UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Comparing Distributed Denial of Service (DDoS) Attack Classification Using Machine Learning Techniques in IoT Environment

Muhammad Fairuz Abdul Muin[1], Marina Md-Arshad[2], Adlina Abdul-Samad[3*], Anazida Zainal[4]
Faculty of Computing,
Universiti Teknologi Malaysia,
81310, UTM Johor Bahru, Johor, Malaysia
Email: mfairuz56@graduate.utm.my[1], marinama@utm.my[2], adlina6@graduate.utm.my[3], anazida@utm.my[4]

Submitted: 15/10/2024. Revised edition: 5/2/2025. Accepted: 17/5/2025. Published online: 27/5/2025
DOI: https://doi.org/10.11113/ijic.v15n1.497

***Abstract*—In the current information where everything has started to become more interconnected than ever, almost every individual in the world who are in developed, developing, and even 3rd world countries have access to the internet. IoT devices that make use of this technology become an integral part of our society. Although the conveniences that these devices bring are plentiful and benefit our society there are security concerns that must be addressed when looking at these IoT devices as they are vulnerable to different types of attacks. One of the simplest and most widely known attacks is the Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack. This type of attack aims to exhaust the devices or network resources which causes them to become unusable. The purpose of this research is to compare the performance of two different Machine Learning Algorithms which are Multi-Layer Perceptron (MLP) and Support Vector Machine (SVM) in classifying DDoS attacks in an IoT environment. The public dataset which is BoT-IoT uses real-world IoT situations that will demonstrate flood attacks which are most used for DDoS attacks on IoT devices. The dataset will go through three phases which are pre-processing, implementation of the machine learning algorithm and performance measurement. The experimental result shows that the best result when it comes to classifying DDoS attacks in an IoT environment is MLP.**

***Keywords*—IoT Security, DDoS Attacks, Support Vector Machine, Multi-Layer Perceptron**

I. INTRODUCTION

The Internet of Things (IoT) is a system consisting of interconnected computing devices, mechanical and digital machines, objects, people or even animals that are provided with a unique identifier (UIDs) and can transfer data through a network without requiring human-to-human or human-to-machine interaction. As technology advances, the adoption of IoT technology had expand so does the security that revolves around it. More devices are getting connected to the internet which includes industrial devices and even household devices. Smart homes, wearables, IoT devices, smart retail are examples of these devices.

Currently, many industries and individuals are beginning to change to adapt these devices that are connected to the internet into their daily lives or businesses because of its convenience. If we look at the statistics alone, there are nearly 22 billion IoT devices deployed worldwide by the end of 2018 and a further 17 billion will be added by the end of 2025 [1]. According to Cisco, the predicted number of devices that would be connected to an IP network will be more than three times the global population by 2023 which is approximately 29.3 billion [2]. The statistics show that the number of devices that are connected to the internet which will use IoT systems will increase every day and will continue to increase for years to come.

The complexity of DDoS attacks in IoT networks stems from the diverse nature of the devices involved, which can range from simple sensors to complex actuators. As highlighted by [3], DDoS attacks can significantly disrupt the services provided by IoT networks, making them one of the most challenging security risks in this domain [3]. The potential ramifications of such attacks include not only service interruptions but also financial losses and threats to public safety [4]. Therefore, developing effective anomaly detection systems is crucial for identifying and mitigating these threats.

While these devices are starting to become widely used by the population, security concerns remain regarding the systems and networks that these devices are connected to. These

devices are potentially vulnerable to malicious attacks which could cause significant damage to the network and devices. Vulnerabilities in a network or system consist of weaknesses that can be exploited by attackers which may lead to dangerous impacts such as having personal information stolen or causing the device to stop functioning. It could bring negative damage in terms of finances, damages to devices and even identity theft. There are many such attacks used by attackers to take advantage of vulnerabilities in a system for their own personal reasons. These threats could come from many different sources and can be a hassle to identify. One such attack is called a Distributed Denial of Service (DDoS) attack. Unlike DoS attacks, DDoS attacks use many hosts to attack and exhaust a system of its resources. Many existing studies use different types of machine learning algorithms to detect different types of DDoS attacks.

Therefore, this study aims to evaluate an optimum machine learning algorithm for detecting DDoS attacks by using two different machine learning algorithms. Machine Learning is a branch of Artificial Intelligence (AI) that focuses on imitating the way that humans learn and gradually improving its accuracy based on the given data. Using TCP and MLP, the different types of DDoS attacks which include HTTP flood, UDP flood and TCP flood are used as the labels for attack detection. This research also utilizes the public dataset called BoT-IoT dataset. The dataset undergoes various processes of data cleaning and feature selection using RapidMiner. Programming languages such as Python are used to apply to the machine learning algorithms to classify different types of attack detection. The confusion matrix provides results such as accuracy, recall, precision, and F1 score, which measure the performance of the machine learning algorithm in detecting DDoS attacks. A comparison between SVM and MLP are conducted to determine which algorithm delivers the most optimal results.

II. LITERATURE REVIEW

There exist existing works on this and there is a need to conduct a literature review therefore existing works of literature such as IoT background, vulnerabilities in an IoT environment, Different Machine Learning techniques that use supervised and unsupervised learning, types of DDoS attacks and how the DDoS attacks are classified in an IoT environment.

A. IoT Background

The Internet of Things has been growing in popularity, and the concept of IoT has evolved and undergone numerous changes, which will most likely continue in the future as new technologies become available. The Internet of Things (IoT) is a global information society infrastructure that connects (physical and virtual) things to enable improved services based on existing and evolving information and communication technologies [5].

The Internet of Things architecture can be thought of as a system that can be physical, virtual, or even a hybrid of the two. The Internet of Things is made up of numerous active physical components, such as actuators, sensors, cloud services, and IoT protocols. An IoT system is composed of several functional blocks that combine to form the system's various functions: device, communication, services, management, security, and application. The IoT Architecture was shown in Fig. 1.

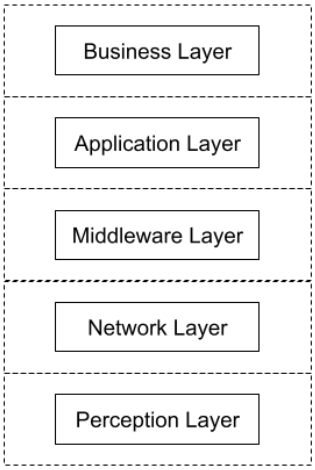

Fig. 1. IoT Architecture

B. Vulnerabilities in the IoT Environment

While the network layer is critical in an IoT environment, it is also critical in all other forms of information and communication. Two sublayers make up the network layer: the access layer and the internet layer. The access sublayer oversees data acquisition, data transfer to the core network, and data forwarding to the middleware layer. This layer protects against security threats such as unauthorized network access, integrity violations, denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, and confidentiality breaches.

The cloud-based middleware layer manages the scalability and flexibility. As a result, it is capable of large-scale data processing. Malicious users may be able to obtain unauthorized access to and manipulate data stored in other virtual machines. This is possible because the architecture enables the coexistence of multiple machines from various IoT service providers on a single physical server [6].

C. High Profile Cyberattacks in IoT Environment

In 2019, the Amazon-owned Ring faced a barrage of privacy concerns and scandals. Researchers discovered vulnerabilities in IoT devices that could allow attackers to spy on families or even reveal Wi-Fi network passwords. Several attackers even took the footage and sold it to interested parties. Later, it partnered with over 600 police departments to enable camera owners to request access to their cameras' footage. Finally, Senators from the United States demanded that Amazon disclose the camera's footage and who has access to it. Another attack, Malware Bricks Thousands of IoT Devices, occurred in June 2019 and was perpetrated by a 14-year-old hacker. The attacker launched an attack against up to 4,000

insecure Internet of Things devices using a novel strain of malware. By erasing their devices' storage, disabling their firewalls, and even reconfiguring their network configuration, the malware rendered their devices unusable. Silex is a new malware that was inspired by the infamous Bricker Bot malware that was responsible for bricking millions of Internet of Things (IoT) devices in 2017.

The attacker's primary motivation for developing the malware was "to remove vulnerable IoT devices on which it was built in order to prevent other script kiddies from building botnets." The 14-year-old assailant had no idea the situation would spiral out of control. This malware's primary effect is to force users to reinstall the firmware on their devices. Because most users believe it is a hardware failure rather than a malware attack, they will discard their devices, as installing the device's hardware is tedious work for most people. According to researchers from a cyber security firm, ten vulnerabilities affecting NSC Linear eMerge E3 devices have been disclosed in May 2019 [7]. CVSSv3 score of 9.8 out of 10 for the applied risk Directory traversal, cross-site scripting, command injection, unrestricted file upload, privilege escalation and authorization bypass, clear-text storage of passwords and hard-coded credentials, cross-site request forgery, version control failure, stack-based buffer overflow, and root access via SSH are all vulnerabilities that are present.

These attacks demonstrate that, while IoT technology evolves and is increasingly adopted globally, the vulnerabilities of these systems grow as well, and that vulnerabilities must be detected and mitigated as quickly as possible, as information is now more valuable than gold.

D. DDoS Attacks Classification

Since IoT technology often have limited security and computing resources, they are highly prone to the attacks. There are three type of the DDoS attack such as volumetric attacks, protocol attacks and application attacks in Fig. 2 [8]. Based [8], the volume-based attacks refer to the attacker floods the victim with massive traffic to exhaust the bandwidth. It could be likely the attacker X sends massive requests to example.com using the victim Y's Internet Protocol (IP) such as (2.2.2.2), causing the victim Y to receive a lots of responses to consume its network capacity. Moreover, the protocol-based attacks exploit the vulnerabilities in the network protocols such as Layer 3 and Layer 4 to exhaust the system resources. For example, the attacker X manipulate the example.com and other domains to respond with massive data beyond the victim Y's storage capacity, leading to the system failure. Furthermore, the application layer attacks which lead to the target the application layer by overloading the server processes. For example, the attacker X makes repeated complex request to consume the victim Y's processing power to prevent it from handling the taskes. Each type of the attack aims to overwhelm the victim's resources, causing the disruption and service failure. Therefore, in this study, the main focus attack is the volumeteric attacks.

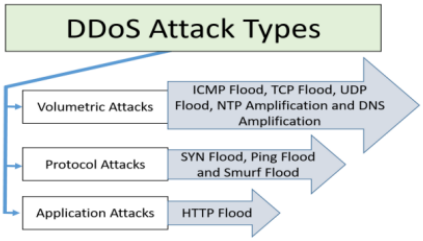

Fig. 2. Type of DDoS attack [8]

E. Supervised Learning

There are many machine learning technique had been used in the detection of DDoS attacks. Machine learning techniques can be categorized into supervised, unsupervised, semi-supervised and deep learning method [9]. Supervised learning makes use of a labelled data set to generate a function that maps input to the desired output based on Fig. 3. By and large, supervised learning is the most frequently used technique for training neural networks and decision trees. It can be classified into two categories: classification and regression. The labelled data for classification is discrete, whereas the label for regression is continuous. SVM shows effectively deals with high-dimensional feature spaces, making it suitable for detecting complex traffic patterns in the past studies [10] whereas MLP can be scaled easily by adjusting the number of layers and neurons, allowing them to adapt to the complexity of the dataset [11]. While other models such as Random Forests (RF) and k-Nearest Neighbors (KNN) are also used in DDoS detection, they may not offer the same level of performance in high-dimensional spaces or the ability to model complex relationships as effectively as SVMs and MLPs. For example, RFs can struggle with interpretability and may require extensive hyperparameter tuning to achieve optimal performance [12]. Similarly, KNN is sensitive to the choice of distance metrics and can be computationally expensive in high-dimensional settings [13]. Therefore, there are two main algorithm that focus in this research which are SVM algorithm and MLP algorithm and discuss in the next subsection.

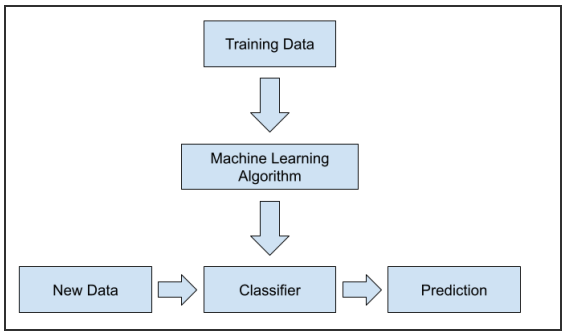

Fig. 3. Supervised learning

1) Support Vector Machine

SVM is a supervised machine learning algorithm that combines classification and regression capabilities. The support vector machine algorithm's primary objective is to locate a hyperplane that classifies the data points in N-dimensional space (N minus the number of features).

Support Vectors are used to categorize data points into two distinct classes. This results in a large number of additional hyperplanes for this algorithm. This algorithm's objective is to find the plane that has the greatest margin or distance between two classes of data points.

The development of specialized datasets for training machine learning models is critical for effective DDoS detection. The availability of comprehensive datasets that reflect the unique characteristics of IoT traffic allows for better training and validation of models like SVM. For instance, the work by [14] emphasizes the importance of utilizing diverse datasets to assess the performance of various ML classifiers in detecting DDoS attacks [14]. This is essential for ensuring that the models can generalize well across different IoT scenarios and attack vectors.

2) Multi-Layer Perceptron (MLP)

The multi-layer perceptron (MLP) is a supervised machine learning technique that performs classification by utilising the underlying Neural Network. MLP is a feedforward artificial neural network in its simplest form. It employs multiple layers of input nodes. It trains the data using backpropagation.

The neural network's primary components are artificial neurons that generate a specific output in response to an input that activates under certain conditions.

The input layer is frequently referred to as the visible layer because it is the exposed portion of the network that will receive data. The term "hidden layer" refers to the fact that it is not directly exposed to the input. The term "deep learning" refers to a neural network with numerous hidden layers. It is so named because training would be extremely slow, but modern technology has advanced to the point where it may take seconds or minutes to train. The simplest hidden layer structure is a single neuron that outputs the value directly. The hidden layer accepts a set of weighted inputs and outputs an activation function-based output. Finally, the output layer produces the neural network's output.

MLP functions through backpropagation, a process that begins by reading values from the input layer. It then moves through the hidden layer using initial weights, which are often randomly assigned. After computing the output for each neuron from the input layer to the output layer, it calculates the error in the resulting output.

$$\text{ErrorB} = \text{Actual Output} - \text{Desired Output} \quad (1)$$

MLP can achieve high accuracy in detecting DDoS attacks when trained on appropriate datasets. For instance,[15]emphasized the importance of feature selection in enhancing the performance of MLP models for DDoS detection in IoT networks [15]. By selecting relevant features that capture the characteristics of normal and malicious traffic, MLP can improve its classification accuracy.

III. FRAMEWORK FOR DDOS ATTACK DETECTION

There are three phases to this experiment. The first phase of the experiment is the Preparation and preprocessing dataset which will include the review and study of existing literature and also the pre-processing of the dataset. The second phase is the implementation of the Machine Learning Algorithm which will focus on the dataset being applied to the Machine learning Algorithm. The final phase is a performance analysis which will compare and review SVM and MLP in classifying the DDoS attacks.

A. Phase 1: Preparation and Preprocessing Dataset

Bot-IoT dataset that contain raw network packets (PCAP) files were produced using the tshark programme in the Cyber Range Lab of Australian Center for Cyber Security (ACCS) which includes both regular and unusual traffic. This dataset was chosen based on it can stimulates on IoT environment and creates a realistic scenario in which many different types of attacks are done. The attributes of the dataset are examined during the data-preprocessing after going through the data cleaning process which will create a role for the dataset on RapidMiner, the unnecessary labels are also removed such as the Category and attack labels. The label used for this experiment is the Subcategory. As MLP and SVM do not accept Polynomial attributes, the attributes must be changed to a Nominal format. Fig. 4 shows the weighted results of the attribute after the feature selection is done.

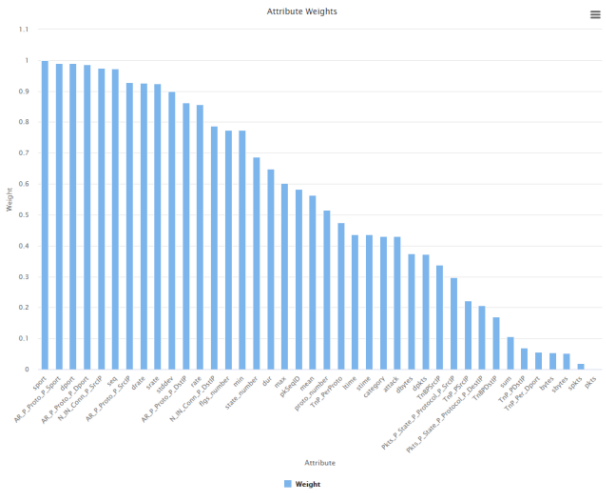

Fig. 4. Weighted results of the attribute

The correlation score in Table I shows the strength of the relationship between the sport and AR_P_Proto_P_Sport. This means that if one variable changes in value, the other variable will tend to change in a specific direction. In a way, it can act as a perfect positive relationship. As such, the attributes that have a higher correlation score than >0.95 are removed because it can cause the result to become overfitted.

TABLE I. CORRELATION SCORE

Variable	Correlation Score
sport	1.0
AR_P_Proto_P_Sport	0.9900952515618446
dport	0.9899641386125908
AR_P_Proto_P_Dport	0.9860048299387463
N_IN_Conn_P_SrcIP	0.9737861547921559
seq	0.9729837059441484
AR_P_Proto_P_SrcIP	0.9276102596763258
drate	0.9256501126650414
srate	0.9236094204980478
stddev	0.8986794265827721
AR_P_Proto_P_DstIP	0.8625796348974513
rate	0.8568420811699891
N_IN_Conn_P_DstIP	0.7882030616925523
flgs_number	0.7734922798131477
min	0.7732058947299759
state_number	0.6865091358726256
dur	0.6492514367932158
max	0.602237740975196
pkSeqID	0.5818852659648358
mean	0.5639673504902384
proto_number	0.5162755244487706
TnP_PerProto	0.4746496960503682
ltime	0.4371183323242465
stime	0.4369762873153839
attack	0.4309640548450202
category	0.4309640548450202
dbytes	0.37533846918800545
dpkts	0.3717208254043727
TnBPSrcIP	0.3371057407622926
Pkts_P_State_P_Protocol_P_SrcIP	0.2967562072309441
TnP_PSrcIP	0.22212212273675358
Pkts_P_State_P_Protocol_P_DestIP	0.2063985936759634
TnBPDstIP	0.1702925660621388
sum	0.10625914503160187
TnP_PDstIP	0.06994190641339457
TnP_Per_Dport	0.05619969263754979
bytes	0.05544279858694816
sbytes	0.05157189608378051
spkts	0.01852314334819767
pkts	0.0

The typical network in an IoT network will contain these attributes which are destination address, packets, protocol, rate, source address and state, therefore, these attributes will be included [16].

Afterward, a process called Principal Component Analysis (PCA) is one of the dimensionality reduction techniques. It is used to reduce the attributes of the dataset so that the implementation process will be more optimized.

B. Phase 2: Implementation of Machine Learning Algorithm

The goal of this phase is to implement the Machine Learning Algorithm using Python and classify the DDoS attacks.

The SVM and MLP algorithm uses Python 3.10 and uses libraries such as pandas to read the csv and sklearn to train the model. After the dataset is loaded into Python, it will begin the Machine Learning process. There are specific hyperparameters used for SVM and MLP in classifying DDoS attacks from the BoT-IoT dataset to ensure reproducibility. Table II shows the hyperparameter values for both algorithm.

TABLE II. HYPERPARAMETER VALUES FOR SVM AND MLP MODEL IN SKLEARN

Model	Classifier	Hyperparameter values
SVM	SVC	random_state = 0 tol = 1e-5 max_iter = 20000 dual = False
MLP	MLP classifier	random_state = 1 Max_iter = 3000

The Model for the SVM uses Linear Support Vector Classification (SVC) to train the model because the dataset contains more than 1 million rows. There are 20000 iterations in the model for the SVM Model. The dataset is split 70% as the training sample and 30% as the test sample.

The Model for the MLP uses the MLP classifier from sklearn in Python which is part of the sklearn neural network library. The classifier only has 3000 iterations because MLP is a very heavy computational classifier.

C. Phase 3: Performance Evaluation

The last phase of this research is the performance evaluation and the benchmarking of the machine learning algorithm. The performance of the algorithm is evaluated using the confusion matrix.

The confusion matrix consists of Accuracy, Precision, Recall and F1 score. These performance parameters are calculated, and results are benchmarked. Using the following results, the most accurate machine learning algorithm between the two techniques can be decided for classifying the DDoS attack.

The reason why the precision score in Python as shown in Fig. 5 is 96% while the recall and F1-score are low is because of the low amount of data in the dataset that contains the Normal packet. The normal packets in the network where a DDoS attack is present will always be much lower as compared to the abnormal packets to the point where the normal packets would sometimes get drowned in the influx of the network traffic from the attack. The total accuracy for the SVM Model is 78%. This shows that the accuracy is dominated by the performance on TCP and UDP because they constitute the most of the dataset.

```
PS D:\Research\psm\psm> python svm.py
['TCP' 'TCP' 'UDP' ... 'UDP' 'TCP' 'TCP']
              precision    recall  f1-score   support

      Normal       0.96      0.17      0.29       140
         TCP       0.73      0.89      0.81    293445
         UDP       0.86      0.66      0.75    284249

    accuracy                           0.78    577834
   macro avg       0.85      0.58      0.61    577834
weighted avg       0.79      0.78      0.78    577834
```

Fig. 5. Result of SVM

The MLP uses two hidden layers which will accept six inputs which is the selected features that include daddr, pkt, proto, rate, saddr and state based on Fig. 6. The selected features for the relevance in distinguishing between Normal, TCP, and UDP traffic, as they capture key network behaviors such as protocol type, traffic rate, and packet patterns. These features enable the MLP model to effectively identify abnormal traffic by learning complex relationships through its two hidden layers and mapping them to the three output labels.

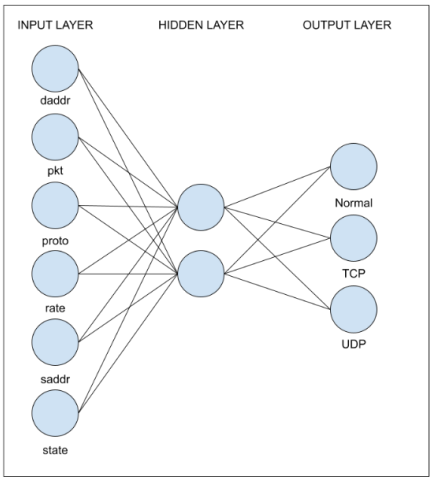

Fig. 6. Result of MLP

IV. RESULT ANALYSIS

There are three classes are involved in the classification of the DDoS attacks which are Normal, TCP and UDP. Based on the results obtained as shown in Table III, the MLP algorithm gives a much better result as compared to the SVM algorithm. This is shown by the average accuracy of the results.

The performance evaluation comparison between SVM and MLP models for DDoS attack detection, as shown in Table II, highlights distinct differences in their classification abilities. The SVM model demonstrates strong precision for detecting normal packets (96%), but its recall is significantly low (17%), indicating that it fails to detect a large number of actual normal packets. This results in a low F1-score (0.29), making SVM less effective in identifying normal traffic. However, SVM performs moderately well for TCP and UDP packet classification, with balanced precision, recall, and F1-scores in both categories. Despite this, the overall accuracy of the SVM model is 78%, reflecting its limitations in reliably detecting normal traffic while performing better in classifying attack traffic.

In contrast, the MLP model excels across all subcategories, showing superior performance in both precision and recall. For normal packets, MLP achieves a recall of 77%, significantly higher than SVM, and an F1-score of 0.85, indicating its ability to detect a greater number of actual normal packets without sacrificing precision. For TCP and UDP packet classification, MLP outperforms SVM, with both subcategories showing high precision (98% and 92%) and recall (92% and 98%), resulting in F1-scores of 0.95 for both. This consistent performance across different packet types, combined with an overall accuracy of 95%, makes MLP the more effective model for DDoS attack detection, particularly in environments where accurate differentiation between normal and attack traffic is critical.

TABLE III. PERFORMANCE EVALUATION BASED ON SVM MODEL AND MLP MODEL

Model	Subcategory	Precision	Recall	F1-Score	Accuracy
SVM	Normal	0.96	0.17	0.29	0.78
	TCP	0.73	0.89	0.81	
	UDP	0.86	0.66	0.75	
MLP	Normal	0.95	0.77	0.85	0.95
	TCP	0.98	0.92	0.95	
	UDP	0.92	0.98	0.95	

V. CONCLUSION

In conclusion, this study demonstrates that the MLP model significantly outperforms the SVM model in detecting DDoS attacks across multiple subcategories of traffic. While SVM achieves high precision, particularly for normal traffic, its low recall leads to poor overall performance in identifying normal packets, resulting in an overall lower F1-score and accuracy. SVM performs moderately well in detecting TCP and UDP packets but still falls short compared to the MLP model. On the other hand, MLP consistently delivers high precision, recall, and F1-scores across all subcategories, including normal, TCP, and UDP packets, resulting in a much higher overall accuracy of 95%. This makes MLP the more robust and reliable model for DDoS attack detection, providing a better balance between precision and recall, especially in distinguishing between normal and attack traffic in a network environment.

VI. FUTURE WORKS

Currently, the machine uses 16GB of memory, with only half available for the experiment as the rest is utilized by the system. In the future, increasing the memory capacity is essential to enhance the performance, and exploring the integration of real-time data into detection frameworks is another area ripe for exploration. Real-time traffic analysis can significantly improve the responsiveness of DDoS detection systems, allowing for immediate identification and mitigation of attacks as they occur.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to our supervisor, Ms Marina Md Arshad, for her invaluable guidance and insightful feedback in this research. Her expertise and encouragement were instrumental in shaping our work and overcoming challenges. We deeply appreciate her dedication

and the time she invested in helping us refine our ideas and achieve our goals.

CONFLICTS OF INTEREST

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Mercer, D. (2019). Global Connected and IoT Device Forecast Update. Strategyanalytics.com. https://www.strategyanalytics.com/access-services/devices/connected-home/consumer-electronics/reports/report-detail/global-connected-and-iot-device-forecast-update.

[2] Cisco. (2020). Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper. Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.htm.

[3] Khedr, W., Gouda, A., & Mohamed, E. (2023). FMDADM: A Multi-layer DDoS Attack Detection and Mitigation Framework using Machine Learning for Stateful Sdn-based IoT Networks. IEEE Access, *11*, 28934–28954. https://doi.org/10.1109/access.2023.3260256.

[4] Mohammed, B. (2023). Anomaly Detection of Distributed Denial Oof Service (DDoS) in IoT Network using Machine Learning. https://doi.org/10.21203/rs.3.rs-3496063/v1.

[5] Ray, P. P. (2018). A Survey on Internet of Things Architectures. *Journal of King Saud University - Computer and Information Sciences, 30*(3), 291–319. https://doi.org/10.1016/j.jksuci.2016.10.003.

[6] Ivan, C., Vujic, M., & Husnjak, S. (2016). Classification of Security Risks in the IoT Environment. *DAAAM Proceedings*, 0731–0740. https://doi.org/10.2507/26th.daaam.proceedings.102.

[7] Krstic, G. (2019). Nortek Linear eMerge E3-Series 1.00-06 Multiple Vulnerabilities. https://applied-risk.com/assets/uploads/whitepapers/Nortek-Linear-E3-Advisory-2019.pdf.

[8] Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2023). DDoS Attacks Detection using Machine Learning and Deep Learning Techniques: Analysis and Comparison. *Bulletin of Electrical Engineering and Informatics*, *12*(2), 930–939.

[9] Aljuhani, A. (2021). Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments. *IEEE Access*, *9*, 42236–42264.

[10] Mishra, S., J. Albarakati, A., & Sharma, S. (2022). Cyber Threat Intelligence for IoT using Machine Learning. *Processes*, *10*(12), 2673. https://doi.org/10.3390/pr10122673.

[11] Mopuru, B. (2024). Enhanced Intrusion Detection in IoT with a Novel PRBF Kernel and Cloud Integration. *Engineering Technology & Applied Science Research, 14*(4), 14988–14993. https://doi.org/10.48084/etasr.7767.

[12] Rihan, S. D. A., Anbar, M., & Alabsi, B. A. (2023). Meta-learner-based Approach for Detecting Attacks on Internet of Things Networks. *Sensors, 23*(19), 8191. https://doi.org/10.3390/s23198191.

[13] Nitish, A., Hanumanthappa, J., Prakash, S. P. S., & Krinkin, K. (2021). Expert Knowledge Correlated Intrusion Detection System Evaluation Framework for Heterogeneous IoT. https://doi.org/10.36227/techrxiv.16722784.v2

[14] Musa, M. (2024). A Framework for the Detection of Distributed Denial of Service Attacks on Network Logs using ml and dl Classifiers. *Scientia Africana*, *22*(3), 153–164. https://doi.org/10.4314/sa.v22i3.14

[15] Roopak, M., Tian, G., & Chambers, J. (2020). Multi‐objective‐based Feature Selection for DDoS Attack Detection in IoT Networks. *Iet Networks, 9*(3), 120–127. https://doi.org/10.1049/iet-net.2018.5206.

[16] Gurulakshmi, K., and A. Nesarani. (2018). Analysis of IoT Bots against DDOS Attack Using Machine Learning Algorithm. *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI).* 10.1109/icoei.2018.8553722.