International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Machine Learning-Based Detection of Distributed Denial-Of-Service Attacks in SDN

Dr. D.J. Ashpin Pabi [1], R. Mounesh [2], P. Uday Kiran[3], B. Sai Sreedhar Reddy[4]
Assistant Professor[1], UG Students [2,3,4]
Computer Science and Engineering, Madanapalle Institute of Technology and Science, Madanapalle , Andhra Pradesh, India

ARTICLEINFO

Article History:

Accepted: 01 May 2023
Published: 11 May 2023

Publication Issue
Volume 9, Issue 3
May-June-2023

Page Number
135-142

ABSTRACT

(SDN) is a technique for digitally building and designing hardware components. Dynamic changes can be made to the network connection settings. Because the link in the traditional network is fixed, dynamic change is not possible. Although SDN is a fantastic strategy, DDoS attacks are still possible. The DDoS attack is a danger to the internet. DDoS attacks can be mitigated by using the machine learning algorithm. DDoS attacks occur when multiple systems collaborate to target a single host at the same time. Devices in the infrastructure layer are managed by software from the control layer, which sits between the application and infrastructure layers in SDN. In this paper, we use a machine learning method called Decision Tree to detect malicious communications. Our results show that the Decision Tree determines whether the assault is safe or not.

Keywords : SDN, attacks, DDoS, Decision Tree

I. INTRODUCTION

A distributed denial-of-service (DDoS) attack is a malicious attempt to obstruct regular traffic to a server, service, or network by saturating the target or its surrounding infrastructure with data an excessive amount of Internet traffic[1]. By using several hacked computer systems DDoS attacks are made more effective by using attack traffic sources. Computers and her networked devices resources, like as IoT devices, can be exploited machines. When viewed from a distance, a DDoS assault resembles an unexpected Congestion on the road that prevents regular traffic from reaching its destination. Internet-connected device networks are used to carry out DDoS assaults. These networks are made up of computers and other gadgets that have been infected with malware, allowing an attacker to remotely manipulate them (such as IoT gadgets). These particular gadgets are known as bots (or zombies), and a botnet is a collection of bots[2]. Once a botnet has been created, the attacker may control an attack by giving each bot remote commands. While the victim's server or network is being targeted by the botnet, each bot in the botnet sends queries to the IP address of that server or network. This may cause the server or network to become overloaded. result in a denial-of-service attack

on regular traffic. It might be challenging to distinguish attack traffic from regular traffic because each bot is an actual Internet device.

An abrupt slowdown or unavailability of The most visible sign of a DDoS attack is a website or service. However, due to a variety of factors, including a genuine increase in traffic, performance may suffer. concerns, more research is often needed. You may identify some of these tell-tale symptoms of a DDoS assault Using traffic analytics tools, unusual spikes in traffic to a single page or endpoint, suspicious amounts of traffic from a single IP address or IP range, or a flood of users with the same device, geographic area, or web browser version[3]. Unusual traffic patterns, such as spikes at unusual times of day or patterns that seem abnormal (such as a spike every ten minutes), Depending on the type of assault, there are other, more precise indications of DDoS attacks.

By separating the control from data plane devices, the developing paradigm of "software defined networking" overcomes the limits of traditional network design. The data plane, control plane, and application plane are the three planes that make up SDN. In accordance with the controller's decision, the data plane carries the network traffic. The routing tables are computed by the control plane to determine the traffic flow. Apps like load balancers, firewalls, The application plane manages applications such as quality of service (QoS)[4]. By dividing the network control and forward functions, the SDN design enhances network performance. Multiple routers throughout the network will be under the control of control programmes operating in a conceptually centralised controller.

Applications only have access to the complete network's information through the SDN. Integration of many apps aids in load balancing and intrusion detection during periods of heavy traffic. The application instructs the controller to modify the data plane in order to fix any anomalies that are found.[5]On routers spread throughout the network, the control and data planes both function, and the devices have open interfaces that can be managed by software.

Multiple devices can be configured simultaneously in an SDN framework. Device configuration for networks is carried out at the application layer. The control layer (control plane), which is composed of the same controller, is the brain of the SDN architecture. API is used to communicate between these two levels. A common protocol is used by The infrastructure layer (data plane) connects the controller to the network devices. A good security system is necessary to analyse and identify suspicious communications since the controller handles a large quantity of traffic. We provide a machine learning-based method for detecting malicious SDN activity by analysing the traffic properties.

II. RELATED WORKS

DDoS Attack Detection Method in Software-Defined Networks Based on Improved KNN with DDoS Attack Degree:[1] Since decades, the Distributed Denial of Service (DDoS) assault has significantly decreased network availability, and there is still no reliable solution against it. But the newly developed Software Defined Networking (SDN) offers a fresh perspective on how to rethink the security against DDoS attacks. In this work, we provide two approaches for spotting DDoS attacks in SDN. One approach uses the DDoS attack's intensity to determine its level. The alternative technique finds the DDoS assault using the enhanced K-Nearest Neighbors (KNN) algorithm based on Machine Learning (ML). Theoretical analytical findings and actual findings on datasets demonstrate that our suggested approaches are superior to previous ways at detecting DDoS attacks.

DDoS attacks in SDN and cloud computing environments[2]: SDNs (software defined networks) and cloud computing have recently gained a lot of

traction in academia and business. However, security concerns have made these revolutionary networking models difficult to implement. to gain general acceptance. Attackers have increased their attacks as a result of advancements in processing technology, such as DDoS attacks have evolved into distributed DoS (DDoS) attacks that are rarely detected by traditional firewalls. We outline the current state of DDoS assaults in SDN and cloud computing situations in this study. In particular, we concentrate on the examination of the cloud computing and SDN architecture. In addition, we review ongoing research projects and difficulties in detecting and mitigating DDoS assaults.

DDoS detection method based on semi-supervised K-means using a hybrid feature selection algorithm[3]: A distributed denial of service (DDoS) attack attempts to overload a website with traffic from multiple sources in order to make it unavailable. As a result, it is critical to provide an effective method for detecting DDoS attacks among other things. heavy data flow. The current approaches, however, have several drawbacks, such as the necessity for huge quantities of labelled data for supervised learning methods and the poor detection rate and high false positive rate of unsupervised learning algorithms. This study provides a semi-supervised weighted k-means detection technique to deal with these issues. To find the best feature sets, we first present a hybrid feature selection method based on Hadoop. To address the issue of outliers and local optimality, we propose an improved density-based initial cluster Centre selection procedure approach. Then, in order to identify assaults, we provide the Semi-supervised K-means technique employing hybrid feature selection (SKM-HFS). Finally, we do the verification experiment using data from the DARPA DDoS dataset, CAIDA "DDoS assault 2007" dataset, CICIDS "DDoS attack 2017" dataset, as well as a real-world dataset. The experiment results show that the proposed approach outperforms the benchmark in terms of detection performance and strategy for order preference when compared to an ideal solution (TOPSIS) evaluation factor.

Detection of distributed denial of service attacks in software-defined networks using machine learning algorithms[4]: A new and promising networking technology called Software Defined Networking (SDN) divides the data and control planes and has centralized network control. With this new method, lower-level functionality is abstracted, and network managers may programmatically initiate, control, modify, and manage network behaviour. The primary The benefit of SDN, centralized control, can sometimes pose a serious security risk. The attacker would get access to the whole system if he were to successfully hack the central controller. The controller is highly vulnerable to Distributed Denial of Service (DDoS) attacks. which cause the system resources to be depleted and result in the controller's services not being available. Early detection of assaults on the controller is essential. For this, several algorithms and methods have been developed. SDN networks, however, have received little research attention. One such method is to categorize the connections into genuine and fraudulent ones using machine learning techniques. To identify suspicious and damaging connections, we employ two machine learning methods, the Support Vector Machine (SVM) classifier and the Neural Network (NN) classifier.

DDoS Detection and Defense Using SDN and Machine Learning[5]: SDN (Software Defined Network) has received a great deal of attention as a new network paradigm. Security is critical for SDN. as a result. DDoS attacks, also known as distributed denial of service attacks, have plagued the Internet. In some SDN-applied settings now, like the university network, it poses a danger. Based on machine learning, we provide an SDN framework for recognizing and resisting DDoS attacks. in order to reduce the DDoS attack on the campus network. The traffic collecting flow table delivery module, DDoS attack identification module, and are the three components that make up this system. To get ready for traffic identification, the traffic collecting module gathers traffic characteristics. The controller collects the network traffic characteristics

from statistics flow table data and utilizes the support vector machines (SVM) method for detecting attack traffic while installing a DDoS attack detection system using SDN network architecture's flexibility and multidimensionality. The forwarding policy is then dynamically modified by the flow table delivery module. in response to the traffic identification result to defend against DDoS assaults. KDD99 dataset is used in the experiment. The experiment's findings demonstrate how well the DDoS assault detection technique works.

A two-level security mechanism employing entropy-based and C4. 5 techniques to detect a DDoS flooding attack in software-defined networks[5]: A secure system and/or an accurate intrusion detection system (IDS) are now necessities for many businesses and/or governments in order to protect their network services and the user's private data. Developing a reliable detection system for distributed denial of service (DDoS) attacks is one of the most difficult issues in network security. DDoS attacks employ a swarm of cracker-hijacked bots to overload the target server's network service. numerous packets. Many businesses' and/or governments' servers have fallen prey to the assaults. It is quite challenging to identify the crackers in such an assault since they merely send a command using several bots from another network, and then promptly exit the bots after the command executes. The proposed approach entails using network packet analysis to identify DDoS attack patterns and machine learning techniques to analyze the patterns in order to create an intelligent DDoS detection system. With the assistance of a support vector machine with a radial basis function (Gaussian) kernel, we constructed the detection system in this study after analysing a sizable number of network packets given by the Centre for Applied Internet Data Analysis. DDoS assaults are accurately detected by the detection system.

III. METHODOLOGY

Proposed system:

We suggest this application, which may be seen as a valuable system since it aids in reducing the constraints brought about by conventional and other existing ways. The study's goal is to provide an effective and efficient dependable approach for precisely detecting DDoS impacts. In a Python-based environment, we developed a potent algorithm to design this system.

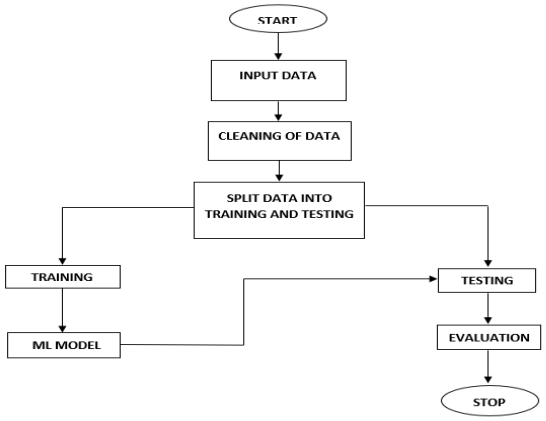


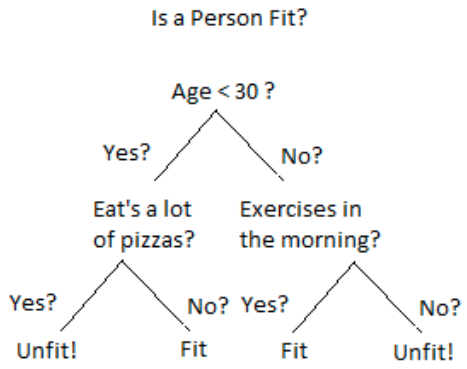
Figure 1:Block diagram

IV. IMPLEMENTATION

The project has implemented by using below listed algorithm.

Decision Tree:

The most effective and well-liked The decision tree is a technique for categorization and prediction. A decision tree is a type of diagram. tree structure that resembles a flowchart, in which each leaf node (terminal node) bears a class label, each internal node implies a test on an attribute, and each branch shows the test's result.



Simple Decision Tree

By dividing the source set into subgroups based on an attribute value test, a tree may be "trained". It is known as recursive partitioning to repeat this operation on each derived subset. When the split no longer improves the predictions or when the subset at a node has the same value for the target variable, the recursion is finished. Decision tree classifier design is suitable for exploratory knowledge discovery since it doesn't require any parameter configuration or domain understanding. High dimensional data may be handled via decision trees. Decision tree classifiers are often accurate. A popular inductive method for learning classification information is decision tree induction.

The strengths of decision tree methods are:

Decision trees are capable of producing clear rules.

Decision trees can accomplish categorization with little computational effort.

Continuous and categorical variables may both be handled by decision trees.

Decision trees clearly show which fields are most crucial for categorization or prediction.

The weaknesses of decision tree methods:

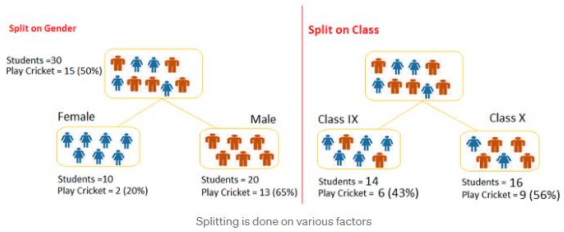
When it comes to estimating assignments where the objective is to forecast the value of a continuous characteristic, decision trees are less suitable.

Classification issues with multiple classes and a dearth of training samples make decision trees vulnerable to mistakes.

Training a decision tree can be costly computationally. A decision tree's growth requires extensive computing work. Each potential splitting field at each node must first be sorted in order to determine which split is optimal. Some algorithms employ combinations of fields, hence it is necessary to look for the best combining weights. Due to the necessity of creating and comparing several candidate sub-trees, pruning algorithms can also be costly.

Summary

A non-parametric supervised learning technique for classification and regression is called a decision tree (DT). Decision trees use a series of if-then-else decision rules to learn from data and approximate sine curves. The decision criteria are more complicated and the model is more accurate the deeper the tree.



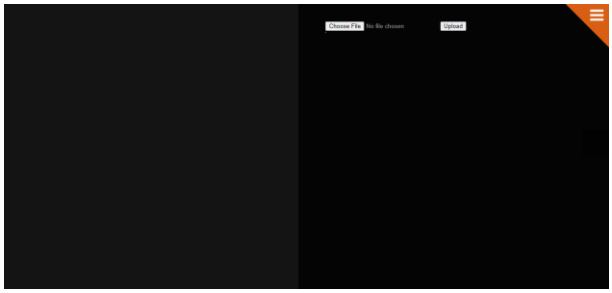
Splitting is done on various factors

V. RESULTS AND DISCUSSION

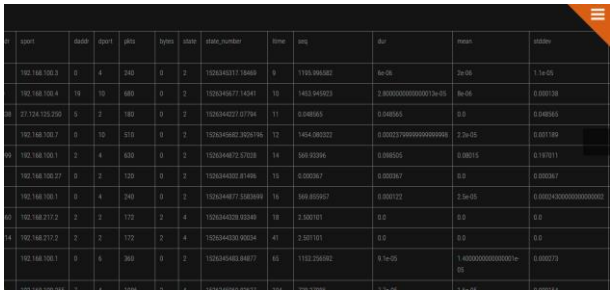
The following screenshots are depicted the flow and working process of project.

Home Page: In our project, we are detecting the whether the network is DDos attacked or not and this is our home page.

Upload page: Here user needs to upload the dataset.



Upload (View data): Uploaded data is visible in this particular tab.



Input files: User need to enter his inputs here.

Detection page gives output as the network is safe for the particular inputs submitted.

VI. CONCLUSION

Machine learning-based detection of distributed denial-of-service (DDoS) attacks in Software-Defined Networking (SDN) is a rapidly developing area of research that aims to detect and mitigate these types of attacks. SDN is an emerging technology that separates the network control plane from the data plane, providing greater flexibility and programmability to network administrators. However, this separation also introduces new challenges for network security, as traditional security measures may not be sufficient to protect against attacks.

DDoS attacks are a common form of cyber-attack that can have devastating effects on network performance, causing denial of service to legitimate users and resulting in significant financial losses. These attacks are typically launched from multiple sources and are difficult to detect and mitigate using traditional security measures.

Machine learning is a subfield of artificial intelligence that focuses on the development of algorithms and models that can learn from data and make predictions or decisions based on that learning. Machine learning has been applied to a wide range of problems, including image recognition, natural language processing, and predictive modeling. In the context of network security, machine learning can be used to detect anomalies in network traffic that may indicate the presence of a DDoS attack.

One of the main advantages of using machine learning for DDoS detection in SDN is the ability to analyze network traffic in real-time, enabling quick and accurate identification of DDoS attacks. Machine learning algorithms can be trained on large datasets of network traffic to identify patterns and anomalies that may be indicative of an attack. This can help network administrators to respond quickly and effectively to DDoS attacks, reducing the potential damage to the network and its users.

Several different machine learning-based approaches have been proposed for DDoS detection in SDN. These include supervised learning methods such as support vector machines (SVMs) and neural networks, as well as unsupervised learning methods such as clustering and anomaly detection. Some approaches use a combination of these methods to achieve better performance.

However, machine learning-based detection methods are not perfect and can sometimes result in false positives or false negatives. False positives occur when normal traffic is misclassified as attack traffic, while

false negatives occur when attack traffic is not detected. These errors can be costly, both in terms of lost revenue and in terms of the time and resources required to investigate false alarms. Therefore, it is essential to continuously improve the accuracy and reliability of these methods by refining the algorithms and incorporating additional features that can help distinguish between normal and attack traffic.

Another challenge in using machine learning for DDoS detection in SDN is the potential for adversarial attacks. Adversarial attacks are attacks that are designed to evade detection by machine learning algorithms. Adversaries can modify or craft network traffic to evade detection or to mislead the machine learning model. This requires the development of more robust machine learning models that are resistant to these types of attacks.

In conclusion, the use of machine learning in SDN for DDoS detection shows great promise and is likely to become an increasingly important tool in the fight against cyber threats. Machine learning-based approaches can provide quick and accurate detection of DDoS attacks, enabling network administrators to respond quickly and effectively. However, the accuracy and reliability of these methods need to be continuously improved to reduce the risk of false alarms and to make these methods more resistant to adversarial attacks. As the use of SDN continues to grow, machine learning-based detection of DDoS attacks is likely to become an essential component of network security.

VII. REFERENCES

[1]. Dong, S., & Sarem, M. (2019). DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks. IEEE Access, 8, 5039-5048.

[2]. Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813- 80828.

[3]. Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semi supervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351- 64365.

[4]. N. Meti, D. G. Narayan, and V. P. Baligar (2017, September). Machine learning algorithms are used in software defined networks to detect distributed denial of service attacks. In 2017, the International Conference on Advances in Computing, Communications, and Informatics (ICACCI) held its annual meeting in San Francisco (pp. 1366-1371). IEEE.

[5]. IEEE DDoS Attack Identification and Defense Using SDN Based on Machine Learning Method, 15th International Symposium on Pervasive Systems, Algorithms, and Networks, 2018.

[6]. 6.Muthamil Sudar, K., and P. Deepalakshmi (2020). A two-tiered security mechanism for detecting DDoS flooding attacks in software-defined networks that employs an entropy-based and C4. 5 technique. (Preprint), Journal of High Speed Networks, 1- 22.

[7]. 7.Deepa, V., Sudar, K. M., and P. Deepalakshmi (2018, December). DDoS attack detection on the SDN control plane using Hybrid Machine Learning Techniques. The International Conference on Smart Systems and Innovative Technology (ICSSIT) was held in 2018. (pp. 299-303). IEEE.

[8]. Deepa, V., Muthamil Sudar, K., and Deepalakshmi, P.

[9]. Deepalakshmi. "Design of Ensemble Learning Methods for DDoS Detection in SDN Environment." 2019 International Conference on Vision for Emerging Communication and Networking Trends (ViTECoN). IEEE, 2019.\s9. "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN,.

[10]."DDoS detection and defense mechanism based on cognitive-inspired computing in SDN,"

[11]."Time-based DDoS detection and mitigation for SDN controller," N. I. G.

[12].Time-based DDoS detection and mitigation for SDN controller," N. I. G

[13].A. Botta, W. de Donato, V. Persico, and A. Pescapé, Integration of cloud computing and the internet of things: A survey, Future Generation Computer Systems 56 (2016) 684-700.

[14].Han B., Gopalakrishnan V., Ji L., Lee S., Network function virtualization: Challenges and Opportunities for Innovation, IEEE Commun. Mag. 53 (2) (2015) 90-97. SDN OS, in: The Workshop on Hot Topics in Software Defined Networking, 2014, pp. 1–6.

Cite this article as :

Dr. D. J. Ashpin Pabi, R. Mounesh, P. Uday Kiran, B. Sai Sreedhar Reddy, "Machine Learning-Based Detection of Distributed Denial-Of-Service Attacks in SDN", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 3, pp.135-142, May-June-2023.