Machine Learning Technique for SDN: DDOS Attacks and Defense Mechanisms

Dr. K. Uday Kumar Reddy, Associate Professor, Department of Computer Science and Engineering, Annamacharya Institute of Technology and Sciences(Autonomous), Rajampet, Andhra Pradesh, India-516126.

K. Lakshmi Prasanna , H. K. Kavya Sree, K. Anuradha, T. Badri Nath , S. Showkat Ali, Department of Computer Science and Engineering, Annamacharya Institute Of Technology and Sciences(Autonomous), Rajampet, Andhra Pradesh, India, 516126.

ABSTRACT:

Network architecture called a "software-defined network" (SDN) allows for the virtual construction and design of hardware components. The configuration of network connections can be changed dynamically. Since the link in the traditional network is fixed, changes cannot be made on the fly. Although SDN is a sound strategy, DDoS attacks can still happen. Internet users are at risk from the DDoS attack. The machine learning algorithm is useful for preventing DDoS attacks. Multiple systems working together to simultaneously target a specific server constitute a DDoS attack. When using SDN, the infrastructure layer's devices are controlled by software from the control layer, which is centrally located and connected to both the application and infrastructure layers. In this article, we suggest using Decision Tree and Support Vector Machine (SVM) machine learning techniques to identifying harmful traffic Our test results demonstrate that the Support Vector Machine (SVM) and Decision Tree algorithms offer superior accuracy and detection rates.

KEYWORDS:

Security, Distributed Denial of Service(DDoS), Machine Learning, Software defined network (SDN), Support Vector Machine (SVM), Decision Tree.

INTRODUCTION

A distributed denial-of-service (DDoS) attack is a malicious attempt to obstruct a targeted server's, service's, or network's regular traffic by saturating the target or its surrounding infrastructure with a torrent of Internet traffic. Several compromised computer systems are used as sources of attack traffic in DDoS attacks to achieve efficacy. Computers and other networked devices, including IoT gadgets, can be exploited machinery. A DDoS assault might be compared to an unforeseen traffic congestion that blocks the roadway from a distance, preventing ordinary traffic from reaching its destination. With networks of Internet-connected devices, DDoS attacks are conducted. These networks are made up of computers and other devices infected with malware, such as Internet of Things (IoT) devices, allowing an attacker to remotely manage them. A collection of these devices is known as a botnet, and each individual device is referred to as a bot (or zombie). An attacker can control an attack once a botnet has been established by sending each bot remote instructions. Each bot in the botnet sends queries to the IP address of the victim's server or network while it is being targeted by the botnet, which may overwhelm the victim's server or network and disrupt normal traffic. Separating attack traffic from regular traffic can be challenging because each bot is a valid Internet device.

A website or service suddenly becoming delayed or unavailable is the most evident sign of a DDoS assault. However, since numerous factors, including a real increase in traffic, might result in performance problems, more research is typically needed. You can recognize some of these DDoS assault telltale signals 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 flood of users with the same device, geographic location, or web browser version. Unusual traffic patterns, such as spikes at strange times of day or patterns that seem abnormal (such as a spike every ten minutes), Depending on the type of assault, there are further, more precise indications of DDoS attack.

By separating the control from the data plane devices, software defined networking, an emerging paradigm, solves the drawbacks of traditional network architecture. Data, control, and application planes are the three components that make up SDN. Depending on the decision taken by the controller, the data plane carries the network traffic. Through the use of routing tables, the control plane determines how traffic will move. Other applications, such firewalls, load balancers, and Quality of Service (QoS) apps, are managed by the application plane. By separating the forward and control functions of the network, SDN architecture enhances network performance. A network's many routers will be under the control of the control programs running in a logically centralized controller. The only way for applications to access all network data is through the SDN. For load balancing and intrusion detection during periods of high traffic, several apps can be integrated. The application notifies the controller to modify the data plane if an anomaly is found, and the controller is then ordered to do so. On routers dispersed throughout the network, where the hardware has open interfaces that can be managed by software, the control and data planes are both operated.

It is possible to simultaneously reconfigure several devices under the SDN architecture. Network device configuration is done at the application layer. The control layer (control plane), which is composed of the same controller, serves as the SDN architecture's central processing unit. Through API, these two levels talk to one another. Using a centralized protocol, the infrastructure layer (data plane) connects the controller and network devices. Given the volume of communication going through the controller, it is crucial to have an effective security system in place to analyze and spot questionable traffic. By analyzing the traffic features, we provide a machine learning-based approach to detect malicious SDN activity.

LITERATURE REVIEW AND OBJECTIVES:

There is still no reliable security mechanism against the Distributed Denial of Service (DDoS) assault, which has been substantially reducing network availability for decades. A fresh approach to rethinking the protection against DDoS attacks is offered by the newly developed Software Defined Networking (SDN). In this article, we recommend two techniques for spotting DDoS attacks in SDN. To identify a DDoS assault, one way uses the attack's intensity. The other technique finds the DDoS attack using an enhanced version of the K-Nearest Neighbors (KNN) algorithm based on machine learning (ML). Our suggested approaches can identify the DDoS assault more effectively than other methods, according to the results of the theoretical analysis and the experimental findings on datasets. Cloud computing and software defined networks (SDNs) have recently gained significant traction among academics and business. The security risks have prevented these revolutionary networking models from being widely adopted, though. The rise of distributed DoS (DDoS) attacks, which are rarely detected by traditional firewalls, is one example of how advances in processing technologies have aided attackers in escalating attacks. Using SDN and cloud computing as examples, we provide the state of the art for DDoS attacks in this study. The examination of SDN and cloud computing architecture is where we spend our attention. In addition, we provide a summary of ongoing research projects and unresolved issues related to recognizing and countering DDoS attacks.

The goal of a distributed denial of service (DDoS) assault is to overwhelm a website with traffic from several sources in an effort to render it unavailable. As a result, it is essential to suggest an efficient technique for identifying DDoS attacks among heavy data flow. The current approaches, however, have some 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 weighted semi-supervised k-means detection approach to address these problems. To discover the best feature sets, we first provide a Hadoop-based hybrid feature selection algorithm. To address the issue of outliers and local optimality, we then propose an enhanced density-based initial cluster centres selection approach. Then, in order to identify attacks, we offer 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. Results of the experiment show that the suggested method outperforms the benchmark in terms of detection performance and technique for order preference by comparison to an ideal solution (TOPSIS) evaluation factor.

SDN, a novel and promising networking idea, separates the data and control planes and has centralized control over the network. The network administrators may initiate, control, adjust, and manage network behaviour programmatically thanks to this innovative technique, which provides abstraction of lower-level operations. Despite being the main benefit of SDN, centralized control can occasionally pose a serious security risk. The system would become accessible to the intruder if he is successful in attacking the central controller. Due to distributed denial of service (DDoS) assaults that drain system resources and render the controller's services unavailable, the controller is extremely susceptible to these types of attacks. The controller must be attacked early on, therefore this is crucial to detecting.

SDN (Software Defined Network), a new networking model, has generated a lot of interest. As a result, SDN security is crucial. The Internet has been plagued by Distributed Denial of Service (DDoS) attacks. It now poses a concern in some SDN-applied environments, such the university network. We provide an SDN framework based on machine learning to recognize and defend DDoS attacks in order to lessen the DDoS attack on the campus network. The three components of this framework are the flow table delivery module, the DDoS attack identification module, and the traffic gathering module. In the traffic collecting module, traffic characteristics are extracted in order to set up traffic identification. In order to create a DDoS attack detection system, the controller takes advantage of the adaptable and multifaceted properties of SDN network architecture. A support vector machine (SVM) approach is used by the controller to identify attack traffic after extracting network traffic characteristics from statistical flow table data. Once the traffic identification result has been determined, the flow table delivery module dynamically modifies the forwarding policy to fend off DDoS attacks. Use of the KDD99 dataset is made for the experiment. Results of the trial demonstrate how well the DDoS assault detection system works.

To protect their network services and the users' private information, many businesses and/or governments nowadays need a secure system and/or an effective intrusion detection system (IDS). One of the difficult issues in network security is creating a precise 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 a large number of packets. The attacks have affected the servers of numerous businesses and/or governments. Because they merely employ several bots from another network to convey a command, and then rapidly abandon the bots after the instruction has been executed, crackers in such an attack are very difficult to identify. The suggested course of action is to create a sophisticated DDoS assault detection system. The suggested approach entails employing network packet analysis to identify DDoS attack patterns and machine learning techniques to analyze the patterns in order to create an intelligent detection system for DDoS attacks. With the help of a support vector machine with a radial basis function (Gaussian) kernel, we constructed the detection system in this study after analyzing a sizable number of network packets provided by the Centre for Applied Internet Data Analysis. DDoS attacks can be accurately detected by the detection system.

EXISTING SYSTEM

Machine learning is becoming more and more prevalent, and there are now machine learning and traditional computer techniques. The relevant research on DDoS attacks is discussed in this part, along with how machine learning techniques outperform conventional ones. Several methodologies are utilised for model development, and the current methodology in this project has a specific flow. The result, however, is inaccurate and requires a huge memory.

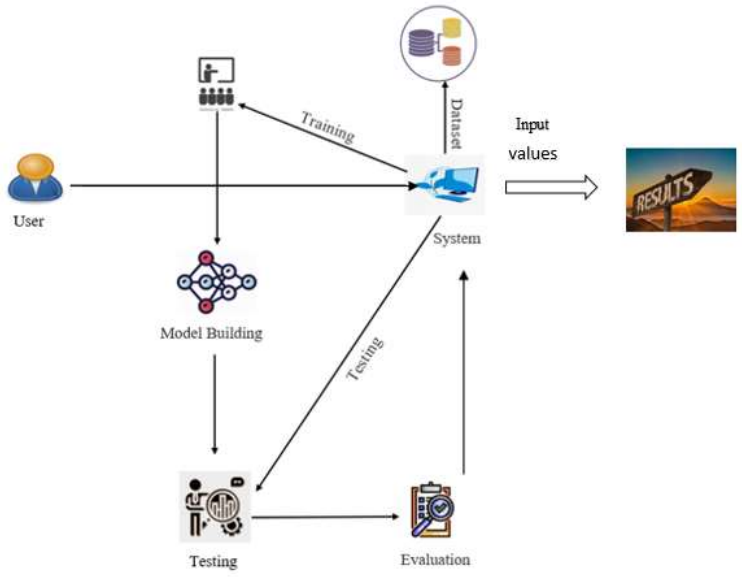
Disadvantages:

- Low accuracy
- high complexity
- high inefficiency are drawbacks.
- requires skilled individuals

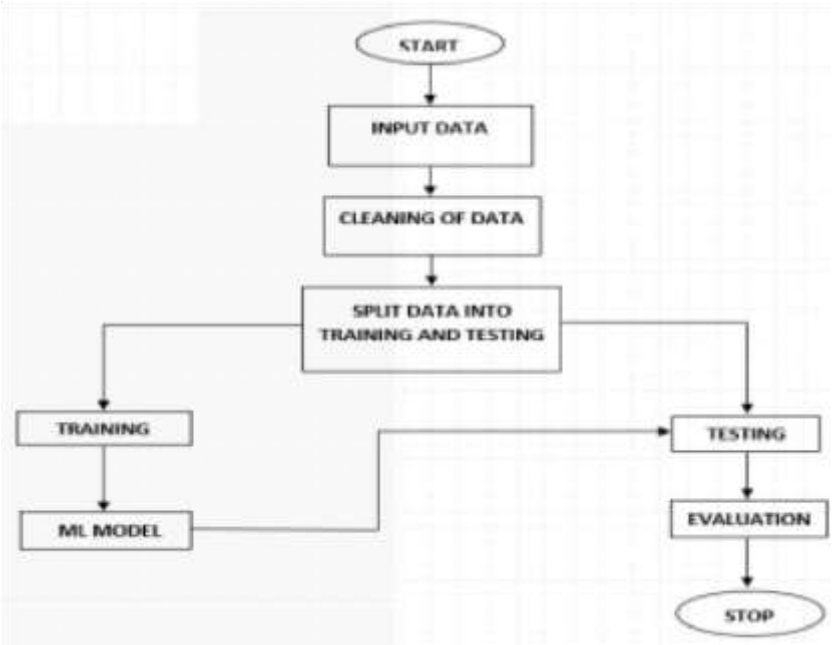
PROPOSED SYSTEM

We suggest this strategy, which is valuable in that it helps to overcome the drawbacks of conventional and other approaches. The goal of this study is to create an efficient and trustworthy approach for precisely detecting DDoS effects. We employed a potent algorithm in a Python-based environment to design this system.

ARCHITECTURE



BLOCK DIAGRAM



Advantages:

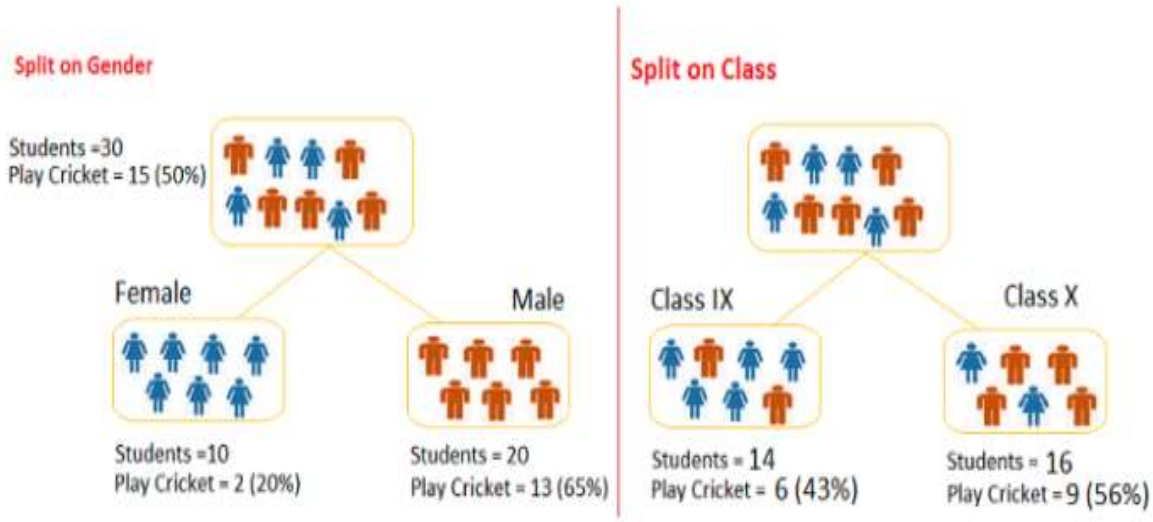
- Accuracy is good.
- Low complexity.
- Highly efficient.
- No need of skilled persons

METHODOLOGY AND ALGORITHMS:

1. Decision Tree:

The strongest and most widely used technique for categorization and prediction is the decision tree. A decision tree is a flowchart-like tree structure in which each internal node represents a test on an attribute, each branch a test result, and each leaf node (terminal node) a class label.

For classification and regression, decision trees (DTs) are a non-parametric supervised learning technique. With a set of if-then-else decision rules, decision trees learn from data to approximate a sine curve. As the depth of the tree increases, so does the complexity of the decision rules and the model's fit.



Splitting is done on various factors

CONCLUSION AND FUTURE SCOPE:

We have successfully developed a system to detect DDoS attacks in this application. This is made in a user-friendly setting using Flask and Python programming. The system is likely to gather data from the user in order to determine whether or not the network is attacked. The ability to identify numerous attacks could be added to this application in the future. With the updated data set, we plan to examine the prediction strategy and use the most precise and pertinent machine learning algorithms for detection.

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]. 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]. Muthamil Sudar, 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. Muthamil Sudar, 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_c Netw. Oper. Manage. Symp. (APNOMS), Aug. 2015, pp. 550_553.