
Journal of Informatics and Web Engineering

Vol. 3 No. 3 (October 2024)

eISSN: 2821-370X

DDoS Attack Detection with Machine Learning

Wei-Wu Tay¹, Siew-Chin Chong^{1*}, Lee-Ying Chong¹

¹Faculty of Information Science & Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia

*corresponding author: (chong.siew.chin@mmu.edu.my; ORCID: 0000-0003-0421-4367)

Abstract - Nowadays, Distributed Denial of Service (DDoS) attacks are a major issue in internet security. These attacks target servers or network infrastructure. Similar to an unanticipated traffic jam on highway (lagging/crash) that prevent normal traffic reach to destination. DDoS may prevent users to access any system services. Researchers and scientists have developed numerous methods and algorithms to improve the performance of DDoS detection. In this paper, a DDoS detection method utilizing machine learning is proposed. There are three type of supervised machine learning classification methods which are K-Nearest Neighbor, Multilayer Perceptron and Random Forest, are applied in the proposed work to assess the accuracy of the model in training and testing processes. RF classification provides robustness and interpretability, MLP offers deep learning capabilities for complex patterns, and K-NN delivers simplicity and adaptability for instance-based learning. Together, these methods can contribute to a comprehensive DDoS attack detection system using machine learning. There are two types of classification setups: binary and multi-class classification. Binary classification involves identifying traffic as either a DDoS attack or normal using the NSL-KDD dataset. Multi-class classification, on the other hand, distinguishes between various types of DDoS attacks (such as DoS, Probe, U2R, and Sybil) and normal traffic using the NSL-KDD dataset. Feature engineering is also involved in this experiment to convert the categorical features into numerical values for detecting DDoS attack. Our model's performance was effective compared to other machine learning methods. RF achieved the highest accuracy rates: 99.35% in binary classification and 97.71% in multi-class classification. K-NN followed with 99.15% in binary and 97.35% in multi-class classification, while MLP achieved 90.63% in binary and 84.33% in multi-class classification.

Keywords – DDoS Attack, Random Forest, Machine Learning, Multilayer Perceptron, K-Nearest Neighbor

Received: 03 July 2024; Accepted: 21 August 2024; Published: 16 October 2024

This is an open access article under the [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.



1. INTRODUCTION

The rapid expansion of online services and the growing complexity of network infrastructures have elevated DDoS attacks to a major threat to the availability and security of web services. A DDoS attack involves overwhelming a target system with an influx of malicious traffic, causing it to become unresponsive to legitimate users. To resolve this issue, DDoS Attack detection is a way to fix this problem. In the meantime, this project aims to first classify its protocol and use a simple binary model (0,1) to identify any attack. To achieve this, it is essential to study machine learning techniques in the realm of DDoS Attack detection.

There are various of DDoS attack such as DoS attack, Probe attack, U2R, Sibir, etc [1], which the major to threat the security network. Therefore, detection of DDoS attacks is important as to detect the normal activities and malicious activities in the dataset. For improvement and enhancement of DDoS attack detection, many algorithms and methods

are being designed and researched. DDoS attack is a cybercrime, and it disrupts the target server on the normal traffic, network, or service by flooding (creating a massive amount of traffic). Similar to an unanticipated traffic jam on highway that prevent normal traffic reach to destination. DDoS attack can employ multiple compromise computer system to achieve attack traffic source. For example, they allow malware which is botnet (zombies) to attack your computers or devices (IoT devices) with remote controlled. In this case, victim's server or network will receive repeated requests target's IP address from the bot, causing overwhelmed and become denial-of-service to normal traffic. DDoS attack has a lot of techniques and methods. To detection and mitigation progress, there are a way to category those attack which is attack rate, including low-rate and high-rate attack and protocol exploitation attack to be consider.

Low-rate attack is target to someone by slow rate sends malicious traffic. This attack utilizes loopholes of TCP's congestion control mechanism to fulfil repeated sent malicious traffic (pulsing attack) to constant attack. The default of low-rate attack [2] is its rate must below 1000bps or 100bps and attack target background of network traffic by 10% - 20%. Another high-rate attack is target to someone through large packets malicious traffic, it also called flooding. For example, UDP, ICMP, SYN, and HTTP flood. Lastly, protocol exploitation attack is to use up resources on the server utilizes the vulnerabilities of the exploiting network protocol. For example, SYN flooding (TCP-SYN flooding). Those attack to the hosts that on the services over by TCP. Include HTTP, FTP, SSH, IMAP, SMTP and Telnet. Another that is UDP flooding. This attack is seeding excess UDP packet to different server's port. If the packet did not intended destination, the server will return the ICMP packet to the sender as unreachable. So, it will cause server slow and will be non-responding. To solve this problem, there are a detection called instruction detection system (IDS) used to network security technology build to detection by exploits the against target on application or computer.

In this experiment, the NSL-KDD dataset will be used by dataset. These datasets include the record simple intrusion detection network and real IDS face to the traffic's ghost (only traces existent). Besides, there are 43 features in each record, 41 of these are their traffic input and last two of both are labels and score, which is normal/attack and seriousness of traffic input. NSL-KDD dataset's data exists with 4 different classes of attack, which is DoS, U2R, Probe, and the last is R2L. There are 125973 total values of dataset collect in KDDTrain, and 22544 in KDDTest contain with normal, DoS, Probe, U2R and R2L internet traffic attack. There are also features like feature engineering which is called LabelEncoder to transform the categorical features/labels into equivalent numbers such as protocol types, service and flag. This transformation enables algorithms to effectively interpret and utilize categorical information, thereby enhancing the overall predictive performance of the models. 3 types of classification which is RF, MLP & K-NN will be used as evaluation performance for this experiment DDoS attack detection.

2. LITERATURE REVIEW

2.1 Random Forest (RF)

Random Forest is a machine learning algorithm that utilizes the bagging technique and feature randomness to generate a diverse ensemble of decision trees. Developed by Breiman and Cutler [3], it is widely used for solving various classification and regression problems [4],[5],[6]. It aids in accurately predicting outcomes in large datasets. The Random Forest technique merges multiple classifiers to address various complex problems. By averaging the outputs from different trees, Random Forest enhances prediction accuracy. Additionally, increasing the number of trees generally leads to greater precision in the results [7]. The Random Forest method overcomes limitations of the decision tree algorithm, enhancing precision by reducing dataset variance. While individual trees in the forest are weak learners, they collectively form strong learners. RF is fast and effective for large and unbalanced datasets, though it has limitations in training with diverse datasets, particularly in regression problems.

Various traditional algorithms have been employed, including Logistic Regression (LR), C4.5, and Random Forest (RF). LR models the relationship between a dependent binary variable and independent variables. C4.5 is commonly applied in data mining as a decision tree classifier to make decisions based on provided datasets. Traditionally, algorithms combining Threshold optimization (T) and Bayes' Minimum Risk Classifiers (M.R.) have been used for grouping fraudulent transactions by adjusting the decision threshold. These techniques enhance prediction accuracy and reduce overall costs. However, LR excels in regression problems as it handles model overfitting better than decision trees. Nonetheless, real-time scenarios with linear problems are rare. Since DDoS attack datasets are nonlinear, LR is not suitable for this context.

Furthermore, the research in [8] introduces a new method for detecting DDoS attacks by leveraging machine learning combined with feature selection techniques. This approach utilizes Mutual Information (MI) and Random Forest

Feature Importance (RFFI) to determine the most significant features from two prominent datasets, CICIDS 2017 and CICDDoS 2019, which are established benchmarks in cybersecurity research. To identify and classify attacks, the study uses machine learning algorithms which form the core of the detection framework. The results show that the proposed method significantly improves accuracy and reduces misclassification errors, thereby enhancing DDoS attack detection capabilities. The primary contribution of this research lies in its emphasis on mitigating misclassification errors through the strategic selection of relevant features and optimization of machine learning parameters. This approach not only enhances detection accuracy but also holds promise for bolstering cybersecurity defense strategies in practice. RF are the best accuracy between other as 99.99%.

Additionally, a machine learning model based on RF to detect DDoS attack is proposed by [9]. In RF, it has a great number of decision trees under Gini index and Entropy criteria to improve accuracy detection. The datasets that are used in this experiment is CICDDoS2019, it contains a large amount of DDoS attack traffic. This rf model aim to detect DDoS attack on network server by transport layer of network using two-fold classification Benign and Attack. The accuracy rate in this experiment showing as 97.23%. Moreover, the detection of local attacks, which is captured using attack packets combined with normal data packets [10], employs machine learning to train open-source tools for DDoS attacks, specifically Tribe Flood Network 2000 (TFN2K), to identify DDoS attack traffic. This method can target one or multiple attack targets to deplete resources from the machine by utilizing numerous agents. Examples of such attacks include TCP, UDP, and ICMP flood attacks. Each packet capture tool uses network data analysis tools such as TcpDump. TcpDump is a classification system used to analyze data packets from the network based on user-defined criteria. The best accuracy achieved by RF is 98.10% (TCP), 99.49% (UDP) and 98.56% (ICMP).

Random forest algorithms are present for detecting DDoS attacks by analyzing network traffic based on the relevant features. However, their effectiveness in this regard depends on several factors. Firstly, choosing the right features is crucial for accurately distinguishing between normal and malicious traffic. Features such as packet rate, size distribution, and protocol usage play a significant role in this classification. Additionally, training a random forest model requires a large dataset with labeled examples of both regular and attack traffic. Besides, their suitability for real-time detection is limited by the computational resources needed, particularly in fast-paced network environments. Moreover, the evolving nature of DDoS attacks means that models need regular updates to maintain their effectiveness. Nonetheless, when combined with other detection methods as part of an ensemble approach, random forests can contribute to improving detection accuracy and resilience against DDoS threats. For example, this paper presents an experiment using basic machine learning algorithms to detect DDoS attacks by analyzing network traffic [11]. The dataset using CICIDS2017 dataset and the classification using Random Forest, Logistic Regression, and Neural Network. There are provided also model comparisons such as ROC and AUC. All the results show that random forests are better than others.

2.2 Multilayer Perceptron (MLP)

MLP [12] is made by a layer of nodes, includes the input, hidden, and output layer. Each node has its own node to connect with them and have associated weights and thresholds. Once the output of a node was higher than specify threshold, it will send to next level of network's layers. For example, each node has linear regression model, weight (w_i), consists with input data (x_i), bias and output. All relationships of each perceptron model have a limit. During the training process, these weights are adjusted iteratively using algorithms such as backpropagation, which involves calculating the gradient of a loss function with respect to the weights and updating the weights in the direction that minimizes the loss. MLPs are powerful models capable of learning complex patterns and relationships in data. The hidden layers allow MLPs to capture non-linearities in the data, enabling them to solve a wide range of machine learning tasks, including classification, regression, and pattern recognition. Each node in the hidden layers applies a non-linear activation function to its inputs, allowing the network to model complex mappings between inputs and outputs. Common activation functions used in MLPs include sigmoid, tanh, and rectified linear unit (ReLU).

Despite their effectiveness, MLPs have some limitations. They require large amounts of data to train effectively, and the choice of architecture, including the number of layers and nodes, can significantly impact performance. Additionally, training MLPs can be computationally intensive, especially for deep architectures with many layers. However, with proper tuning and optimization, MLPs can achieve state-of-the-art performance on a wide range of machine learning tasks and are widely used in various fields, including computer vision, natural language processing, and speech recognition. [13] utilizes MLP with backpropagation to detect DDoS attacks. Real-world network traffic data is used to extract the relevant features by training with the MLP model. For the training, there was evaluated using a separate test dataset to compute its performance, various evaluation metrics have been calculated. These

metrics offer valuable insights into the model's capability to accurately identify instances of DDoS attacks while minimizing false positives and false negatives. By employing MLPs and conducting thorough performance evaluations, this study contributes to the advancement of DDoS detection methods, potentially bolstering network security measures in practical settings.

Additionally, the approach in [14] utilized the MLP method to detect DDoS attacks by statistically analyzing network traffic. Sequential feature selection was integrated with MLP to choose the optimal features during the training phase, and a feedback mechanism was designed to dynamically reconstruct the detector when significant detection errors were detected. This method achieved an accuracy of 99.67%.

The MLP has produced accuracy in detecting DDoS attacks with a classification accuracy of 99.30% and minimal false positives. It achieved precision rates of 99.90% for safe traffic and 98.30% for hostile traffic, along with recall rates averaging 98.70% and an average F1 score of 98.90%. With 82,314 True Positives and low False Negatives, the model demonstrated robust performance in identifying hostile traffic. Multilayer Perceptron (MLP) is a powerful tool that provided detecting DDoS attacks. Its offering unique advantages over existing machine learning methods such as Its ability to model complex, non-linear relationships useful for identifying DDoS attacks. Additionally, MLP's allows it to recognize new attack types as they emerge, and its speed enables quick categorization of network data to prevent or mitigate attacks. Moreover, MLP's scalability makes it suitable for handling large volumes of network traffic in real-time, crucial for networks with heavy traffic loads. Overall, MLP was produced as a powerful and effective solution for enhancing network security against DDoS attacks.

2.3 K-Nearest Neighbour (KNN)

KNN [15], is a non-parametric to classify the individual/group of data point. It can also find similar point near each other. For example, is can calculate the new data (packet or flow) between with distance in a dataset. To determine the closest of the data point to query point, distance between query point must be calculated. It can help to divide the point into different region. KNN is a supervised learning algorithm and non-parametric to classify the individual/group of data point. It performs also classification by computing the query instance's prediction value from simple majority decision on category of nearest neighbors. The parameter 'K' in KNN means the number of closest neighbors when processing the voting based on the majority.

A paper explored the centralized control of SDN (Software Defined Network) devices, highlighting its superiority over traditional network architectures [16]. Some advantages of SDN such as greater scalability, high programmability, security features and management. In SDN, DDoS attack occurs certainly. DDoS attacks present a significant threat to network security, often leading to complete network shutdowns. Traditional methods are often insufficient for effectively identifying DDoS attacks. Therefore, to enhance detection, two algorithms, LR and KNN—are employed. The accuracy of Logistic Regression is roughly 91% and the accuracy of the KNN algorithm is roughly 99%. From the analysis KNN is better rather than Logistic Regression.

Besides, there is a paper that provides detecting DDoS attack in SDN [17]. SDN offers manageability, scalability, and improved performance but is vulnerable to DDoS attacks, which can overload the controller and degrade network performance. This study focuses on detecting DDoS attacks in SDN using machine learning models. A dataset was created by extracting features from both normal and attack traffic, and feature selection methods were applied to simplify the models and reduce training time. The datasets, with and without feature selection, were trained and tested using SVM, Naive Bayes, ANN, and KNN models. The KNN classifier combined with wrapper feature selection achieved the highest accuracy rate of 98.3%. The results indicate that machine learning and feature selection algorithms improve DDoS attack detection in SDN while reducing processing loads and times.

Additionally, NB and KNN are applied to detect DDoS attack for network forensics [18]. In this experiment, it used NSL-KDD dataset and KDD'99 dataset to comprise the network traffic data. It separates the 41 dataset's features and classified into 4 types U2R, R2L, DoS and Probing. It trains the data with distinguish with 2 types called normal and attack. After split dataset, RF and K-NN is used to evaluate performance which K-NN achieve a best accuracy rate of 98.51% in NSL-KDD and 96.42% in KDD'99.

For decades, DDoS attacks have severely compromised network availability, and an effective defense mechanism remains elusive. However, the advent of SDN offers a fresh perspective on defending against DDoS attacks [19]. This paper proposes two methods for detecting DDoS attacks in SDN: one assesses the severity of the attack, while the other uses an enhanced KNN algorithm based on machine learning for detection.

2.4 Naïve Bayes (NB)

NB is used for classification in ML based on Bayes' Theorem [20]. It generates the class or category of the model's input. Bayes' Theorem is used for continuous events in which more information added may affect early probability. These probabilities are prior and rear probabilities. A priori probability is the beginning probability before a given condition occurs. Rear probability is a probability that after observing the data on an event. Conditional probability is a calculation that measure to occur any event's probability such as presumption, proof, supposition or assertion. For example, $P(\text{YES}|\text{Book}) = P(\text{Book}|\text{YES}) (0.35) * P(\text{YES}) (0.66) / P(\text{Book}) (0.36)$, in this section, $P(\text{YES}|\text{Book}) = 0.35 * 0.66 / 0.32 = 0.64$, where the probability is higher. This algorithm used text classification (n/p) and multiple categories of problem.

A paper presents an approach that utilizes the Gaussian Naive Bayes method for detecting DDoS attacks by performing statistical analysis on network traffic [21]. DDoS attacks are characterized by leveraging volume, strength, and cost mitigation strategies, posing a major threat to network integrity and availability. Known as "zombies", It can overwhelm the service, application and network, rendering them inaccessible to authorized users and causing substantial disruptions to Internet services. The proposed Gaussian Naive Bayes method proposed approach seeks to establish correlations with Intrusion Detection Systems (IDS) by statistically analyzing the average and standard deviation of network packets to predict the presence of DDoS attacks. Ultimately, this research aims to enhance network security by providing a robust mechanism for the early detection and mitigation of DDoS threats.

This research identified 9 instances of DDoS detection using ML [22], where attackers overwhelm system resources with high traffic volumes, leading to network congestion. The targeted systems did not involve the capture of sensitive information or compromised credentials. The study focuses on distinguishing between normal and attack scenarios using the CAIDA 2007 dataset. Machine learning algorithms such as Logistic Regression and NB were employed, with NB assuming better accuracy by leveraging individual feature probabilities based on Bayes' theorem.

Besides, ML can also detect with low-rate and high-rate attack using algorithm of machine learning [23]. The dataset CCIDS2017, which is a real-world data (PCAPs) is used to represent the size & length of the packet, duration of flow, packets, and other attributes of packet to become DDoS attack. These DDoS attacks target normal server, service, and network traffic, flooding them and potentially causing higher traffic rates, larger packet sizes, and increased lengths. They tested the CCIDS2017 dataset using the SVM classification algorithm and the Naive Bayes algorithm. Another study utilized Naïve Bayes to detect DoS attacks based on the KDD'99 dataset, specifically in the context of IoT [24]. IoT, a rapidly expanding technology facilitating automation through interconnected networks, faces vulnerabilities such as DoS. This research aimed to implement Naïve Bayes for class prediction using the NSL-KDD dataset formatted from KDD'99, focusing on DoS attacks targeting IoT devices. The study achieved an accuracy rate of 64.02% across the entire dataset.

Lastly, there is a paper that used NB classification to frequency-based DDoS attack detection [25]. This paper study to know the threat of DDoS attack on web servers which disrupt by flooding with bogus packets. To prevent it, this paper proposed to used frequency domain to analysis as detection approach. So, NB is used in this experiment as classifier to classify both dataset which is Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) by differentiating the network traffic by normal and attack. At last, the accuracy rate that achieve by NB is 94.72% (DTF), 90.64% (DWT) & 95.93% (Both).

The Gaussian Naive Bayes method uses average and standard deviation as reference points as integral in constructing a set of classes. The average serves as the center of the class set, while the standard deviation delineates the extent of its distribution. Each class set's width contributes to the specificity of its members. With the Gaussian Naive Bayes method, precise and accurate predictions are facilitated. In the future research may attempt are poised to explore larger datasets to thoroughly evaluate the method's accuracy and efficacy. Table 1 shows the summary of the state-of-the-art methods.

3. RESEARCH METHODOLOGY

The overall flow of the proposed work is presented in Figure 1. In this model, transaction data undergoes preprocessing before applying ML models. The process includes data splitting, preprocessing, and using ML algorithms to detect DDoS attacks, followed by an evaluation of the model's performance.

Table 1. Summary of the State-of-the-Art Methods

Authors	Year	Methods/Techniques	Dataset	Accuracy
Alduailij, M., Khan, Q. W., Tahir, M., Sardaraz, M., Alduailij, M., & Malik, F.	2022	RF, GB WVE & K-NN	CICIDS 2017 & 2019	RF(Best) 99.99%
Kimmi Kumari & M. Mrunalini	2022	LR & NB	CAIDA 2007	LR (99.83%) NB (98.67%)
Wang, M., Lu, Y., & Qin, J.	2020	MLP	ISOT & ISCX dataset	MLP (99.67%)
Polat, Hüseyin & Polat, Onur & Çetin, Aydın. D	2020	SVM, NB, ANN & K-NN	Own Create Dataset	K-NN(Best) (98.3%)
Priya, G. G., Shriram, S. H., Jeeva, S., Priya, G. S., & Balasubadra, K.	2024	LR & K-NN	Own Create Dataset	LR (91%) K-NN (99%)
Rimal, A. N., & N, R	2020	NB & SVM	CCIDS 2017	NB (75.31%) SVM (99.68%)
Sarem, Shi Dong & Mudar	2019	NB, K-NN, SVM, CIC-SVM, DDADA & DDAML	Own Create Dataset	DDAML (Best) (91.20%)
Thai S. C., Weisheng S., Simeon S. & Quang V. N.	2022	RF	CICDDoS2019	RF (97.23%)
Frans Fery Setiadi, Antara Kesiman & Yota Ernanda	2021	NB	KDD'99	NB (64.02%)
Jiangtao Pei, Yunli Chen & Wei Ji	2019	RF & SVM	Own Create Dataset	[(TCP)] RF (98.10) SVM (98.2) [(UDP)] RF (99.49) SVM (98.2) [(ICMP)] RF (98.56) SVM (95.49)
Amit V Kachavimath, Shubhangeni Vijay Nazare & Sheetal S Akki	2020	K-NN & NB	NSL-KDD & KDD'99	[(NSL-KDD)] K-NN (98.51%) NB (91.31%) [(KDD'99)] K-NN (96.42%) NB (93.95)
Anarim, Emin & Fouladi, Ramin & Kayatas, Cemil.	2016	NB	DFT & DWT	[(DFT)] NB (94.72%) [(DWT)] NB (90.64%) [(Both)] NB (95.93%)

In this experiment to detect DDoS attacks using machine learning, three methods will be employed: RF, MLP, and K-NN. Each method will be tested separately on the same dataset to evaluate their performance in identifying DDoS attacks. There are two classification approaches: binary classification, which differentiates between normal and attack traffic, and multi-class classification, which identifies specific types of attacks. RF will utilize its robust ensemble learning capabilities and ability to handle high-dimensional data. MLP will leverage its deep learning capabilities to

capture complex patterns within the dataset. Finally, K-NN will classify instances based on their proximity to known normal and attack pattern.

3.1 Algorithm Method

In this experiment to detect DDoS attacks using machine learning, three methods will be employed: RF, MLP, and K-NN. Each method will be tested separately on the same dataset to evaluate their performance in identifying DDoS attacks. There are two classification approaches: binary classification, which distinguishes between normal and attack traffic, and multi-class classification, which identifies specific types of attacks. RF will utilize its robust ensemble learning capabilities and ability to handle high-dimensional data. MLP will leverage its deep learning capabilities to capture complex patterns within the dataset. Finally, K-NN will classify instances based on their proximity to known normal and attack patterns.

3.1.1 Random Forest

This is an ensemble of individual decision trees that work collaboratively. Each tree in the forest provides a class prediction, and the class with the most votes from the trees is chosen as the model's prediction.

Gini index is an algorithm in decision tree including with Random Forest. Gini index used to evaluate split and partition the data to different class. For example, it can split a feature as know pure or not pure as mean yes or no in dataset. Assume there are a training dataset of DDoS attack will be sampling with set $x = \{x_1, \dots, x_n\}$ and $Y = \{y_1, \dots, y_n\}$ from class n . x is the feature 1 as root node and y is a feature 2 and inside the feature 1 and 2 may has yes or no for attack. J_i is child node's instances number of x or y and J is parent node's the total of instance number and calculation will show in Equation (1) [26].

$$Gini\ Index = 1 - \sum_{i=1}^n (P_i)^2 = 1 - [(P_+)^2 - (P_-)^2] \quad (1)$$

Equation (2) shows the calculation of the total of split for Gini index (weighted Gini index):

$$Weighted\ Gini\ Index = \left(\sum_{i=1}^n \left(\frac{J_i}{J} * [Gini(P_i)] \right) \right) \quad (2)$$

3.1.2 Multilayer Perceptron

Multi-layer Perceptron (MLP) classifier relies on underlying Neural Network to perform the task of classification.

ReLU help the model to learn the complicated patterns sin data and import non-linearity. The function of ReLU preserve the positive elements and abandon negative elements. Assume the input is positive when the output of ReLU is 1, and the input is negative when the ReLU's output is 0. Refer to Equation (3) [27].

$$ReLU(x) = \max(x, 0) \quad (3)$$

pReLU is a mutation of the ReLU that extra a new linear term. Assume the argument is negative, but still can be able to get the information by using Equation (4).

$$pReLU(x) = \max(0, x) - ax \quad (4)$$

3.1.3 K-Nearest Neighbor

This algorithm is a non-parametric, supervised learning classifier, which uses proximity to make classifications or predictions about the grouping of an individual data point. It is one of the popular and simplest classification and regression classifiers used in machine learning today.

In this experiment, the classification KNN's weight that using in this detection DDoS attack is uniform. Weight is important in this classification as it used to prediction. For uniform means the weight of all the point in each neighborhood are equal. Besides, the algorithm is used to calculate nearest neighbors. There are 3 type of algorithm

which is auto, ball tree, kd tree and brute in KNN. Auto is using in this experiment as to decide which algorithm are suitable for value passed to fit the method. The metric which is minkowski that used for calculating distance. It defined as by parameter p, which controls on how much given on larger or smaller of emphasis between with coordinates. Refer to Equation (5) [28].

$$dist(x|z) = \sum_{r=1}^d |x_r - z_r|^r \tag{5}$$

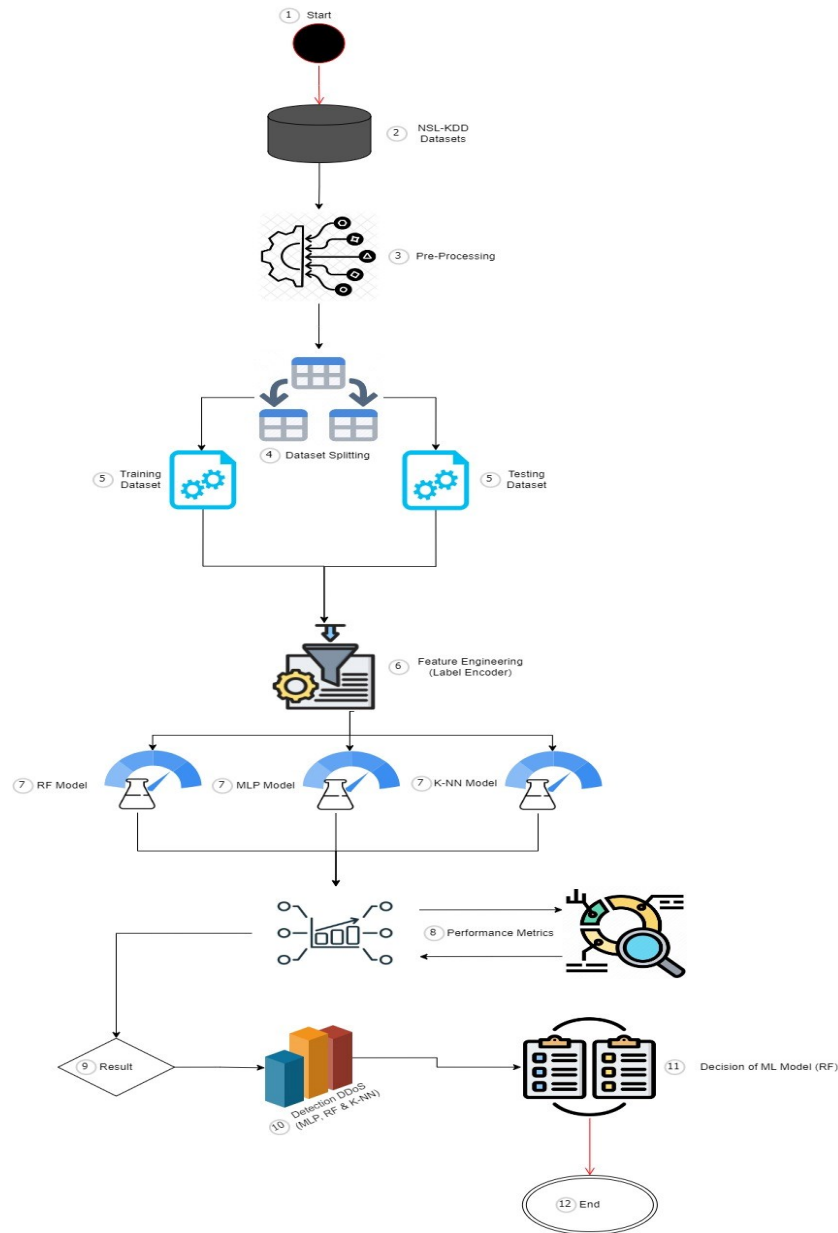


Figure 1. Overall Flow of the Proposed Work

4. RESULTS AND DISCUSSIONS

In our work, we carried out experiments on Windows 11 platform, 12th Gen Intel(R) Core(TM) i5-12500H 2.50 GHz laptop to test the efficiency of algorithms that was mentioned before.

4.1 Dataset Used

The rest of this section is organized as Dataset used, Evaluation Matrices and Result Discussion.

The NSL-KDD dataset, an upgraded version of the KDD'99 dataset, was used in this experiment. It is a popular dataset for today’s internet traffic standards [1]. The KDD'99 dataset originated from the KDD Cup (Data & Knowledge Mining Tournament) in 1999 as its first version. It encompassed all internet data records compiled during the tournament, later evolving into the NSL-KDD dataset. This dataset serves as an effective standard for researchers to compare different intrusion detection methods. It includes 4 subsets for training and testing purposes: KDDTest-21 for testing and KDDTrain_20Percent as a 20% subset of the entire training dataset. These datasets focus on simple intrusion detection in network traffic, capturing existing traces. Each record consists of 43 features, with 41 representing traffic inputs and the last two indicating labels and scores for normal/attack status and severity of traffic inputs. The NSL-KDD dataset covers four attack classes: DoS, U2R, Probe, and R2L. The dataset comprises 25,192 records in KDDTrain20%, 125,973 in KDDTrain, and 22,544 in KDDTest, encompassing various types of internet traffic attacks, including normal traffic. Detailed information on the NSL-KDD Dataset is provided in Figure 2.

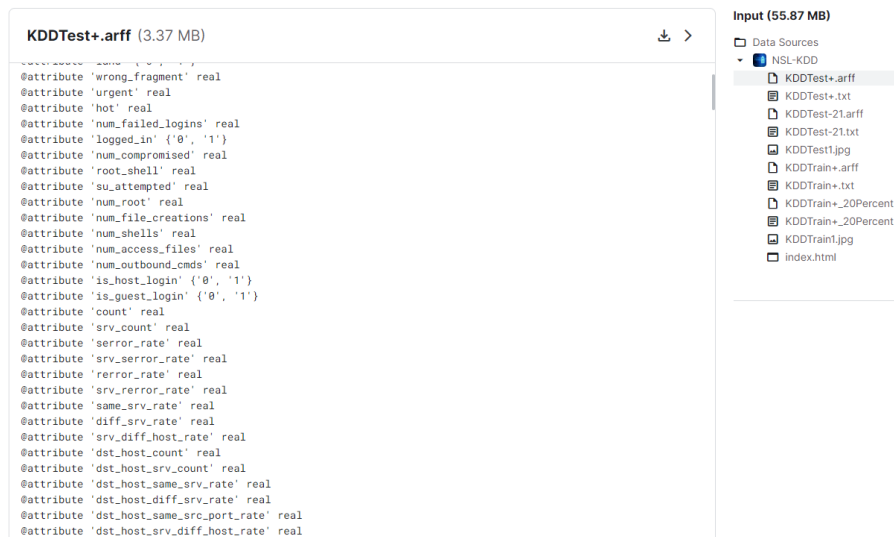


Figure 2. Train And Test Subsets Of NSL-KDD Dataset.

An analysis is provided that thoroughly examines common protocol types and various network attacks, highlighting potential vulnerabilities in network traffic. For detailed information, please refer to Tables 2 and 3.

Table 2. Types of Protocol Attack

Attack	Description
back	Backdoor attack types
buffer overflow	Buffer Overflow attack types
ftp write	Attempts to write file with FTP (File Transfer Protocol)
guess passwd	Attempts to guess password
imap	Targeting the Internet Message Access Protocol
ipsweep	Try reconnaissance on network attempts to scan IP addresses
land	Land attack type
loadmodule	Load modules/ executables
multihop	Multiple hops/ intermediate points
neptune	Neptune Denial of Service (DoS) attack
nmap	Try to attempt network scanning using nmap tools
normal	Non-attack
perl	Perl-based attacks

phf	Exploit the PHF (Remote File Access) vulnerability
pod	Ping of Death attack
portsweep	Try reconnaissance on network attempts to scan port number
rootkit	Rootkits on target system
satan	Try to attempt network scanning using satan tools
smurf	Smurf Denial of Service (DoS) attack
spy	Spyware attack
teardrop	Teardrop Denial of Service (DoS) attack
warezclient	Attempts to warez (Pirated software) clients
warezmaster	Master servers/ entities that related with warez

Table 3. Details of Protocol

Traffic Protocols	Benign	Malicious
ICMP	1309	6982
TCP	53599	49089
UDP	12434	2559

4.2 Evaluation Metrics

4.2.1 Confusion Metrics

The performance evaluation of these systems is typically conducted using the information provided by the matrix shown in Table 4.

Table 4. System Performance Measurement

		Predicted Class	
		Normal	Attack
Actual Class	Normal	TP	FP
	Attack	FN	TN
		Normal	Attack

4.2.2 Precision

The total number of correctly predicted DDoS attack instances divided by the sum of predicted true and false DDoS attacks as shown in Equation (6).

$$Precision = \frac{TP}{TP+FP} \quad (6)$$

4.2.3 Recall

Equation (7) calculates Recall using the total number of predicted DDoS attacks divided by the total number of actual DDoS attacks.

$$Recall = \frac{TP}{TP+FN} \quad (7)$$

4.2.4 F1-Score

F1-score can be calculated using Equation (8).

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

4.2.5 Accuracy

The role of metrics for evaluating classification models is evaluated for the accuracy and predictions with the percentage. For example, the accuracy of detection DDoS attack can be evaluated based on faultlessly classified with attacks in database (see Equations (9) and (10)).

$$\text{Accuracy} = \frac{\text{Number of correct prediction}}{\text{Total number of prediction}} \quad (9)$$

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

4.3 Result Discussion

To detect various attacks from the NSL-KDD datasets, Jupyter Notebook was used to perform both binary and multi-class classification. Table 5 shows the performance of binary classification with 3 algorithms (RF, MLP & K-NN) and Table 6 shows the summary of the accuracy achievement. Table 7 displays the performance of multi-class classification and Table 8 shows the summary of it. It depicts the comparison of predicted precision values, recall values, f1-score values, support, macro/weighted average and accuracy of all classes for each classifier. From the table, it is clear that RF outperforms others in both binary and multi-class classification.

Table 5. Performance Of Binary Classification

RF				
	Precision	Recall	F1-Score	Support
Normal	100%	99%	99%	13385
Attack	99%	99%	99%	11810
Accuracy			99%	25195
Macro Average	99%	99%	99%	25195
Weight Average	99%	99%	99%	25195
MLP				
	Precision	Recall	F1-Score	Support
Normal	90%	93%	91%	13385
Attack	92%	88%	90%	11810
Accuracy			91%	25195
Macro Average	91%	90%	91%	25195
Weight Average	91%	91%	91%	25195
K-NN				
	Precision	Recall	F1-Score	Support
Normal	99%	99%	99%	13385
Attack	99%	99%	99%	11810
Accuracy			99%	25195
Macro Average	99%	99%	99%	25195
Weight Average	99%	99%	99%	25195

Table 6. Accuracy Achievement of Binary Classification

Method	Binary Accuracy
RF	99.35%
MLP	91%
K-NN	99.15%

Table 7. Performance of Multi-Class Classification

RF				
	Precision	Recall	F1-Score	Support
Normal	100%	99%	99%	13388
DoS	95%	99%	97%	9268
Probe	98%	82%	90%	2334
U2R	67%	73%	70%	11
Sybil	99%	96%	98%	194
Accuracy			98%	25195
Macro Average	92%	90%	91%	25195
Weight Average	98%	98%	98%	25195
MLP				
	Precision	Recall	F1-Score	Support
Normal	97%	84%	90%	13388
DoS	86%	89%	87%	9268
Probe	44%	76%	56%	2334
U2R	100%	0%	0%	11
Sybil	100%	0%	0%	194
Accuracy			84%	25195
Macro Average	85%	50%	47%	25195
Weight Average	88%	84%	85%	25195
K-NN				
	Precision	Recall	F1-Score	Support
Normal	99%	99%	99%	13388
DoS	95%	99%	97%	9268
Probe	98%	80%	88%	2334
U2R	100%	45%	62%	11
Sybil	99%	95%	97%	194

Accuracy			97%	25195
Macro Average	98%	84%	89%	25195
Weight Average	97%	97%	97%	25195

Table 8. Accuracy Achievement of Multi-Class Classification

Method	Multi-Class Accuracy
RF	97.71%
MLP	84.33%
K-NN	97.35%

Figures 3 and 4 will display the confusion matrix of RF methods resulting in detection DDoS attack. RF has an ability to handle a large dataset, provides also the robust of predictions and offers a insights that for the feature importance. In this experiment, RF classification used to predict normal and attack network traffic. It can label the testing data (normal and attack) to classify new or unseen instances of traffic. Besides, RF can also predict the amount of network traffic and future traffic volumes based on historical data.

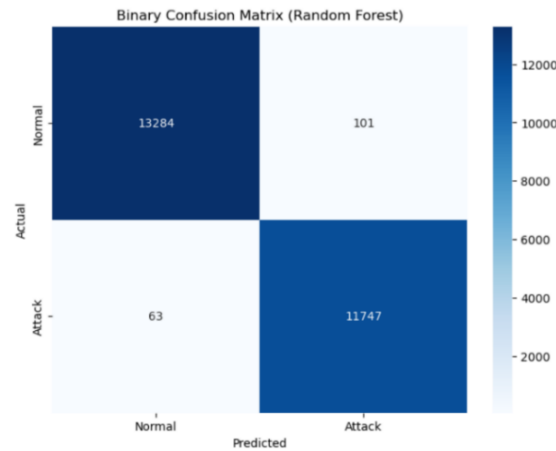


Figure 3. Binary Confusion Matrix of RF

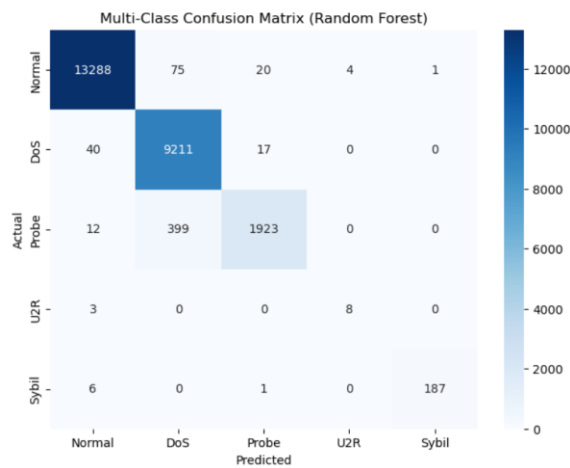


Figure 4. Multi-class Confusion Matrix of RF

Binary and multi-class ROC curve plots for the Random Forest, Multilayer Perceptron, and K-Nearest Neighbors models, are shown in Figures 5 and 6. These plots allow for a visual comparison of the models' performance by illustrating the trade-off between the True Positive Rate and the False Positive Rate for each model.

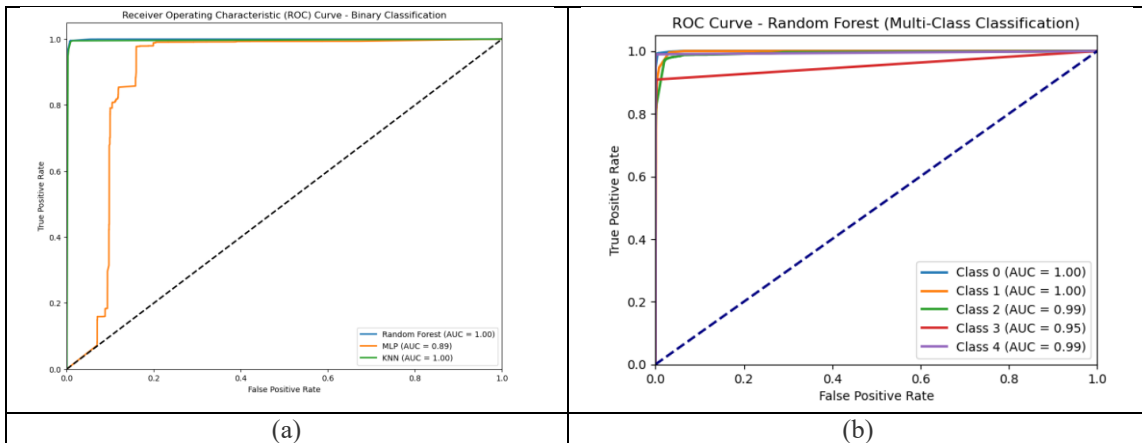


Figure 5. ROC Curve: (a) Binary Class for Random Forest; (b) Multi-Class for Random Forest

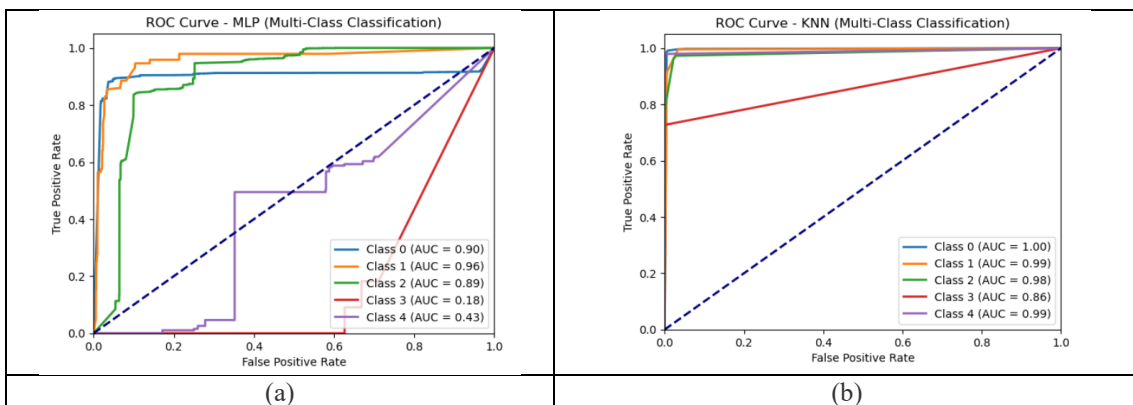


Figure 6. Multi-Class Classification ROC Curve: (a) MLP; (b) KNN

It can be summarized that Random Forest achieves the best performance among other classification methods. It gets the highest accuracy of 99.35% for binary classification and 97.71% for multi-class classification. MLP in this experiment performs slightly poorer with 90.63% in binary classification and 84.33% in multi-class classification whereas KNN achieves 99.15% for binary classification and 97.35% for multi-class classification. Figure 7 shows the comparison of three classification models which are Random Forest, Multilayer Perceptron and K-Nearest Neighbors.

5. CONCLUSION

This paper proposes a novel DDoS detection method that leverages the Random Forest Classification model. By integrating Random Forest Classification with network traffic characteristics and addressing the limitations of existing machine learning algorithms, this approach enhances detection accuracy. The paper introduces the concept of attack-specific information entropy to differentiate between TCP flood, UDP flood, and ICMP flood attacks. Separate detection models are established for each attack type to improve detection precision. Simulation results show that the Random Forest Classification model effectively differentiates between normal and attack traffic, achieving a higher detection rate and a lower false alarm rate compared to both Multilayer Perceptron (MLP) and K-Nearest Neighbors (KNN). This improved performance highlights the efficacy of the Random Forest Classification model in enhancing DDoS detection capabilities. The project utilizes the NSL-KDD dataset to compare Random Forest, MLP, and Naive Bayes (NB) in detecting DDoS attacks. It highlights the effectiveness of preprocessing and algorithm selection,

although it notes limitations such as the lack of feature engineering and Label Encoding. Future work aims to address these issues and enhance detection capabilities. Random Forest achieved 99% accuracy in binary classification and 97% in multi-class classification, demonstrating its effectiveness and potential for handling complex datasets.

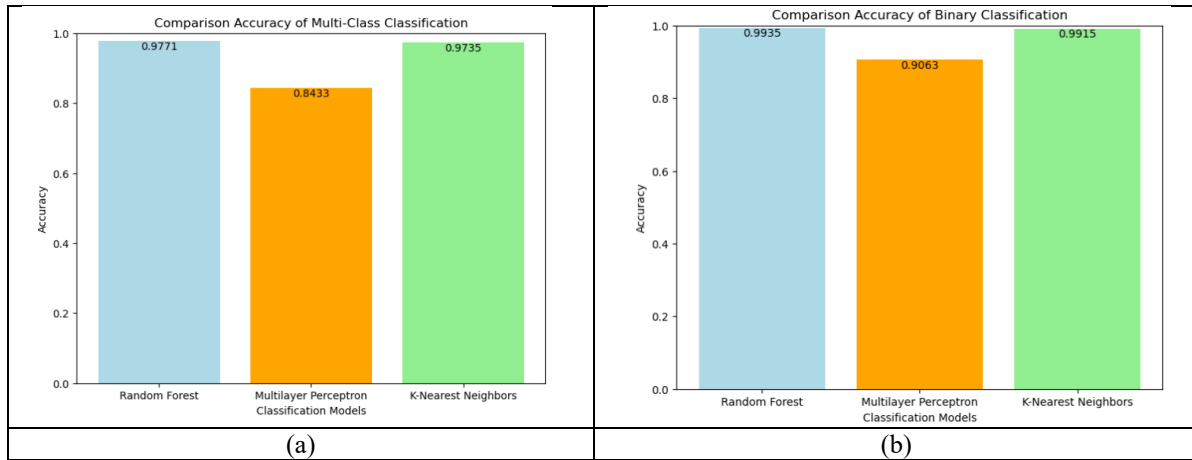


Figure 7. Comparison Accuracy of: (a) Multi-Class Classification; (b) Binary Classification.

ACKNOWLEDGEMENT

The authors received no funding from any party for the research and publication of this article.

FUNDING STATEMENT

This research received no specific grant from any funding agency

AUTHOR CONTRIBUTIONS

Wei-Wu Tay: Model Training, Methodology, Validation, Writing – Original Draft Preparation;
Siew-Chin Chong: Project Administration, Supervision, Writing – Review & Editing;
Lee-Ying Chong: Data Tuning, Writing – Review & Editing.

CONFLICT OF INTERESTS

No conflict of interests was disclosed.




REFERENCES

- [1] Datasets, Canadian Institute for Cybersecurity, [Online]. Available: <https://www.unb.ca/cic/datasets/index.html>
- [2] A. N. Rimal and R. Praveen, “DDOS Attack Detection Using Machine Learning”, 2020. <https://www.jetir.org/view?paper=JETIR2006031>.
- [3] IBM, “Random Forest.” [Online]. Available: <https://www.ibm.com/topics/random-forest>.

- [4] T. A. Khan, R. Sadiq, Z. Shahid, M. M. Alam, and M. M. Su'ud, "Sentiment Analysis using Support Vector Machine and Random Forest," *Journal of Informatics and Web Engineering*, vol. 3, no. 1, pp. 67–75, 2024, doi: 10.33093/jiwe.2024.3.1.5.
- [5] L. C. Wei-Jie, S.-C. Chong, and T.-S. Ong, "Masked face recognition with principal random forest convolutional neural network (PRFCNN)," *Journal of Intelligent & Fuzzy Systems*, vol. 43, no. 6, pp. 8371–8383, 2022, doi: 10.3233/jifs-220667.
- [6] H. Nurwarsito and M. F. Nadhif, "DDoS Attack Early Detection and Mitigation System on SDN using Random Forest Algorithm and Ryu Framework," in *Proc. 8th Int. Conf. Computer and Communication Engineering (ICCCE)*, 2021, pp. 178-183, doi: 10.1109/iccce50029.2021.9467167.
- [7] N. Mohapatra, K. Shreya, and A. Chinmay, "Optimization of the Random Forest Algorithm," in *Lecture notes on data engineering and communications technologies*, 2020, pp. 201–208. doi: 10.1007/978-981-15-0978-0_19.
- [8] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method," *Symmetry*, vol. 14, no. 6, p. 1095, 2022, doi: 10.3390/sym14061095.
- [9] T. S. Chu, W. Si, S. Simoff, and Q. V. Nguyen, "A Machine Learning Classification Model Using Random Forest for Detecting DDoS Attacks," *International Symposium on Networks, Computers and Communications (ISNCC)*, 2022, doi: 10.1109/isncc55209.2022.9851797.
- [10] J. Pei, Y. Chen, and W. Ji, "A DDoS Attack Detection Method Based on Machine Learning," *Journal of Physics Conference Series*, vol. 1237, no. 3, p. 032040, 2019, doi: 10.1088/1742-6596/1237/3/032040.
- [11] T. E. Ali, Y.-W. Chong, and S. Manickam, "Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review," *Applied Sciences*, vol. 13, no. 5, p. 3183, 2023, doi: 10.3390/app13053183.
- [12] Scikit-learn, "Neural network models." [Online]. Available: https://scikit-learn.org/stable/modules/neural_networks_supervised.html.
- [13] M. S. Christo, J. J. Menandas, M. George, and S. V. Nuna, DDoS Detection using Multilayer Perceptron, *International Conference on Electronics and Sustainable Communication Systems (ICESC)*, India, 2023, pp. 688-693, doi: 10.1109/ICESC57686.2023.10193406. d
- [14] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," *Computers & Security*, vol. 88, p. 101645, Oct. 2019, doi: 10.1016/j.cose.2019.101645.
- [15] IBM, "K-Nearest Neighbors (KNN)." [Online]. Available: [https://www.ibm.com/topics/knn#:~:text=The%20k%2Dnearest%20neighbors%20\(KNN,used%20in%20machine%20learning%20today](https://www.ibm.com/topics/knn#:~:text=The%20k%2Dnearest%20neighbors%20(KNN,used%20in%20machine%20learning%20today).
- [16] G. G. Priya, S. H. Shriram, S. Jeeva, G. S. Priya, and K. Balasubadra, "Detection of Distributed Denial of Service (DDoS) Attack Using Logistic Regression and K Nearest Neighbor Algorithms," *International Journal of Intelligent Systems and Applications in Engineering*, 12(16s), pp. 503–508. <https://ijisae.org/index.php/IJISAE/article/view/4863>

- [17] H. Polat, O. Polat, and A. Cetin, "Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models," *Sustainability*, vol. 12, no. 3, p. 1035, 2020, doi: 10.3390/su12031035.
- [18] A. V. Kachavimath, S. V. Nazare and S. S. Akki, "Distributed Denial of Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics," *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, India, 2020, pp. 711-717, doi: 10.1109/ICIMIA48430.2020.9074929.
- [19] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2019, doi: 10.1109/access.2019.2963077.
- [20] S. Ray, "Naive Bayes Classifier Explained: Applications and Practice Problems of Naive Bayes Classifier," *Analytics Vidhya*, Aug. 23, 2024. <https://www.analyticsvidhya.com/blog/2017/09/naive-bayes-explained/>
- [21] A. Fadlil, I. Riadi, and S. Aji, "Review of Detection DDOS Attack Detection Using Naive Bayes Classifier for Network Forensics," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 2, pp. 140–148, 2017, doi: 10.11591/eei.v6i2.605.
- [22] K. Kumari and M. Mrunalini, "Detecting Denial of Service attacks using machine learning algorithms," *Journal of Big Data*, vol. 9, no. 1, 2022, doi: 10.1186/s40537-022-00616-0.
- [23] F. F. Setiadi, M. W. A. Kesiman, and K. Y. E. Aryanto, "Detection of dos attacks using naive bayes method based on internet of things (iot)," *Journal of Physics Conference Series*, vol. 1810, no. 1, p. 012013, 2021, doi: 10.1088/1742-6596/1810/1/012013.
- [24] R. F. Fouladi, C. E. Kayatas, and E. Anarim, "Frequency based DDoS attack detection approach using naive Bayes classification," *International Conference on Telecommunications and Signal Processing (TSP)*, Austria, 2016, pp. 104-107, doi: 10.1109/TSP.2016.7760838.
- [25] G. Saporito, "A Deeper Dive into the NSL-KDD Data Set - Towards Data Science," *Medium*, Jul. 13, 2023. [Online]. Available: <https://towardsdatascience.com/a-deeper-dive-into-the-nsl-kdd-data-set-15c753364657>
- [26] L. Chen, Y. Zhang, Q. Zhao, G. Geng, and Z. Yan, "Detection of DNS DDoS Attacks with Random Forest Algorithm on Spark," *Procedia Computer Science*, vol. 134, pp. 310–315, 2018, doi: 10.1016/j.procs.2018.07.177.
- [27] M. S. Christo, J. J. Menandas, M. George, and S. V. Nuna, "DDoS Detection using Multilayer Perceptron," *International Conference of Electronics and Sustainable Communication Systems (ICESC)*, 2023, doi: 10.1109/icesc57686.2023.10193406.
- [28] Z. Ma and B. Li, "A DDoS attack detection method based on SVM and K-nearest neighbour in SDN environment," *International Journal of Computational Science and Engineering*, vol. 23, no. 3, p. 224, Jan. 2020, doi: 10.1504/ijcse.2020.111431.

BIOGRAPHIES OF AUTHORS

	<p>Wei-Wu Tay is a dedicated student at Multimedia University, where he is pursuing a Bachelor of Information Technology (Hons) in Security Technology. With a strong passion for cybersecurity, Wei Wu has honed his skills and knowledge in this field. For his final year project, he developed an innovative approach to detecting DDoS attacks using machine learning techniques. This project highlights his ability to tackle real-world security challenges and demonstrates his commitment to advancing cybersecurity through cutting-edge technology.</p>
	<p>Siew-Chin Chong, an IEEE Senior Member, earned her B.IT in Software Engineering, M.Sc in Information Technology, and Ph.D. in Information Technology from Multimedia University in 2003, 2006, and 2018, respectively. Currently, she is the Deputy Dean of Student Experience & Alumni at the Faculty of Information Science and Technology, Multimedia University, Malaysia. Her research interests include machine learning, biometric security, and mobile app development, and she has published extensively in these areas. Additionally, she has served as an Editorial Board Member for several journals and as Technical Chair for numerous international conferences.</p>
	<p>Lee-Ying Chong received B. IT. (Hons.) majoring in Information System Engineering in year of 2003. She received her Master degree in Science, majoring Information Technology from Multimedia University, in the year of 2007. She obtained the degree of Doctor of Philosophy (Information Technology) in year 2018. Her current research interests include biometrics authentication, computer vision and machine learning. She is senior member of IEEE since 2013. Currently she is working as a senior lecturer in Faculty of Information Science and Technology, Multimedia University, Malaysia.</p>