Babylonian Journal of Machine Learning
Vol.2024, **pp**. 133–141
DOI: https://doi.org/10.58496/BJML/2024/013; ISSN: 3006–5429
https://mesopotamian.press/journals/index.php/BJML

Research Article

A Novel Method of Using Machine Learning Techniques to Protect Clouds Against Distributed Denial of Service (DDoS) Attacks.

Sangeeta Devi [1,*], Pranjal Maury [1], Upendra Nath Tripathi [1]

[1] *Department of Computer Science, DDUGU, Gorakhpur, Uttar Pradesh, India*

ARTICLE INFO

Article History
Received 20 May 2024
Revised 28 June 2024
Accepted 22 Jul 2024
Published 15 Aug 2024

Keywords

Distributed Denial of Service
DDoS
Cloud Computing
Security and Machine Learning
Learning Vector Quantization
Principal Component Analysis

ABSTRACT

The term "cloud computing" describes a method of providing hardware and software-based services over the internet. This allows users to access their data and apps from any device. The benefits of cloud computing include scalability, virtualization, access to user assets, lower infrastructure costs, and flexibility. However, one drawback is that it is susceptible to distributed denial of service attacks, which occur when multiple computer systems collaborate to target a particular resource, website, or server. Distributed denial of service (DDoS) attacks present a serious risk to computer networks and constitute a major cyber security challenge. This results in a denial of service for end users, as a result of false connection requests, a flood of messages, and twisted packets causing the system to slow down or even crash. Real people and services cannot access cloud computing. The issue of machine learning algorithms for identifying distributed denial of service (DDoS) attacks is explored in this article. In order to identify and defend cloud systems from harmful assaults, we developed a new machine learning approach in this work that is based on transfer learning. This study offers NSL-KDD datasets and two methodologies. There are two types of filters available: the Learning Vector Quantization (LVQ) Filters and the Principal Component Analysis (PCA) method, which reduces dimensionality. The features selected from each method were pooled using Decision Tree (DT), Naïve Bayes (NB), and Support Vector Machine (SVM) to detect distributed denial of service attacks (DDoS). We contrasted the results of several classifications. In terms of attack detection, LVQ-based DT performed better results as compared to other methods.

1. INTRODUCTION

In the field of network security, the most dangerous attack is known as a distributed denial of service attack (DDoS). DDoS attacks disrupt the regular operation of vital services for a range of web apps. In the face of DDoS attacks, systems continue to process fake requests (Bots) instead of serving actual users. These attacks are become more frequent and sophisticated by the day. It is now more challenging to identify these assaults and protect internet services from them.

Current intelligent learning approaches that have been demonstrated by academics to be effective in a variety of domains and capable of implementing network security include Machine learning (ML), Deep learning (DL), and Ensemble learning. Two examples of Internet-based platforms that reduce infrastructure are the Cloud [1], [2]. Distributed denial of service attacks are a tactic used by attackers to prevent services from being accessed by legitimate users [3]. In this type of attack, the attackers overwhelm the target server with a massive volume of requests, overloading its bandwidth and rendering the target server unavailable to normal users [4].

Brute-force distributed denial-of-service attacks are easily executed by infecting devices on a network using Botnet malware. Based on their objectives and traits, distributed denial of service attacks can be broadly divided into three categories. These assaults might, for example, target traffic, bandwidth, or apps. Via a deluge of TCP or UDP packets, traffic-focused assaults drastically lower the server's performance by overloading it. In an attempt to create congestion, bandwidth attackers transmit a deluge of private information. It is difficult to defend systems against application assaults because they are so frequent [5]. DDoS attack detection is made possible by the use of attack-machine-learning prediction.

The field of artificial intelligence (AI) is a rapidly developing field that holds great promise for resolving real-world problems in domains such as medical image processing [6][20], sentiment analysis [7], and cloud utilization forecast [8].

*Corresponding author. Email: sangeeta2316@gmail.com

Machine learning is used in intrusion detection in cloud computing [9], and researchers have proposed several methods for creating intrusion detection systems for the cloud: auto adaptive evolutionary extreme learning is used to detect DDoS attacks [10], while a Deep Belief Neural Network (DBNN) and a Deep Neural Network (DNN) are used to identify distributed denial of service attacks [11], [12]. It is amazing how accurately literary approaches can be performed to various dataset kinds. This article proposes a strategy for detecting distributed denial of service threats using feature selection and machine learning. Numerous measures are used to evaluate the proposed method, including the F measure, recall, accuracy, and precision. The proposed strategy outperforms the current methods in terms of accuracy and miss classification issues. This study suggests improving the Machine learning model and identifying the most crucial factors in order to reduce the number of miss categorization errors that occur when detecting DDoS attacks[21].

Machine learning techniques are necessary to increase the accuracy of anomaly detection. These algorithms are constantly learning from historical data and adjusting to new attack techniques. This is made possible by the ongoing procedure of learning from the data [8][23]. Furthermore, in the realm of online technology, the use of specialized DDoS detection tools and cloud-based reduction services has proliferated. These systems use the most recent information on potential threats, analyze traffic patterns globally, and have excellent capacity to minimize and conflicts distributed denial of service attacks at the network's most outer layer in order to prevent distributed denial of service attacks from achieving the infrastructure that is supposed to be targeted.

The most current studies indicate that IDS regularly uses machine learning techniques, especially deep learning. Experiments on traffic data acquired from many datasets or natural surroundings have shown the effectiveness of the proposed methodologies. The NSL-KDD is a popular research tool in these datasets since it offers a large sample space and supports multiple attack types. To summarize, the algorithm iteratively modifies the weights by measuring the Euclidean distance between the input vector and the weighted vector. It updates the weights in accordance with predetermined criteria, gradually lowers the learning rate, and ends when predetermined thresholds are satisfied. This method aids in progressively reducing error and enhancing model performance.

2. RELATED WORK

Scholar’s states that cloud-based HTTP DDoS attacks can now be detected. The suggested detection approach is powered by a combination of RF ensemble learning methodologies and information theoretic entropy (ITE) [13]. In a Cloud setting built on the Open Stack platform, the entropy of the network header characteristic of incoming traffic signals is determined with a time-based sliding window approach. It declares that when the pre-processing presented entropy is greater than the usual range, classification jobs are generated. Using an anomalous intrusion detection examine at the hypervisor layer, [14] increase the accomplishment of distributed denial of service (DDoS) attacks across virtual machines. The discovering mechanism was developed by the autonomously evolving neural network.

PSO (particle swarm optimization) is integrated with evolving neural networks to classify traffic data and identify distributed denial of service threats [14]. Previous studies concentrated on how well the algorithms performed using the KDD CUP 99 and NSL-KDD datasets. The bulk of the dataset's information relates to traffic produced by virtual machines (VMs), while host machine traffic may also be included in future studies. In reference to cloud computing, [15] proposed a method for DDoS attack detection. The unique detection approach makes use of voting ELM, or VELM.

For intrusion detection, we can use the ISCX or NSL-KDD datasets. The proposed system performs more accurately than Adaboost, ELM, random forest, black hole optimization ANN, and the previously stated artificial neural networks (ANNs). This paper [16] proposes an ELM-based model for identifying Distributed Denial of Service threats. A sample dataset for experiments using NSL-KDD. The proposed detection model indicates that a high detection rate and a short calculation time are achievable.

DDoS attack detection is part of the Third Party Auditor Notification Generator (TPA). The optimum method for detecting detection has been proposed to be the TPANGNDn architecture, which incorporates both detection information and third-party auditor notification. In order to defend public cloud environments from TCP flood assaults that cause distributed denial of service (DDoS), [17] developed a categorization methodology. Now, arriving packets can be identified using novel techniques for detecting distributed denial of service attacks, and decisions about protecting stored data can be made based on the classification results. Wireshark assisted in detecting and thwarting a flood attack. As part of the protective process, the recommended detection techniques examine a packet to determine whether or not it was created by an attacker.

Support vector machines (SVM) are the foundation of a detection method presented by [17]. Recall, specificity, accuracy, and f measure are areas where the Support Vector Machine (SVM) performs better than the other two techniques. Random

Forest is ranked second. Tor Hammer can be used to compromise cloud-stored datasets [16]. developed a distributed denial of service attack detection system that makes use of cloud computing and machine learning. This specific detection method uses information about virtual machines and hypervisors to stop network packages from leaving the system [17].

3. MATERIALS AND METHODS

In order to detect DDoS assaults, we analyze the NSL-KDD dataset [18] in this section. The process of the intrusion detection model is shown in Figure 1. Two different feature selection methods are used to minimize features. Numerous classification algorithms make use of the confined feature set. Utilizing the confusion matrix as a guide, compute validation metrics. Real distributed testing network setup is a costly endeavor. Simulation is useful for network researchers because it makes it possible to evaluate problems under various protocols, traffic patterns, and topologies at a reasonable cost.

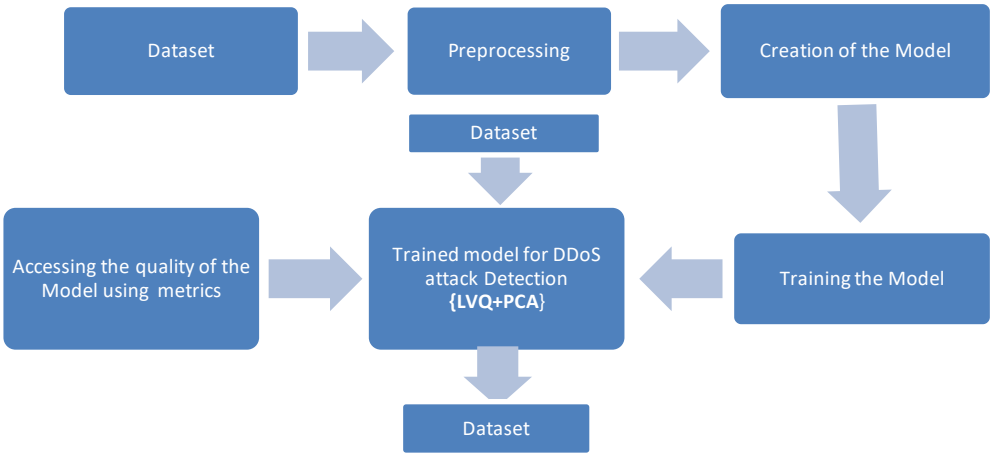

Fig .1. Proposed Model for Attack Detection in Cloud Environment

Either the direct or the public sets of data are available for us to access. Direct data sets are produced using open source tools, whereas public datasets are user-generated through a range of web platforms. We use the publicly available dataset NSL-KDD [19] for this investigation. The original data set has 42 attributes, 2,26,283 occurrences, and four different assault classifications. This study solely focuses on the 15,452 distributed denial of service attack cases. 30% percent of the data set is the testing set, and 70% is the training set.

3.1 Features Selection

The key elements that affect the predicted variable are found using the feature selection approach. Whenever feature selection data is added or withdrawn, the prediction data won't change. Feature selection techniques are used in the proposed strategy. Filtering and dimension- -ality reduction are both applicable.

A. The Filter Technique

Supervised learning LVQ algorithm is one algorithm used by artificial neural networks. The LVQ's design calls for n input and m output units. Each weighted layer is connected to the others. As per [20], LVQ utilizes a k-NN technique. x, T, wj, Cj, and j are the LVQ parameters that are employed in the training process. x(x1,x2,...,xn) is a training vector. The weight vector for the jth output unit is wj, and the class for the training vector x is T. The class linked to the jth output unit is Cj.

Algorithm:

Step 1: Initialize, determine the initial weight, the maximum epoch (the total number of training cycles to be carried out), and the learning rate (alpha).

Step 2: Perform steps 2 through 8 if the repetition criteria is met.

Step 3: Assign epoch = 0 as the starting condition.

Step 4: Set epoch = epoch + 1, If the condition (epoch < MaxEpoch).

Step 5: Calculate the minimum distance ‖ xi – wj‖ using Euclidean distance.

Step 6: Update weight wj with the conditions:

If T = Ci, then wi (new) = wi (old) + α (x – wi `(old))

If T ≠ Cj, then wj (new) = wj (old) – α (x – wj (old))

Step 7: Reduce learning rate (α) = α – (0, 1 * α)

Step 8: Stop condition test : the condition where the learning rate (α) and the error reach the

specified target value.

B. The method of dimensionality reduction

Reducing dimensionality is accomplished by progressively eliminating unnecessary attributes. Analyzing power metrics decreases dimensions. A big set of data variables is reduced to a reasonable quantity by PCA [20]. Using data set patterns makes it simple to see the variables in the data. With the use of an orthogonal statistical variable distribution, principal component analysis (PCA) modifies the data variables. Principal component analysis (PCA) makes use of mathematical concepts such as eigenvalues, eigen vectors, and standardization.

3.2 Methods of Classification

The classification techniques are applied to the NSL-KDD data analysis. Data prediction can benefit from the use of classification techniques. To transfer the values of the predictors to the values of the targets, classification algorithms employ a model [20]. Depending on the relationship, a model may represent data for unknown classes. The categorization techniques employed in this work are Naïve Bayes, Support Vector Machine, and Decision Tree categories. To predict data sets, these classification techniques distinguish between records that are safe and records that are risky.

A. Naïve Bayes (NB)

A machine learning approach based on the Bayes theorem The foundation of Naive Bayes is probability theory. It can be used in a variety of classification jobs. It is necessary to compute the feature probabilities and select the largest one. The assumptions made by naive Bayes classifiers pertain to unrelated features. It is estimated that there may be malicious records in the dataset.

B. SVM, or Support Vector Machine

A decision plane is required to partition sizable datasets including discrete class members. It is possible to create decision planes with defined bounds by using support vector machines (SVM). After obtaining the data, it draws a line that divides the classes, assuming that's possible. The pairs of data points from each class that are closest to the line are what we refer to as "support vectors". The separation between support vectors and hyperplanes is known as the margin. The hyperplane with the biggest margin is the optimum one [20]. With the given data set, the SVM algorithm produced LVQ and PCA values of 0.9345 and 0.9786, respectively.

C. Decision Tree (DT)

DTs, or Decision trees, are helpful tools for categorization and prediction. The decision tree algorithm generates possible future outcomes based on the current situation. When creating this algorithm, we took into account every scenario that could result from our choices. DT is a huge collection of subsets and the nodes that depicts every decision and its outcome [20]. The DT approach more accurately captures the data since it makes use of a tree-like structure to account for all possible final conclusions. This method's application mostly depends on recursive decision-making. It keeps accuracy while working with multi-dimensional data. The supplied data set produced LVQ accuracy of 0.9878 and PCA accuracy of 0.9882 when the DT approach was applied.

4. RESULTS

4.1 NSL-KDD Dataset

The NSL-KDD dataset is recommended for use in resolving a number of KDD'99 issues. For increased accuracy, this dataset's sample size has been decreased, and the traffic has been analyzed. In total, there are forty-one distinct qualities. The NSL-KDD is divided into five types based on the activities or target of the cyber attacker. The five types are such as Normal, DoS, U2R, R2L, and Probe.

A. DoS (Denial of Service) Attacks:

The NSL-KDD dataset has the highest frequency of this assault. It can be described as cyber-attacks that send more connection request to a server than it can handle, preventing the server from responding or shutting down to protect itself. This prevents regular users from obtaining service. For example, DoS attacks are being used to stop students from obtaining online tests in higher education institutions during the COVID-19 epidemic, where online education is becoming more popular. Even though these test systems use distributed servers, these attacks eventually damage the network architecture and render the system utterly unusable.

The results have been acquired. Using the NSL-KDD data, an R-based predictions of the malicious record is generated. A set of categorization features can be obtained by feature selection techniques. Tables 2 and 3 display the validation metrics that were attained by using the f-measure, recall, specificity, accuracy, and precision. These measurements are shown in the tables.

4.2 Performance Metrics

This section explains metrics that are commonly used in IDS performance assessment. Initially, the confusion matrix's structure is provided. After that, we provide a quick explanation of the performance metrics' computation. The standard confusion matrix representation is shown in Table 1.

TABLE I. THE STRUCTURE OF CONFUSION MATRIX

	Intrusions	Normal	Total
Intrusion	TP	FN	TP+FN
Normal	FP	TN	FP+TN
Total	TP+FP	FN+TN	N

The variables TP, TN, FP, and FN are included in the confusion matrix, as explained below. We can calculate the equations that range from 1 to 5 utilized for performance evaluations once these variables have been identified.
True Positive (TP): positively classified, positive sample quantity.
True-Negative (TN): negatively classified, negative sample quantity.
False-Negative (FN): negatively classified, Positive sample quantity.
False-positive (FP): positively classified, negative sample quantity.

We can see how well the model for prediction is performing by using assessment measures. This study assessed machine learning's ability to identify distributed denial of service (DDoS) threats using precision, accuracy, recall, and F score.

A. Accuracy

The most important performance metric is accuracy, which is the proportion of data that could have been correctly predicted. For accuracy to be a useful criterion for evaluation, datasets must be homogeneous and contain an equal proportion of false positives and false negatives. We can observe from Equation (1) that the classifier performs well in forecasting upcoming data items.

$$Accuracy = \frac{TP}{TP+TN+FP+FN} \quad (1)$$

B. Precision

The ratio of expected positive observations to the total number of predicted an observation is known as accuracy. A crucial element of high accuracy is lowering false-positives. Precision is the accuracy with which classifiers forecast positive classifications. The calculation of accuracy is done using equation (2).

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

C. Recall

The percentage of positive observations that have been accurately anticipated in relation to all of the observations in a class is known as recall. Equation (3) states that the precision of the classifier determines how accurately it predicts the positive class.

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

D. F1 Score

The F1 Score is composed of normalized recall and accuracy. As a result, this score includes both false positives as well as false negatives. In situations where the distribution of classes is unclear, F1score performs better than accuracy, despite its seeming simplicity. Equation (4) illustrates that the F1 value is the harmonic mean of the recall and accuracy scores.

$$FMeasure = 2X \frac{PR}{P+R} \quad (4)$$

4.3 Classification on features using Learning Vector Quantization method

The results of the tests run on the dataset are displayed in Table 1 and Image 2. Following the application of LVQ, DT, SVM, and NB are employed for classification. The DT classifier is more effective at identifying fraudulent data than NB and SVM.

TABLE II. RESULT OF LEARNING VECTOR QUARTIZATION METHOD

Parameter	Naïve Bayes	SVM	Decision Tree
Accuracy	0.9397	0.9345	0.9878
Precision	0.9287	0.9469	0.9987
Recall	0.9823	0.9876	0.9923
Specificity	0.8634	0.8423	0.9767
F-Measure	0.9478	0.9623	0.9945

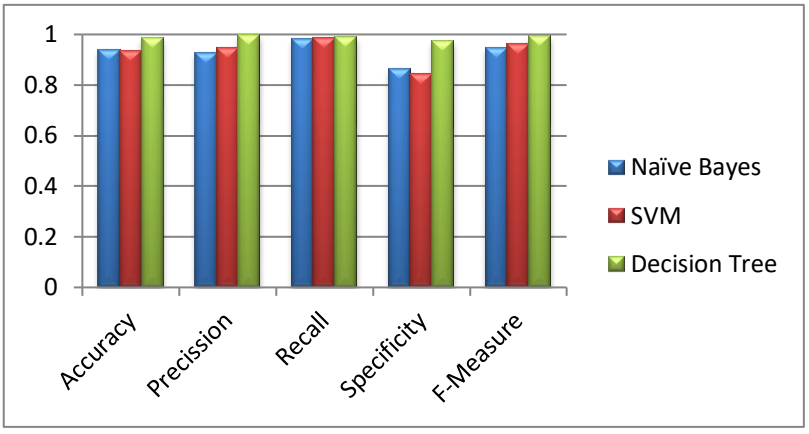

Fig .2. Learning Vector Quantization Method

4.4 Classification on features using Principal Component Analysis Method

The results of Principal Component Analysis (PCA) dimensionality reduction are shown in Image 3. Table 2 illustrates how the DT strategy performs better than the NB and SVM approaches with a detection accuracy of 0.9882. 26 qualities are taken into account in this feature selection method out of 42.

TABLE III. RESULTS OF PRINCIPAL COMPONENT ANALYSIS METHOD

Parameter	Naïve Bayes	SVM	Decision Tree
Accuracy	0.8397	0.9786	0.9882
Precission	0.9656	0.9956	0.9984
Recall	0.8662	0.9956	0.9884
Specificity	0.9458	0.9878	0.9987
F-Measure	0.9478	0.9897	0.9945

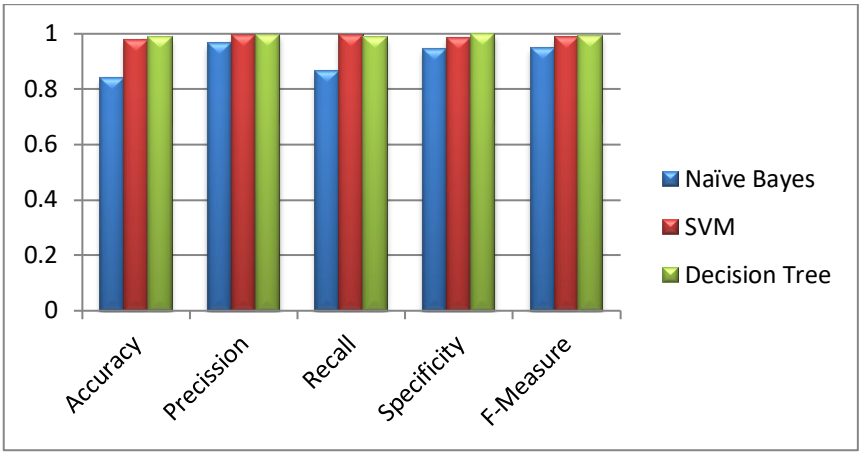

Fig .3. Principal Component Analysis Method

5. CONCLUSION

Small, medium, and large-scale enterprises are beginning to adopt cloud computing due to its easily accessible architecture, network-focused methodology, and adaptable nature. This is true given the increasing popularity of cloud computing. This notwithstanding, the advent of cloud computing has led to the creation of novel ideas like resource sharing, multi-tenancy, outsourcing, and reliance on outside data and services. There are several security issues with these principles. These days, Distributed Denial of Service (DDoS) attacks are among the most popular techniques employed in cyber-attacks. The goal of this project is to develop a machine learning approach that will increase cloud computing security's effectiveness.

Our work focused on analyzing the "classifier models" which are used as early warning systems for distributed denial of service (DDoS) attacks. It has become possible to use the models generated to create software that monitors, detects, and steers clear of hazards with minimal assistance from people. DT, SVM, and NB classifiers are used in this study to build both classification and forecasting models for distributed denial of service (DDoS) assaults. Prior to working with the models, every record in the set of data underwent optimization and normalization. Optimization came after normalization. It was determined that in terms of accuracy metrics, the SVM, MLP, and NB classifiers performed better. The predictions led to the conclusion that was drawn.

One common distributed difficulty is detecting denial-of-service (DDoS) assaults. Since this threat interferes with cloud services, detection is essential. Such an attack may be detectable by machine learning models. Identifying distributed denial of service attacks with more accuracy is the motivation behind this research. The data intrusion detection system included within the NSL-KDD benchmark data set is one instance of an actual system in use. Only data related to distributed denial of service attacks are taken into account in this study. A combination of Machine Learning algorithms (DT, SVM, and NB) and selection feature techniques (PCA and LVQ) was used to classify the attacks. Based on the algorithms' performance, different types of distributed denial of service attacks have been identified. The PCA scored 26 and the LVQ scored 23 out of 42 qualities. The findings demonstrate that the DT model's LVQ-based feature selection mechanism detects attacks more accurately than alternative methods. In comparison to other models, the model performs better in terms of Accuracy, Precision, Recall, Specificity and F-Measure.

Traffic congestion offers a myriad of troubles that impact both people and society at huge. One of the most evident problems is the tremendous boom in travel instances throughout top hours, leading to delays and frustration among commuters. This now not most effective influences individuals seeking to reach their locations however also disrupts deliver chains and logistics, ultimately impacting companies and the economic system. Moreover, congestion contributes to environmental degradation via multiplied vehicle emissions. The slow-transferring or idling visitors feature of congested regions ends in higher degrees of air pollutants, posing fitness dangers to residents and contributing to weather change.

The dependency on non-public vehicles also ends in better fuel consumption and carbon emissions, exacerbating environmental concerns. In addition to environmental and monetary influences, site visitors' congestion has social effects. It can contribute to heightened pressure stages among commuters, affecting basic well-being and great of life. Congestion

Conflicts Of Interest

None.

Funding

None.

Acknowledgment

The author extends gratitude to the institution for fostering a collaborative atmosphere that enhanced the quality of this research.

References

[1] A. Alahmadi et al., "DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions," Electronics, vol. 12, no. 14, p. 3103, 2023.

[2] J. Bhayo et al., "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," Engineering Applications of Artificial Intelligence, vol. 123, p. 106432, 2023.

[3] W. Alhalabi et al., "Machine learning-based distributed denial of services (DDoS) attack detection in intelligent information systems," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 19, no. 1, pp. 1-17, 2023.

[4] A. K. Jakkani et al., "Design of a Novel Deep Learning Methodology for IOT Botnet based Attack Detection," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 9, pp. 4922–4927, 2023, doi: 10.17762/ijritcc.v11i9.10109.

[5] S. Potluri et al., "Detection and prevention mechanisms for ddos attack in cloud computing environment," in Proc. 11th Int. Conf. on Computing, Communication and Networking Technologies (ICCCNT)*, 2020, pp. 1-6.

[6] P. K. Srivastava and A. K. Jakkani, "Non-linear Modified Energy Detector (NMED) for Random Signals in Gaussian Noise of Cognitive Radio," in Advances in Electronics, Communication and Computing. ETAEERE 2020, P. K. Mallick, A. K. Bhoi, G. S. Chae, and K. Kalita, Eds., Singapore: Springer, 2021, vol. 709, pp. 823-834, doi: 10.1007/978-981-15-8752-8_65.

[7] K. N. Rajapraveen and R. Pasumarty, "A Machine Learning Approach for DDoS Prevention System in Cloud Computing Environment," in Proc. 2021 IEEE Int. Conf. on Computation System and Information Technology for Sustainable Solutions (CSITSS), 2021, pp. 1-6.

[8] P. K. Srivastava, "Prof. Anil Kumar Jakkani, "Android Controlled Smart Notice Board using IOT"," International Journal of Pure and Applied Mathematics, vol. 120, no. 6, pp. 1-10, 2021.

[9] M. Arunkumar and K. A. Kumar, "Malicious attack detection approach in cloud computing using machine learning techniques," Soft Computing, vol. 26, no. 23, pp. 13097-13107, 2022.

[10] P. K. Srivastava and A. K. Jakkani, "FPGA Implementation of Pipelined 8×8 2-D DCT and IDCT Structure for H.264 Protocol," in Proc. 3rd Int. Conf. for Convergence in Technology (I2CT), Pune, India, 2018, pp. 1-6, doi: 10.1109/I2CT.2018.8529352.

[11] S. Sambangi and L. Gondi, "A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression," Concurrency and Computation: Practice and Experience*, vol. 32, no. 16, p. e5402, 2020.

[12] A. Mishra et al., "Classification based machine learning for detection of ddos attack in cloud computing," in Proc. 2021 IEEE Int. Conf. on Consumer Electronics (ICCE), 2021, pp. 1-6.

[13] S. Peneti and E. Hemalatha, "DDOS attack identification using machine learning techniques," in Proc. 2021 Int. Conf. on Computer Communication and Informatics (ICCCI), 2021, pp. 1-6.

[14] A. M. Makkawi and A. Yousif, "Machine Learning for Cloud DDoS Attack Detection: A Systematic Review," in Proc. 2020 Int. Conf. on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), 2021, pp. 1-6.
[15] A. R. Wani, Q. P. Rana, and N. Pandey, "Machine learning solutions for analysis and detection of DDoS attacks in cloud computing environment," Int. J. Eng. Adv. Technol., vol. 9, no. 3, pp. 2205-2209, 2020.
[16] P. S. Samom and A. Taggu, "Distributed denial of service (DDoS) attacks detection: A machine learning approach," in Applied Soft Computing and Communication Networks: Proceedings of ACN 2020, Springer Singapore, 2021, pp. 1-6.
[17] M. Ouhssini and K. Afdel, "Machine Learning Methods for DDoS Attacks Detection in the Cloud Environment," in Proc. Int. Conf. on Advanced Intelligent Systems for Sustainable Development*, Cham: Springer International Publishing, 2020, pp. 1-6.
[18] R. Santos et al., "Machine learning algorithms to detect DDoS attacks in SDN," Concurrency and Computation: Practice and Experience, vol. 32, no. 16, p. e5402, 2020.
[19] M. Revathi, V. V. Ramalingam, and B. Amutha, "A machine learning based detection and mitigation of the DDOS attack by using SDN controller framework," Wireless Personal Communications, vol. 121, no. 1, pp. 1-25, 2021.
[20] T.-K. Luong, T.-D. Tran, and G.-T. Le, "Ddos attack detection and defense in sdn based on machine learning," in Proc. 7th NAFOSTED Conf. on Information and Computer Science (NICS), 2020, pp. 1-6.
[21] S. salman Qasim and S. M. NSAIF , Trans., “Advancements in Time Series-Based Detection Systems for Distributed Denial-of-Service (DDoS) Attacks: A Comprehensive Review”, BJN, vol. 2024, pp. 9–17, Jan. 2024, doi: 10.58496/BJN/2024/002.
[22] A. Alsajri, A. Steiti, and H. A. Salman , Trans., “Enhancing IoT Security to Leveraging ML for DDoS Attack Prevention in Distributed Network Routing”, BJIoT, vol. 2023, pp. 74–84, Oct. 2023, doi: 10.58496/BJIoT/2023/010.
[23] A. S. . Bin Shibghatullah, “Mitigating Developed Persistent Threats (APTs) through Machine Learning-Based Intrusion Detection Systems: A Comprehensive Analysis”, SHIFRA, vol. 2023, pp. 17–25, Mar. 2023, doi: 10.70470/SHIFRA/2023/003.