Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
VOLUME:8, ISSUE:2, AUGUST 2025, PAPER NUMBER:31

Detection of DDoS (distributed denial of service) attacks using machine learning

Sudhamsh Kumar Mellachervu[1], Brahmateja Yamanuri[2], Sai Kumar Kandukuri[3], Anil Babu Pandraka[4], Kundan Kumar[5], Amandeep Kaur. M.E.[6],

[1,2,3,4,5] Students, and [6] Faculty
Dept. of Computer Science Engineering,
Lovely Professional University, Punjab, India.
sudhamshkumarmellachervu@gmail.com

Abstract: *The availability and integrity of computer networks are seriously threatened by the rise in Distributed Denial of Service (DDoS) attacks. As these attacks get larger and more complex, effective detection systems are needed to lessen their damage. Researching the application of machine learning methods for DDoS attack detection in network traffic is the aim of this project. The project's goal is to provide a complete framework that uses supervised, unsupervised, and semi-supervised learning techniques to identify abnormal patterns that point to DDoS activity. The suggested system aims to differentiate malicious assaults from normal network traffic by examining various characteristics such as packet size, packet rate, protocol type, and flow duration. Real-world datasets will be used to evaluate detection performance, appropriate machine learning models will be selected and trained, and network traffic data will be collected and preprocessed. The project will involve selecting and training appropriate machine learning models, compiling and prepping network traffic data, and evaluating detection performance using real-world datasets. The team hopes to give companies the resources they need to develop cybersecurity defenses and stop DDoS attacks with this research.*

Keywords: *Machine Learning (ML), Distributed Denial-of-Service (DDoS) assaults, Real-time detection, Conventional defense strategies.*

1. INTRODUCTION:

These days, internet services are crucial for both people and corporate organizations. Intruders have intensified their attacks against network-based services in response to the rise in demand for these services, with the goal of stopping the provision of services to authorized users. DDoS assaults are those that disrupt or slow down network application services. Attackers can launch a denial-of-service (DDoS) assault by seizing control of millions of publicly accessible computer systems online. As a result, servers get busy processing the requests that the assaults create while refusing to respond to users who are authentic. These attacks are more often on well-known websites, such as banks, social networking sites, colleges, etc. Intrusion detection systems, Firewalls, and antivirus programs are a few examples of security solutions that computer networks should use to protect sensitive data and services from hackers. We discuss and evaluate the relevant research using machine learning to identify DDoS assaults in:

- A comprehensive analysis of prior research on DDoS detection employing several machine learning algorithms. This means studying many models, including Neural Networks and Decision Trees, and figuring out how feature selection impacts the models' accuracy, scalability, and speed in identifying DDoS attacks.
- Showcasing these ML models' effectiveness using various datasets. This will demonstrate how well machine learning techniques can identify DDoS assaults.

DDoS assaults seek to deplete a target's resources to obstruct authorized user access and could result in data breaches, outages, monetary losses, and harm to the target's reputation. It's difficult to identify bogus packets, especially when black hat hackers are skilled. For network security, an intelligent Intrusion Detection System (IDS) that uses machine learning techniques such as anomaly-based analysis is essential. Figure 1 illustrates how DDoS packet behavior may be identified by classifying DDoS assaults into Volume Based assaults (ICMP Flood, SYN Flood, UDP Flood) and Protocol Attacks

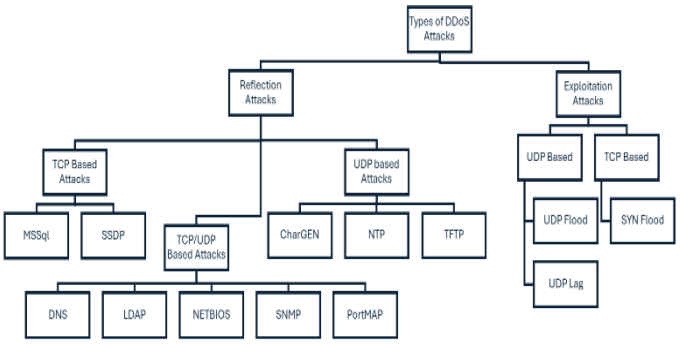

Figure 1 different types of DDoS attacks.

(Smurf DDoS, Ping of Death, TCP Connection Attack, HTTP Flood). Various attacks like Smurf assaults, HTTP floods, and SIDDoS (SQL injection DoS) actively target networks, disrupting services by inundating web servers with excessive duplicate traffic. However, many of the publicly accessible datasets are out of date, lacking the latest attack forms like Smurf assaults, HTTP floods, and SIDDoS. Our research leverages the DDoS SDN dataset, containing 104,346 rows of timestamped information, switch ID, source, and destination IP addresses, facilitating effective DDoS assault identification through machine learning techniques.

2. BACKGROUND AND RELATED WORK:

Finding the most pertinent data, or features, in datasets is an essential first step in many areas, particularly prior to utilizing deep learning or machine learning models. Feature re-duction is a procedure that frequently results in notable improvements to model efficiency in both the training and testing stages. As opposed to other issue areas, internet traffic anomaly detection presents a special challenge when it comes to differentiating between regular and aberrant traffic. Thus, while modelling network behaviors, it is crucial to ex-tract relevant characteristics from network data. This makes it possible to distinguish attack behaviors from normal ones with clarity.

Many research groups have investigated the problem of feature extraction in the context of network security. [19] used a dataset with five different classes and 27 attributes. To categorize assaults in the dataset, they used four distinct classifiers: J48, MLP, Random Forest, and Naive Bayes. The J48 classifier fared better than the other two when the data from the three classifiers were analyzed. J48 obtained 98.64% accuracy, While MLP, Random Forest, and Naive Bayes achieved accuracy of 98.63%, 98.10%, and 96.93%, in that order. [17] Employed the Random Forest algorithm to train their model, achieving an impressive classification accuracy of 99.76% for correctly classified instances.

Reference [8] Carried out research in which they tested ten different techniques on a range of 50 to 1000 movie re-views apiece. Support Vector Machine (SVM) consistently surpassed Naive Bayes (NB) and k-Nearest Neighbors (kNN) in terms of accuracy, regardless of the dataset size, according to their research's findings. SVM yielded an average accuracy of 73.903%, whilst NB and kNN produced accuracies of 64.23% and 65.528%, respectively.

Using a recently disclosed dataset, [10] proposed a hybrid method for detecting DDoS attacks early on. While other pertinent studies have been conducted on various datasets, they often lack a comprehensive examination of how DDoS attacks are reflected. Since the CICDDoS2019 dataset encompasses a a variety of assault methods, it is suitable for both training and assessing our techniques. First, the performance of each classifier was assessed in the absence of feature selection, and its accuracy was assessed using the whole feature set. The findings showed that XGBoost achieved an accuracy of 96.677%. After that, chi-square, Extra Tree, and ANOVA were used in several exhaustive rounds to pinpoint important traits and reduce the complexity of the data. After these iterations, it was found that the combined accuracy of XGBoost and ANOVA with 15 features was 98.374%. Indicating an 82.5% feature reduction rate. Our hybrid approach allows for the quick identification of DDoS assaults on IoT devices by concentrating on important features.

Reference [5] underscores the substantial impact of DDoS attacks on network stability, underscoring the potential for complete disruption if not promptly addressed. With these attacks growing in

Sophistication and eluding conventional defense mechanisms, in order to mitigate network security risks, Software Defined Networking (SDN) now requires the integration of machine learning algorithms. Decision Trees (DT), Naive Bayes (NB), and Logistic Regression (LR) are used to create explicit or implicit models from accessible data, enabling computers to learn on their own and find hidden patterns for more in-depth understanding. The intelligent mitigation of DDoS assaults is made possible by the further enhancement of network efficiency via the application of machine learning. Surprisingly, DT outperformed its peers in the research with the greatest accuracy of 99.90% among the assessed machine learning algorithms.

Reference [16] To start off, the researchers took a look at how many requests came in and how quickly they were processed (throughput) for each hour. They used the CAIDA dataset from 2007 to do this. What they found was that there is an inverse relationship between query interarrival time and throughput. A mathematical model should be used and not just a machine learning one for DDoS attack detection, as per their recommendation. For this purpose, logistic regression among other ML techniques like Naive Bayes were employed to evaluate their effectiveness; however logistic regression turned out to have better results than Naive Bayes did. Furthermore, it was shown that these models performed only slightly worse when compared with their machine learning counterparts. While boasting a perfect score on accuracy, the mathematics model achieved 99.75%.

Reference [15] Make the case for classifying denial-of-service (DDoS) attacks on networks using a deep learning (DL) model rather than a standard machine learning model. They propose that an effective option for this task is the Long Short-Term Memory (LSTM) model, which performs better in feature selection and extraction than shallow machine learning techniques. The researchers' work used the LSTM model to classify actions as benign or harmful using the CICDDoS2019 dataset. When used as a deep learning model, the LSTM model outperformed the KNN and ANN models, achieving a classification accuracy of nearly 98.6% for DDoS attacks. Moreover, employing LSTM with the CICDDoS2019 dataset to identify DDoS attacks not only demonstrates the technique's effectiveness but also provides valuable data for additional research on DDoS intrusion detection. Due to its excellent attack detection accuracy, the LSTM model integration into software-based networks seems to be a workable approach.

Reference [3] used a Deep Learning system based on a contractive autoencoder to effectively predict typical traffic data. To find anomalies in the dataset, a stochastic threshold approach based on reconstruction error is applied. The NSL-KDD, CIC-IDS2017, and CIC-DDoS2019 benchmark datasets are used to assess the approach's efficacy. Their results show that the proposed method may detect abnormalities up to a remarkable 97.58% of the time.

Reference [2] Provide an MLP classification model to identify DDoS attacks at the application level based on internal data. Their model has a 98.99% accuracy rate and a false positive rate of 2.11%. Subsequent studies aim to improve detection accuracy, distinguish DDoS attacks at the application level from transient events, and explore integration with real-time cyberattack detection systems.

Author(s)	Methodologies Used	Accuracy Achieved
Saini, P. S et al.,	J48, MLP, Random Forest, Native Bayes (NB)	98.64%, 98.63%, 98.10%, 96.93%
Pande, S et al.,	Random Forest	99.76%
Bhavitha, B et al.,	SVM, NB, kNN	73.903%, 64.23%, 65.528%
Gaur, V et al.,	XGBoost, ANOVA, chi-square, Extra Tree	98.374%
Altameni, A. J et al.,	Decision Trees (DT), NB, Logistic Regression(LR)	99.90%
Kumari, K et al.,	LR, NB	100%, 99.75%
Kumar, D et al.,	Long Short-Term Memory (LSTM)	98.6%
Aktar, S et al.,	Contractive autoencoder, Stochastic threshold strategy	97.58%
Ahmed, S et al.,	MLP	98.99%

Table 1 Comparison of Methodologies Used in Detection of DDoS Attack with Achieved Accuracy

3. DATASET USED:

The "DDoS SDN dataset" employed in this research study comprises 104,345 rows and 23 columns. This dataset, sourced from Kaggle, serves as a crucial resource for classifying network traffic into normal or malicious categories using classical Machine Learning algorithms.

A. Features

Time stamp (dt), switch identifier, source and destination addresses (src, dst), packet count (pktcount), byte count (bytecount), duration (dur), total duration (tot_dur), number of flows (flows), packet insertion count (packetins), packets per flow (pktperflow), bytes per flow (byteperflow), packet rate (pktrate), pair flow identifier (Pairflow), network protocol (Protocol), bytes received (rx_bytes), port number (port_no), bytes transmitted (tx_bytes), transmitted kilobytes per second (tx_kbps), received kilobytes per second (rx_kbps), and total kilobytes per second (tot_kbps) are among the features included in the dataset. Figure 2 Shows all vs. malicious requests from IP's.

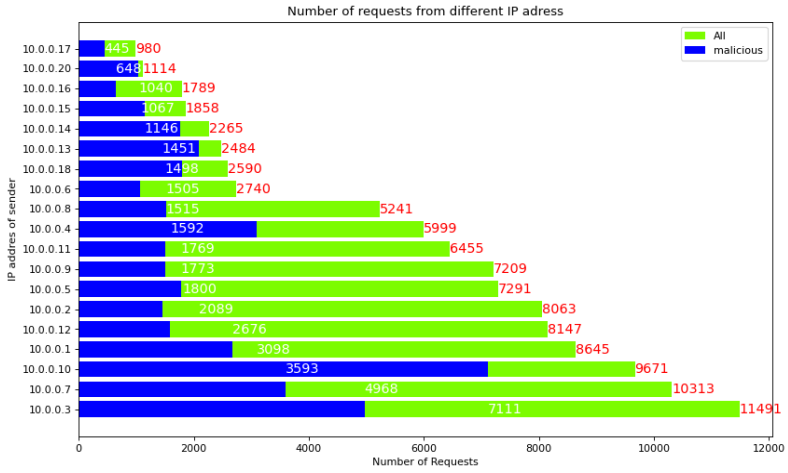

Figure 2 Shows requests from IPs, all vs. malicious.

B. Target Variable

The 'label' represents a single target variable in the dataset, indicating whether the traffic was malicious (1) or not (0). This Kaggle dataset could be utilized to gain insights into the behavior of network traffic, enabling Software Defined Networking (SDN) systems to accurately detect and mitigate DDoS attacks. Figure 3 illustrates the percentages of benign and malicious queries, derived from a dataset used for training algorithms.

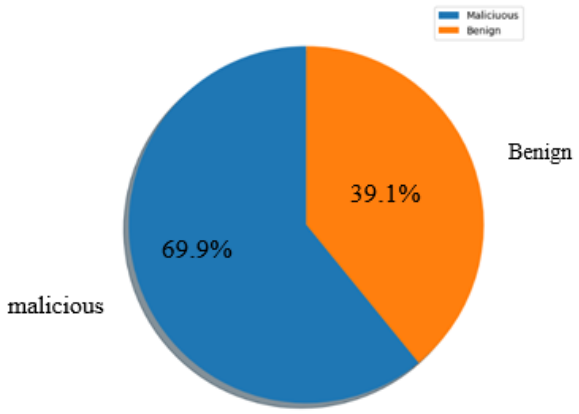

Figure 3 The percentage of Benign and Malicious Requests in dataset Model Training

4. METHODOLOGY:

Classifiers are essential to machine learning because they arrange data according to patterns. We used seven different classifiers: Support Vector Machine (SVM), Random Forest (RF), Decision Trees (DT), K Nearest Neighbors (KNN), Long Short-Term Memory (LSTM), Multilayer Perceptron (MLP), and

Logistic Regression (LR). These classifiers increase the accuracy of DDoS attack detection and mitigation in network traffic.

The procedures involved in DDoS detection and mitigation are shown in Figure 4, which includes data preprocessing, model validation, and deployment. To analyze network traffic patterns and spot possible DDoS attacks, each classifier is essential. We guarantee strong mitigation measures are in place and improve DDoS detection efficacy by utilizing a combination of these classifiers.

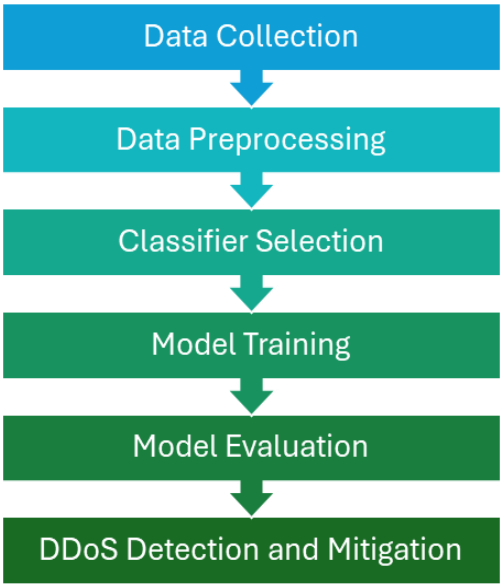

Figure 4 DDoS detection architecture.

A. Logistic Regression

For binary classification problems, the linear classification technique known as logistic regression is commonly used. By fitting a logistic curve to the data, it determines the likelihood of a binary result that depends on one or more predictor components. The logistic function is used in logistic regression to modify the outcome and guarantee that it is restricted to a number between 0 and 1. This makes it appropriate for jobs whose results are binary, such figuring out if an email is spam or not. Because it works well, is easy to implement, and works well with big datasets that have linear connections, LR is widely employed.

(1)

$$y = \frac{e^{(b_0 + b_1 X)}}{1 + e^{(b_0 + b_1 X)}}$$

Equation 1 Represents the Logistic Regression Here, (X) represents the input value, (y) represents the predicted output, (b0) stands for the bias or intercept term, and (b1) denotes the coefficient for the input (x).

B. K-Nearest Neighbors (KNN)

A non-parametric, supervised learning classifier, the k-nearest neighbours (KNN) algorithm use proximity to classify or predict how a single data point will be grouped. It is one of the most often used and straightforward regression and classification classifiers in machine learning today.

(2)

$$\operatorname{dist}(\mathbf{x}, \mathbf{z}) = \left(\sum_{r=1}^{d} |x_r - z_r|^p \right)^{1/p}.$$

Equation 2 Represents the K-Nearest Neighbors Here dist(X,Z) represents the Minkowski distance between points X and Z and P is a parameter that defines defines the order of the Minkowski distance calculation

C. Decision Trees (DT)

Decision Trees are interpretable and versatile classification techniques that recursively partition the feature space into regions. Every area has a link to a unique class label. The decision tree technique maximises the homogeneity of the resultant subsets by choosing the optimum feature at each node based on factors like information gain or Gini impurity. Because decision trees are simple to comprehend and depict, they are a valuable tool for preliminary data analysis. But particularly when dealing with intricate datasets, they may be vulnerable to overfitting.

$$Gain(S, A) = Entropy(S) - \sum_{v}^{A} \frac{|S_v|}{|S|}.Entropy(S_v) \quad (3)$$

Equation 3 Represents the Decision Trees Here (S) represents the set of instances, (A) is an attribute, Values (A) represents the set of potential values of attribute(A), (v) denotes a single value attribute(A) can have, (Sv) is the subset of(S) corresponding to v

D. Random Forest (RF)

Random Forest is a decision tree-based ensemble learning technique. During training, it builds many decision trees, from which it produces the mean prediction (regression) or the mode of the classes (classification). By adding randomization to the feature selection and bootstrapping processes, Random Forest reduces the overfitting propensity of decision trees. It often does well on a range of classification tasks and is resilient to noise and outliers.

E. *Long Short-Term Memory (LSTM)*

Long short-term memory is a property of recurrent neural network (RNN) architecture that is intended to capture long-term dependencies in sequential input. Natural language text and other sequential data, including time series, are particularly well suited for LSTM processing and classification. They are able to store knowledge for extended periods of time and selectively update or forget it based on the situation, all because of gating processes and particular memory cells. LSTMs have demonstrated state-of-the-art results in numerous sequential classification challenges.

F. Multilayer Perceptron (MLP)

An input layer, an output layer, plus one or more hidden layers make up a multilayer perceptron, a kind of feedforward neural network. MLPs can discover complex non-linear correlations between input features and target labels by using a method known as forward propagation and backpropagation. In domains including audio recognition, picture recognition, and natural language processing, they are frequently used to address categorization issues. Regularization algorithms and hyperparameters of MLPs may need to be modified appropriately to prevent overfitting.

G. Support Vector Machine (SVM):

Inspiration A potent supervised learning method for regression, classification, and outlier identification is the vector machine. To optimize the margin between classes, SVM searches the feature space for the optimum hyperplane to divide instances of various classes. When high-dimensional data cannot be divided linearly, support vector machines (SVMs) can manage it by using kernel functions to move the input into a higher-dimensional space. SVMs are widely recognized for their exceptional ability to broadly apply fresh data and their resilience against overfitting, particularly in domains with high dimensions. Trials and outcomes.

5. EXPERIMENTS AND RESULTS

We did our research on Google Colab using Python code, a platform that allows access to virtual machines with different configurations. Although it can work with many configurations, Colab does not specify any hardware requirement. During our study we employed several python packages such as TensorFlow, scikit-learn, pandas, NumPy, matplotlib and seaborn. In our classification tasks we used different machine learning classifiers including K-Nearest Neighbors, Random Forests, Decision Trees, Logistic Regression (LR), Long Short-Term Memory (LSTM), and Support Vector Machines.

Firstly, we trained a Logistic Regression model with around 72.2% accuracy on the training data. Then an accuracy of approximately 92.1% was achieved by KNN classifier with five neighbors.

Surprisingly the Random Forest classifier performed almost equally well as the Decision Tree classifier which had an accuracy of nearly 99.9%. After standardizing and reshaping input data, LSTM model having two LSTM layers which included Batch Normalization and Dropout layers for overfitting reduction gave about 99.3% test data accuracy.

Model	Accuracy
Logistic Regression	72.2%
KNN	92.1%
Random Forest	~99.9%
Decision Tree	~99.9%
LSTM	~99.3%
MLP	98.9%
SVM	~96.8%
Average accuracy	**94.186%**

Table 2 Outlines the accuracy achieved by each model/classifier on the test data.

Furthermore, 98.9% accuracy was attained on the test set by an MLP model with two hidden layers, each of 128 and 64 units, that used Dropout layers to prevent overfitting. Ultimately, using the test data, an SVM classifier using an RBF kernel had an accuracy of almost 96.8%. This comparison of various algorithms' accuracy is illustrated in Figure 5 and Table 2.

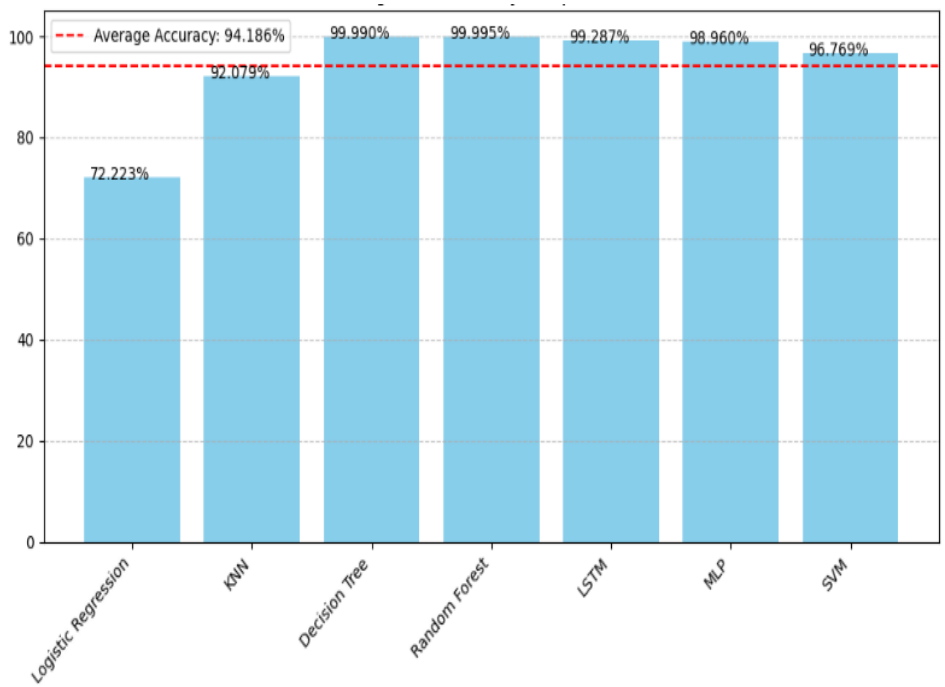

Figure 5 Comparison of Various Algorithms' Accuracy.

6. CONCLUSION

In this research, we examined different machine learning classifiers for DDoS attack detection in SDN systems using Python code on Google Colab. Among the classifiers examined were logistic regression, Random Forest, K-Nearest Neighbours (KNN), decision trees, Support Vector Machine (SVM), Long Short-Term Memory (LSTM), and Multilayer Perceptron (MLP) models. The remarkable accuracy of

almost 99.9% indicates how well the decision tree and random forest classifiers distinguished between benign and malicious network data. Similarly, the LSTM model showed promising accuracy, demonstrating its ability to identify complex patterns indicative of DDoS attacks. Traditional classifiers such as KNN and Logistic Regression performed well, but the MLP model showed competitive accuracy, highlighting its usefulness in classifying network data. Our research also showed how crucial feature selection, data pre-processing, and model optimisation are to increasing classification performance; standardisation and hyperparameter tweaking greatly increase classifier `SDN systems, future research may concentrate on investigating sophisticated feature engineering techniques, utilising ensemble learning approaches, and incorporating real-time monitoring capabilities.

7. REFERENCES

[1] Ahmad, I., & Kumar, R. (2018). DDoS attack detection using machine learning algorithms. In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.

[2] Ahmed, S., Khan, Z. A., Mohsin, S. M., Latif, S., Aslam, S., Mujlid, H., ... & Najam, Z. (2023). Effec-tive and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron. Future In-ternet, 15(2), 76.

[3] Aktar, S., & Nur, A. Y. (2023). Towards DDoS attack detection using deep learning approach. Com-puters & Security, 129, 103251.

[4] Al-Shareeda, M. A., Manickam, S., & Ali, M. (2023). DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison. Bulletin of Electrical Engineering and Infor-matics, 12(2), 930-939.

[5] Altamemi, A. J., Abdulhassan, A., & Obeis, N. T. (2022). DDoS attack detection in software defined networking controller using machine learning techniques. Bulletin of Electrical Engineering and Infor-matics, 11(5), 2836-2844.

[6] Arachchilage, N. A. G., & Love, S. (2017). Application of machine learning algorithms for DDoS attack detection. Journal of Cyber Security Technology, 1(1), 40-53.

[7] Banaee, H., & Moradi, M. H. (2016). DDos attack detection method based on PCA and artificial immune systems. In 2016 11th International Conference on Information Technology New Generations (pp. 421-426). IEEE.

[8] Bhavitha, B. K., Rodrigues, A. P., & Chiplunkar, N. N. (2017, March). Comparative study of machine learning techniques in sentimental analysis. In 2017 International conference on inventive communica-tion and computational technologies (ICICCT) (pp. 216-221). IEEE.

[9] Garcia-Teodoro, P., Diaz-Verdejo, J. E., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1-2), 18-28.

[10] Gaur, V., & Kumar, R. (2022). Analysis of machine learning classifiers for early detection of DDoS at-tacks on IoT devices. Arabian Journal for Science and Engineering, 47(2), 1353-1374.

[11] Gharaibeh, A., & Abdallah, A. E. (2017). A comprehensive review on DDoS attack, detection, prevention, and mitigation techniques. International Journal of Computer Applications, 175(1), 23-29.

[12] Jahanbakhsh, O., & Hatzinakos, D. (2014). Online DDoS attack detection and mitigation: A survey. IEEE Communications Surveys & Tutorials, 16(1), 229-247.

[13] Kang, Y., & Poovendran, R. (2017). Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. IEEE Control Systems, 37(1), 46-72.

[14] Kaur, A., & Gupta, D. (2022, September). A Hybrid Classification Model for Prediction of Academic Performance of Students: An EDM Application. In International Conference on Emergent Converging Technologies and Biomedical Systems (pp. 59-71). Singapore: Springer Nature Singapore.

[15] Kumar, D., Pateriya, R. K., Gupta, R. K., Dehalwar, V., & Sharma, A. (2023). DDoS detection using deep learning. Procedia Computer Science, 218, 2420-2429.

[16] Kumari, K., & Mrunalini, M. (2022). Detecting Denial of Service attacks using machine learning algo-rithms. Journal of Big Data, 9(1), 56.

[17] Pande, S., Khamparia, A., Gupta, D., & Thanh, D. N. (2021). DDOS detection using machine learning technique. In Recent Studies on Computational Intelligence: Doctoral Symposium on Computational In-telligence (DoSCI 2020) (pp. 59-68). Springer Singapore.

[18] Rajesh, M., & Varalakshmi, P. (2019). A comparative analysis of machine learning classifiers for DDoS attack detection. Journal of Ambient Intelligence and Humanized Computing, 10(8), 3177-3186.

[19] Saini, P. S., Behal, S., & Bhatia, S. (2020, March). Detection of DDoS attacks using machine learning algorithms. In 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 16-21). IEEE.

[20] Sarigiannidis, P., & Argyroudis, S. (2017). A survey of DDoS attack and DDoS defense mechanisms in the IoT. IEEE Internet of Things Journal, 4(6), 1803-1819.

[21] Sofi, I., Mahajan, A., & Mansotra, V. (2017). Machine learning techniques used for the detection and analysis of modern types of ddos attacks. Int. Res. J. Eng. Technol, 4(6), 1085-1092.

[22] Sonkavde, G., Dharrao, D. S., Bongale, A. M., Deokate, S. T., Doreswamy, D., & Bhat, S. K. (2023). Forecasting stock market prices using machine learning and deep learning models: A systematic review, performance analysis and discussion of implications. International Journal of Financial Studies, 11(3), 94.

[23] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defense Applications 2009 (pp. 53-58). IEEE.

[24] Vavilapalli, S., & Deopura, M. (2017). A survey on DDoS attack and defense mechanisms in cloud environment. International Journal of Computer Science and Information Security, 15(12), 45-50.

[25] Wang, Y., Zhang, L., Wang, C., Yang, Y., & Xie, Y. (2016). DDoS attack detection method based on improved K-means algorithm. In 2016 9th International Conference on Intelligent Computation Technology and Automation (pp. 249-253). IEEE.

[26] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials, 15(4), 2046-2069.

[27] Zargar, S. T., Nazari, M., & Tipper, D. (2015). A survey of DDoS attacks and defense mechanisms in cloud computing. Journal of Network and Computer Applications, 60, 19-45.

[28] Zhang, M., Cai, Z., Chen, B., & Wu, J. (2017). Research on DDoS attack detection algorithm based on extreme learning machine. In 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 221-224). IEEE.