained an excellent AUC score of 1.00, highlighting its robustness in distinguishing classes. While it is well-suited for analysing sequential patterns in network traffic, its slightly lower recall and higher computational requirements compared to simpler models may limit its applicability in environments where real-time detection is critical.

The Convolutional Neural Network (CNN) exhibited exceptional performance, attaining a high accuracy of 98%. This optimal performance demonstrates the model's strong generalization ability, confirming it satisfaction as best model for real-world utilization. The CNN's high recall (0.99) indicates its ability to correctly classify nearly all occurrences of DoS attacks, which is crucial in security-sensitive scenarios where undetected threats can have severe consequences. Additionally, the model's perfect AUC score of 1.00 underscores its excellent discriminatory power in distinguishing between benign and malicious traffic.

Extreme Gradient Boosting (XGB) demonstrated balanced performance, with 97% accuracy across both training and test datasets. It achieved high recall (0.98) and precision (0.97), this confirms it as a highly suitable option for scenarios where both low false positives and high detection rates are required. XGB showcased an ability to maintain consistency across datasets which reflects its strong generalization capabilities. Though it has a higher computational efficiency than deep learning models, careful hyperparameter tuning might still be necessary to get the best results.

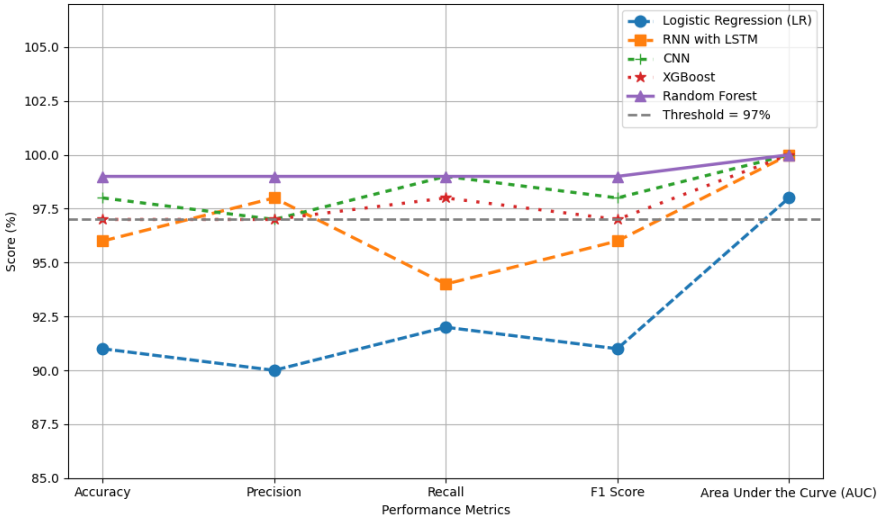

Figure 8: Metrics Analysis Across Models

Random Forest (RF) came out as the top-performing model, with above 99% scores in all the performance metrics. These metrics indicate that RF exhibits minimal overfitting while

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

maintaining exceptional performance. Its AUC score of 1.00 further validates its ability to accurately classify between normal and anomalous patterns as highlighted in Figure 8. The simplicity and interpretability of Random Forest make it a reliable and scalable option for real-world deployment. However, its reliance on ensemble decision trees can result in longer inference times compared to linear models, which might pose challenges in real-time detection scenarios.

RESULT DISCUSSION

The analysis highlights Random Forest (RF) and Convolutional Neural Network (CNN) as the best-performing models for detecting Denial-of-Service (DoS) attacks. Its exceptional performance is highlighted in Figure 9.

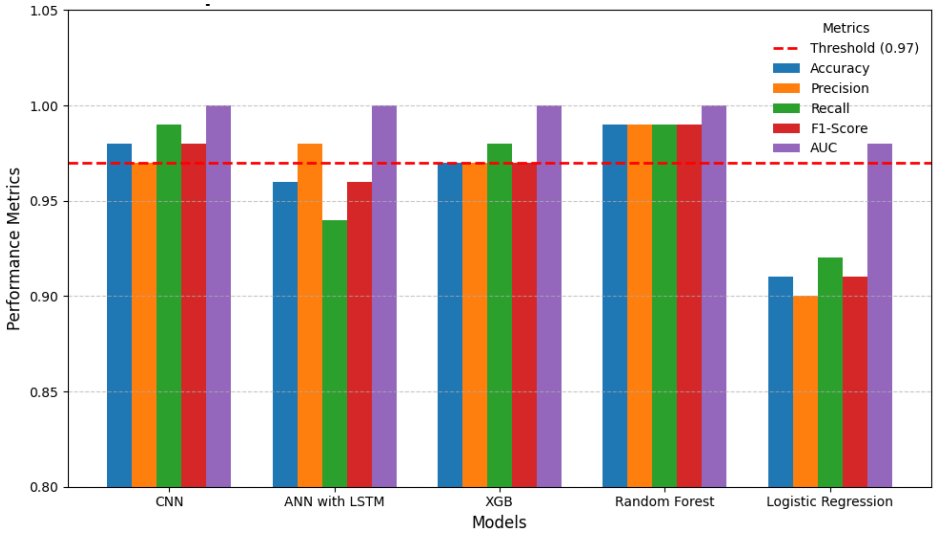

Figure 9: Model Performance Comparison

Random Forest achieved a near-perfect accuracy of 99% across both training and test datasets, alongside exceptional precision, recall, and F1-score metrics of 99%, demonstrating its ability to generalize effectively without overfitting. Its interpretability and ability to rank feature importance further enhance its reliability in real-world deployment. Similarly, the CNN excelled with an accuracy of 98%, a high recall of 99%, and a perfect AUC score of 1.00, showcasing its strength in capturing complex patterns in the dataset. The CNN's capability to extract hierarchical features from raw data renders it highly effective for complex tasks such as detecting anomalies in network traffic. Together, these models stand out for their precision, robustness, and scalability, making them ideal choices for accurate and efficient DoS attack detection in diverse operational environments.

The comparison between Ensemble Learning and Deep Learning models presented in Figure 10 highlights their respective strengths in detecting Denial-of-Service (DoS) attacks. Random Forest (RF) and Extreme Gradient Boosting (XGB), demonstrated consistently high performance across all metrics, with RF achieving near-perfect scores of 99% and above in all the recorded performance metrics and XGB complemented the achieving 97% accuracy and robust recall (98%). There gives credence to ensembled models of which these 2 (two) models are classified to be in addition to being presented as tree-based models.

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

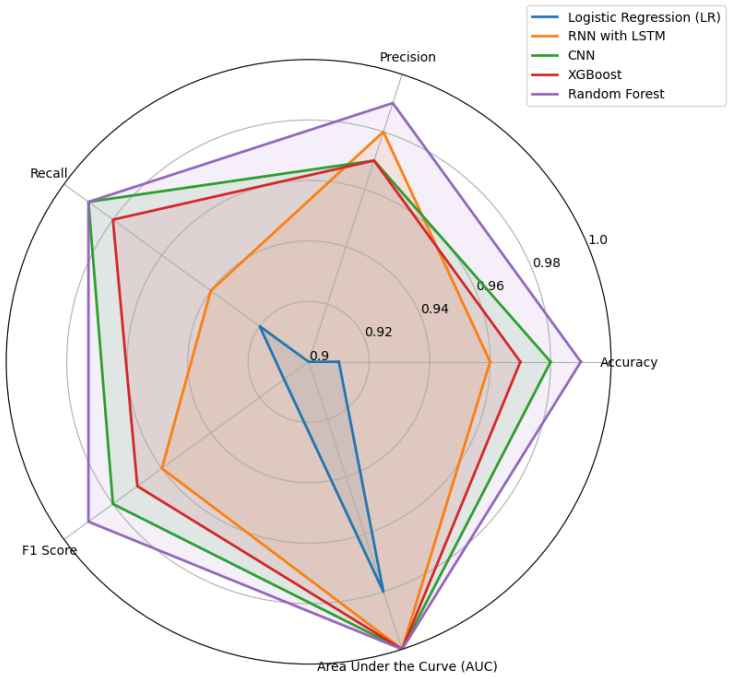

Figure 10: Model Performance Across Metrics

These models excel in reliability, interpretability, and computational efficiency, making them ideal for structured data with well-defined features. Deep Learning models, such as Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN), showed exceptional capabilities in learning complex patterns from data. CNN achieved 98% accuracy and a perfect AUC of 1.00, while RNN maintained competitive precision (98%) but slightly lower recall (94%). While Ensemble Learning models are often more resource-efficient and interpretable, Deep Learning models are better suited for capturing intricate and non-linear relationships, offering superior scalability for large, unstructured datasets. Together, these approaches complement each other, with their applicability depending on the complexity of the dataset and the operational constraints.

CONCLUSION

The enhancement of Artificial Intelligence has enhanced the adoption of automated tools the gives credence to the effectiveness of machine learning and deep learning models in detecting Denial-of-Service (DoS) attacks as demonstrated in the performance for various models highlight their strengths and trade-offs. Ensemble Learning models, specifically, Random Forest and Extreme Gradient Boosting which also double as tree-based models, excelled with high accuracy, interpretability, and adaptability efficiency, making them suitable for real-world applications with structured datasets. Deep Learning models, such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) with LSTM, showed superior capabilities in capturing complex data patterns, achieving competitive performance metrics and scalability for larger datasets. By leveraging feature selection methods using Recursive Feature Elimination (RFE) and balancing methods to enhance data quality, the study ensured robust and reliable model performance. The findings highlight the importance

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

of model selection based on specific operational requirements. Random Forest and CNN showcased optimal performance for DoS attack detection. This highlight capacity of Random Forest and Convolutional Neural Network in combating DoS attacks and is recommended for personalized and corporate application.

FUTURE WORK

Future work should explore hybrid approaches that combine the interpretability of Ensemble Learning with Deep Learning for improved scalability and performance to further enhance cybersecurity defences. Exploring other balancing techniques is also essential to assess how models perform on both normal and synthetic datasets.

ACKNOWLEDGEMENTS

All thanks go to God Almighty for guidance and direction.

REFERENCES

Abdelwahab, O., Awad, N., Elserafy, M., & Badr, E. (2022). A feature selection-based framework to identify biomarkers for cancer diagnosis: A focus on lung adenocarcinoma. *PloS One*, *17*(9), e0269126. https://doi.org/10.1371/journal.pone.0269126

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection. *IEEE Access*, *6*, 33789–33795. https://doi.org/10.1109/ACCESS.2018.2841987

Ahmed, N., Hassan, F., Aurangzeb, K., Magsi, A. H., & Alhussein, M. (2024). Advanced machine learning approach for DoS attack resilience in internet of vehicles security. *Heliyon*, *10*(8), e28844. https://doi.org/10.1016/j.heliyon.2024.e28844

Ahmed, S. F., Alam, M. S. Bin, Hassan, M., Rozbu, M. R., Ishtiak, T., Rafa, N., Mofijur, M., Shawkat Ali, A. B. M., & Gandomi, A. H. (2023). Deep learning modelling techniques: current progress, applications, advantages, and challenges. *Artificial Intelligence Review*, *56*(11), 13521–13617. https://doi.org/10.1007/s10462-023-10466-8

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, *132*, 103352. https://doi.org/10.1016/j.cose.2023.103352

Akwaronwu, B. G., Akwaronwu, I. U., & Adeniyi, O. J. (2025). Brute Force Attack Detection in Network Traffic Using Convolutional Neural Networks. *Asian Journal of*

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

Research in Computer Science, *18*(5), 387–402. https://doi.org/10.9734/ajrcos/2025/v18i5662

Al-Jarrah, O. Y., Alhussein, O., Yoo, P. D., Muhaidat, S., Taha, K., & Kim, K. (2016). Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection. *IEEE Transactions on Cybernetics*, *46*(8), 1796–1806. https://doi.org/10.1109/TCYB.2015.2490802

Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2023). DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison. *Bulletin of Electrical Engineering and Informatics*, *12*(2), 930–939. https://doi.org/10.11591/eei.v12i2.4466

Alabassi, A., Jahromi, A. N., Karimipour, H., Dehghantanha, A., Siano, P., & Leung, H. (2022). A Self-Tuning Cyber-Attacks' Location Identification Approach for Critical Infrastructures. *IEEE Transactions on Industrial Informatics*, *18*(7), 5018–5027. https://doi.org/10.1109/TII.2021.3133361

Ali, T. E., Chong, Y.-W., & Manickam, S. (2023). Comparison of ML/DL Approaches for Detecting DDoS Attacks in SDN. *Applied Sciences*, *13*(5), 3033. https://doi.org/10.3390/app13053033

Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data*, *8*(1), 53. https://doi.org/10.1186/s40537-021-00444-8

Arroyabe, M. F., Arranz, C. F. A., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Asadi, M., Jamali, M. A. J., Heidari, A., & Navimipour, N. J. (2024). Botnets Unveiled: A Comprehensive Survey on Evolving Threats and Defense Strategies. *Transactions on Emerging Telecommunications Technologies*, *35*(11). https://doi.org/10.1002/ett.5056

Azevedo, B. F., Rocha, A. M. A. C., & Pereira, A. I. (2024). Hybrid approaches to optimization and machine learning methods: a systematic literature review. *Machine Learning*, *113*(7), 4055–4097. https://doi.org/10.1007/s10994-023-06467-x

Balarezo, J. F., Wang, S., Chavez, K. G., Al-Hourani, A., & Kandeepan, S. (2022). A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. *Engineering Science and Technology, an International Journal*, *31*, 101065. https://doi.org/10.1016/j.jestch.2021.09.011

Barbierato, E., & Gatti, A. (2024). The Challenges of Machine Learning: A Critical Review. *Electronics*, *13*(2), 416. https://doi.org/10.3390/electronics13020416

Beattie, J. R., & Esmonde-White, F. W. L. (2021). Exploration of Principal Component Analysis: Deriving Principal Component Analysis Visually Using Spectra. *Applied Spectroscopy*, *75*(4), 361–375. https://doi.org/10.1177/0003702820987847

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/S2212-5671(15)01077-1

Chen, C., Liang, J., Sun, W., Yang, G., & Meng, X. (2024). An automatically recursive feature elimination method based on threshold decision in random forest classification. *Geo-Spatial Information Science*, 1–26. https://doi.org/10.1080/10095020.2024.2387457

Chen, L., Xiao, J., Zou, P., & Li, H. (2022). Lie to Me: A Soft Threshold Defense Method for

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

Adversarial Examples of Remote Sensing Images. *IEEE Geoscience and Remote Sensing Letters*, *19*. https://doi.org/10.1109/LGRS.2021.3096244

Crombé, A., Lafon, M., Nougaret, S., Kind, M., & Cousin, S. (2022). Ranking the most influential predictors of CT-based radiomics feature values in metastatic lung adenocarcinoma. *European Journal of Radiology*, *155*. https://doi.org/10.1016/j.ejrad.2022.110472

Eduardo Márquez Díaz, J. (2021). Internet of Things and Distributed Denial of Service as Risk Factors in Information Security. In *Bioethics in Medicine and Society*. IntechOpen. https://doi.org/10.5772/intechopen.94516

Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, *122*, 149–171. https://doi.org/10.1016/j.future.2021.03.011

Ersavas, T., Smith, M. A., & Mattick, J. S. (2024). Novel applications of Convolutional Neural Networks in the age of Transformers. *Scientific Reports*, *14*(1), 10000. https://doi.org/10.1038/s41598-024-60709-z

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

Gebreyes, A. (2020). Denial of Ser Denial of Service Attacks: Diff ttacks: Difference in Rates, Dur ence in Rates, Duration, and ation, and Financial Damages and the Relationship Between Company Assets and Revenues. *Walden University*. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=11004&context=dissertations

He, X., Su, Y., Liu, P., Chen, C., Chen, C., Guan, H., Lv, X., & Guo, W. (2023). Machine learning-based immune prognostic model and ceRNA network construction for lung adenocarcinoma. *Journal of Cancer Research and Clinical Oncology*, *149*(10), 7379–7392. https://doi.org/10.1007/s00432-023-04609-1

Howser, G. (2020). The OSI Seven Layer Model. In *Computer Networks and the Internet* (pp. 7–32). Springer International Publishing. https://doi.org/10.1007/978-3-030-34496-2_2

Hulayyil, S. B., Li, S., & Xu, L. (2023). Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security. *Electronics (Switzerland)*, *12*(18). https://doi.org/10.3390/electronics12183927

Islam, M. M., Shahid, S., Bakhat Awar, K., Khan, R., & Sohail, M. (2021). Cyber-Security: Dos Attack Outcomes are Dangerous. *European Journal of Electrical Engineering and Computer Science*, *5*(3), 54–59. https://doi.org/10.24018/ejece.2021.5.3.297

J. O., A., S. O., O., & B. G., A. (2025). Real-Time Detection of Examination Malpractices Using Convolutional Neural Networks and Video Surveillance: A Systematic Review with Meta-Analysis. *British Journal of Computer, Networking and Information Technology*, *8*(2), 15–50. https://doi.org/10.52589/BJCNIT-QC5EELJE

Kiranashree, B. K., Ambika, V., & Radhika, A. D. (2021). Analysis on Machine Learning Techniques for Stress Detection among Employees. *Asian Journal of Computer Science and Technology*, *10*(1), 35–37. https://doi.org/10.51983/ajcst-2021.10.1.2698

Kumar, G. (2016). Denial of service attacks – an updated perspective. *Systems Science & Control Engineering*, *4*(1), 285–294. https://doi.org/10.1080/21642583.2016.1241193

Loan Prediction System. (2023). *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/IRJMETS43769

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13*(12), 155014771774146. https://doi.org/10.1177/1550147717741463

Mercuri, V., Saletta, M., & Ferretti, C. (2023). Evolutionary Approaches for Adversarial Attacks on Neural Source Code Classifiers. *Algorithms*, *16*(10). https://doi.org/10.3390/a16100478

Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, *10*(2). https://doi.org/10.1080/23311916.2023.2272358

Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2019). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet of Things Journal*, *6*(3), 4815–4830. https://doi.org/10.1109/JIOT.2018.2871719

Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2023). DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. *Engineering Reports*, *5*(12). https://doi.org/10.1002/eng2.12697

Natarajan, R., Ranjith, C. P., Mohideen, M. K., Gururaj, H. L., Flammini, F., & Thangarasu, N. (2024). Utilizing a machine learning algorithm to choose a significant traffic identification system. *International Journal of Information Management Data Insights*, *4*(1), 100218. https://doi.org/10.1016/j.jjimei.2024.100218

Okeh, O. D., Ajayi, O. F., Emuobonuvie, E. A., & Ekokotu, D. A. (2023). A Review of Network Attacks and Security Solutions in a Networked Environment. *Asian Journal of Engineering and Applied Technology*, *12*(2), 24–28. https://doi.org/10.51983/ajeat-2023.12.2.3965

Onuiri, E., Akwaronwu, B. G., & Umeaka, K. C. (2024). Environmental and Genetic Interaction Models for Predicting Lung Cancer Risk Using Machine Learning: A Systematic Review and Meta-Analysis. *Asian Journal of Computer Science and Technology*, *13*(1), 45–58. https://doi.org/10.70112/ajcst-2024.13.1.4266

Osazuwa, O. M. C. (2023). Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature. *International Journal of Innovative Science and Research Technology*, *8*(12). https://doi.org/https://doi.org/10.5281/zenodo.10464076

Owaid, M. A., & Hammoodi, A. S. (2024). Evaluating Machine Learning and Deep Learning Models for Enhanced DDoS Attack Detection. *Mathematical Modelling of Engineering Problems*, *11*(2), 493–499. https://doi.org/10.18280/mmep.110221

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, *07*(03), 185–194. https://doi.org/10.4236/jis.2016.73014

Qaid, T. S., Mazaar, H., Al-Shamri, M. Y. H., Alqahtani, M. S., Raweh, A. A., & Alakwaa, W. (2021). Hybrid Deep-Learning and Machine-Learning Models for Predicting COVID-19. *Computational Intelligence and Neuroscience*, *2021*(1). https://doi.org/10.1155/2021/9996737

Qureshi, R., Zhu, M., & Yan, H. (2021). Visualization of Protein-Drug Interactions for the Analysis of Drug Resistance in Lung Cancer. *IEEE Journal of Biomedical and Health Informatics*, *25*(5), 1839–1848. https://doi.org/10.1109/JBHI.2020.3027511

Şahin, C. B., Dinler, Ö. B., & Abualigah, L. (2021). Prediction of software vulnerability based deep symbiotic genetic algorithms: Phenotyping of dominant-features. *Applied Intelligence*, *51*(11), 8271–8287. https://doi.org/10.1007/s10489-021-02324-3

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2021). *NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems* (pp. 117–135).

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y

https://doi.org/10.1007/978-3-030-72802-1_9

Sarker, I. H. (2021a). Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. *SN Computer Science*, *2*(6), 420. https://doi.org/10.1007/s42979-021-00815-1

Sarker, I. H. (2021b). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, *2*(3), 160. https://doi.org/10.1007/s42979-021-00592-x

Sathishkumar, P., Gnanabaskaran, A., Saradha, M., & Gopinath, R. (2024). Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network. *Ain Shams Engineering Journal*, 103052. https://doi.org/10.1016/j.asej.2024.103052

Shargunam, S., & Rajakumar, G. (2022). Predictive Analysis on Sensor Data Using Distributed Machine Learning. *Asian Journal of Computer Science and Technology*, *11*(1), 1–4. https://doi.org/10.51983/ajcst-2022.11.1.3071

Singh, A., & Gupta, B. B. (2022). Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–43. https://doi.org/10.4018/IJSWIS.297143

Singh, D., & Uma Mageswari, R. (2025). *Securing the Internet of Things: A Comprehensive Examination of Machine and Deep Learning Approaches Against Denial of Service Attacks BT - Broadband Communications, Networks, and Systems* (X. Cheng (Ed.); pp. 176–188). Springer Nature Switzerland.

Suryateja, P. S. (2018). Threats and Vulnerabilities of Cloud Computing: A Review. *International Journal of Computer Sciences and Engineering*, *6*(3), 297–301. https://doi.org/10.26438/ijcse/v6i3.298303

Talafha, S., Wu, D., Rekabdar, B., Li, R., & Wang, G. (2021). Classification and Feature Extraction for Hydraulic Structures Data Using Advanced CNN Architectures. *2021 Third International Conference on Transdisciplinary AI (TransAI)*, 137–146. https://doi.org/10.1109/TransAI51903.2021.00032

Tien, P. W., Wei, S., Darkwa, J., Wood, C., & Calautit, J. K. (2022). Machine Learning and Deep Learning Methods for Enhancing Building Energy Efficiency and Indoor Environmental Quality – A Review. *Energy and AI*, *10*, 100198. https://doi.org/10.1016/j.egyai.2022.100198

Tuli, B., Kumar, S., & Gautam, N. (2022). An Overview on Cyber Crime and Cyber Security. *Asian Journal of Engineering and Applied Technology*, *11*(1), 36–45. https://doi.org/10.51983/ajeat-2022.11.1.3309

Uddin, R., Kumar, S. A. P., & Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. *Ad Hoc Networks*, *152*, 103322. https://doi.org/10.1016/j.adhoc.2023.103322

Article DOI: 10.52589/BJCNIT-I0V0HK0Y
DOI URL: https://doi.org/10.52589/BJCNIT-I0V0HK0Y