ISSN 2278-3091

Volume 10, No.4, July - August 2021

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse221042021.pdf

https://doi.org/10.30534/ijatcse/2021/221042021

A Machine Learning-Based Intrusion Detection of DDoS Attack on IoT Devices

Suleman Mohammed

Altinbas University,Department of Electrical &Computer Engineering, Turkey, sulemanmohammed@ogr.altinbas.edu.tr

ABSTRACT

DDoS attack aims to prevent legitimate users from getting access to a targeted system service by exhausting the resources, bandwidth and so on. Though, there are different intrusion mechanisms for detection DDoS attack, having an automated system that can learn the nature of the attack and instantly detect it is the reason why machine learning is used in this work. Decision tree, KNN and Naïve Bayes are the algorithms used classify a benign traffic from a DDoS attack. About nineteen different feature was carefully selected from CIC2019DDoS dataset. The DDoS attack types used for the experiment are UDP, DNS, SYN and NetBIOS. The results of the experiment indicate that Decision tree and KNN proved to be the most effective with an accuracy of 100% and 98% respectively. Naïve Bayes gave a very poor result with an accuracy of 29%.

Key words: Distributed Denial of Service (DDoS) attack, IoT, Machine learning, Intrusion Detection, DNS, SYN

1. INTRODUCTION

Devices are now connected internationally through the internet with the help of internet protocols and this is what has come to be known as internet of object or internet things; IoT for shot. Smart phones, TV, vehicles and so on can communicate and share data through a process often referred to as machine-to-machine (M2M communication)[1].One major challenge that hinders a smooth functionality of the IoT is security issues[2].Distributed denial of service attack (DDoS) is one of the common attack on IoT devices[1]. A large group of compromised workstations called botnet are used to simultaneously launch a massive attack. The primary goal is to prevent legitimate users access to system service or to degrade system performance[3]. It is easy and simple to implement but the damages are massive[4]. Master DDoS is a special malware that the attacker installs to detect device with vulnerabilities in the network. The effect of the attack largely depends on the period by which service is suspended and the size of the attack[5]. A large quantity of bots gives computer the power to develop prime tools to carryout malicious activities like the spread of SPAM email, virus, click fraud and so on[3]. Flooding, Spoofing, User to root port scanning, oversized XML, Coercive Parsing Web-service addressing Spoofing and Reflective attack are some of the common type of DDoS attacks[6].

Even though, there are various intrusion detection systems (IDS) in place for protecting systemsin addition to the traditional security methods such as firewall, there are daily reports on serious cyber-attack[7][8].The firewall for instance is effective in detecting external attacks but very poor in detecting internal attacks[6].

It is therefore important to make a smart detection of this attack by using machine learning techniques. Machine learning has made a great progress in recent years in detecting DDoS attack[9].

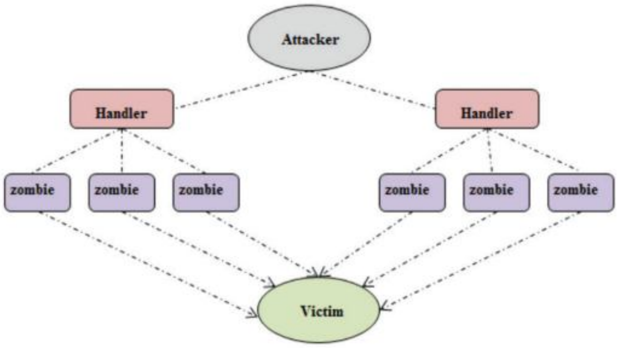


Figure 1: DDoS Flooding Attack Architecture[5]

This research proposes an intrusion detection and prevention on IoT devices using machine learning techniques. A DDoS attack dataset is obtained from Canadian institute of cyber security for the training purposes. The machine learning algorithms used in here include Decision tree, Naïve Bayes, K-NN and then the accuracy rate is compared for a best result.

2. METHODOLOGY

The research employed the Cross Industry Process for data mining (CRISP-DM) methodology as reference model for all the activities carried out in the analysis phase. CRISP-DM is a six phased cyclic or process model that for data mining projects. The six phases of the CRISP-DM are:

1) Business Understanding: The concept of DDoS attack and how to use machine learning to handle the task is tackled here.

2) Data understanding: The CICDDoS2019was obtained from Canadian Institute of Cyber-security (CIC) after following a Sign Acceptance Use Policy (AUP). The dataset has about 500006249 DDoS attack as well as 56863 instance of benign (legitimate) network traffic. DNS, SYN, UDP and NetBIOS are the attacks analyzed. Features to be used are extracted.
3) Data Preprocessing: The data is splitted into training and testing. About 80% of the data went into training while the other 30% was used for testing.
4) Modeling: The analysis of the dataset was carried out by carefully selecting three different supervised machine learning algorithms training and testing purposes.
5) The result of the experiment is evaluated and the accuracy of the all the algorithms[10] involved compared.

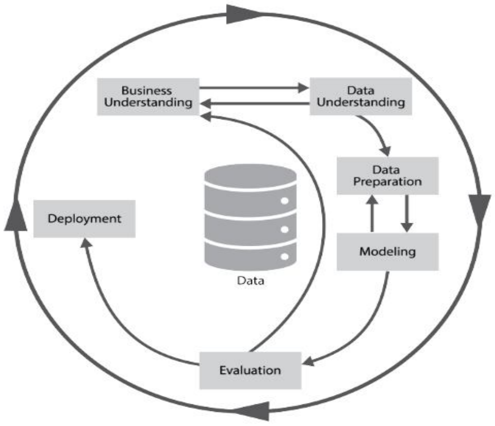


Figure 2: The six-phase project life cycle[11]

3 .LITERATURE REVIEW

There has been numerous research work with respect to intrusion detection and prevention using machine learning techniques.
Stefanos Kiourkoulis research work focuses on comparing between the performance of intrusion detection and prevention using 3 different publicly available datasets. The work made use of five different machine learning algorithms to analyze performance of the datasets. The research concluded that, large dataset such as the CEC-CIC-IDS2018 produced better result with high performance compared to small dataset. Random forest algorithm produced the best result while SVM was the least[12]. A research work conducted by Kubra Saeedi explains about the security threats and vulnerabilities of IoT devices from the packet core perspective. It applies four different machine learning algorithms for the mitigation of DDoS attack on IoT devices. The supervised learning classification algorithms were used and their performance were evaluated respectively. The result of the test indicated that KNN algorithm produced that highest accuracy while Naïve Bayes was the lowest[2]. Jiangtao Pei et al.[13]proposed DDoS attack detection using machine learning techniques. His work used only the random forest algorithm in training of the attack models which produced a best detection rate. A research work done by Yasar Shahid Hussain used the CICDDoS2019 dataset that contained 80 features part of which are legitimate traffic[14] whole the rest are DDoS attack. His work was titled network intrusion detection of DDoS attack using machine learning classification techniques. Waikato Environment for knowledge Analysis (WEKA) tool was used by the researcher to carry out the machine learning algorithms using k-fold (k = 5) cross validation. The algorithms that were used for the evaluation were Bootstrap Aggregating (Bagging), Bayesian Network(BayesNet), Sequential Minimal Optimization (SMO), k-Nearest Neighbors (KNN) and Simple Logistic[15].

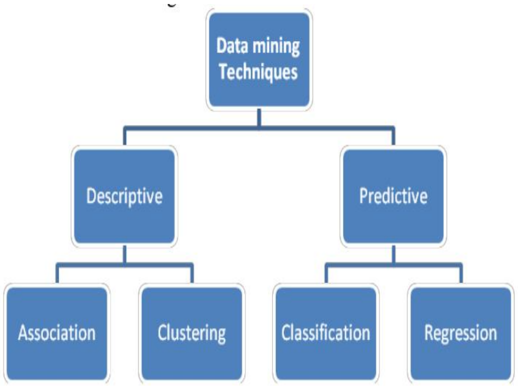


Figure 3: Machine Learning Algorithm types[16]

4. OVERVIEW OF MACHINE LEARNING

Machine learning (ML) is a sub-division of artificial intelligence (AI) which solves problems through computerized techniques according to previous information. In order to solve problems or make prediction[17], ML algorithms study the unseen pattern in a data then classifies them. The availability of labels is what is what categorized ML algorithms[10] is grouped into supervised (predictive) and unsupervised (descriptive). Supervised learning demands a predetermined result in addition to the input attributes. Analytical operations are carried out using training data, hence contingent function are created for mapping generated attribute instances. Supervised learning are again categorized into classification and regression[18].

4. 1Decision Tree

It is one of the popular machine learning algorithm which is been used in generating a classifier to classify desired data from an available one. There can be binary decision and non-binary decision and this research work made use of binary decision tree since it is used to determine(predict) if a network traffic is normal or attack. A root and internal nodes together with leaf nodes constitute the structure of a decision tree. Decision occurs in a top-down recursive way where all the observations are contained in the root node while every internal node contains the feature test[2]. The leafs are returned as the result. Non-leaf nodes are regarded to as the component and every branch is considered as a value that can be derived from the branch. Classification of data occurs starting from the route node and eventually ending at the leaf according to the characteristics of the CICDDoS2019 datasets. The predicted value is defined by the leaf[19].

4. 2 k-Nearest Neighbor (KNN)

KNN is a type of supervised learning algorithm that assumes that same data mining exist nearby[20].It is sometimes known as an instance-based learner because the algorithm remembers the training instance other than studying the training models. As a supervised learning algorithm there is a need for labelled datasets of the training samples (x, y) so as to be able to make prediction of the relationship between x and y. For the KNN to do its analysis, it needs three main parameters; a given positive integer (K), a similarity metric d and a hidden observation h(x)[2].The "nearest neighbor" are considered the k training tuples. Closeness is however, defined as with regards to distance metric such as Euclidean distance given as:

$$d(x,y)=\sqrt{\sum_{i=1}^{n}(y-x)}^{2} \quad (1)$$

4. 3 Naïve Bayes

This probabilistic algorithm which operates based on the Baye's Theorem and it is an ideal algorithm for big datasets[2]. Values are presumed to be independent to simple computation but however, there can be dependence between variables in practice. Naïve Bayes makes a class conditional presumption (assumption). The assumption made by Naïve Bayes can simple be stated as the availability of particular of a class has no relation with the presence of another feature of the class. It becomes the best classifier out of all in terms of comparison if the assumption becomes true. In binary classification cases such as in this research, Naïve Bayes is very efficient in predicting if a network traffic is DDoS attack or a legitimate network traffic.

This theorem can be mathematically represented in the equation [21] below:

$$P(A|B)=\frac{P(B|A)P(A)}{P(B)} \quad (2)$$

Where:

A and B represents 2 independent events
P(A) and P(B) represent the probability of A and B
P(A|B) probability of A given that B is true

P(B|A) probability of B given that A is true

5. CLASSIFICATION AND IMPLEMENTATION

5.1 Feature Extraction

In order to be able to differentiate between a normal IoT traffic as well as DDoS attack traffic, there is a need to select packet features that shows DDoS attack for machine learning to classify them. Nineteen different features are chosen for the machine learning.

Table 1: Features used in the ML

Features	Description
Source_IP	Source device IP address
Source_Port	Sent address
Destination_IP	IP of the destination devices
Destination_Port	Address to receive packets
Protocol	DNS or UDP for data transmission
Flow_Duration	Time between two packets
Total_Fwd_Packets	Total number of forward packets
Total_Backward_Packets	Sum of backward packets
Total_Len_Fwd_Packets	Total Length forward packets
Total_Len_Bwd_Packets	Total Length of backward packets
Fwd_Header_Length	Length of Forward header
Bwd_Header_Length	Length of backward header
Fwd_Packets_per_sec	Forward packets per second
Bwd_Packets_per_sec	Backward packet per second
SYN_Flag_Count	Synchronous flag cunt
ACK_Flag_Count	Acknowledged flag count
Average_Packet_Size	Average size of packet
Avg_Fwd_Segment_Size	Average forward segment
Avg_Bwd_Segment_Size	Average backward segment

5.2DDoS Attack that are Used in the Experiment

Every data in the dataset symbolizes a network traffic at a particular time. These traffics are labelled according to 2 types; malicious and benign. Five different class labels are used in the classification and theses are explained in the table below.

The class labels that are used in the, DNS, UDP, NetBIOS and Benign).

The attacks are predicted according to the 19 features in Table 4.1 above.

5.2 DDoS Attack Types Used in the Training

In this research, the dataset that was used contains the captured data of these four DDoS attack. These attacks have been briefly explained below.

5.2.1 SYN Flood Attack

It is a type of DDoS attack that produces a large volume of half-opened connection to exhaust the server with aim of denying service to legitimate users by shutting down the server or network[22]. In this type of DDoS attack, attacker sends a packet that does not have a source IP address. Three hand-shake is established after receiving a request from the attacker, the request is stored by the server in the memory stack and waits for the conformation that will never come. The compilation of the half way connection after a period of time floods the server hence, no more processing of any request [3].

5.2.2 DNS Attack

DNS protocol is in charge of converting domain names into IP addresses as well giving an infrastructure for keeping various resource records(RR). Usually a recursive DNS receives a request and then resolves the domain name. Sometimes, the DNS makes contact with a third party name server in order to return a request. The size of a query response packet is normally bigger than the query packet itself.[3]
With this protocol the attacker aims to deny access to service by making the server unable to distinguish between large UDP packets[23] from normal requests[24].

5.2.3 UDP Attack

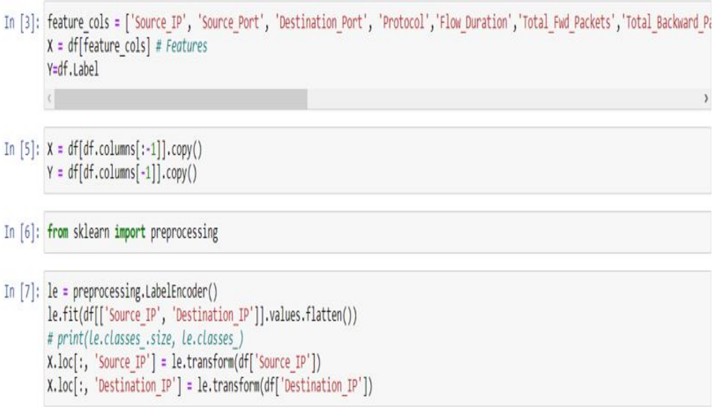
User Datagram Protocol (UDP) occurs when a datagram is sent to a random port on the victim's device to verify what is listening on that port. An ICMP message is sent as a reply to the spoofed IP address for closed ports. The targets eventually will be out of service out of the related enormous traffic[22].

5.2. NetBIOS

Network Basic Input/ Output System allows the communication of applications on different computers as well as facilitating the sharing of resources by opening sessions[24].

5.3 Data Pre-processing Phase

The .csv file was imported from CICDDoS2019 and the features (discussed above) extracted from the pool of dataset. Normal traffics are labelled differently from DDoS attack traffic. The data was cleaned to remove unwanted value. Normal network traffic denoted as zero while DDoS attack also denoted as one.

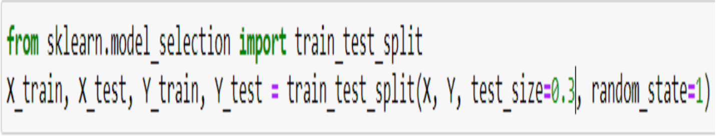


```
In [3]: feature_cols = ['Source_IP', 'Source_Port', 'Destination_Port', 'Protocol','Flow_Duration','Total_Fwd_Packets','Total_Backward_Pa
        X = df[feature_cols] # Features
        Y=df.Label

In [5]: X = df[df.columns[:-1]].copy()
        Y = df[df.columns[-1]].copy()

In [6]: from sklearn import preprocessing

In [7]: le = preprocessing.LabelEncoder()
        le.fit(df[['Source_IP', 'Destination_IP']].values.flatten())
        # print(le.classes_.size, le.classes_)
        X.loc[:, 'Source_IP'] = le.transform(df['Source_IP'])
        X.loc[:, 'Destination_IP'] = le.transform(df['Destination_IP'])
```

Figure 4: Data Preprocessing with Python

5.4 Splitting Datasets

For a model to function properly, there is a need for the dataset to be divided into 2 categories; the training and the testing data.The train_test_split from scikit-learn library was used to split the data into training (70%) and testing (30%). As shown in the snapshot below.



```
from sklearn.model_selection import train_test_split
X_train, X_test, Y_train, Y_test = train_test_split(X, Y, test_size=0.3, random_state=1)
```

Figure 5: Training and Splitting Codes in Python

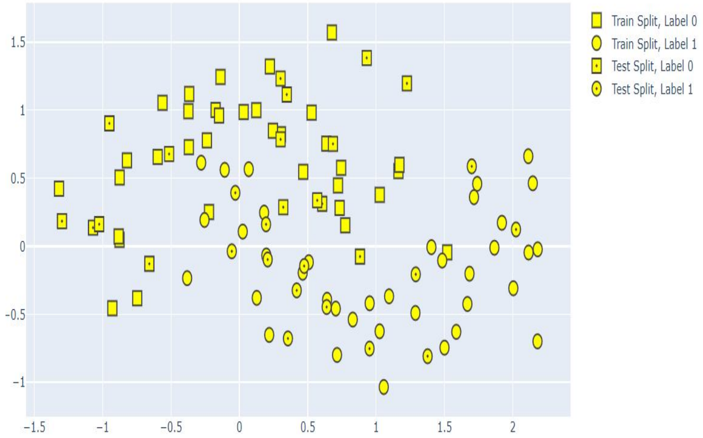


Figure 6: Train and Split, 0: Legitimate traffic and 1: DDoS attack

5.5 Evaluation Metrics

The evaluation metrics that are used in the calculation of the predictions are explained below.
True Positive (tp**):** it is the number of DDoS traffic are regarded as attack.
True Negative (tn**):** it is the set of DDoS attack traffic that are identified as the normal or legitimate traffic.
False Positive (fp**):** Legitimate network traffic that are misidentified to be DDoS attack.
False Negative (fn): the amount of DDoS attack traffic that are taken to be legitimate network traffic.
Precision: It is the ratio of positive labels on data indicated through specific classifier.

Precision (p) is given as, $p = \frac{tp}{tp+fp}$ (3)

Recall: It is efficiency of positive labels that is identified by a classifier.

$$r = \frac{tp}{tp+fn} \quad (4)$$

F-score is the weighted harmonic mean of precision and recall and is given by

$$f\text{ - score} = 2 \times \frac{precision \times recall}{precision + recall} = 2 \times \frac{p \times r}{p+r} \quad (5)$$

Table 2: Result of the experiment

Classifier	Decision Tree	KNN	Naïve Bayes
Precision	100%	96%	27%
f1-score	100%	97%	42%
Recall	100%	97%	100%

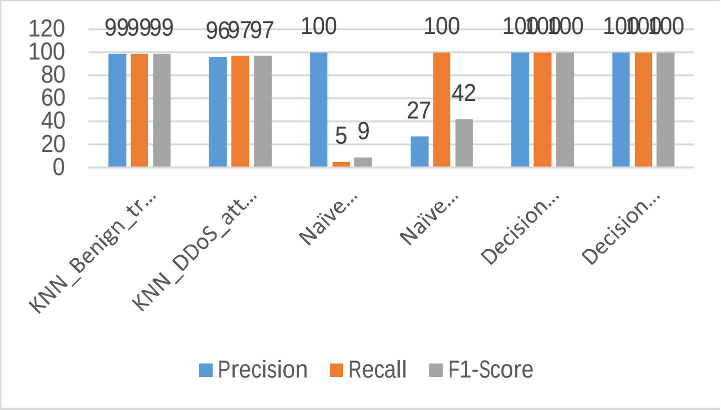


Figure 7: Benign and DDoS attack result representation

Accuracy: The final accuracy of a prediction that is successful can be found using the formula below:

$$accuracy = \frac{tp+tn}{fn+fp+tp+yn} \quad (6)$$

Table 3: Accuracy of the classifiers

Classifier	Accuracy
Decision Tree	100%
KNN	98%
Naïve Bayes	29%

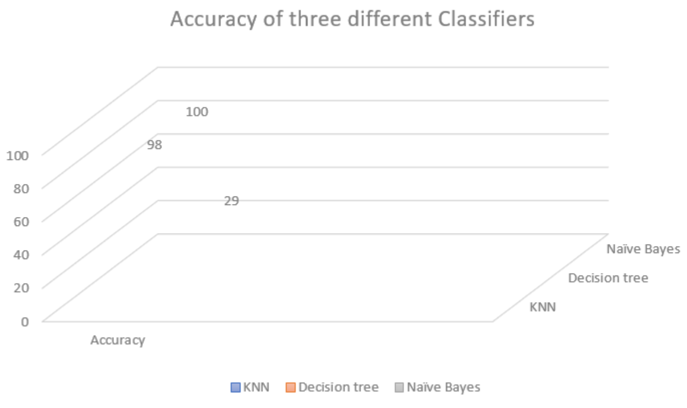


Figure 8: Comparing accuracy of classifiers

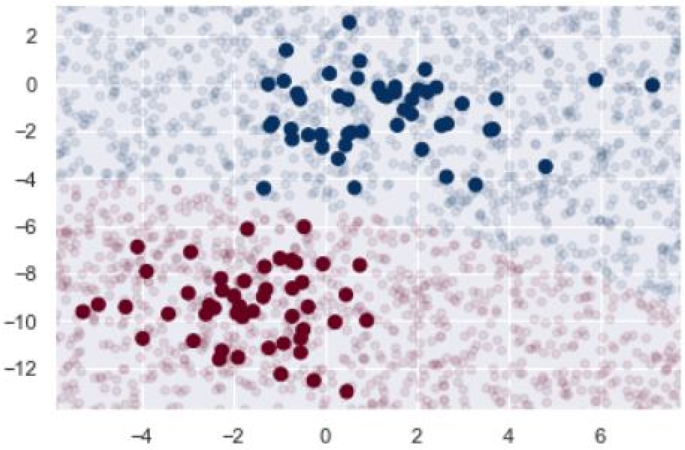


Figure 9: Prediction of Naïve Bayes

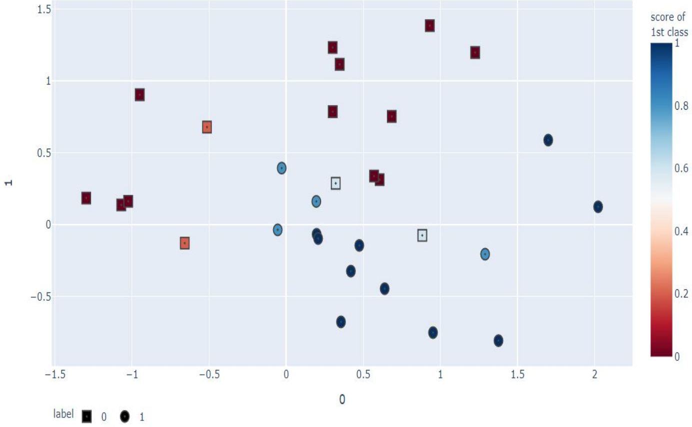


Figure 10: Prediction chart of KNN

6. CONCLUSION

The three algorithms that were used in the analysis performed differently. According to the result of the experiment obtained above, Naïve Bayes performed poorly in identifying DDoS attack traffic. It was able to make predictions with an accuracy of 29% though it was precise with a legitimate traffic but could hardly predict a DDoS attack therefore it does not fit for the work since the aim is to detect DDoS attack. This could be due to its stringent assumption of data technique or the training data was not large enough. Decision tree and KNN performed excellently compared to Naïve Bayes with a accuracy of 100% and also 98% respectively. Meaning they are able to differentiate between a normal network traffic from a DDoS attack. Decision tree scored 100% because the analysis used binary classification methods.

ACKNOWLEDGMENT

The research was supported by the Department of Electrical and Engineering of Istanbul Altinbas University.

REFERENCES

[1] R. M. Alguliyev, R. M. Aliguliyev, and F. J. Abdullayeva, “Deep Learning Method for Prediction of DDoS Attacks on Social Media,” *Adv. Data Sci. Adapt. Anal.*, vol. 11, no. 01n02, p. 1950002, 2019.

[2] K. Saeedi, “Machine Learning for Ddos Detection in Packet Core Network for IoT,” *Comput. Sci. Eng.*, 2019.

[3] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, “Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art,” *Int. J. Comput. Appl.*, vol. 49, no. 7, pp. 24–32, 2012.

[4] F. S. De Lima Filho, F. A. F. Silveira, A. De Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, “Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning,” *Secur. Commun. Networks*, vol. 2019, 2019.

[5] A. Aljuhani, T. Alharbi, and B. Taylor, “Mitigation of Application Layer DDoS Flood Attack Against Web Servers,” *J. Inf. Secur. Cybercrimes Res.*, vol. 2, no. 1, 2019.

[6] A. Carlin, M. Hammoudeh, and O. Aldabbas, “Defence for Distributed Denial of Service Attacks in Cloud Computing,” *Procedia Comput. Sci.*, vol. 73, no. Awict, pp. 490–497, 2015.

[7] C. Huang, J. Han, X. Zhang, and J. Liu, “Automatic identification of honeypot server using machine learning techniques,” *Secur. Commun. Networks*, vol. 2019, 2019.

[8] T. Ni, X. Gu, H. Wang, and Y. Li, “Real-time detection of application-layer DDoS attack using time series analysis,” *J. Control Sci. Eng.*, vol. 2013, 2013.

[9] A. Kumar, H. Dhawan, and B. Sowmiya, “DDoS Detection Using Machine Learning Ensemble Turkish Journal of Computer and Mathematics Education Research Article,” vol. 12, no. 12, pp. 1647–1655, 2021.

[10] M. Al-Qaraghuli, S. Ahmed, and M. Ilyas, “Encrypted Vehicular Communication Using Wireless Controller Area Network,” *Iraqi J. Electr. Electron. Eng.*, vol. sceeer, no. 3d, pp. 17–24, 2020.

[11] R. Wirth and J. Hipp, “CRISP-DM: towards a standard process model for data mining. Proceedings of the Fourth International Conference on the Practical Application of Knowledge Discovery and Data Mining, 29-39.” 2000.

[12] S. Kiourkoulis, “DDoS datasets,” 2020.

[13] J. Pei, Y. Chen, and W. Ji, “A DDoS Attack Detection Method Based on Machine Learning,” *J. Phys. Conf. Ser.*, vol. 1237, no. 3, 2019.

[14] M. M. A. Alkadhmi, O. N. Uçan, and M. Ilyas, “An Efficient and Reliable Routing Method for Hybrid Mobile Ad Hoc Networks Using Deep Reinforcement Learning,” *Appl. Bionics Biomech.*, vol. 2020, 2020.

[15] Y. S. Hussain, “Network Intrusion Detection for Distributed Denial-of-Service (DDoS) Attacks using Machine Learning Classification Techniques,” 2020.

[16] M. A. Prriyadarshini and S. Renuka Devi, “Detection of DDoS attacks using supervised learning technique,” *J. Phys. Conf. Ser.*, vol. 1716, no. 1, 2021.

[17] J. Rasheed, A. Jamil, A. Ali Hameed, M. Ilyas, A. Ozyavas, and N. Ajlouni, “Improving Stock Prediction Accuracy Using CNN and LSTM,” *2020 Int. Conf. Data Anal. Bus. Ind. W. Towar. a Sustain. Econ. ICDABI 2020*, no. January 2021, 2020.

[18] M. W. Berry, “Supervised and Unsupervised Learning for Data Science,” no. January, 2020.

[19] A. Alharan and A. Al-haboobi, “Popular Decision Tree Algorithms of Data Mining Techniques : A Review,” no. March, 2019.

[20] J. Chaki, S. T. Ganesh, S. K. Cidham, and S. A. Theertan, “Machine learning and artificial intelligence based Diabetes Mellitus detection and self-management : A systematic review,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2020.

[21] A. Fadlil, I. Riadi, and S. Aji, “Review of detection DDOS attack detection using naive bayes classifier for network forensics,” *Bull. Electr. Eng. Informatics*, vol. 6, no. 2, pp. 140–148, 2017.

[22] B. Bouyeddou, B. Kadri, F. Harrou, and Y. Sun, “DDOS-attacks detection using an efficient measurement-based statistical mechanism,” *Eng. Sci. Technol. an Int. J.*, vol. 23, no. 4, pp. 870–878, 2020.

[23] A. R. Alabbas, L. A. Hassnawi, M. Ilyas, H. Pervaiz, Q. H. Abbasi, and O. Bayat, “Performance enhancement of safety message communication via designing dynamic power control mechanisms in vehicular ad hoc networks,” *Comput. Intell.*, no. May 2021, 2020.

[24] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, “Detection and mitigation of DoS and DDoS attacks in iot-based stateful SDN: An experimental approach,” *Sensors (Switzerland)*, vol. 20, no. 3, pp. 1–18, 2020.