# DETECTION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS IN SDN USING MACHINE LEARNING TECHNIQUES

V.Balu
Assistant Professor of Computer Science and Engineering
SCSVMV
Kanchipuram,Enathur

M RAKESH REDDY
Computer Science Engineering
SCSVMV
Kanchipuram,Enathur

PV ABHI RAM
Computer Science Engineering
SCSVMV
Kanchipuram,Enathur

***Abstract*—The term "software-defined network" (SDN) refers to a network architecture that is used to digitally construct and create hardware components. The network connection settings can be changed dynamically. Because the link is fixed in the traditional network, dynamic change is not possible. SDN is a wonderful strategy, but DDoS attacks 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 attack is when several systems work together to simultaneously target a certain host. In SDN, the infrastructure layer's devices are controlled by software from the control layer, which sits in the middle of the application and infrastructure layers. We suggest a machine learning method called Decision Tree in this research to identify malicious communications. The results of our test indicate that the Decision Tree can determine if an attack is safe or not.**

**Keywords—** Attacks, DDoS, Decision Tree SDN.

## 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. DDoS attacks are made successful by utilising several compromised computer systems as sources of attack traffic. Computers, other networked resources, and IoT devices can all be misused. From a distance, a DDoS assault resembles an unexpected traffic jam that blocks the road and prevents ordinary traffic from reaching its destination.. Networks of connected computers are used to carry out DDoS attacks.

## II. PROBLEM STATEMENT

We suggest this application, which can be seen as a valuable system because it aids in removing the constraints brought about by conventional and other existing ways. The goal of this study is to create an efficient and dependable approach for precisely detecting DDoS effects. We used a potent algorithm in a Python-based framework to design this system.

## III. LITERATURE SURVEY

Since decades, the Distributed Denial of Service (DDoS) assault has significantly decreased network availability, and there is still no reliable solution against it. Yet the newly developed Software Defined Networking (SDN) offers a fresh perspective on how to rethink the security against DDoS attacks. In this work, we suggest two approaches for spotting DDoS attacks in SDN.

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 rarely detected by conventional firewalls.

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. Thus, a reliable approach for identifying DDoS

attacks from large amounts of data traffic must be proposed.

A new and promising networking technology called Software Defined Networking (SDN) separates the data and control planes and has centralised control over the network. With this new method, lower-level functionality is abstracted, enabling network managers to programmatically initiate, control, alter, and manage network behaviour.

According to the proposal of "Khushab uA.bokde,Tisksha P.Kakade," the major goal is to categorise the clustered crimes depending on how frequently they occur over time.

## IV. PROPOSED SYSTEM

We present an application that may be considered a valuable system since it helps to reduce the constraints gained from traditional and other existing methods. The goal of this study is to create an efficient and dependable approach for precisely detecting DDoS effects. We used a potent algorithm in a Python-based framework to design this system.

By combining several graphs, such as bar graphs, line graphs, heap maps, etc., visualisation can be done..

## V.ARCHITECTURE

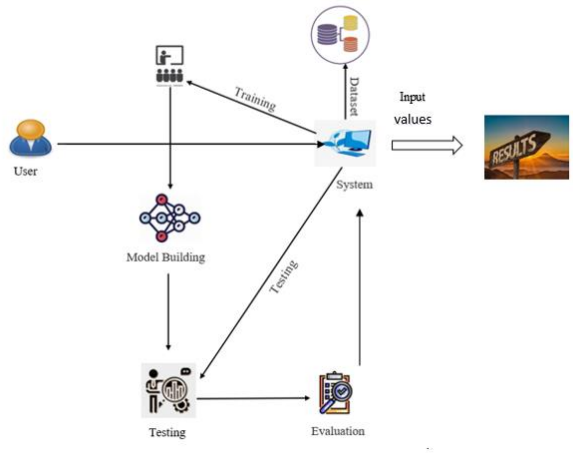


Fig 1 – System Architecture

Above shown diagram is the system architecture that clearly depicts every module of our system. The issue is created, and the National Crime Records Bureau of India is consulted for the necessary information. The collected data is then preprocessed, cleaned, wrangled, munged, and nan values are removed. This data is analysed in accordance with many features of crime patterns, including clustering states and districts based on crime intensity, future crime ratio projections, comparative crime analysis at the district level, etc. A dynamic webpage displays all of the forecasts.

- Problem Identification : visualisation of crime data to forecast crime rates and severity in various regions of the nation based on India's criminal histories from the previous year.
- Data Acquisition : data collection from the National Crime Records Bureau (NCRB), Open Government Data, and Census India official government websites.

- Data Cleaning and Preprocessing :
  - Eliminating redundant values,
  - Handling missing/NA values,
  - Data transformation

- Exploratory Data Analysis :

Future Crime Rate Prediction: This architectural module would forecast crime trends for the next four years.

State-level Comparison Analysis: This module will give comparative observations for all user types, including comparisons by region and by crime type.

Visualizations: This module is for visualising comparison data in order to make the study process simpler and more engaging for users.

- Model : This section displays the entire system model, including every subsection and functional algorithm.
- Deploy : Users can readily access the website to analyse and verify the predictions for various regions and crimes now that the system has been installed.

We only have information about crimes that are known to have occurred, thus by using this method, we may determine the pattern of crime in a specific location. As a result, a classification method that relies on already solved crimes and existing methodologies will not provide accurate predictions of future crimes. Also, the nature of crimes fluctuates, thus clustering algorithms perform better to be able to identify novel and undiscovered patterns in the future..

## VI.CONCLUSION

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

## 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. 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. 7, 80813- 80828.

[3] G u, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semisupervised K-means DDoS detection method using hybrid feature selection algorithm.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).

[5] 15th International Symposium on Pervasive Systems, Algorithms and Networks 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).