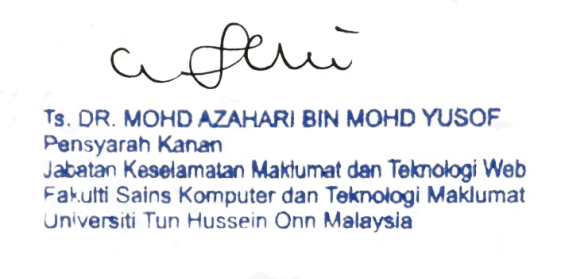
****

|  |  |  |
| --- | --- | --- |
|  |  | **DDoS ATTACK DETECTION USING MACHINE LEARNING**  **Nurallisya Mohd Ali**1**, Mohd Azahari Mohd Yusof**1\*  1Faculty of Computer Science and Information Technology,  Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA  DOI: https://doi.org/10.30880/aitcs.0000.00.00.000  Received 00 Month 2023; Accepted 01 Month 2023; Available online 02 Month 2023  ***Abstract:*** *Distributed Denial of Services (DDoS) attacks become a very dangerous issue in cyber threats due to the demand of new technologies that encourage attackers to find any possible approach to carry out such attacks. DDoS attacks work by sending amount of network traffic to servers that exceed normal traffic capacity that can cause damage on device functionality and slow down network performance. One of the ways to detect DDoS attacks is by using machine learning techniques that has been proven effectively combats DDoS attacks. Numerous researchers have investigated this topic with improved accuracy on different datasets using variety of classifiers but the result still not the best for the detection. The results of this research will be shown in terms of accuracy, precision and detection rate and will be conducted using UNSW-NB15 dataset. The important processes that need to go through to obtain the best features are starting with data preprocessing, feature selection and then data splitting. Meanwhile, for the classification process the algorithms that will be used are Support Vector Machine (SVM), Naïve Bayes (NB) and K-Nearest Neighbor (KNN). At the end of the experiment, KNN produced the highest percentage of detection in terms of accuracy, precision and detection rate.*  ***Keywords:*** *DDoS attacks, machine learning, dataset, accuracy, precision, detection rate* |

1. **Introduction**

There are many malicious attacks nowadays done by attackers to fulfill their desire for some specific purpose. One of the most frequent attacks that happen is Detection of Distributed Denial-of-Service (DDoS) attacks that give such a serious impact and damage if reduction and mitigation processes are not implemented to reduce the attack [2]. DDoS attack is a malicious intrusion attack to disrupt the normal operation of an intended server, service, or network by overwhelming the target or surrounding architecture with large amounts of Internet traffic [7].

This project will be focused on Detection of Distributed Denial-of-Service (DDoS) attacks using machine learning. The various implementations of cyber technologies nowadays gives such a deep and serious impact which can be leveraged by attackers to step forward in doing sophisticated DDoS attacks through the vulnerabilities of Internet-of-Things (IoT) [6]. Frequently, the DDoS attackers target any online services and websites which are actively in networks by sending them a bunch of traffic through the network and some other flood attacks such as Common Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) flood attacks [3].

Besides, a lot of research has been done and some progress has been made by researchers in order to prevent and decrease the crime which is DDoS attacks. Based on research [8], it used supervised and unsupervised machine learning algorithms for detection. At the end of experiment, the supervised algorithms surpass unsupervised learning algorithms which KNN, Naive Bayes and SVM algorithms are better at detecting web attacks than the other algorithms. The research result for those three algorithms obtained the highest score in terms of accuracy, precision and detection rate that will show in section 4. This existing research support this proposed research to be implemented to provide better results for DDoS detection.

Consequently, due to the variety of DDoS attack modes and changeable size of traffic packets, until now it is still quite tough to find the best detection method with adequate detection accuracy. DDoS attacks are one of the computer crimes that will become seriously ill in an organization and apparently it will be more dangerous if done late prevention [11].

The purpose of this research is to implement detection methods using machine language for DDoS attack produce a good detection rate percentage for the current popular mode of DDoS attack. The machine learning that has been chosen in this project is Support Vector Machine (SVM), K-Nearest Neighbor (KNN) and Naive Bayes with some test on chosen dataset, UNSW-NB15 dataset to improve detection accuracy for DDoS attack. Moreover, to determine the effectiveness of intrusion detection, there are some measure parameters used, detection accuracy, precision and detection rate percentage.

The remaining of this paper will discuss the works related to this proposed research and contain a comparison of existing researches obtained from reliable sources through the internet in section 2. Section 3 will explain the the research methodology framework used to complete the experiment that consist of dataset preparation, data preprocessing, feature selection and data splitting and lastly classification algorithms on DDoS attacks. Lastly, section 4 will be discuss on results and discussion related to the proposed research.

1. **Related Work**

DDoS attacks are malicious cyber-attacks that infiltrate a targeted server's traffic by sending excessive requests, causing the website to crash [8]. Common targets include online shopping, banking transactions, and government sites. Mitigation and prevention measures are crucial to reduce these attacks and protect websites. DDoS attacks detection using machine learning technique is a method that the most widely used and trusted by many researchers to reduce the attack. This section consist of how DDoS attacks, DDoS works, DDoS features and DDoS attack detected between three previous research [1][4][6] and proposed research.

The first existing research [1], has successful detect a few classes of attacks in the CICIDS2017 dataset. This research evaluation considers numerous variables, including various types of raw network datasets and recommended performance measures which more details to generate results using machine learning technique. Moreover, the strength of this research is comparative studies has been carried out to evaluate the development of effective machine learning algorithms which is not only for supervised but also containing of unsupervised Machine Learning algorithms such as Artificial Neural Network (ANN), Decision Tree (DT), K-Nearest Neighbor (KNN), Naïve Bayes (NB), Random Forest (RF), Support Vector Machine (SVM), Convolution Neural Network (CNN), Expectation-Maximization (EM), K-means, and Self-Organizing Map (SOM). However, the performance of related algorithm models with multi-classification, have limits in recognizing novel sorts of attacks which the accuracy result obtained did not achieve the best result for accuracy. This will cause low result in terms of detection rate for this research.

According to the second research [4] there were two different datasets has been used to conduct the experiment. There are KDD CUP 99 and NSL-KDD datasets. Furthermore, the classifiers used for this research only two namely KNN and NB. The strength of this study is it shows the performance of classification algorithm results clearly using a few parameter measurements which are Accuracy, Precision Recall, F-Measure, Sensitivity, Specificity, Efficiency, and Error Rate. Unfortunately, this research used only two techniques which cannot be references to other researches that are not related and also the accuracy results obtained for both techniques still shows the lowest between other research result.

Besides, this research [6] is unique than other previous research that has been mentioned. This research uses a new dataset collected with modern DDoS attacks. The technique used for this research was SVM, KNN, NB, Random Forest and Neural Network. The strength of this research can be shown with the used of more supervised machine learning technique that can provides the highest result for DDoS detection. Consequently, the result in terms of accuracy for SVM, KNN and NB are still not the highest result obtained for accuracy that can mitigate the attacks. Because of that, it will affect the lower detection rate score either for normal or DDoS attacks.

2.5 Comparative Technique between Previous Research and Proposed Research

Table 1 shows the comparison of classification algorithms technique in detecting DDoS attacks between three existing research and proposed system:

**Table 1: Comparison techniques between previous ​research​ and proposed research**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Authors | Technique | | | DDoS Packet Detected | |
| p | SVM | NB | KNN | Benign | DDoS |
| Proposed Research | **√** | **√** | **√** | **√** | **√** |
| [1] | **√** | **√** | **√** | **√** | **√** |
| [4] | N/A | **√** | **√** | **√** | **√** |
| [6] | **√** | **√** | **√** | **√** | **√** |

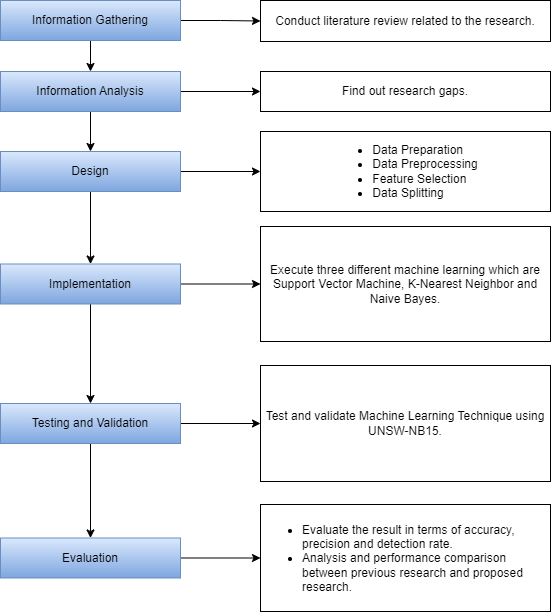
Table 1, shows the comparison technique between three different previous research and proposed research. The first research [1] the performance of related algorithm models with multi-classification, have limits in recognizing novel sorts of attacks which the accuracy result obtained did not achieve the best result for accuracy. This will cause low result in terms of detection rate for this research.

The second research [4] gaps can be seen that this research only used two techniques which cannot be references to other researches that are not related with the study. While, the accuracy results obtained for both techniques still shows the lowest between other research results.

The third research [6] constraints can be seen that the highest result in terms of accuracy for SVM, KNN and NB are still not gained the highest result of accuracy that can reduce the attacks. Because of that, it can cause lower detection score to detect either normal packets or DDoS attacks.

**3. Research Methodology**

Based on the Figure 1, it shows all phases that are sophisticated to be conducted to get the better result for DDoS detection. This section will explain about Information Gathering, Information Analysis, Design, Implementation, then continue with data preprocessing, feature selection, data splitting and lastly classification of DDoS attacks.



**Figure 1: Framework for DDoS attacks detection**

3.1 Information Gathering

Information gathering in DDoS detection using machine learning techniques that involves studying various research papers and articles to understand the different approaches and methods used to detect DDoS attacks using machine learning algorithms. The implementation of research on DDoS detection using machine learning techniques is based on information gathered through the reading process of various research papers and articles. The literature review was conducted, involving the selection of three different machine learning algorithms, namely SVM, KNN, and Naive Bayes. In addition, the reading about parameter measurement that has been used in existing research, especially in terms of accuracy, precision, and detection rate, is also highlighted as an important part of the literature review to observed and evaluate the performance of algorithms. The study of UNSW-NB15 dataset has been conducted, and a few things obtained from reading, such as the packet capture tool compares captured attack packets, finds attack rules, and converts them into attack data characteristics for machine learning input, which the attacks will be classified into two classes that are normal packets and DDoS attacks. The limitations of several DDoS detection technologies, including statistical and machine learning methods, have been investigated.

3.2 Information Analysis

Information analysis is an important part to find out research gaps that are important to analyze the information gathered from various sources. This will assist in identifying the strengths and drawbacks of current techniques and highlighting areas where additional research is required related to machine learning technique. Furthermore, the research gaps can be discovered and addressed by undertaking a literature survey, systematic review, survey, and taxonomy to increase the effectiveness of DDoS detection using machine learning techniques. The research gap for the proposed research is that, this research only uses three classification algorithms such as SVM, KNN and Naïve Bayes. In order to demonstrate the effectiveness of using machine learning techniques to detect DDoS attacks, it is recommended to use more algorithms to measure the performance of classifiers for reducing DDoS attacks.

3.3 Design

The research design for this proposed research consists of four phases. There are data preparation, data preprocessing, feature selection and data splitting on the chosen dataset, UNSW-NB15. In the next subtopics, the explanation of each phase in more detail.

* Data Preparation

In this research, the dataset name as UNSW-NB15 dataset was taken from an online source, gitHub.com with source file in .csv will be used as input to detect DDoS attacks. Throughout this experiment, DDoS attacks can be seen clearly in many types of network traffic such as Normal, Backdoor, Analysis, Fuzzers and more attacks from the chosen dataset. It is very helpful for the purpose of this research which is to classify the attacks into normal packet category or other types of DDoS attacks.

* Data Preprocessing

Data Preprocessing in this purpose research involves data selection and data reduction methods to select only the highest rank of features and the lowest one will be removed. The DDoS attack can be easily classified into normal packet traffic or other DDoS attack traffic. The data removing step is very helpful and important to reduce time consuming in the learning process and also increase the detection accuracy to determine the attacks. The result after the preprocessing process, from forty-five features in total only five features reduction that is not important in producing the best score of accuracy, precision and detection. It is because the other five features are in String data type which can be outliers in the dataset. If these outliers are not being terminated, the feature selection cannot proceed.

* Feature Selection

Feature Selection is a process to select the best features from datasets for DDoS attacks by going through some filter steps which part of it name as Information Gain method [5]. This technique has its own benefits where it can filter all features by only taking relevant data based on the specific purpose, improve learning accuracy rate and get rid of unrelated sample data. As for the proposed research, only the highest rank of features takes for the experiment and remove all unnecessary features which only five from the original total of features which is forty-five features.

* Data Splitting

Data splitting is a process to split a dataset for training the model and testing the sample data by using the classification algorithms. Moreover, this process consists of two approaches which are cross-validation and holdout. The most common technique used is cross-validation as it produces better results than holdout which shows less bias as it takes all available data in action. As for this research, the split ratio for training and testing the selected features is 80:20 for this experiment. The best result obtained for training the model should be 80% while for the testing it should be 20%. It is stated that the ratio for train and test data is 80:20 in the analysis process using machine learning techniques, which is acceptable. The data splitting process can make the classifiers learn the sample data better with diverse features of DDoS attacks. Basically, data splitting needs to be done in machine learning techniques to prevent over fitting of the data and the model obtained will generate biased results for the experiment.

3.4 Implementation

In this section, the implementation of this research involving the execution of three different machine learning algorithms will be explain in detail which are Support Vector Machine, K-Nearest Neighbor and Naive Bayes. This subtopic will discuss the significance and benefits of each classifier to the research for a better result of detection.

Firstly, this research has chosen SVM classifier as it is the most commonly used for handling problems related to Machine Learning technique. This classifier can be declared as one of the classification algorithms that generate the highest result in terms of detection accuracy which is appropriate for this research. The SVM algorithm represents each data point as a point in n-dimensional space (where n is the number of features), with the value of each feature being the value of a specific coordinate. After that, the classification process will be carried out by selecting the hyper-plane that effectively differentiates the two classes.

The second choice of classifiers for this research is Naive Bayes classifier. Based on the information stated in the IBM page, Naive Bayes assumes the independence of each and every predictor by using Bayes algorithms .The benefits of choosing this classifier for this proposed research is less time consuming for training and testing the sample data. Addition, it is also simple and easy to implement because it uses simple language that is readable and understandable for the learning process.

Lastly, the classifier used for this research is KNN. It works by classifying a new data point based on similarity. Moreover, The KNN is an effective passive learning algorithm that has been used in a variety of applications [9]. Based on the information obtained through reading, the advantages of the classification process by KNN algorithm is that there is no explicit training phase and that all work is done during prediction. In conclusion, at the end of the experiment, the classifier will successfully classify DDoS attacks into two groups, namely normal attacks and other DDoS attacks and be able to produce parameter evaluation metrics in terms of precision, accuracy and detection rate.

3.5 Testing and Validation

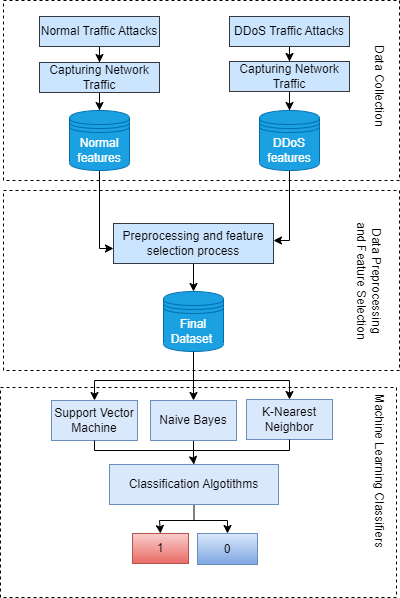
The UNSW-NB15 dataset is widely used to test and validate machine learning approaches in intrusion detection systems, mainly used to detect DDoS attacks. The original amount of features in the dataset is 45 features and different types of DDoS attacks that need to classify. The dataset file stored in .CSV files. The dataset is divided into a training set and a testing set, with 140,272 records in the training set and 35069 records in the testing set. To ensure the performance of classifier models, the dataset is analyzed in terms of accuracy, precision and detection rate. The most informative input features are extracted to prevent misleading clustering results and reduce computational cost. The UNSW-NB15-Test is utilized for testing the validated models, ensuring that none of the models are over fitting. Other information that can be mentioned here is that many research papers have been published on the UNSW-NB15 dataset, focusing on Intrusion Detection Systems built using machine learning techniques, such as deep learning models and feature selection methods.

3.6 Evaluation

The evaluation of DDoS attack detection using machine learning techniques can be done by analyzing the accuracy, precision, and detection rate of the proposed classification algorithms. The selected machine learning algorithms (SVM, KNN and Naive Bayes) used in the proposed research can be predicted to successfully recognize patterns and deviations in network traffic that signal DDoS attacks with high accuracy and efficiency which is critical for effective DDoS detection [10]. The evaluation of results obtained from the algorithms performance on the selected dataset will be compared to determine which algorithms produce the best result of detection. After that, to show the contribution of this research, the comparison of technique used will be made between previous research and proposed research.

3.7 Architecture

The experimental research framework for this research will starts with installing Anaconda software in the computer research and using the Jupyter Notebook tool. Thus, Python Language is regarded as an appropriate programming language for both simulations and practical programming. For model learning, it is regarded as the most potent high level language and obviously the most effective language to run the analysis for DDoS attacks detection.

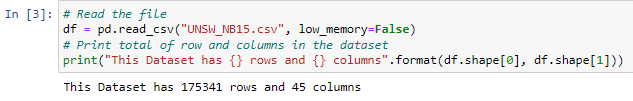


**Figure 2: Experimental design for proposed research**

Figure 2 shows the experimental design for the proposed research. First of all, the experiment cannot be implemented without having a collection of sample data called as a dataset and this phase called, data preparation. As mentioned, the dataset for this proposed research is the UNSW-NB15 dataset. The next phase should be data preprocessing which the function is transforming raw data into something that can be used by a machine learning model. Then, the feature selection process is a phase by only taking the highest rank of features and getting rid of the irrelevant features. The experiment continues with data splitting which the dataset needs to be trained and tested using the classification algorithms. Lastly, the phase should be classification algorithms using Support Vector Machine (SVM), Naive Bayes and K-Nearest Neighbor (KNN). In order to find the effectiveness and the smartest classifiers for DDoS attacks detection, the highest result obtained in terms of accuracy, precision and detection rate need to be observed at the end of the experiment with successfully classified the DDoS attacks into normal packet and other types of DDoS attacks.

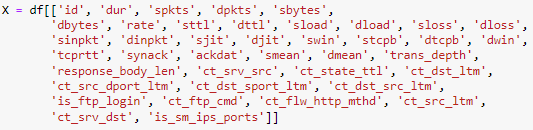
**4. Result and Conclusion**

Data preparation is a crucial step in implementing machine learning techniques for DDoS detection. There are datasets available for classifying network traffic, and for this research UNSW\_NB15 dataset has been selected.



**Figure 3: Coding part to read the dataset in .csv file**

Figure 3 shows a part of Python coding to show the total amount of records in the dataset that consist of 175,341 records with 45 features.



**Figure 4: Cleaned features of UNSW-NB15 after preprocessing**

Figure 4 shows the data preprocessing and feature selection in order to ensure only relevant features and highest rank of features used for DDoS detection. While, irrelevant features will be removing from the dataset to ensure the highest score gained by machine learning algorithms to detect normal and DDoS attacks. The technique involved in preprocessing is data cleaning process, where the dataset must be cleaned of duplicates, missing values ​​and unnecessary information before continue with feature selection. This ensures the dataset is accurate and comprehensive for classifier models to generate appropriate results for detection. The total of original features is 45 but in Figure 4 shows only 40 features was selected which mean another 5 features are not necessary for experiment.

**Table 2: Result of training and testing sets in UNSW-NB15 dataset**

|  |  |  |
| --- | --- | --- |
| Total Data | Training (80%) | Testing (20%) |
| 175,341 | 140,272 | 35069 |

The implementation of data splitting process is to train and test the ability of algorithms which are SVM, KNN and Naïve Bayes to identify DDoS attacks either normal traffic packets or other DDoS attacks. Basically to generate such an accurate result for this research, the dataset needs to be divided into two subsets. As for this experiment, the chosen ratio for training and testing is 80:20 which is 80% for the training and 20% for the testing set. According to Table 2, the result for the training set consists of 140,272 records while the testing set has 35,069 records.

**Table 3: Classification algorithms performance result for proposed research**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Machine Learning Algorithms | Accuracy (%) | Precision | Detection Rate | |
| Normal | DDoS |
| SVM | 98.70 | 97.50 | 89.85 | 98.52 |
| NB | 90.67 | 95.00 | 79.22 | 93.91 |
| KNN | 99.60 | 98.58 | 91.63 | 96.58 |

The classification algorithms performance result can be seen in Table 3 which the highest score obtained for DDoS attacks detection is provided by KNN and the second place should be SVM and last but not least go to Naive Bayes. The highest accuracy obtained is KNN with 99.60% followed by SVM with a score of 98.70% and finally NB, 90.67%. The first place for precision is also earned by KNN with the highest score, 98.58%, SVM with 97.50% and the score of NB is 95.00%. Then, the highest score for detection rate for normal attacks is obtained by KNN with score 91.63%, while the score of SVM and NB each of them 89.85% and 79.22%. Thus, the detection rate for DDoS attacks for SVM is the highest with score 96.58%, KNN obtained about 98.52% and 93.91% for NB. In short, the between SVM, NB and KNN results, the highest score obtained by KNN among other classifiers.

**Table 4: Comparison results between three previous research and proposed research**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Technique | Machine Learning Algorithms | Accuracy (%) | Precision | Detection Rate | |
| Normal | DDoS |
| Proposed technique | SVM | 98.70 | 97.50 | 89.85 | 98.52 |
| NB | 90.67 | 95.00 | 79.22 | 93.91 |
| KNN | 99.67 | 98.58 | 91.63 | 96.58 |
| Maseer et al,. 2021 | SVM | 96.72 | 99.27 | 96.72 | N/A |
| NB | 98.86 | 99.01 | 98.86 | N/A |
| KNN | 99.49 | 99.50 | 99.49 | N/A |
| Amit Kachavimath and Said Akki, 2020. | SVM | N/A | N/A | N/A | N/A |
| NB | 93.95 | 97.74 | N/A | N/A |
| KNN | 98.51 | 98.90 | N/A | N/A |
| Maslan et al,. 2020 | SVM | 98.41 | 100 | 100 | 84.80 |
| NB | 97.96 | 92.00 | 99.10 | 88.00 |
| KNN | 97.63 | 89.40 | 98.80 | 87.50 |

Table 4 shows the comparison between three previous research results with proposed research. The classification algorithms performance result for the proposed research has been explained in Table 3. In this section, it will be explain the result of those three previous research related to this research which is DDoS attacks detection using machine learning technique.

The result of classification algorithms performance for research [1] can be seen in Table 3 which the highest score obtained for DDoS attacks detection is provided by KNN and the second place should be NB and last but not least go to SVM. The highest accuracy obtained is KNN with 99.49% followed by NB with a score of 98.86% and finally SVM, 96.72%. The first place for precision is also earned by KNN with the highest score, 99.50%, SVM with 99.27% and the score of NB is 99.01%. Then, the highest score for detection rate for normal attacks is obtained by KNN with score 99.49%, while the score of NB and SVM each of them 98.86% and 96.72%. Thus, the detection rate for DDoS attacks for SVM, KNN and NB are not shown in the research paper.

The performance result of classification algorithms in research [4] can be seen in Table that the highest score obtained for DDoS attacks detection is provided by KNN and the second place should be Naive Bayes. The highest accuracy obtained is KNN with 98.51% followed by NB with a score of 93.95%. While, the first place for precision is also earned by KNN with the highest score, 98.90%, and the score of NB is 97.74%. Thus, the detection rate for DDoS attacks for KNN is the highest with score 97.80% and 95.54% for NB.

Lastly, the classification algorithms performance result for the research [6] which the highest score obtained for DDoS attacks detection is provided by SVM and the second place should be NB and last but not least go to KNN. The highest accuracy obtained is SVM with 98.41% followed by NB with a score of 97.96% and finally KNN, 97.63%. The first place for precision is also earned by SVM with the highest score, 100%, NB with 92.00% and the score of KNN is 89.40%. Then, the highest score for detection rate for normal attacks is obtained by SVM with score 100% while the score of NB and KNN each of them 99.10% and 98.80%. Thus, the detection rate for DDoS attacks for NB is the highest with score 88.00%, KNN obtained about 87.50% and 84.80% for SVM.

In conclusion the result of classification algorithms using machine learning techniques for the proposed research obtained the highest score among other three different researches that have been mentioned in this research. This section is implemented to show the contribution of the proposed research to provide such a clear and highest result for DDoS attacks detection.

**4. Conclusion**

In this proposed research, the dataset used name as UNSW-NB15 which includes normal packets and DDoS attacks that need to be classify in this research. There are 175,341 records characteristics and 45 features in the dataset. This research methodology consist of six compulsory phases that need to be implemented one by one to provide the highest level of results in terms of accuracy, precision and detection rate in detecting DDoS attacks. The phases are information gathering, information analysis, design (data preparation, data preprocessing, feature selection and data splitting), implementation, testing and validation and lastly should be evaluation. There is training and testing of selected features from the datasets using three different of classification techniques: SVM, KNN and NB. According to the result of this research in detecting DDoS attacks using machine learning technique, the KNN classification technique achieved the best level of accuracy (99.67%) with highest score for precision (98.58%) and the highest in detecting normal traffic of DDoS (91.63%) among two classification techniques tested. In short, this means that the technique can accurately detect DDoS attacks on the application that will be developed.

**Acknowledge**

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support.

**References**

1. Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. Foozy, “Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset,” *IEEE Access*, vol. 9, pp. 22351–22370, 2021. doi:10.1109/access.2021.3056614
2. Zekri, M. et al. (2017) ‘DDoS attack detection using machine learning techniques in cloud computing environments’, 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech) [Preprint]. doi:10.1109/cloudtech.2017.8284731.
3. E.A.R.Coelho,"DDoS Detection Using Machine Learning Techniques," ResearchGate, p. 8, 2022.
4. Kachavimath, A.V., Nazare, S.V. and Akki, S.S. (2020) ‘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) [Preprint]. doi:10.1109/icimia48430.2020.9074929.
5. M. Aqil et al., “Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms,” 2021. Accessed:Jan.06, 2023.[Online]. Available: [www.joiv.org/index.php/joiv](http://www.joiv.org/index.php/joiv).
6. Maslan, A., Bin Mohamad, K.M. and Binti Mohd Foozy, F. (2020) ‘Feature selection for ddos detection using Classification Machine Learning Techniques’, IAES International Journal of Artificial Intelligence (IJ-AI), 9(1), p. 137. doi:10.11591/ijai.v9.i1.pp137-145.
7. Qian Li, Linhai Meng, Jinyao Yan and Yuan Zhang, “DDoS Attacks Detection Using Machine Learning Learning,” SpringerLink, p.2,2019.
8. Saini, K. and Raj, P. (2022) ‘Edge platforms, frameworks and applications’, Advances in Computers, pp. 237–258. doi:10.1016/bs.adcom.2022.02.005.
9. Dong, S. and Sarem, M. (2020) ‘DDoS attack detection method based on improved KNN with the degree of ddos attack in software-defined networks’, IEEE Access, 8, pp. 5039–5048. doi:10.1109/access.2019.2963077.
10. Abu Bakar, R. et al. (2023) ‘An intelligent agent-based detection system for ddos attacks using automatic feature extraction and selection’, Sensors, 23(6), p. 3333. doi:10.3390/s23063333.
11. Lee, S.-H. et al. (2022) ‘Detection and prevention of ddos attacks on the IOT’, Applied Sciences, 12(23), p. 12407. doi:10.3390/app122312407.