The Classification of DDoS Attacks Using Deep Learning Techniques

Jirasin Boonchai
Faculty of Information Technology
Thai-Nichi Institute of Technology
Bangkok, Thailand
bo.jirasin_st@tni.ac.th

Kotcharat Kitchat
Department of Computer Science and Information Engineering
National Central University
Taoyuan 320, Taiwan
kotcharat@ieee.org

Sarayut Nonsiri
Faculty of Information Technology
Thai-Nichi Institute of Technology
Bangkok, Thailand
sarayut.n@tni.ac.th

2022 7th International Conference on Business and Industrial Research (ICBIR) | 978-1-6654-9475-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICBIR54589.2022.9786394

***Abstract*— Distributed Denial of Service (DDoS) is a well-known attack with the power of damage. The process of DDoS is to disrupt the normal traffic of a targeted server by overwhelming it with a flood of Internet traffic. This action affects the legitimate users inaccessible to the resources. Moreover, many businesses today have been faced with DDoS attacks derogation that not only take the physical damage of resources, but also cause a massive financial damage. The idea of this research is to find good ways to detect and classify DDoS attacks that aim to avoid the cause of failure due to network attacks by using deep learning techniques. Therefore, our proposed models based on deep neural networks have been provided to perform the capability in the multiclass classification of DDoS. CICDDoS2019 is a new taxonomy of the DDoS attacks dataset that has been utilized as the reference of this framework. Two proposed models have been implemented with the simple DNN structure and the Convolutional autoencoder. The highest accuracies obtained from the proposed models are high up to 87% and 91.9%, respectively. Overall results showed that the proposed networks display the satisfying outcome with the high accuracy, precision, recall, and F1-score. The comparison of the proposed models with other machine learning algorithms, namely, Logistic Regression, and Naïve Bayes are also indicated in this research and the results point out the outperforming efficiency of our proposed models.**

Keywords—DDoS attacks, Deep learning, CICDDoS2019, DNN, CNN

I. Introduction

Presently, the internet and technology have become inescapable in our everyday life. The advantages of them make our life easier, faster and more comfortable. So, they have important roles in many fields such as business, economic development until the personal requirements. We cannot deny that the advancement of technology comes with vulnerabilities and attacks. One of the most attacks that affect cybersecurity today is "Distributed Denial of Service" (DDoS) attacks.

Sending huge packets to the web servers from attackers' instruments is called the denial of service attack (DoS) and the ordinary cyber a risk on the internet serves as the DDoS [1]. The data security companies and administrations of many countries have traversed a critical thought to keep away from the DDoS attacks. Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), and Hypertext Transfer Protocol (HTTP) have been utilized in the network, transport, and also application layers to obstruct the attacks. DDoS attacks have been around for quite a while. The previously happened around 20 years ago at the University of Minnesota when Trin00, a perilous script containing in a computer and attacked 114 different computers [2]. The attacks also obviously showed a few years ago, on October 21, 2016, a Domain Name System (DNS) service provider called Dyn was attacked causing the networks to be blocked off in a while that affect most users from unavailability web services [2], [3]. On February 28, 2018, GitHub was hit by 1.35 terabits per second of DDoS attacks [4]. This event shows the malignity of DDoS attacks which struck the developer platform at once. As mentioned in [2], the Kaspersky Lab reports show the financial loss that gain from the DDoS attacks. The reports evaluated the damage of each attack to the medium-sized businesses and large organizations that high up to $2 million. These emphasize that apart from being incapable of resources to be of benefit after being attacked it can moreover cause big monetary damage to the victims.

Nowadays, Artificial Intelligence (AI) is widely applied in several fields such as robotics, image processing, natural language processing, and also network security [5]. AI is involved in computer science. It has strong capabilities in prediction and targeting by enabling machines to exhibit intelligence and make decisions like humans [6]. One part of AI that has been most talked about today is Deep Learning (DL). DL is an impressive form biologically-inspired programming paradigm which has been used in the field of classification and pattern recognition with high performance. To classify between normal and intrusion traffics, DL has been utilized to detect the danger of attacks. Yuan et al. [7] showed the DeepDefense which is the deep learning approach based on Recurrent Neural Network (RNN) to identify DDoS attacks. They evaluated the model on the DDoS attacks dataset called ISCX2012 by choosing 2 days out of 7 days' network traffic to compare. The results indicated that their DeepDefense model reduces the error rate by around 36.69% and reduces the error rate from 7.517% to 2.103% in the larger dataset with high accuracy of more than 90%. In [8], the researchers also proposed their model to classify DDoS attacks based on deep learning with autoencoder. The dataset from Cyber Security Laboratory located at the Australian Cyber Security Center was used in their research. It contains 45,332 records for malicious traffics and 37,000 records for normal traffics. The results showed that their autoencoder based deep neural network model obtains high precision, high recall and best F1 score when using ReLU as the activation function. Moreover, they also showed that the model can be applied to the KDDCUP'99 dataset [9] which includes several types of attacks belonging to 1999 and still archived the great performance. There are successful projects of deep learning in DDoS detection, but old datasets do not contain the current attacks. These bring to the proposed idea. The proposed idea is to use a new DDoS attacks dataset that includes more recent attacks and apply it with deep learning techniques.

In this research, the new DDoS attacks dataset named CICDDoS2019 has been used and the classification algorithm of deep learning has also been applied to learn from the dataset for the purpose of a suitable neural network structure that can separate normal data and attack data. There are some works that refer to DL techniques applied with CICDDoS2019 and obtained great results [2], [10], [11] but those only classified the problem in binary class classification and may not cover all classes of DDoS attacks. To improve the solution of DDoS attacks classification, this research focuses on the multiclass classification as the starting point of DDoS attacks detection that can distinguish the data more than normal and abnormal.

This research paper has been organized into the following segments: Introduction – Related Theory – Proposed Models – Experiment and Results – Discussion and Future Work.

II. Related Theory

A. *Distributed Denial of Service (DDoS)*

Various researches proposed DDoS attack taxonomy. Based on [12], the new taxonomy has been proposed using TCP/UDP-based protocols (Transmission Control Protocol and User Datagram Protocol) at the application layer to identify new attacks. The classification illustrated in terms of reflection-based and exploitation-based attacks.

- **Reflection-based attacks**

  These kinds of attacks are associated with legitimate intervenor components. To cover the victim with response packets, the attackers will send the packets with source internet protocol address batch to the target internet protocol address of the sufferer. As shown in Figure 1, TCP-based attacks can separate into MSSQL and SSDP while UDP-based attacks divided into CharGen, NTP, and TFTP. The DNS, LDAP, NETBIOS, SNMP, and PORTMAP are classified in TCP/UDP-based attacks group.

- **Exploitation-based attacks**

  The exploitation-based attacks can also be executed through application layer using TCP and UDP protocol. The attackers sent the packets with source and target internet protocol address to the reflector servers, the response packets will damage the victim. The TCP-based exploitation attacks cover SYN flood and Figure 1 shows that UDP flood and UDP-Lag are a part of UDP-based attacks.

The details about SYN flood, UDP flood, and UDP-Lag, the process has been referred in [12], [13]. SYN flood is one of the most common attacks of DDoS which was frequently occurred. The attacker connected to the server utilizing the TCP three-way handshake method. The target server received the repeated SYN packets with massive numbers without the final ACK (Acknowledgement) to finish the three-way handshake through the TCP protocol. These made the server crash and the requests from legitimate clients were denied because the server's queue was overwhelmed.

UDP flood is a type of DDoS attack in which the random ports on the target server were overwhelmed by a huge number of UDP packets sending from the remote host. When the host does not find applications, it will reply with ICMP (Internet Control Message Protocol) messages that the destination is unreachable. These made the host is forced to send many ICMP destination unreachable packets. Then, the resources of the server are consumed and the system performance is degraded, making the host stops responding to legitimate clients.

UDP-Lag attack will disturb the connection between client and server. It has two ways in which UDP-Lag attacks can be carried in. The first way is to use a hardware switch called lag switch and the second way is to use a software program that runs on the network to hog the bandwidth of other users. This attack is largely found in the online gaming field when the players want to outmaneuver other players by decelerating or interrupting their movement.

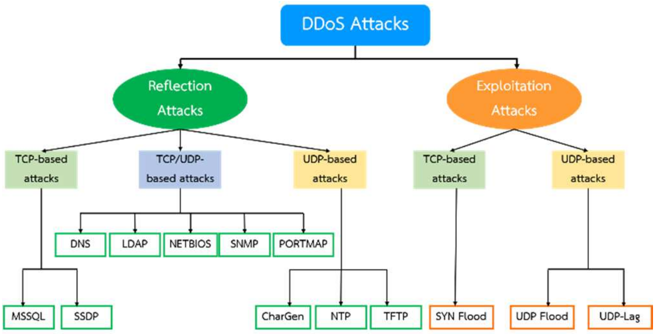

Fig. 1. The new taxonomy of DDoS attacks on reflection-based and exploitation-based attacks.

B. *Artificial Intelligence (AI)*

Artificial Intelligence or AI is the part of computer science that design the intelligent computer system which has capability like the intelligence in human. This intelligent machine imitates human problem-solving to perform tasks and execute iteratively progress itself based on data. AI can separate into two main parts consist Machine Learning and Deep Learning.

Machine Learning (ML) is a method of data analysis that stands on the system or algorithm that can learn from data by automating analytical model building. That caused the machine can make the decision and identify problem patterns.

Next is Deep Learning (DL), which is a subset of Machine Learning in AI that has a network for learning from observational data also known as "Neural Network". Neural Network is beautiful biologically-inspired programming that looks like the structure of the human brain. About Artificial Intelligence techniques, some examples of machine learning algorithms and deep learning techniques which are well-known and be a part of this research experimental are explained below:

- **Naïve Bayes**

  Naïve Bayes [14] is a popular classification algorithm with its simplicity but can classify the data incredibly well. The name of naïve is from the formula that makes some naive hypotheses. It a supervised learning algorithms based on Bayes' theorem. Naïve Bayes is a sensible classifier that fasts to train with its minimal storage. It has been applied in many applications such as web pages types classification and automatically spam filtering. Moreover, it is easy to utilize and is not needed any complicated parameters. In various works, this technique is one of the best possible classifiers that robust and perform very well. In this case, Gaussian Naïve Bayes method is applied in the experiment.

- **Logistic Regression**

  Logistic Regression [15] is a process of designing the probability model of a discrete outcome from the input variable. A binary outcome is the common logistic regression model. This model will show two possible values such as yes/no or true/false etc. However, the logistic regression model has also been utilized in the multiple class problems. The logistic regression that can model more than two possible discrete outcomes called "Multinomial logistic regression". Logistic regression is one of the useful analysis methods for the classification. It helps users to determine the category that is the best fit for new samples. So, in the cyber security field, this is one technique that has been used to classify attack detection.

- **Multilayer Perceptron (MLP)**

  Perceptron is a network that every node will connect to the node in the next layer with different weights. So, a Multilayer Perceptron is a network that consists of more than one layer. The first layer called the input layer which will pass the calculated values to the following layer known as the hidden layer. Then, the process continues by sending all values until to the last output layer. It can be said that a multilayer perceptron is a feedforward artificial neural network, which is the basis of all neural networks as well as deep learning.

- **Deep Neural Network (DNN)**

  In [16], [17] have described DNN, which is the neural network inspired by the visual system of mammalian that contains many layers of neural. Generally, DNN is the model that has at least 2 hidden layers. In other words, it is a neural network with a depth more than or equal to 4 including input and output layer. A Multilayer Perceptron that contains more than one hidden layer also be the DNN structure. DNN has a stronger performance in feature extraction than the shallow neural network. It will extract the features in each layer to find the distributed expression of data.

- **Convolutional Neural Network (CNN)**

  Deep Convolutional Neural Networks (DCNN) is one of the main types of DNN. It has frequently been applied in many tasks [18], [19]. A Convolutional Neural Network is the feedforward network utilizing the convolutional layer, pooling layer, and fully-connected layer. This deep learning algorithm will process the data with grid-like topology. The name of convolution is the mathematical operation used in this network. CNN can significantly reduce the number of parameters in the network by using local connectivity that is the connection between the neurons and the nearby neurons in the next layer. This process is different from the traditional artificial neural networks (ANNs) in that each neuron will connect to all neurons in the next layer, so it takes the large numbers of parameters representing each connection.

C. *Related work*

DDoS attack exhausts the resources to make network and system unavailable for the legitimate users so users can not access to their network services [20]. Moreover, it also causes big financial damage to the victims. Attackers can deplete the targets which are personal computers or web servers by creating the different situations and hard to discover. The concept to detect the DDoS attack was occurred to prevent its danger.

Dataset is an important part of developing new techniques to deal with the attacks. CICIDS2017 [21], the dataset with common updated attacks including DDoS is composed of eight distinctive files containing five ordinary days and attacks activity data of the Canadian Institute of Cybersecurity [22]. In [23], they used CICIDS2017 on the log file of Friday afternoon applying with Multiple Linear Regression for DDoS attack detection. The dataset consisted of two class labels which is Benign and DDoS. They mentioned that they used Information Gain method for feature selection step to keep the most optimal feature. The result showed that they obtained 73.79% accuracy using the Multiple linear regression model with the top 16 attributes dataset. Another dataset is indicated in [24], it has all 27 features without duplicate records of 4 DDoS attacks which are HTTP Flood, SIDDOS, UDP Flood, and Smurf. Maslan et al. [25] extracted the 25 features of the dataset for their research. The dataset comprised of 5 classes (Smurf Attack, UDP Flood, SQL Injection, HTTP Flood, and Normal class). Then, they found the most optimal feature value for detecting DDoS attacks using linear regression. The results showed that only 4 attributes are very significant in DDoS attacks detection. Furthermore, they also compared the performance of five machine learning techniques including Naïve Bayes, Random Forest (RF), Neural Network, Support Vector Machine (SVM), and K-Nearest Neighbors. In summary, the highest accuracy is 98.70% obtained by using the RF algorithm and Neural Network equally. Tang et al. [26] compared various techniques with their deep neural network on the NSL-KDD dataset which is the reference to analyze the Network Intrusion Detection System (NIDS) models. They constructed a DNN model with an input layer, three hidden layers, and an output layer. Six features of the NSL-KDD dataset were chosen to do the experiments and implemented for binary classification problem. The results showed that their DNN model gave the best accuracy 75.75% and achieved a lower false positive value when compared to other algorithms (Naïve Bayes, SVM, Decision Tree).

In 2019, the researchers from Canadian Institute for Cybersecurity [12] presented a new DDoS dataset called "CICDDoS2019" to fix the limitations of existing dataset. The dataset contains benign and the most up-to-date common DDoS attacks. They executed 12 DDoS attacks on the training day containing NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and TFTP and 7 attacks in the testing day including PortScan, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag and SYN. Elsayed et al. [10] used CICDDoS2019 in their research. They proposed RNN with autoencoder named DDoSNet to classify benign and DDoS attacks. They separated the dataset into normal and malicious. In data preprocessing step, the researchers removed unwanted features such as source and destination IP, Source and destination port, timestamp, and flow ID to avoid the overfitting problems. Next, they removed all missing and infinity values from the data followed by normalization and labeled binary values for input data. This research showed the impact of the learning rate, they compared the accuracy using different learning rate values. The results indicated that using 0.0001 for learning rate with their proposed model, they achieved overall accuracy up to 99%. In [11], Shieh et al. proposed the model proof of concept for the DDoS attacks detection using deep learning. Their new DDoS detection framework combines Bi-Directional Long Short-Term Memory (BI-LSTM) and Gaussian Mixture Model (GMM) together with an incremental learning scheme. They used CICIDS2017 and CICDDoS2019 datasets as a training set, testing set, and evaluation. Some data of CICDDoS2019 were adopted as the unknown attacks. The results indicated that their BI-LSTM-GMM model performed satisfactory levels and gave high values in accuracy, precision, and recall. Furthermore, it can work well with unknown network attacks. In [2], this research also used deep learning and the CICDDoS2019 dataset to develop the DDoS attack detection framework. They chose three types of DDoS attacks, including SYN Flood, UDP Flood, and UDP-Lag in the experiments, then compared the performance with two deep learning models which are DNN and LSTM. Their results showed that DNN and LSTM have good performances similarly, but LSTM can distinguish normal and abnormal traffics a little better in SYN and UDP Flood, while DNN can do better in UDP-Lag attacks. They obtained overall accuracy values of up to 99%, making deep learning is one of the very best ways of detecting the attacks.

III. Proposed Models

In this part, the network architectures proposed for this research are explained. Two DL models are proposed to compare the performance of DDoS attacks classification in the multi-class problem.

A. *The proposed simple DNN*

The first proposed model is the simple DNN, which is composed of densely connected layers. This model consists of 6 dense layers sequentially, but L2 regularization, dropout, flatten, and batch normalization layers are also applied to improve the efficiency. Initially, the first layer is input layer. The input layer has 83 neurons as the input dimension that cover the 83 attributes of the DDoS attacks dataset used in this research. Then, it follows with the 5 hidden layers that are defined by fully-connected dense layers. The number of neurons for 5 hidden layers are 8192, 4096, 2048, 1024, and 512 respectively. A rectified linear unit (ReLU) is an activation function that is applied in each layer. Before the output layer, the L2 regularization layer with 0.01 as a regularization factor is applied to penalize the layer's kernel followed by batch normalization layer, dropout, and flatten. Batch normalization is the layer that is applied for stabilizing the learning process. The dropout layer in this model is handled by a rate equal to 0.2, then flattening the network using flatten layer. Finally, the last layer is the output layer that used softmax as an activation function and the number of neurons equal to 13 that the same number of all data classes.

B. *The proposed Convolutional autoencoder*

The second proposed network is a Convolutional autoencoder model. This model consists of convolutional layers, max pooling layers, Upsampling layers, and flatten applying with the autoencoder technique. Four convolutional layers are implemented using ReLU as an activation function. The lastly dense layer, 13 neurons number and softmax activation function are configured for the output. Autoencoder (AE) [8] is an unsupervised neural network that learns to efficiently compress multidimensional input data and reconstruct the compressed data from the hidden space. The encoding layer provided a smaller size of reduced multidimensional data and the decoding layer will process the input reconstruction by increasing the size of the compressed hidden space. The input regeneration from the encoding is for validating and refining the encoding. The autoencoder learns the representation (encoding) of the network flows for a set of data or training the network to overpass insignificant data for dimensionality reduction. The objective of this hybrid model is to accurately classify and characterize the malicious flow packets.

The architectures of two proposed models are shown in Figure 2. The hyperparameters set up are defined in Table I for the proposed simple DNN model and proposed convolutional model, respectively.

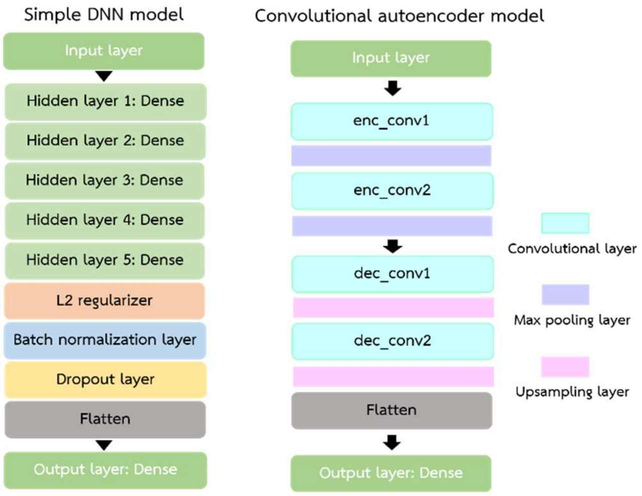

Fig. 2. The architectures of the proposed models are the simple DNN model (left) and the Convolutional autoencoder model (right).

TABLE I. THE CONFIGURED HYPERPARAMETERS FOR TWO PROPOSED MODELS

Model	Hyperparameter	Configuration
Simple DNN model	Number of hidden layers	5
	Number of neurons per layer (hidden layer 1 to 5)	8192, 4096, 2048, 1024, 512
	L2 regularization factor	0.01
	Dropout rate	0.2
	Adam optimizer learning rate	0.00001
	Batch size	64
Convolutional autoencoder model	enc_conv1, dec_conv2 (filters, kernel size)	(512, 5)
	enc_conv2, dec_conv1 (filters, kernel size)	(256, 3)
	Max pooling (pool size, strides)	(2, 2)
	Upsampling (size)	2
	Adam optimizer learning rate	0.00001
	Batch size	64

IV. Experiment and Results

The CICDDoS2019 dataset has been categorized into 13 classes that consist of benign class and 12 DDoS attacks, namely, DNS, LDAP, MSSQL, NetBIOS, NTP, SNMP, SSDP, SYN, UDP, TFTP, UDP-Lag, and WebDDoS. Before training the DL models for multiclass classification, the dataset has been preprocessed by removing the unwanted features and replacing missing and infinity values with zero. Next, the dataset has also been chosen 50,000 records per class and adjusted to be a balanced dataset by the technique called SMOTE [27]. Then, it has been separated into 10-fold for evaluating the model performance based on 4 common evaluation metrics, namely, accuracy, precision, recall, and F1-score. The amount of data for training, validating, and testing as shown in Table II. Naïve Bayes and Logistic Regression are the machine learning algorithms that have been adopted to compare the performance with the two proposed models. For the two proposed models, batch size fine-tuning results are shown in Table III and the best condition has been use to compare with two ML algorithms. The averaging results are indicated in Table IV.

TABLE II. THE AMOUNT OF DATA USED FOR TESTING AND EVALUATING MODELS

All Data	**Train set**		**Test set**
	Training	***Validating***	
650,000	468,000	117,000	65,000

Each class of data has been split equally.

TABLE III. THE RESULTS OF THE TWO PROPOSED DL MODELS VARY IN THE DIFFERENT BATCH SIZES

Model	**Batch size**	**Evaluation metrics**			
		Accuracy	***Precision***	***Recall***	***F1-score***
Simple DNN model	1	0.753	0.823	0.753	0.770
	32	0.768	0.834	0.768	0.784
	64	0.812	0.845	0.812	0.819
	128	0.777	0.818	0.777	0.787
Convolutional autoencoder model	1	0.725	0.827	0.725	0.748
	32	0.790	0.816	0.790	0.794
	64	0.851	0.877	0.851	0.856
	128	0.761	0.855	0.761	0.783

TABLE IV. THE RESULTS OF THE TWO PROPOSED DL MODELS COMPARED WITH TWO ML ALGORITHMS

Method	**Evaluation metrics**			
	Accuracy	***Precision***	***Recall***	***F1-score***
Naïve Bayes	0.211	0.310	0.211	0.151
Logistic Regression	0.431	0.501	0.431	0.403
The proposed simple DNN	0.812	0.845	0.812	0.819
The proposed Convolutional autoencoder	0.851	0.877	0.851	0.856

The results show that our two proposed models achieve the appropriate high accuracy in the detection of DDoS attacks and obtain the best results when using 64 as batch size. The proposed DNN and Convolutional autoencoder perform the good capability to classify this multiclass classification problem. They can identify between normal traffics and malicious traffics and also distinguish the 12 types of DDoS attacks separately. The first proposed model gave 81.2% accuracy, 84.5 % precision, 81.2% recall, and 81.9% for F1-score. The second proposed model, the CNN with autoencoder archives the best results in every evaluation metrics. This proposed model accomplished the highest averaging accuracy, precision, recall, and F1-score as 85.1%, 87.7%, 85.1%, and 85.6%, respectively. Overall results indicated that our proposed networks outperformed two ML algorithms with outstandingly higher values.

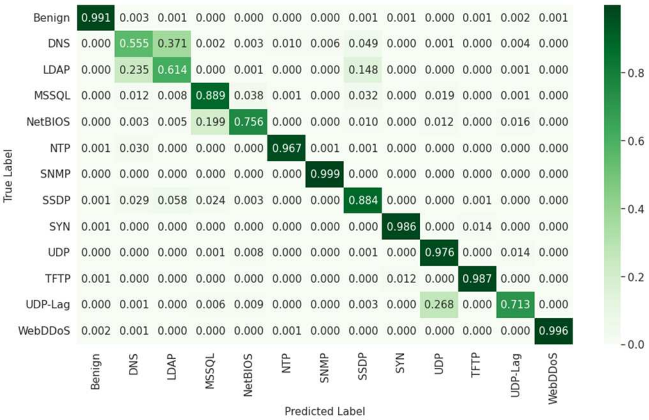

Fig. 3. The normalized confusion matrix for the proposed DNN model.

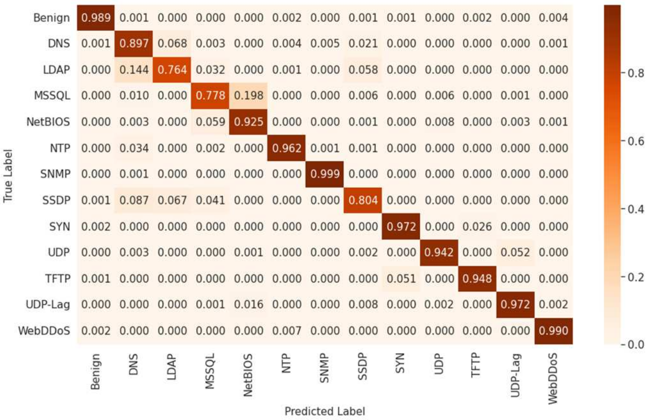

Fig. 4. The normalized confusion matrix for the proposed Convolutional autoencoder model.

In order to demonstrate the performance of our two proposed models, two normalized confusion matrixes for the best result were created, see Figure 3 and Figure 4. Two figures of confusion matrix displayed that the proposed models can discriminate the right normal traffics around 99% and also predict the correct class of each DDoS attack high up to 99.9%. Moreover, the ROC (Receiver Operating Characteristic) curves are plotted to analyze and illustrate the performance of classification models. The curves tell how much the models are capable of differentiating between classes. Figures 5 – 8 show the ROC curves of all methods and AUC, areas under ROC curve are also defined.

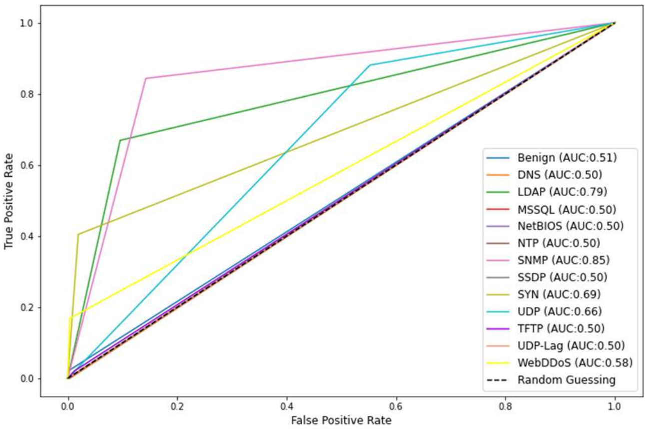

Fig. 5. The ROC curves of DDoS attacks classification using the Naïve Bayes algorithm.

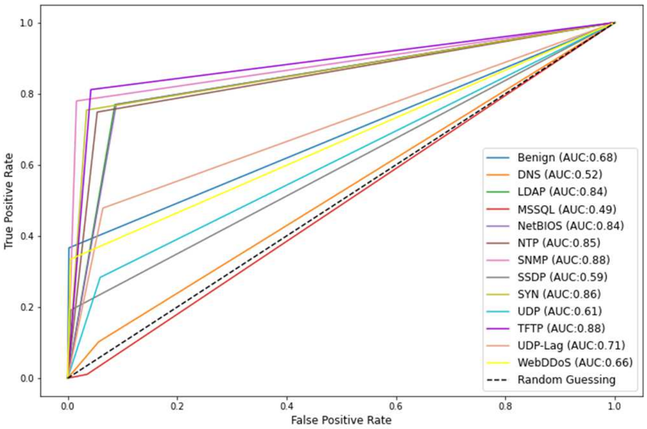

Fig. 6. The ROC curves of DDoS attacks classification using the Logistic Regression algorithm.

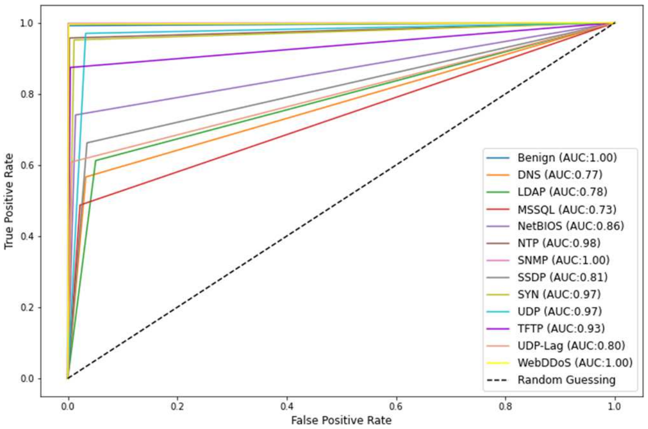

Fig. 7. The ROC curves of DDoS attacks classification using the proposed simple DNN model.

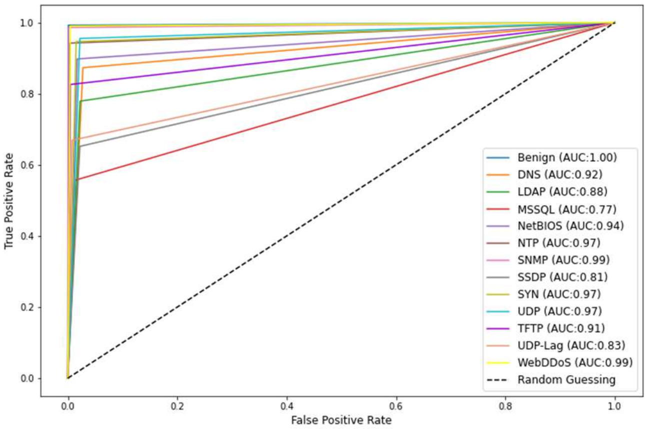

Fig. 8. The ROC curves of DDoS attacks classification using the proposed Convolutional autoencoder model.

V. Discussion and Future Work

This research aims to classify and detect network traffic for avoiding and preventing the damage of DDoS attacks. Nowadays, there are many datasets of DDoS attacks available to use and support to analyze such as KDDCUP99, NSL-KDD, ISCX2012, CICIDS2017 etc., but these datasets are ancient and may not anticipate the present attacks. The new DDoS dataset that is up-to-date and has been chosen to solve the limitation of previous datasets in this research is CICDDoS2019. In this research, various AI technologies were applied to consider and improve DDoS attacks detection. Machine learning was utilized to compared the results with our proposed models. The first proposed model is the simple DNN and the second is the Convolutional autoencoder model. The results showed that the proposed CNN achieved the best efficiency in this multiclass classification and the simple DNN also gave the better performance than Naïve Bayes and Logistic Regression.

From many works that mentioned before, they proved that the DL models can work well and have outstanding performance in the classification of DDoS attacks. The proposed DL models in this research also performed pleasing performance with the averaging value of all classes accuracy, precision, recall, and F1-score more than 81% for the simple DNN and more than 85% for CNN with autoencoder that means the proposed CNN provided the better solution. The highest accuracy obtained from the first proposed model is around 87%, while the highest accuracy of the second proposed model is high up to 91.9%. Although the overall accuracy is lower than some previous work, these proposed models still achieved outstanding efficiency from the simple structure of the networks and the hybrid model that can deal with the multiclass classification problem. Most previous works are the binary class classification framework that can identify between normal and attack class only, but this research focuses on a multiclass problem. Our proposed DNN models can distinguish more than 2 classes. They can classify benign traffics and characterize 12 classes of attacks including DNS, LDAP, MSSQL, NetBIOS, NTP, SNMP, SSDP, SYN, UDP, TFTP, UDP-Lag, and WebDDoS that cover each type of DDoS attacks today. Moreover, in the training and evaluating step the proposed models showed that adjusting the hyperparameters are affected the performance of the model. In case of a long period when training many data, fine-tuning batch size help to reduce training time and also affect the training results.

In the future, each class of data that indicates quite a high fault prediction will be more focused on the nature of the similarity of the attacks. The other scenarios will be designed and created to solve the problem and improve the accuracy of overall results. The new DL techniques will be used to compare the performance with our proposed networks in this research to analyze the best efficiency model. Long Short-Term Memory and other recurrent neural network architectures will be tried to implement from the outstanding performance that showed in many binary class classification problems of DDoS network attacks. Especially, the hyperparameters will be concentrated in more conditions to find the best fine-tuning model setup that outperform the present task. All improvements that have been mentioned is the part of work to enhance the networks performance. These are the important parts to closely solve the real-world issues from the damage of the DDoS attacks.

REFERENCES

[1] A. J. Mohammed, M. H. Arif, and A. A. Ali, "A multilayer perceptron artificial neural network approach for improving the accuracy of intrusion detection systems," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 9, no. 4, pp. 609-615, December 2020.

[2] T. Khempetch and P. Wuttidittachotti, "DDoS attack detection using deep learning," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 10, no. 2, pp. 382-388, June 2021.

[3] Abhishta, R. Rijswijk-Deij, and L. Nieuwenhuis, "Measuring the Impact of a Successful DDoS Attack on the Customer Behaviour of Managed DNS Service Providers," *Proceedings of the 2018 Workshop on Traffic Measurements for Cybersecurity*, *WTMC '18*, Budapest, Hungary, August 20, 2018, pp. 1–7.

[4] H. K. Hyder and C. -H. Lung, "Closed-Loop DDoS Mitigation System in Software Defined Networks," *2018 IEEE Conference on Dependable and Secure Computing*, *DSC 2018*, Kaohsiung, Taiwan, December 10-13, 2018, pp. 1-6.

[5] N. Gupta and N. Choudhary, "Past to Future of Network Security with AI," *Advances in Intelligent Systems and Computing*, vol. 1187, October 2020.

[6] J. Zhou, F. Chen, A. Berry, M. Reed, S. Zhang, and S. Savage, "A Survey on Ethical Principles of AI and Implementations," *2020 IEEE Symposium Series on Computational Intelligence*, *SSCI 2020*, Canberra, ACT, Australia, December 1-4, 2020, pp. 3010-3017.

[7] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," *2017 IEEE International Conference on Smart Computing*, *SMARTCOMP 2017*, Hong Kong, China, May 29-31, 2017, pp. 1-8.

[8] F. O. Catak and A. F. Mustacoglu, "Distributed denial of service attack detection using autoencoder and deep neural networks," *Journal of Intelligent & Fuzzy Systems*, vol. 37, no. 3, pp. 3969-3979, October 2019.

[9] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," IEEE Symposium. Computational Intelligence for Security and Defense Applications (CISDA), vol. 2, July 2009.

[10] M. S. Elsayed, N. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks", WoWMoM 2020, Cork, Ireland, August 31-September 3, 2020, pp. 391-396.

[11] C. -S. Shieh, W. -W. Lin, T. -T. Nguyen, C. -H. Chen, M. -F. Horng, and D. Miu, "Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model," 2021 4th International Conference on Information and Computer Technologies, ICICT 2021, HI, USA, March 11-14, 2021, pp. 27-32.

[12] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," *2019 International Carnahan Conference on Security Technology*, *ICCST 2019*, Chennai, India, October 31, 2019, pp. 1-8.

[13] A. Aljuhani, "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments, *IEEE Access*, vol. 9, pp. 42236-42264, March 2021.

[14] P. Kaviani and S. Dhotre, "Short Survey on Naive Bayes Algorithm," *International Journal of Advance Research in Computer Science and Management*, vol. 4, no. 11, pp. 607-611, November 2017.

[15] T. Edgar and D. Manz, Research Methods for Cyber Security (Chapter 4 - Exploratory Study), Massachusetts: Syngress, 2017.

[16] H. Yi, S. Shiyu, D. Xiusheng, and C. Zhigang, "A study on Deep Neural Networks framework," *2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference*, *IMCEC 2016*, Xi'an, China, March 02, 2017, pp. 1519-1522.

[17] F. Emmert-Streib, Z. Yang, H. Feng, S. Tripathi, and M. Dehmer, "An Introductory Review of Deep Learning for Prediction Models With Big Data," *Frontiers in Artificial Intelligence*, vol.3, pp. 4, February 2020.

[18] N. Wattanavichean, J. Boonchai, S. Yodthong, C. Preuksakarn, C.-H. Huang, and T. Surasak, "GFP Pattern Recognition in Raman Spectra by Modified VGG Networks for Localisation Tracking in Living Cells", *Engineering Journal (Eng. J.)*, vol. 25, no. 2, pp. 151-160, February 2021.

[19] K. Kitchat, N. Khamsemanan, and C. Nattee, "Gender classification from gait silhouette using observation angle-based GEIs," 2019 *IEEE International Conference on Cybernetics and Intelligent Systems (CIS) and IEEE Conference on Robotics, Automation and Mechatronics (RAM)*, *CIS-RAM 2019*, Bangkok, Thailand, November 18-20, 2019, pp. 485-490.

[20] N. Tripathi and B.M. Mehtre, "DoS and DDoS Attacks: Impact, Analysis and Countermeasures," *National Conference on Advances in Computing, Networking and Security*, *NCACNS'13*, Nanded, India, December 22-23, 2013, pp. 93-98.

[21] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *ICISSP 2018*, Funchal, Portugal, January 22-24, 2018, pp. 108-116.

[22] R. Panigrahi and S. Borah, "A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems," *International Journal of Engineering & Technology*, vol. 7, no. 3, pp. 479-482, January 2018.

[23] S. Sambangi and L. Gongi, "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression," *Proceedings of The 14th International Conference on Interdisciplinarity in Engineering*, *INTER-ENG 2020*, Targu Mures, Romania, October 8-9, 2020, pp. 51.

[24] M. Alkasassbeh, G. Al-Naymat, A. Hassanat, and M. Almseidin, "Detecting Distributed Denial of Service Attacks Using Data Mining Techniques," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 7, no.1, January 2016.

[25] A. Maslan, K. Mohamad, and F. Foozy, "Feature selection for DDoS detection using classification machine learning techniques," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 9, no. 1, pp. 137-145, March 2020.

[26] T. A. Tang, L. Mhamdi, D. McLernon, S. Zaidi, M. Ghogho, and F. E. Moussa, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," *2016 International Conference on Wireless Networks and Mobile Communications*, *WINCOM 2016*, Fez, Morocco, October 26-29, 2016, pp. 258-263.

[27] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," *Journal of Artificial Intelligence Research*, vol. 16, no. 1, pp. 321-357, January 2002.