International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Machine Learning Techniques for the Detection of Distributed Denial of Service Attacks in the SDN

G. Anitha[1], G. Lakshmikanth[2]
[1]M.Tech Scholar, [2]Associate Professor & HOD
[1&2]Department of Computer Science and Engineering, Sree Rama Engineering College, Tirupati, India

Article Info
Volume 9, Issue 5
Page Number : 145-151

Publication Issue
September-October-2022

Article History
Accepted : 08 Sep 2022
Published : 20 Sep 2022

ABSTRACT

A network architecture known as a "software-defined network" (SDN) is used to digitally construct and design hardware components. The network connection settings can be changed dynamically. Because the link is fixed in the conventional network, dynamic change is not feasible. SDN is a wonderful strategy, but DDoS assaults can still happen. The DDoS assault poses a threat to the internet. The machine learning algorithm can be used to stop DDoS attacks. The DDoS assault is when several systems work together to simultaneously target a certain host. In SDN, the infrastructure layer's devices are managed by software from the control layer, which sits in the middle of the application and infrastructure layers. We provide a machine learning method called Decision Tree in this research to identify malicious communications. Our test results demonstrate that the Decision Tree determines whether or not the assault is safe.

Keywords : SDN, attacks, DDoS, Decision Tree.

I. INTRODUCTION

A distributed denial-of-service (DDoS) attack is a malicious attempt to obstruct a server, service, or network's regular traffic by saturating the target or its surrounding infrastructure with an excessive amount of Internet traffic. By using several hacked computer systems as sources of attack traffic, DDoS assaults are made effective. Computers and other networked resources, like as IoT devices, can be exploited machines. When viewed from a distance, a DDoS assault resembles an unexpected traffic congestion that blocks the roadway and keeps ordinary traffic from reaching its destination. Networks of Internet-connected devices 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. Once a botnet has been created, the attacker may control an attack by giving each bot remote commands. Each bot in the botnet sends queries to the IP address of the victim's server or

network while that server or network is being targeted by the botnet. This might overload the server or network and 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 a website or service is the most evident sign of a DDoS assault. However, since several factors, including a real increase in traffic, might result in performance concerns, more research is often needed. You may identify some of these telltale symptoms of a DDoS assault using traffic analytics tools, unusual spikes in traffic to a single page or endpoint, suspicious quantities of traffic coming from a single IP address or IP range, or a deluge of users with the same device, geographic area, or web browser version. 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, and quality of service (QoS) applications are managed by the application plane.By separating 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. 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 done at the application layer. The brain of the SDN architecture is the control layer (control plane), which is composed of the same controller. API is used to communicate between these two levels. A common protocol is used by the infrastructure layer (data plane), which connects the controller and 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 Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks: 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.

A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments: SDNs (software defined networks) and cloud computing have recently gained significant traction among academics and business. The security risks have, however, made it difficult for these revolutionary networking models to gain general acceptance. Attackers have increased their attacks as a result of advancements in processing technology, such as the evolution of Denial of Service (DoS) attacks into distributed DoS (DDoS) attacks that are seldom 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 challenges in recognizing and countering DDoS assaults.

Semi supervised K-means DDoS detection method using hybrid feature selection algorithm: The goal of a distributed denial of service (DDoS) assault is to overload a website with traffic from several sources in an effort to render it unavailable. As a result, it is essential to provide an efficient technique for identifying DDoS attacks among 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 address these problems.To discover the best feature sets, we first provide a Hadoop-based hybrid feature selection method. To address the issue of outliers and local optimality, we next suggest an enhanced density-based initial cluster centers selection 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, and real-world dataset. The findings of the experiment show that the suggested approach performs better than the benchmark in terms of detection performance and strategy for order preference by comparison to an ideal solution (TOPSIS) evaluation factor.

Detection of distributed denial of service attacks using machine learning algorithms in software defined networks: A new and promising networking technology called Software Defined Networking (SDN) separates the data and control planes and has centralized control over the network. With this new method, lower-level functionality is abstracted, and network managers may programmatically initiate, control, modify, and manage network behaviour. The primary benefit of SDN, centralized control, can occasionally also 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 extremely susceptible to Distributed Denial of Service (DDoS) assaults, 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 Attack Identification and Defense using SDN based on Machine Learning Method: As a new network paradigm, SDN (Software Defined Network) has generated a lot of attention. SDN security is crucial 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. We provide an SDN framework to recognize and resist DDoS assaults based on machine learning in order to reduce the DDoS attack on the campus network. The traffic collecting module, DDoS attack identification module, and flow table delivery module 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) approach to identify the attack traffic while installing a DDoS attack detection system using the flexible and multi-dimensional features of SDN network architecture. The flow table delivery module then dynamically modifies the forwarding policy 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 to detect a DDoS flooding attack in software-defined networks using entropy-based and C4. 5 technique: 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. One of the difficult issues in network security is creating a reliable detection system for distributed denial of service (DDoS) attacks. DDoS attacks use several cracker-hijacked bots to disrupt the target server's network service by flooding it with 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 suggested approach entails employing network packet analysis to identify DDoS attack patterns and machine learning techniques to analyse the patterns in order to create an intelligent detection system for DDoS assaults. With the help 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. METHODS AND MATERIAL

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 goal of this study is to provide an efficient and dependable approach for precisely detecting DDoS impacts. In a Python-based environment, we developed a potent algorithm to design this system.

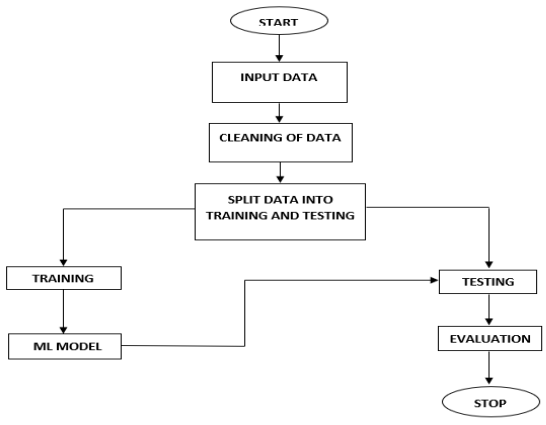


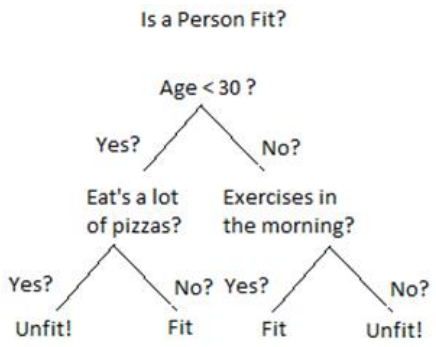
Figure 1: Block diagram

Implementation

The project has implemented by using below listed algorithm.

1. Decision Tree:

The most effective and well-liked technique for categorization and prediction is the decision tree. A decision tree is a 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:

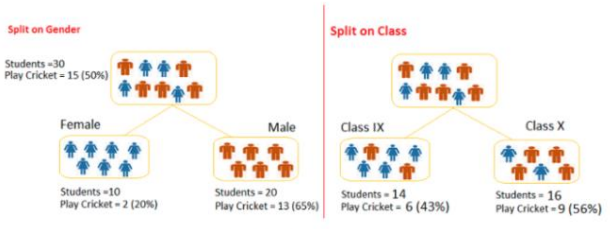
- Decision trees are capable of producing clear rules.
- Decision trees can accomplish categorization with little computational effort.
- Continuous and categorical variables may both be handled by decision trees.
- Decision trees clearly show which fields are most crucial for categorization or prediction.

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.



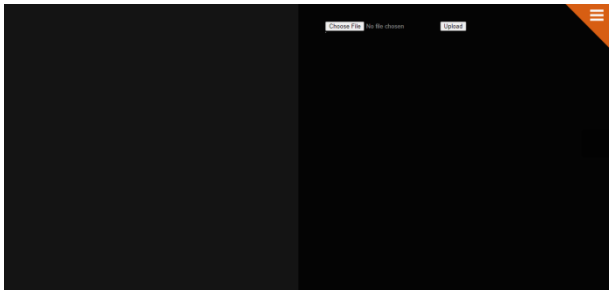
Splitting is done on various factors

IV. RESULTS AND DISCUSSION

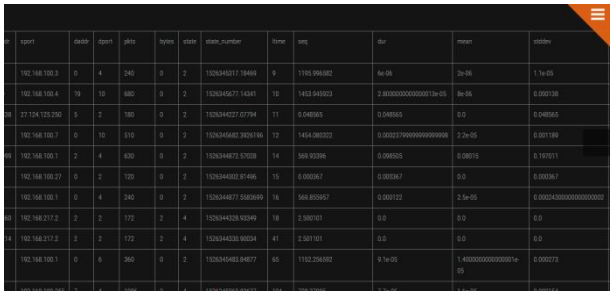
The following screenshots are depicted the flow and working process of project.

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.

V. CONCLUSION

In this application, we have successfully created a system to identify DDoS assaults. This is made in a user-friendly setting using Flask and Python programming. In order to identify whether or whether the network is under attack, the system is likely to collect data from the user.

VI. 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). Semisupervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351- 64365.

[4]. Meti, N., Narayan, D. G., &Baligar, V. P. (2017, September). Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. In 2017 international conference on advances in computing, communications and informatics (ICACCI) (pp. 1366-1371). IEEE.

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

[6]. MuthamilSudar, K., &Deepalakshmi, P. (2020). A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4. 5 technique. Journal of High Speed Networks, (Preprint), 1- 22.

[7]. Deepa, V., Sudar, K. M., &Deepalakshmi, P. (2018, December). Detection of DDoS attack on SDN control plane using Hybrid Machine Learning Techniques. In 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 299-303). IEEE.

[8]. Deepa, V., K. MuthamilSudar, and P. Deepalakshmi. "Design of Ensemble Learning Methods for DDoS Detection in SDN Environment." 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN). IEEE, 2019.

[9]. J. Cui, M. Wang, and Y. Luo, ``DDoS detection and defense mechanism based on cognitive-inspired computing in SDN,'' Future Gener. Comput. Syst., vol. 97, pp. 275_283, Aug. 2019.

[10]. N. I. G. Dharma, M. F. Muthohar, J. D. A. Prayuda, K. Priagung, and D. Choi, ``Time-based DDoS detection and mitigation for SDN controller,'' in Proc. 17th Asia_Paci_cNetw. Oper. Manage. Symp. (APNOMS), Aug. 2015, pp. 550_553.

[11]. Botta A., de Donato W., Persico V., Pescapé A., Integration of cloud computing and internet of things: A survey, Future Gener. Comput. Syst. 56 (2016) 684–700.

[12]. Han B., Gopalakrishnan V., Ji L., Lee S., Network function virtualization: Challenges and opportunities for innovations, IEEE Commun. Mag. 53 (2) (2015) 90–97.

[13]. P. Berde, J. Hart, J. Hart, Y. Higuchi, M. Kobayashi, G. Parulkar, G. Parulkar, G. Parulkar, G. Parulkar, G. Parulkar, ONOS: towards an open, distributed SDN OS, in: The Workshop on Hot Topics in Software Defined Networking, 2014, pp. 1–6.

Cite this article as :

G. Anitha, G. Lakshmikanth, "Machine Learning Techniques for the Detection of Distributed Denial of Service Attacks in the SDN", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 5, pp. 145-151, September-October 2022.
Journal URL : https://ijsrst.com/IJSRST229539