iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.47344

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Mitigation and Detection of DDOS attacks using Software Defined Network (SDN) and Machine Learning

Hemanth kumar R L[1], Bhargava K P[2], Dr. Ashok Kumar A R[3]
Department of Computer Science and Engineering, RV College of Engineering

Abstract: ***An emerging networking paradigm called Software Defined Networking (SDN) enables network control to be restricted to a logically centralized controller. This makes network visibility and management simpler on a global scale. SDN is a suitable network model for extensive deployment in real-world settings since it can be programmed using high-level programming languages. SDN is still vulnerable to a number of network attacks, the most notable of which being the DDoS (distributed denial of service) attack. A DDoS attack has the potential to render the controller, the brain of SDN, inoperable. SDN security is still in its infancy, and both business and academics have done a lot of research in this area. The SDN DDoS mitigation strategy utilizing machine learning (ML) is the main topic of this study. This work also surveys network traffic aspects for DDoS detection.***

Keywords: ***SDN, Mininet, Ryu controller, DDOS Attack SVM Algorithm***

I. INTRODUCTION

A. Overview of Mitigation of DDOS attacks using SDN and Machine Learning

Due to the constantly changing network requirements, achieving network programmability has emerged as a key objective of network research. As a replacement for traditional networks, Software-Defined Networking (SDN), an emerging architecture, has attracted a lot of attention in recent years. Network devices become straightforward packet forwarding elements under SDN, which separates the control plane from the data plane. The SDN controller, a logically centralised unit, programmes network devices using a standardised protocol like OpenFlow. Greater control capabilities for network administration are provided by this division, which in turn makes it easier to build intelligent and automated networks. Additionally, this division provides additional flexibility because it makes it easier to implement new network applications and services. Despite their widespread usage, SDN-based networks are still open to emerging security threats and attacks, including Distributed Denial of Service (DDoS) attacks, which can compromise the resilience and dependability of SDN networks. One of the biggest problems and challenges in the SDN research community right now is the detection of anomalous traffic patterns. The SDN paradigm makes it easier to create attack detection and mitigation approaches because it gives users a global perspective of the network, makes it simple to gather flow statistics, and permits dynamic updating of flow entries.

In traditional networks, this is significantly more challenging because devices must exchange a lot of data in order to infer partially the state of the remaining network components. This results in limited visibility and, thus, limited detection capabilities. For the purpose of discovering attacks in SDN networks, numerous strategies have been put out in the literature. Due to its recent success in detecting abnormalities and promising results, the Machine Learning (ML) technique is now playing a crucial role. However, ML-based techniques have some limitations. The use of packet-based detection by some of them results in significant processing and memory overhead. Other techniques make advantage of aggregated flow data, but they are unable to identify the attack's origin and are therefore helpless to stop it. By closely examining each flow and identifying its peculiarities, some approaches have overcome the aforementioned restrictions. The latter architecture, however, has a drawback in that the native flow properties that were retrieved are frequently insufficient to reliably differentiate between normal and attack flows. To enhance the detection performance, we shall therefore augment these features in this study. In this research, we offer an SDN model that uses machine learning to automatically identify and counteract assaults in SDN networks. The model periodically gathers data on traffic flow from each switch, extracts the original flow features, and then extends them. The average flow packet size, the number of flows to the same host as the current flow in the previous five seconds, and the number of flows to the same host and port over that time frame are the extended flow features.

A detection module uses these additional features in addition to the native counters (such as packet count and byte count) to characterize each flow as either normal or anomalous using a binary classification ML algorithm. When an attack is discovered, its source is prevented. SVM is assessed in relation to the classification ML algorithm employed in the detection module. As a proof-of-concept, we created a prototype system. The REST API was used to create the prototype as a Python script on top of a Floodlight controller. We utilised Mininet emulator Ryu controller to simulate an SDN network architecture, Hping3 to produce attack and regular traffic, and a trained ML model to mitigate DDOS attack traffic. These tests were done to assess the effectiveness of our suggested approach.

B. Related Work

A Flexible SDN-Based Architecture for Machine Learning-Based Low-Rate DDoS Attack Detection and Mitigation. [1] In this study, they attempt to neutralize all assaults previously identified by the IDS system by training an architecture using six machine learning (ML) models, evaluating their performance using the LR-DoS dataset.

Using an extreme gradient boosting algorithm and a bandwidth control mechanism, software-defined networks may be protected from DDoS attacks. [2] In order to provide precise attack detection and effective network resource use, a DDoS mitigation method for SDN is presented in this study. Extreme Gradient Boosting (XGBoost) Algorithm and a bandwidth control mechanism are the two phases used in the approach a dynamic MLP-based DDoS assault detection technique that makes use of feature feedback and selection. [3] To illustrate and address DDOS assault, a multilayer perceptron (MLP) model was developed in this work. To choose the best features during the training phase, they used sequential feature selection with MLP. They also created a feedback system to reconstruct the detector upon seeing significant dynamic detection mistakes. Slow DDoS attack detection using deep learning in networks powered by SDN. [4] In this study, sluggish DDoS assaults on SDN-based networks were detected using a hybrid Convolutional Neural Network-Long-Short Term Memory (CNN-LSTM) model. Based on unique datasets, this method's performance is assessed. A proactive defence framework for IoT networks that is SDN enabled. [5] The suggested method was designed to successfully mitigate DDoS assaults and preserve high performance in IoT networks with a tolerable amount of cost.

Machine and Deep Learning-Based SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection. [6] This article describes the design of a modular and adaptable SDN-based architecture for detecting DDoS assaults at the transport and application layers.

In the direction of a Software-Defined Networks DDoS Detection Scheme that is Effective. [7] The technique for reducing DDoS assaults in SDN is suggested in the study utilizing statistical analysis and traffic entropy. After 1500 packages were analysed, a good performance was found in the identification of assaults, with an accuracy rate above 96%.

A Game Theoretical Based System for DoS/DDoS Mitigation on SDN Networks Using Holt-Winters and Genetic Algorithm with Fuzzy Logic. [8] The paper introduces a Game Theory (GT)-HoltWinters for Digital Signature (HWDS)-based autonomous DoS/DDoS defensive solution for SDNs, which combines the anomaly detection and identification capabilities offered by a HWDS system with an autonomous decision-making model based on GT.

C. Motivation

1) Training the intrusion detection system (IDS) using ML algorithm in our architecture and assess their effectiveness.
2) The further point out that in order to make our deployment as similar to real-world production networks as feasible, we used the open network operating system RYU controller running on a Mininet virtual machine.
3) The intend is to test our architecture and the intrusion prevention, detection system to counteract DDOS attacks.

D. Problem Statement

To develop a security architecture (IDS) for identifying and mitigating DDoS Assaults in SDN for the project "Mitigation of DDOS attacks using Software Defined Network (SDN) And Machine Learning Algorithm". By combining ML algorithms with DDOS-attacked data, we build a model for an intrusion detection system.

E. Objectives

1) To design and implement a modular and flexible security architecture to detect and mitigate DDoS attacks in SDN environments.
2) To Train IDS module to detect flows using ML model

F. Methodology

1) Designed a SDN model for Creating topology for simulation. Generating traffic using Hping3.

2) We trained a SVM Model for analyzing DDOS attack and we collect and train the network traffic to check whether its normal traffic or attacked traffic.

3) We Analyze and compare the traffic by Simulating the given topology with NORMAL traffic and simulating the given topology with ATTACK traffic.

4) The Analyzed Traffic is sent to the ML IDS model using SVM it checks whether its normal traffic or attacked traffic, If it is attacked traffic its updates the information to IPS in SDN network

5) Once the IPS gets alert message it blocks the IP of host.

6)

II. CONCEPTS RELATED TO SOFTWARE DEFINED NETWORK (SDN), DDOS ATTACKS USING MACHINE LEARNING

A. Concepts

1) *Software-Defined Networking:* The high-bandwidth, dynamic nature of today's applications make SDN an excellent emerging architecture since it is dynamic, controllable, affordable, and adaptive. The network control and forwarding operations are separated in this design, allowing for direct programming of the network control and the abstraction of the underlying infrastructure for applications and network services.

a) Mininet just a single command, quickly and easily generates a realistic virtual network running actual kernel, switch, and application code on a single system (VM, cloud, or native).

b) Ryu Controller is a software defined networking framework that is built on components. In order to make it simple for developers to construct new network management and control applications, Ryu offers software components with well defined APIs. For managing network devices, Ryu supports a number of protocols, including OpenFlow, Netconf, OF-config, etc.

2) *Support Vector Machine:* SVM is a well-liked supervised learning method that may be applied to both classification and regression issues. Nevertheless, Machine Learning Classification issues are where it is most frequently employed. The SVM algorithm seeks to define the best line or decision boundary that can divide n-dimensional space into classes so that additional data points can be quickly classified in the future. This optimal decision boundary is known as a hyperplane. The hyperplane's extreme vectors and points are selected using SVM. Support vectors, which are used to represent these extreme circumstances, are the foundation of the SVM technique. See how the figure below uses a decision boundary or hyperplane to divide two distinct categories:

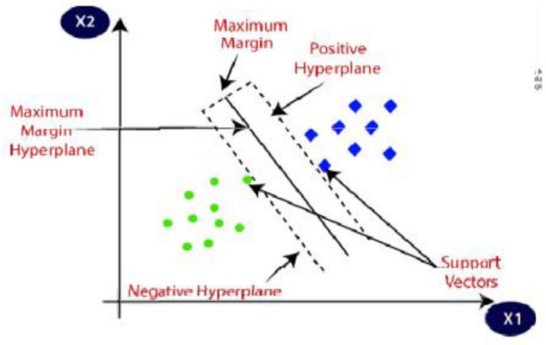


Fig 2.1 SVM Classification

3) *Distributed Denial of Service:* Denial of service (DoS) attacks are a subtype of DDoS assaults. A botnet, or group of interconnected net gadgets, is used in a DDoS attack to flood a target internet site with fictitious visitors. DDoS attacks don't seek to penetrate your protection perimeter as other sorts of cyberattacks do. instead, a DDoS assault seeks to save you accepted customers from getting access to your internet site and servers. DDoS can also be used to disable safety devices and penetrate the target's security perimeter even as serving as a smokescreen for other malicious operations hping A free and open-source TCP/IP packet generator and analyzer was created by Salvatore Sanfilippo. It was used to take advantage of the idle scan scanning method, which was created by the same person who created hping and is now a part of the Nmap Security Scanner. It is one of the tools that is widely used to test and audit the security of networks and firewalls.

B. Applications of SDN

1) *External SDN Applications:* The remainder of the Open Daylight controller software is hosted by applications that are deployed outside and run outside the container. Any language may be used to construct External SDN applications through scripting languages like Bash. On a host other than the controller, these programmes may be run remotely. These applications will also use the REST API and application providing Restful access to the controller's services.
2) *Internal SDN Applications:* Applications put inside the container, which also hosts the remaining Open Daylight controller software, are used. These apps have to be produced in Java, the native language, in order to support ODL. Internal SDN applications must also abide by the execution and design limitations of the controller. Since they both need to execute on the same Java machine, these programmes must be run locally alongside the controller. The MD-SAL apps and Java APIs for the controller are also accessible through the OSGi container.
3) *Compliance and Regulation-Bound Applications:* Major cloud providers can now store and manage workloads that must adhere to compliance regulations. Organizations now have the option to expand designs that were previously relatively restricted in distributed systems and the cloud due to laws. How do you divide the traffic, though? How can you ensure that tasks involving compliance and regulation are regularly protected and tracked? Here, SDN can be helpful. The management of network traffic across switches, network nodes, and even hypervisors is possible with an SDN architecture. Remember that this layer separates virtual functionality from hardware controllers. Then, this resilient layer can reach various sites, including cloud locations and virtualization nodes.
4) *High-Performance Applications:* There are several new application technology categories emerging nowadays. Virtualization has made it possible to deploy sophisticated applications like GIS, CAD, engineering, and graphics design tools. Often, these workloads called for bare-metal systems with independent connections. By comparison, virtualization enables the construction of sophisticated desktop environments through VDI and the streaming of software. At the network layer, we do see SDN being incorporated into application control, though. putting in place strict QoS guidelines, safeguarding personal data, dividing up high traffic, and even putting in place threshold alarms around bottlenecks. Through virtualization, all of these SDN features make it easier to deliver robust, high-performance applications.
5) *Distributed Application Control and Cloud Integration:* One of SDN's biggest benefits is that it can be expanded across the entire data centre. This type of agility integrates distributed sites, the cloud, and the entire organisation. SDN allows for the transmission of essential network traffic across several locations, regardless of the underlying network architecture. Important network controls are abstracted, which simplifies data flow between data centre and cloud locations. SDN is a form of network virtualization, therefore in addition to interfacing with a cloud provider, you can handle some network tasks via robust APIs. This keeps your business agile and lets you precisely manage your workloads.

III. DESIGN

The design in this paper is represented in high level design and detailed design.

A. High Level design

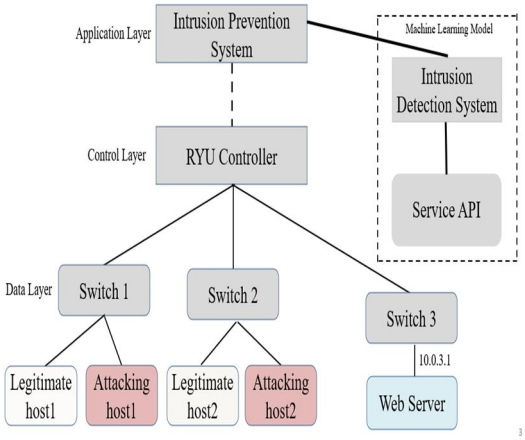


Fig 3.1 Diagrammatic Representation of High-Level Design

The proposed technique makes use of the SDN framework, in which the control plane of the framework is connected to the OpenFlow switch, which defines the SDN protocols, and the data plane of the framework comprises many nodes and hosts that were virtually constructed using Mininet. The control plane establishes rules, regulates the data plane and switches, and keeps track of the movement of network traffic. We use a controller, which gives us the ability to programme and enables us to manage network routing operations. Since Ryu is a Python-based controller and employs a Python-based API to connect with the application layer, in our case an Intrusion Prevention System for Network Traffic Analysis, the control plane is programmed in Python. The analysed data is sent to IDS, which is trained by the SVM algorithm with the DDos attacked dataset. And then the IPS will get the alert message whether it's from an attacker or from a legitimate user. If it's from an attacker, then the IP address of the user will be blocked.

B. Detailed Design

To identify the infected network traffic, we shall first train the SVM algorithm. The Data Collection module must gather information about both legitimate traffic and malicious traffic, then save it in a CSV file for the ML algorithm to use. It is necessary to gather attack traffic data first, followed by regular traffic data. For better accuracy, we collect normal traffic data once again after the attack. The information is gathered taking into account all three feature extraction factors, namely the speed of the source IP, the speed of the flow entries, and the ratio of flow pair entries in the various columns. After the data has been gathered and the controller has been set to the detection state, detection and mitigation take place. When regular traffic is generated, the SVM algorithm anticipates that it will be normal traffic; however, when attack traffic is formed, it quickly recognises the traffic as DDOS attack traffic and sends a block message to the port from which the traffic is incoming on the SDN network. After blocking, other ports on the network are free to receive regular traffic.

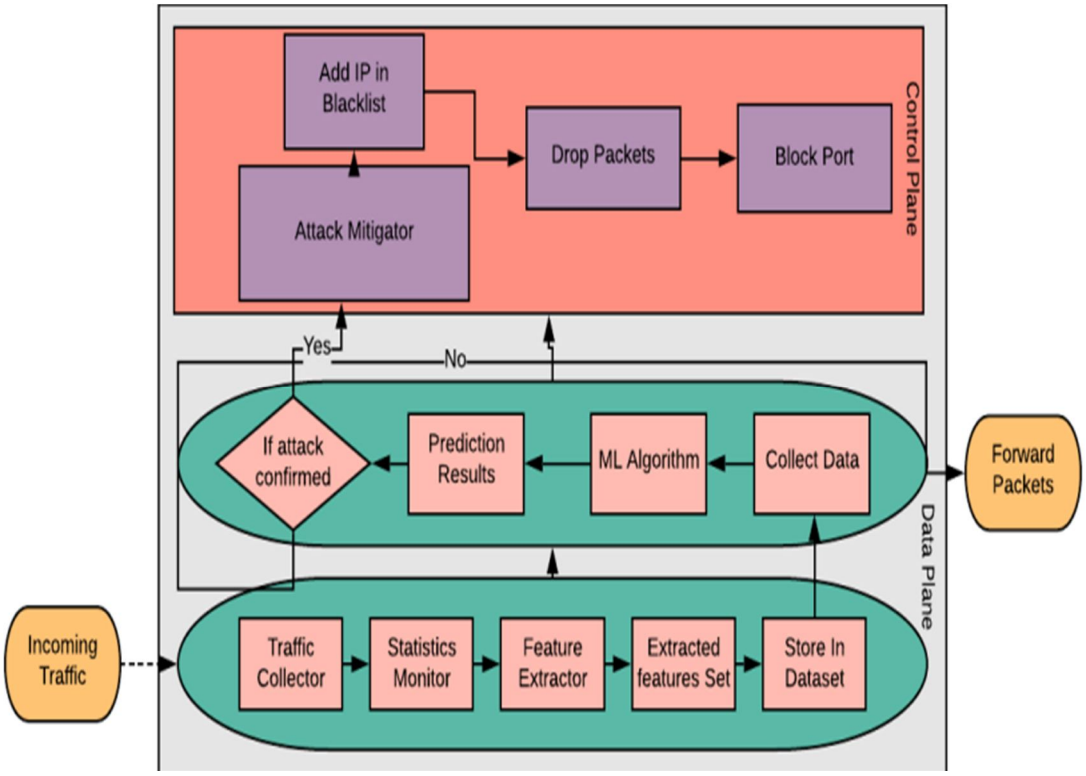
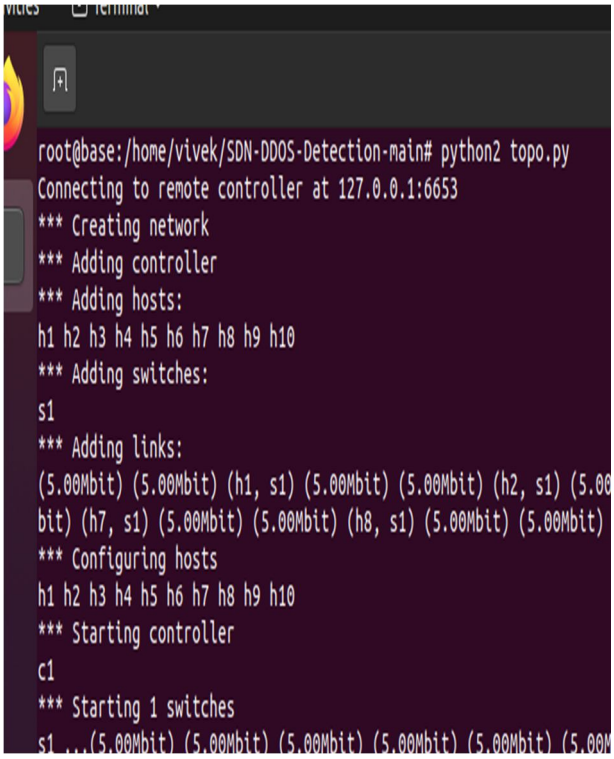


Fig 4.2.1 Detailed Design

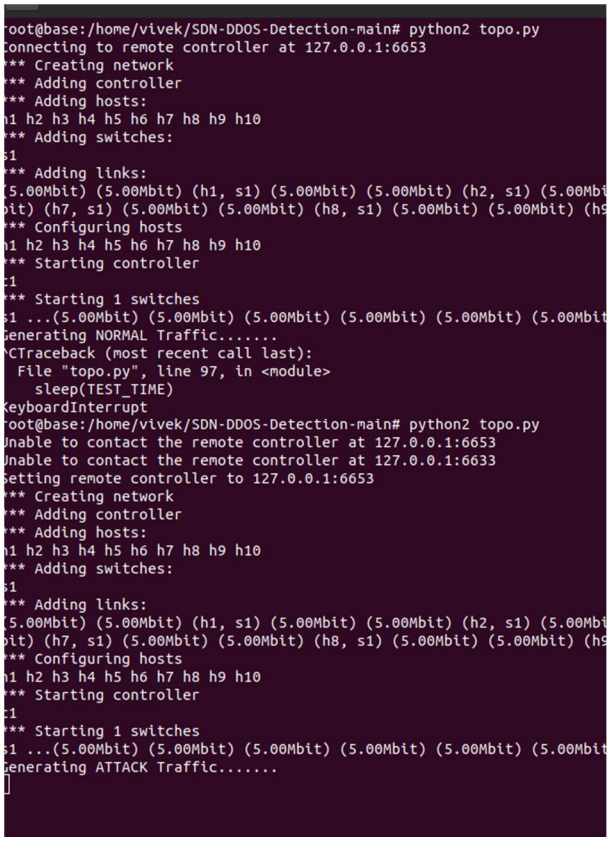
IV. EXPERIMENTAL ANALYSIS AND RESULTS

The results of this detects and mitigates the attacker generated traffic which is DDos attack. We generate normal traffic and attacked traffic and detect which is normal and which is from attacker. To do this we train the IDS module using SVM algorithm using machine learning. Some of the results are mentioned in the below diagrams how we analyzed the attacker traffic using SDN and Machine learning.

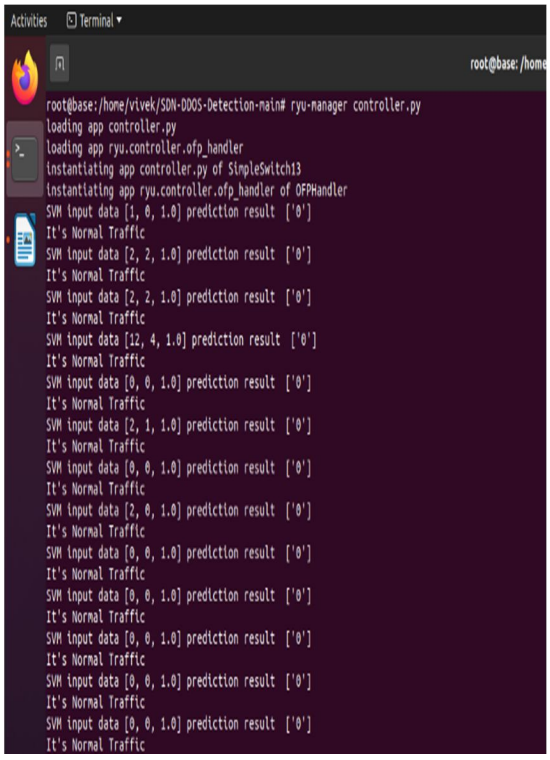
Topology is created for normal mode and it is generating the network traffic.



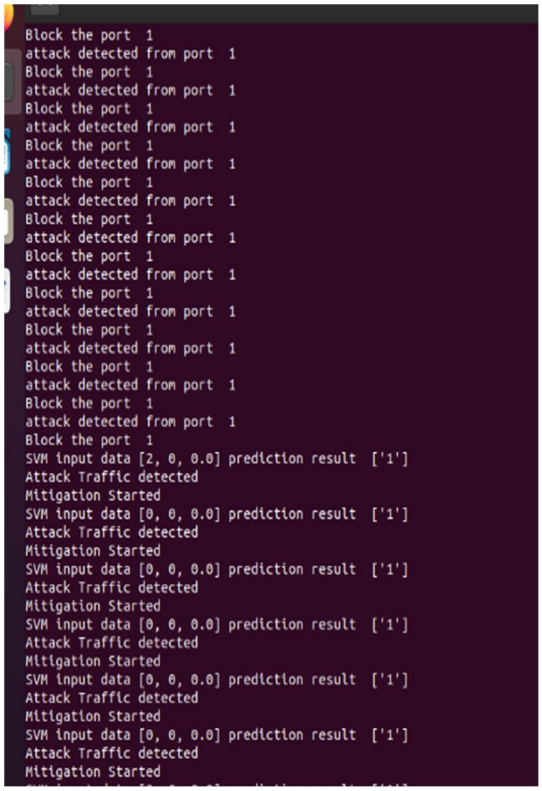
Topology is created for attacker mode and it is generating the network traffic.



The normal network traffic is generated and SVM model is predicting it as normal network traffic



From attacker side network traffic is generated and SVM model is predicting it as attacker generated traffic and sends alert message to block the port.



After getting the alert message from intrusion detection system (IDS) module, Intrusion prevention system which is in application layer of SDN will block the IP of the attacker host.

V. CONCLUSION

This offered a machine learning (ML) model able to automatically detect and mitigate DDoS assaults in SDN networks. The model captures the original flow characteristics from the traffic flow entries from the switches, then expands them by including new features. A detection module uses four criteria to categorise each flow as either normal or anomalous. The attack's source is prevented as soon as it is identified. SVM ML method was assessed in relation to the classification ML algorithm utilised in the detection module.

Results from our trial indicated 98.77% precision. Without disrupting regular traffic, our methodology proved effective at swiftly and correctly identifying and thwarting threats.

A. Future Enhancements

We want to train and evaluate our algorithms using real network traffic datasets with additional assaults as part of our ongoing research. Additionally, we want to research fresh categorization approaches and evaluate them against our chosen ML algorithms. Additionally, we want to employ fresh mitigating techniques. Finally, in order to improve the system's accuracy and performance, we will look for more flow features.

REFERENCES

[1] S. Kaur, K. Kumar and N. Aggarwal, "Analysis of DDoS Attacks in Software Defined Networking," 2022 IEEE Delhi Section Conference (DELCON), 2022, pp. 1-6, doi: 10.1109/DELCON54057.2022.9753224.

[2] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj and P. Chinnasamy, "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402517.

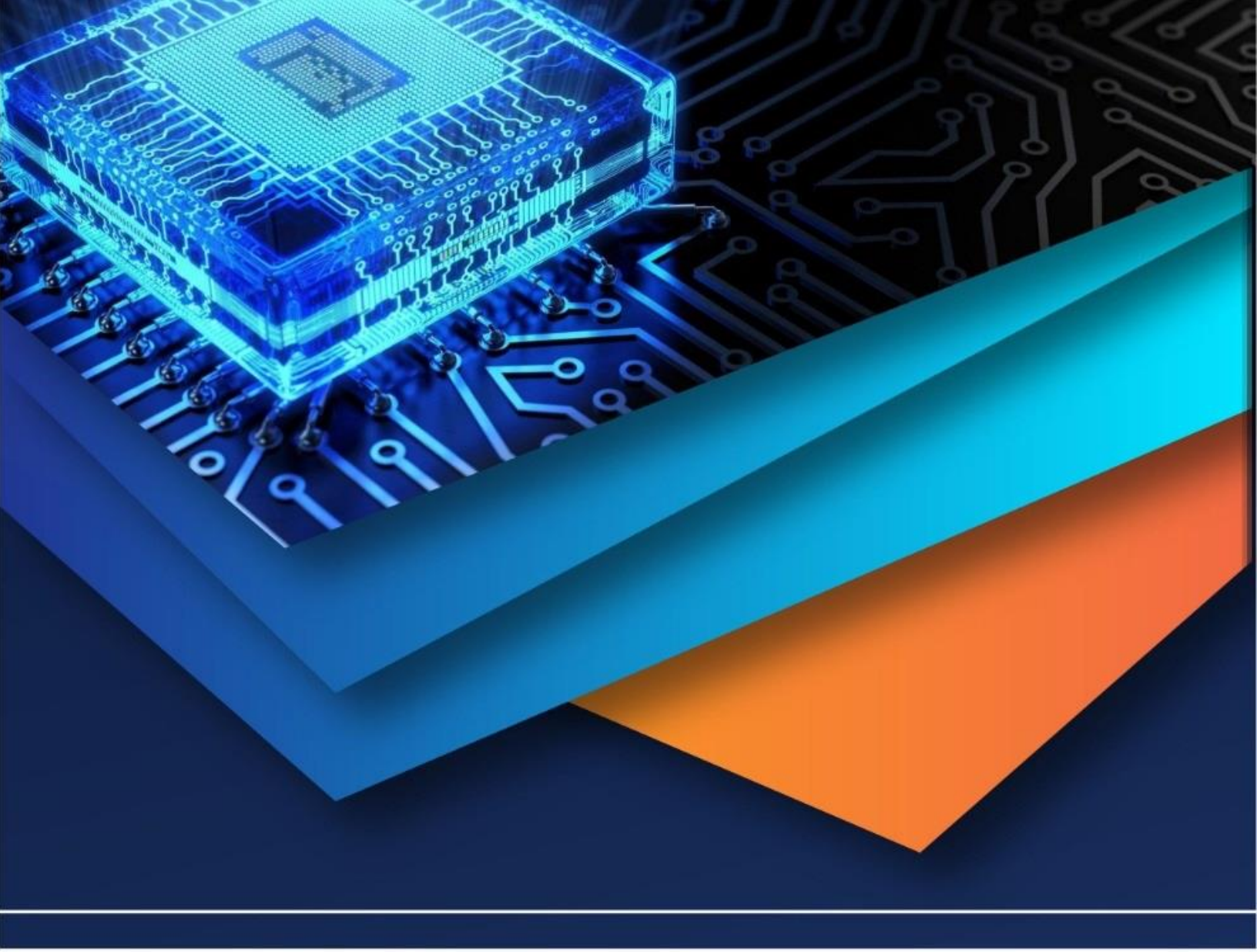
[3] J. K. Chahal, P. Kaur and A. Sharma, "Distributed Denial of Service (DDoS) Attacks in Software-defined Networks (SDN)," 2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), 2021, pp. 291-295, doi: 10.1109/ICEECCOT52851.2021.9708012.

[4] N. M. Yungaicela-Naula, C. Vargas-Rosales and J. A. Perez-Diaz, "SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning," in IEEE Access, vol. 9, pp. 108495-108512, 2021, doi: 10.1109/ACCESS.2021.3101650.

[5] Y. Zhou, G. Cheng and S. Yu, "An SDN-Enabled Proactive Defense Framework for DDoS Mitigation in IoT Networks," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 5366-5380, 2021, doi: 10.1109/TIFS.2021.3127009.

[6] B. Nugraha and R. N. Murthy, "Deep Learning-based Slow DDoS Attack Detection in SDN-based Networks," 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2020, pp. 51-56, doi: 10.1109/NFV-SDN50289.2020.9289894.

[7] J. A. Pérez-Díaz, I. A. Valdovinos, K. -K. R. Choo and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," in IEEE Access, vol. 8, pp. 155859-155872, 2020, doi: 10.1109/ACCESS.2020.3019330.
[8] H. A. Alamri and V. Thayananthan, "Bandwidth Control Mechanism and Extreme Gradient Boosting Algorithm for Protecting Software-Defined Networks Against DDoS Attacks," in IEEE Access, vol. 8, pp. 194269-194288, 2020, doi: 10.1109/ACCESS.2020.3033942.
[9] S. Ali, M. K. Alvi, S. Faizullah, M. A. Khan, A. Alshanqiti and I. Khan, "Detecting DDoS Attack on SDN Due to Vulnerabilities in OpenFlow," 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), 2020, pp. 1-6, doi: 10.1109/AECT47998.2020.9194211.
[10] M. V. O. De Assis, A. H. Hamamoto, T. Abrão and M. L. Proença, "A Game Theoretical Based System Using Holt-Winters and Genetic Algorithm With Fuzzy Logic for DoS/DDoS Mitigation on SDN Networks," in IEEE Access, vol. 5, pp. 9485-9496, 2017, doi: 10.1109/ACCESS.2017.2702341.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY