Machine Learning-Based Feature Engineering to Detect DDoS Attacks

Muhammad Nur Faiz[1], Oman Somantri[2], Arif Wirawan Muhammad[3]

***Abstract*—Distributed network attacks, also known as distributed denial of service (DDoS) are a major threat and problem for internet security. DDoS is an attack on a network aiming to disable server resources. These attacks increase every year with the current state of the COVID-19 pandemic. One of countermeasures to minimize the DDoS impact is the intrusion detection system (IDS) command. IDS techniques are currently still employing traditional methods so that they have many limitations compared to techniques and tools used by attackers because traditional IDS methods only use signature-based detection or anomaly-based detection models which cause many errors. Network data packet traffic has a complex nature, both in terms of sizes and sources. This research utilized the ability of artificial neural network (ANN) to detect normal attacks or DDoS. A classification technique with ANN method is a solution to these issues. Based on the shortcomings of the traditional IDS, this study aims to detect DDoS attacks using feeder machine learning-based feature engineering techniques to improve the IDS development. Using the UNSW-NB15 dataset with the ANN method, this study also aims to analyze and obtain training function combinations and the best hidden layer architectures of ANNs to solve the detection and classification problems of DDoS packets in computer networks. As a result, the training function combinations and hidden layer architectures of the ANN can provide a high level of DDoS recognition accuracy. Based on experiments conducted with three schemes and an ANN schema architecture technique with eight features as input, the highest accuracy was 98.22%. Feature selection plays an essential role in detection result accuracies and machine learning performances in classification problems.**

***Keywords*—DDoS, Feature Selection, Neural Networks, Machine Learning.**

I. INTRODUCTION

In the last decade, along with the rapid increase in the development and influence of information and communication technology (ICT), people's daily activities are now gradually carried out using the internet. As a result, the amount of network traffic is increasing, and the scale of network infrastructure is growing rapidly [1]. ICT itself has become an integral part of modern life. Due to the widespread usage of ICT, numerous types of attacks on networks have been used, including denial of service (DoS), man-in-the-middle attacks, sniffers, and malware [2], [3].

[1,2] *Jurusan Teknik Informatika, Politeknik Negeri Cilacap, 53212 Cilacap, INDONESIA (tel.: 0282-533329; fax: 0282-537992; email: [1]faiz@pnc.ac.id, [2]oman.somantri@pnc.ac.id)*

[3] *Teknik Informatika, Fakultas Informatika, IT Telkom Purwokerto, 53147 Purwokerto, INDONESIA (tel.: 0281-641629; email: [3]arif@ittelkom-pwt.ac.id)*

[Received: 18 November 2021, Revised: 5 July 2022]

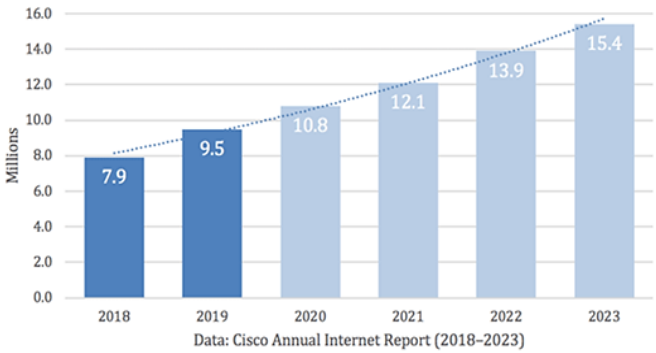

Fig. 1 DDoS attack prediction from 2018 to 2023.

DoS is one of the threats in network infrastructure attacks. It has a variant called distributed denial of service (DDoS). Referring to Fig. 1, the CISCO report [4] has predicted that DDoS attacks will continue growing every year, not to mention the COVID-19 pandemic has caused activities to be carried out using the internet. As seen in Fig. 1, since 2018, the number of DDoS attacks has increased from 7.9 million to over 15 million in 2023, or an average annual increase of 1.5 million. These attacks pose a threat to internet users and all infrastructures on them, including bandwidth, server resource, data integrity, data availability, and data confidentiality stored on servers [5]. Until today, DDoS attacks remain a major cybersecurity threat. Early detection plays a fundamental role in preventing any fatal impacts of DDoS attacks on the server resource [6]. One of the basic preventive measures of DDoS attacks is to install an intrusion detection system (IDS) on the server to monitor the flow of incoming data packets to the internal network or vice versa [7]. The detection system on the IDS only monitors and provides tags/markers for suspicious network activity which is then immediately reported as an alert. It results in the excessively high alert volume due to a high average error rate in recognizing normal data packets as DDoS packets or vice versa, caused by the nonstationary network data traffic. The intrusion detection generally consists of two approaches, namely the signature-based detection and anomaly-based detection. In the signature-based detection, alerts are generated based on specific attack signatures [8]. In this approach, IDS cannot detect unknown attacks caused by outdated signature databases or unavailable signatures. In the anomaly-based detection, it is necessary to profile the typical behavior at the feature level of a particular network activity. This profile is subsequently used as the basis for defining the normal tissue activity [9]. When any network activities stray too far from the profile, an alert is then generated. Although anomaly-based IDS has the advantage of being able to detect new attacks [10], it is more complex than signature-based IDS [11]. The detection model will logically cause many false-positive flags because

the flow of computer network data packets has dynamic properties both in terms of size, source, protocol, and data content [12].

Signature-based IDS and anomaly-based IDS have two major drawbacks. The first is when the IDS detects a weakness starting with the SYN protocol, for example SYN-Flood, because the SYN protocol is a legal and absolute protocol used to initiate communication between two computers/devices in a network [13]. Therefore, it is difficult for ordinary IDS to generate an alert against attacks initiated with SYN protocol artifacts [14]. Another weakness of IDS is mainly due to the transmission control protocol (TCP)/internet protocol (IP) deficit which make it easy for attackers to initiate DDoS attacks, for example using the ping command which is available by default throughout the operating system or using special tools like HOIC, LOIC, XOIC, and GoldenEye [15]. Based on the weaknesses of the ordinary IDS, this study aims to detect DDoS attacks by utilizing machine learning techniques so that IDS device development can be improved. This study utilized a DDoS attack dataset sourced from UNSW-NB15 (University of New South Wales) to be followed up by applying a neural network method to generate machine learning models for the DDoS detection.

Several previous studies related to feature engineering in the DDoS detection analyzed the UNSW-NB15 dataset by looking for feature relevance using an artificial neural network (ANN) [16]. This study categorized the features into five groups based on their type, such as flow-based, content-based, time-based, essential, and additional features. Of these groups, 31 possible combinations of features were evaluated and discussed. The highest accuracy (93%) in this study was obtained using 39 features of the categorized group. In addition, in this study, there was a combination of 23 features selected using a meta estimator called SelectFromModel which selected features based on their scores. The 23 selected features resulted in a higher accuracy (97%) compared to the 39 features described. Reference [12] reported that the number of features in KDD-99 was less than UNSW-NB15, while the first attack class in KDD-99 (DoS) had the highest number of features. Attack detection ACC was also the highest (99.40%). There were only twelve features for the DoS attack class in UNSW-NB15, while the ACC was reported at 86.57%. The number of features selected for attack class KDD-99 was less than that of UNSW-NB15. An average of 25.2 features were selected for attack in KDD-99; at the same time, an average of 19.1 features were selected for attack in UNSW-NB15. It is noteworthy that the lowest number of selected features was for Generic attacks on UNSW-NB15, which was ten features. Further research related to feature engineering was carried out to explore the application of the XGBoost algorithm for feature selection along with several machine learning techniques including the ANN, *k*-nearest neighbor (KNN), decision tree (DT), logistic regression (LR), and support vector machine (SVM) to implement an accurate IDS [7]. The XGBoost-based attribute selection method was applied to the UNSW-NB15 and as a result, nineteen optimal features were selected. The results of this study also considered the configuration of binary and multiclass classifications. The results showed that the XGBoost-based feature selection method allowed methods such as DT to increase the test accuracy from 88.13 to 90.85% for binary classification schemes. Reference [17] aimed to combine the entire UNSW-NB15 dataset into a single file so that one could test the model at once, rather than testing the model separately for each file. After that, the dataset from the attack was used as a new label, so it would develop a dataset label multiclass. The study also investigated the performance of deep learning with enhanced datasets in two classification categories (binary and multiclass). The proposed model yielded an accuracy of 99.59% in multiclass classification and 99.26% in binary classification. Meanwhile, this study focuses on combining selected features using information gain techniques used as input for the ANN classification to increase the value of DDoS detection accuracy.

II. Detection Approach

The DDoS attack detection approach applied in this study was divided into several stages.

A. Dataset

The first step was to obtain the UNSW-NB15 DDoS attack dataset published by the University of New South Wales. The UNSW-NB15 dataset is an attack dataset containing flow records of attack packets and normal packets in the form of a *tcpdump* file which records the data stream for 31 hours [12], [18]. The attack packet flow was synthetically simulated using Ixia software which emulates high-speed low-tread attacks. There were nine types of attacks included in the UNSW-NB15 dataset, which are presented in Table I. The grouping of feature categories of the UNSW-NB15 dataset was carried out systematically, namely, flow, basic, data packet content, timing, and additional features. Basically, the motivation for forming the UNSW-NB15 dataset is to fix the problem of deficiencies in the KDD CUP 99 and NSL-KDD datasets [19], [20].

B. Feature Selection

In this study, the type of record to be analyzed was devoted to the DDoS record group as presented in Table I. The UNSW-NB15 DDoS attack record dataset has features as presented in Table I.

The sixteen features were then selected using the information gain technique with the aim of reducing computation time and obtaining a machine learning model with high accuracy. Information gain is the amount of mutual information obtained from a combination of observational variables and is a divergence from the Kullback-Leibler theory [21]. In machine learning, information gain is useful for selecting several important features based on theories that measure the value of information held by a feature in relation to other features. For feature "a", information gain is the amount of entropy contained by "a" compared to feature "c" of all available features [22]. Important features are indicated by the maximum value of entropy that the features have. The information gain equation is presented in (1).

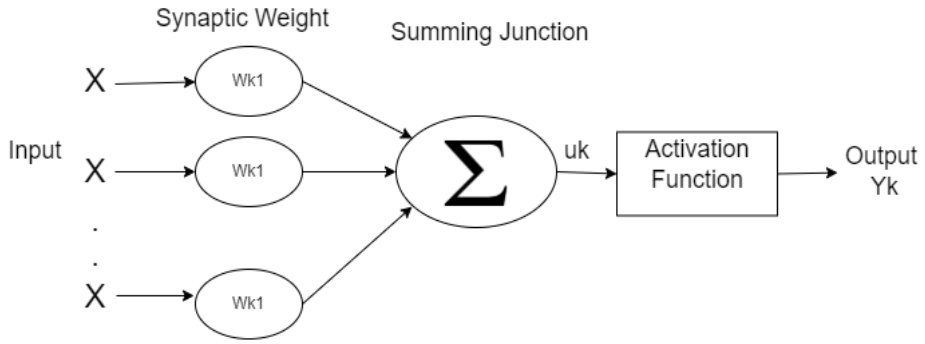

Fig. 2 Components of the ANN.

TABLE I
UNSW-NB15 DDOS FEATURE

Feature No.	UNSW-NB15	Description
1	srcip	Source of IP address.
2	sport	Source of port number.
3	dstip	Destination of IP address.
4	dsport	Destination of port number.
5	proto	Transaction protocol.
6	state	Indication to the state and its dependent protocol.
7	dur	Record total duration.
8	sbytes	Source to destination transaction bytes.
9	dbytes	Destination to source transaction bytes.
10	sttl	Source to destination time-to-live value.
11	dttl	Destination to source time-to-live value.
12	sloss	Source packets retransmitted or dropped.
13	dloss	Destination packets retransmitted or dropped.
14	service	http, dns, ssh, pop3, ftp, smtp.
15	stime	Record start time.
16	Classification	0 for normal and 1 for attack records.

$$info\ gain_a = H(C) - H\left(\frac{c}{a}\right)$$

$$H(c) = -\sum_{c \epsilon C} P(c) * (c) \qquad (1)$$

$$H\left(\frac{c}{a}\right) = -\sum_{c \epsilon A} P(c) * \sum_{c \epsilon C} p\left(\frac{c}{a}\right) * \left(\frac{c}{a}\right)$$

with *H* denotes entropy, while *P* denotes probability.

C. Artificial Neural Network

An ANN is an information processing paradigm inspired by biological neural cell systems, just as the brain processes information. In human brain tissue, there are nerve cells (neurons) which have three constituent components that work together to process information signals. The three components are dendrites (input), cell body (processing input), and axon (output) [23].

Fig. 2 illustrates the components of ANN. *X* is the input that will be sent to the neuron with a certain arrival weight. This input will be processed by a propagation function which adds up the values of all incoming weights symbolized by W_{k1}. Then, the second number of points will be compared with a certain threshold value through the activation function of each neuron. If the input exceeds a certain threshold value, the neuron will be activated, but if not, the neuron will be deactivated. When a neuron is activated, it sends output through its output weight to all associated neurons, which is symbolized by Y_k.

The hidden layer is an imitation of the connective nerve cells in a biological neural network. The hidden layer serves to increase the ability of the ANN to solve a problem. The consequence of this layer is that the training becomes more difficult or longer. The more hidden layers that are used, the more they can be used to solve complex problems. On the other hand, it will prolong the learning process and reduce the performance of the neural network. In theory, the use of one hidden layer in the neural network is sufficient to solve the prediction case [23]. Kolmogorov has stated that the best number of hidden layers to solve a problem with an ANN is $2n + 1$, where n is the number of input neurons [24].

D. Performance Matrix

In this study, several parameters were used to facilitate the analysis of recognition performance. The indicators used are true positive (TP), true negative (TN), false positive (FP), and false negative (FN) [25]. TP is the recognition of DDoS data packets identified by the neural network as DDoS packets; TN is the recognition of normal data packets identified by the neural network as normal packets; FP is the recognition of normal data packets identified by the neural network as DDoS packets; FN is the recognition of DDoS data packets identified by the neural network as normal packets. From the indicators that have been mentioned, an equation can be formed stating the accuracy, as in (2).

$$Accuracy = \frac{TN+TP}{FP+FN+TP+TN}. \qquad (2)$$

Accuracy is the ratio between DDoS packet recognition plus normal packet recognition compared to the whole data packet.

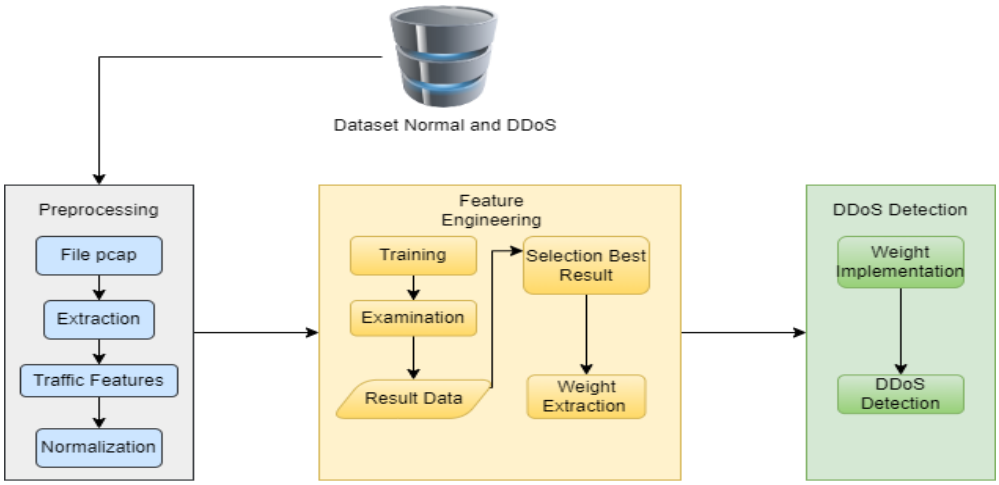

Fig. 3 Research framework.

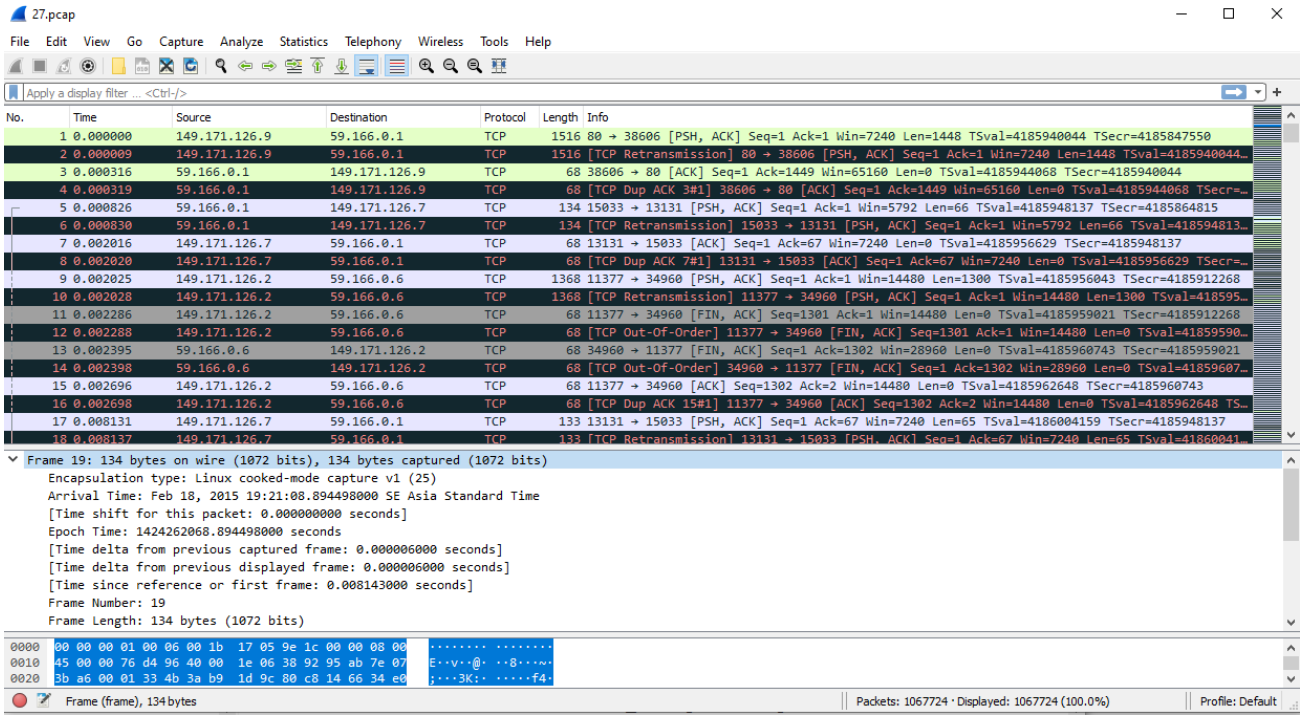

Fig. 4 *.pcap* file from the UNSW-NB15.

TP is the instance level correctly identified as an attack. *TN* is the official traffic level classified as legit. *FP*, sometimes referred to as a type I error, is the official traffic level classified as an attack. *FN*, sometimes referred to as a type II error, is a legitimate traffic level classified as an intrusion.

Recall/sensitivity is actual positives that are correctly categorized as positive class. Precision is a measure of the estimated probability of a positive prediction being correct. F-score/F-measure is comparison of weighted average precision and recall.

$$Recall = \frac{TP}{TP+FN}. \quad (3)$$

$$Precision = \frac{TP}{TP+FN}. \quad (4)$$

$$F1 - Score = 2x \frac{Presisi\ X\ Recall}{Presisi+\ Recall}. \quad (5)$$

E. Research Framework

The steps used in this study are shown in Fig. 3. First, retrieving the dataset of DDoS attack data packets and the normal flow of UNSW-NB15 data packets published by the University of New South Wales [18] in *.pcap* format. Next, converting the *.pcap* dataset to the *.csv* format to extract its contents. The extracted data was then quantified to get network traffic features. Then, the process of normalizing the quantified data was carried out by dividing each quantified data item by its maximum value so that the relative data value was obtained with a maximum value of 1. After that, the normalized neural network data with several training criteria was trained. Next,

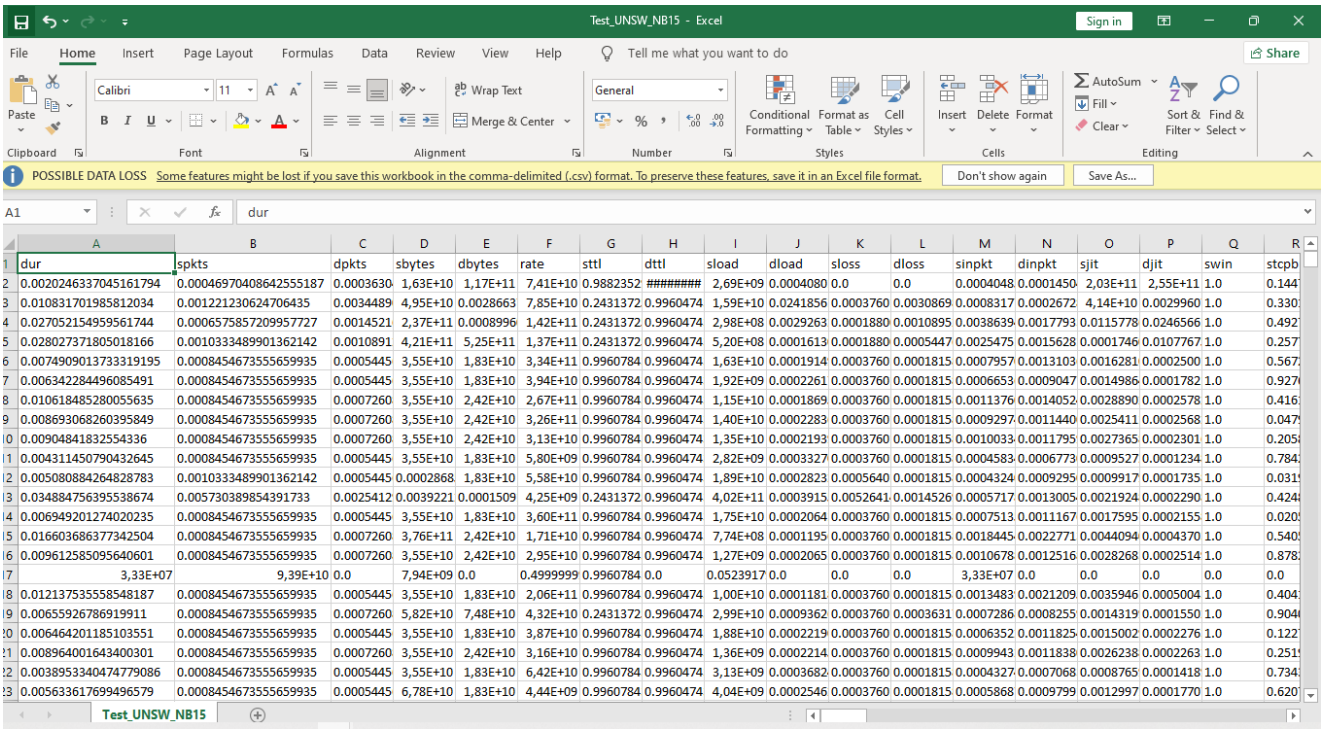

Fig. 5 Dataset extraction.

TABLE II
ARCHITECTURAL SCHEME OF THE ANN

Schema No.	Input Neuron	Total of Hidden Layer Neuron	Output Neuron
1	7	15	2 (Normal and DDoS)
2	8	17	2 (Normal and DDoS)
3	15	31	2 (Normal and DDoS)

TABLE III
EXPERIMENT RESULTS WITH SCHEME 1

Experiment	Accuracy	Precision	Recall	F1-Score
1	98.24%	98.53%	97.52%	98.03%
2	97.71%	96.73%	96.68%	96.71%
3	97.34%	96.95%	96.22%	96.58%

TABLE IV
EXPERIMENT RESULTS WITH SCHEME 2

Experiment	Accuracy	Precision	Recall	F1-Score
1	97.79%	98.12%	99.72%	98.92%
2	99.73%	98.89%	99.94%	99.41%
3	97.15%	97.27%	99.12%	98.19%

extracting the original server log data in the entity-property form. Then, performing the feature engineering on the original server log data through feature compounding, feature splitting, feature merging, and one-hot encoding. Subsequently, incorporating engineering features into machine learning for normal packet flow detection and DDoS attacks. Last, analyzing the performance of machine learning classification in detecting normal data packet flow and DDoS attacks based on the accuracy, precision, recall, and F1-score metrics.

III. RESULT AND DISCUSSION

This study employed MATLAB 2019b software running on the Windows 10 64-bit operating system platform. Since the UNSW-NB15 dataset was quite large in its database, a *27.pcap* series or later was required. These experiments were trained, evaluated, and tested on Microsoft Excel and MATLAB.

Fig. 4 depicts the *.pcap* file or raw data from the UNSW-NB15. The data were ready to be processed and converted into *.csv* for easier analysis. The *27.pcap* file contained 1,067,724 datasets. Fig. 5 shows the conversion result from *.pcap* to *.csv*. The data were processed and tested later. The 49 features in the data were then simplified by finding the refractive index per block according to the selected feature.

In this study, three feature schemes were used as an input for the ANN classifier to determine the training effectiveness and classification accuracy resulting from the feature selection process. Based on the input feature selection scheme, three different ANN architectural schemes were formed based on the theory that the use of one hidden layer in the neural network is sufficient to solve the prediction case [26]. The ANN architectural schemes are presented in Table II. On the other hand, Kolmogorov has stated that the best number of hidden layers for solving problems with ANNs is $2n + 1$, where n is the number of input neurons. Based on the theory proposed by Kolmogorov, in this study, a variety of ANN architectures were formed to find the highest accuracy in solving DDoS network packet detection problems [24], [27].

In this study, three experiments were carried out with husks and a dataset from UNSW-NB15 to find the highest level of accuracy. This level of accuracy was based on the feature input. The feature engineering process was carried out by selecting

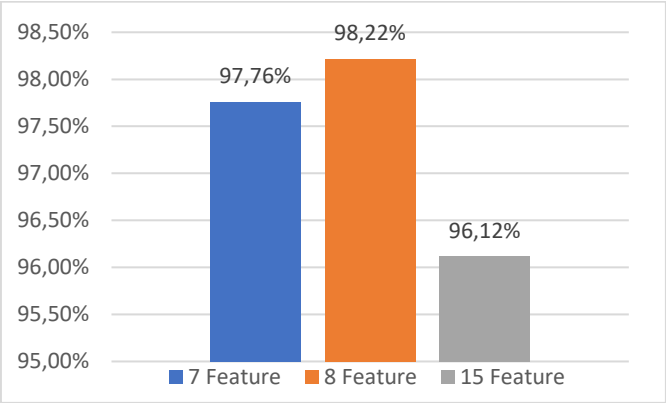

Fig. 6 Graph of the experimental accuracy level.

TABLE V
EXPERIMENT RESULTS WITH SCHEME 3

Experiment	Accuracy	Precision	Recall	F1-Score
1	95.02%	93.20%	96.74%	97.10%
2	97.13%	96.52%	99.29%	97.93%
3	96.22%	95.55%	95.01%	96.00%

TABLE VI
CONCLUSION OF EXPERIMENT RESULTS WITH THREE SCHEMES

Number of Selected Features	Accuracy	Precision	Recall	F1-Score
Seven features with feature number: 2, 6, 9, 10, 12, 1, 3	97.76%	97.40%	96.81%	97.10%
Eight features with feature number: 2, 6, 9, 10, 12, 15, 1, 3	98.22%	98.09%	99.59%	97.93%
Fifteen features	96.12%	95.02%	97.01%	96.00%

features and then combining them according to Table II. The results of the first experiment are shown in Table III. It can be seen that the highest accuracy was obtained from the first experiment with a value of 98.24%. The first experiment also had higher precision, memory, and F1-score values than other experiments. Scheme 1 is the scheme with feature options.

Table IV shows the highest accuracy was obtained from the second experiment with a value of 99.73%. The second experiment also had higher precision, memory, and F1-score values than the other experiments. This scheme with a choice of nine features.

Table V depicts the highest accuracy obtained from the second experiment with a value of 97.13%. The second experiment also had higher precision, memory, and F1-score values than the other experiments. Scheme 3 is a scheme with a choice of fifteen features.

Table VI shows the conclusions from the experimental results. It can be seen that seven selected features could obtain an accuracy rate of 97.76%, whereas by selecting almost all features (fifteen) the accuracy level was even smaller. Subsequent experiments with a combination of eight features obtained 98.22% and became the experiment with the highest accuracy. The accuracy graph can be seen in Fig. 6.

IV. CONCLUSION

Based on the experimental results that have been carried out, it was found that the feature selection plays an essential role in the accuracy of detection results and the efficiency of machine learning training in classification problems. In this study, the combination of the eight main features of the dataset used as input for the classification of ANNs, namely feature numbers 2, 6, 9, 10, 12, 15, 1, and 3; the combination resulted in the highest accuracy value of 98.22% compared to the two main features. The combination scheme of the eight features also produced an ANN model with the best training efficiency. It can be concluded that to cover the shortcomings of the ordinary IDS in solving the problem of detecting DDoS attacks, based on the UNSW-NB15 dataset and ANN, eight selected features out of sixteen available features are needed. Future research is expected to be able to combine several features and other algorithms to increase the level of accuracy in detecting DDoS attacks.

CONFLICT OF INTEREST

The author has no conflicts with any parties during the writing and the course of this research. Any information submitted is the original result as obtained when conducting research and is not influenced by personal opinions or interests.

AUTHOR CONTRIBUTION

This research is collaborative research conducted by three authors. The following is a distribution of the contributions of each author involved in this research. Conceptualization, Muhammad Nur Faiz and Oman Somantri; writing the original draft and administration, Muhammad Nur Faiz, Oman Somantri and Arif Wirawan Muhammad; software and data collection, Muhammad Nur Faiz; supervision and validation, Arif Wirawan Muhammad.

ACKNOWLEDGMENT

This research was supported by various parties, especially Pusat Penelitian dan Pengabdian kepada Masyarakat Politeknik Negeri Cilacap.

REFERENCES

[1] K. Kurniabudi, A. Harris, and A. Rahim, "Seleksi Fitur dengan Information Gain untuk Meningkatkan Deteksi Serangan DDoS Menggunakan Random Forest," *Techno.COM*, Vol. 19, No. 1, pp. 56–66, Feb. 2020.

[2] S. Haider, *et al.*, "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," *IEEE Access*, Vol. 8, pp. 53972–53983, Feb. 2020.

[3] H. Parmar and A. Gosai, "Analysis and Study of Network Security at Transport Layer," *Int. J. Comput. Appl.*, Vol. 121, No. 13, pp. 35–40, Jul. 2015.

[4] Cisco "Cisco Annual Internet Report (2018–2023)," 2020, [Online], https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

[5] I. Cvitić, D. Peraković, M. Periša, and M. Botica, "Novel Approach for Detection of IoT Generated DDoS Traffic," *Wirel. Netw.*, Vol. 27, No. 3, pp. 1573–1586, Jun. 2021.

[6] A.W. Muhammad, C.F.M. Foozy, and A. Azhari, "Machine Learning-Based Distributed Denial of Service Attack Detection on Intrusion Detection System Regarding to Feature Selection," *Int. J. Artif. Intell. Res.*, Vol. 4, No. 1, pp. 1–8, Jun. 2020.

[7] S.M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *J. Big Data*, Vol. 7, pp. 1–20, Nov. 2020.

[8] M. Merouane, "An Approach for Detecting and Preventing DDoS Attacks in Campus," *Autom. Control Comput. Sci.*, Vol. 51, No. 1, pp. 13–23, Mar. 2017.

[9] Z. Ahmad, *et al.*, "Anomaly Detection Using Deep Neural Network for IoT Architecture," *Appl. Sci.*, Vol. 11, No. 15, Jul. 2021.

[10] O.F. Rashid, "DNA Encoding for Misuse Intrusion Detection System Based on UNSW-NB15 Data Set," *Iraqi J. Sci.*, Vol. 61, No. 12, pp. 3408–3416, Dec. 2020.

[11] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)," *2015 Mil. Commun., Inf. Syst. Conf. (MilCIS)*, 2015, pp. 1–6.

[12] M.S. Al-Daweri, K.A.Z. Ariffin, S. Abdullah, and M.F.E.Md. Senan, "An Analysis of the KDD99 and UNSW-NB15 Datasets for the Intrusion Detection System," *Symmetry*, Vol. 12, No. 10, pp. 1-32, Oct. 2020.

[13] J.H. Corrêa, P.M. Ciarelli, M.R.N. Ribeiro, and R.S. Villaça, "ML-Based DDoS Detection and Identification Using Native Cloud Telemetry Macroscopic Monitoring," *J. Netw. Syst. Manag.*, Vol. 29, No. 2, pp. 1–28, Jan. 2021.

[14] M. Tayyab, B. Belaton, and M. Anbar, "ICMPV6-Based DOS and DDoS Attacks Detection Using Machine Learning Techniques, Open Challenges, and Blockchain Applicability: A Review," *IEEE Access*, Vol. 8, pp. 170529–170547, Sep. 2020.

[15] G.A. Jaafar, S.M. Abdullah, and S. Ismail, "Review of Recent Detection Methods for HTTP DDoS Attack," *J. Comput. Netw. Commun.*, Vol. 2019, pp. 1–10, Jan. 2019.

[16] S. Rajagopal, K.S. Hareesha, and P.P. Kundapur, "Feature Relevance Analysis and Feature Reduction of UNSW NB-15 Using Neural Networks on MAMLS," in *Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing*, Vol. 1082, B. Pati, C. Panigrahi, R. Buyya, and K.C. Li, Eds., Singapore, Singapore: Springer, 2018, pp. 321–332.

[17] A.M. Aleesa, M. Younis, A.A. Mohammed, and N.M. Sahar, "Deep-Intrusion Detection System with Enhanced UNSW-NB15 Dataset Based on Deep Learning Techniques," *J. Eng. Sci. Technol.*, Vol. 16, No. 1, pp. 711–727, 2021.

[18] N. Moustafa and J. Slay, "The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Data Set and the Comparison with the KDD99 Data Set," *Inf. Secur. J., A Global Perspec.*, Vol. 25, No. 1–3, pp. 18–31, Apr. 2016.

[19] A. Thakkar and R. Lohiya, "A Survey on Intrusion Detection System: Feature Selection, Model, Performance Measures, Application Perspective, Challenges, and Future Research Directions," *Artif. Intell. Rev.*, Vol. 55, pp. 453-563, Jan. 2021.

[20] N. Kunhare and R. Tiwari, "Study of the Attributes Using Four Class Labels on KDD99 and NSL-KDD Datasets with Machine Learning Techniques," *2018 8th Int. Conf. Commun. Syst., Netw. Technol. (CSNT)*, 2018, pp. 127–131.

[21] B. Bouyeddou, B. Kadri, F. Harrou, and Y. Sun, "Nonparametric Kullback-Leibler Distance-Based Method for Networks Intrusion Detection," *2020 Int. Conf. Data Anal. Bus., Ind., Way Towards a Sustain. Econ. (ICDABI)*, 2020, pp. 1–5.

[22] S. Khan, A. Gani, A.W.A. Wahab, and P.K. Singh, "Feature Selection of Denial-of-Service Attacks Using Entropy and Granular Computing," *Arab. J. Sci. Eng.*, Vol. 43, No. 2, pp. 499–508, Feb. 2018.

[23] G.S. Kushwah and V. Ranga, "Voting Extreme Learning Machine Based Distributed Denial of Service Attack Detection in Cloud Computing," *J. Inf. Secur. Appl.*, Vol. 53, pp. 1-12, Aug. 2020.

[24] J. Schmidt-Hieber, "The Kolmogorov–Arnold Representation Theorem Revisited," *Neural Netw.*, Vol. 137, pp. 119–126, Mei 2021.

[25] G. Kocher and G. Kumar, "Analysis of Machine Learning Algorithms with Feature Selection for Intrusion Detection using UNSW-NB15 Dataset," *Int. J. Netw. Secur., Its Appl.*, Vol. 13, No. 1, pp. 21–31, Jan. 2021.

[26] M. Madhiarasan and S.N. Deepa, "Comparative Analysis on Hidden Neurons Estimation in Multi Layer Perceptron Neural Networks for Wind Speed Forecasting," *Artif. Intell. Rev.*, Vol. 48, No. 4, pp. 449–471, Dec. 2017.

[27] A. Sagheer, M. Zidan, and M.M. Abdelsamea, "A Novel Autonomous Perceptron Model for Pattern Classification Applications," *Entropy*, Vol. 21, No. 8, pp. 1–24, Aug. 2019.