Smart DDoS Detection and Mitigation Using Machine Learning in Software-Defined Networks

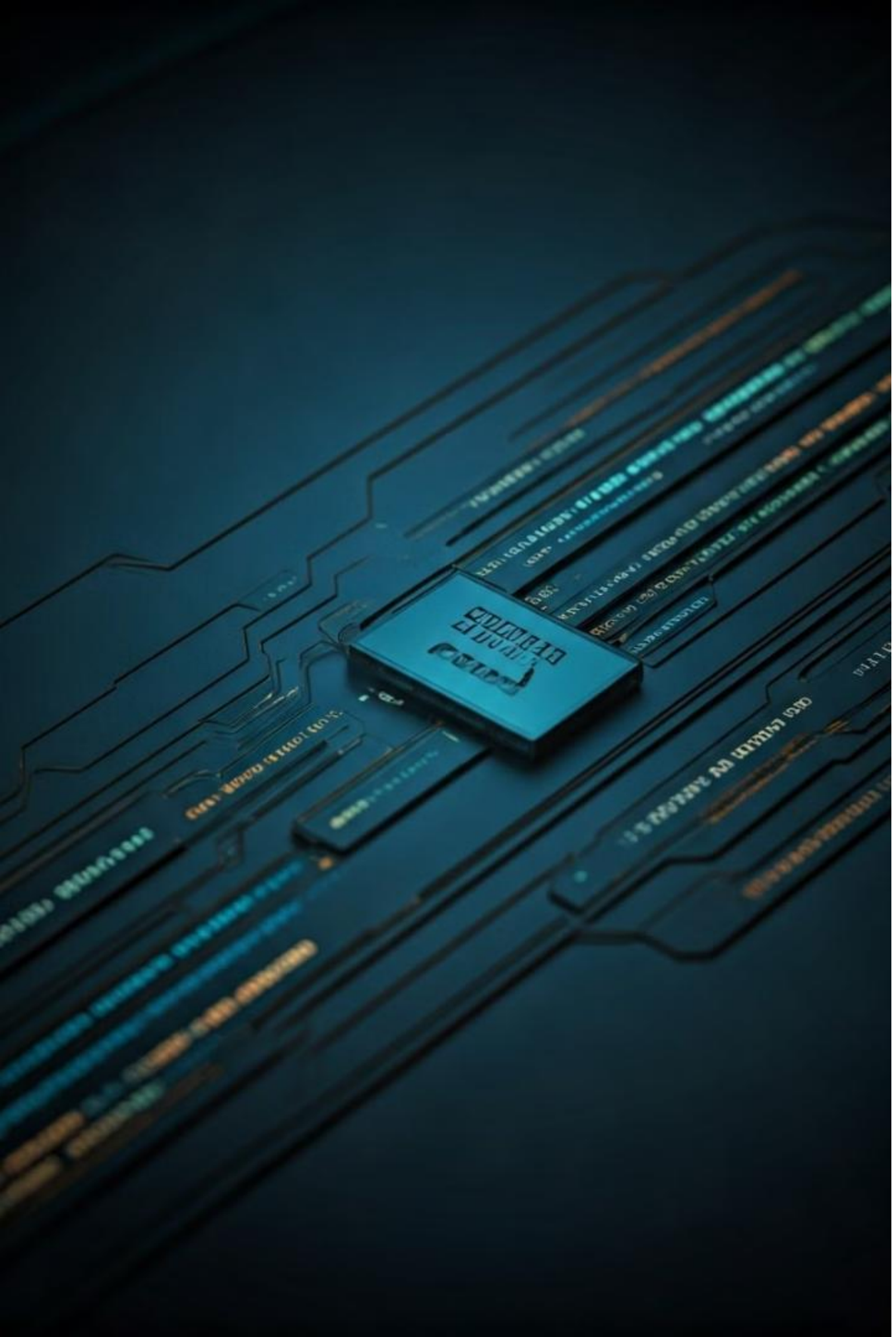
KISHORE KUMAR I

Electronics and Communication Engineering / Third year

R.M.K ENGINEERING COLLEGE

INTRODUCTION

- In today’s network environments, Distributed Denial of Service (DDoS) attacks pose a serious threat by flooding systems with unwanted traffic, causing them to slow down or crash.
- This project focuses on creating a system that can automatically detect and stop DDoS attacks in real-time within Software-Defined Networks (SDNs).
- The system collects data from incoming network traffic and uses machine learning to analyze this data to check for signs of a DDoS attack.
- It is implemented by monitoring and collecting traffic data, then extracting key features to store in a dataset. A machine learning model predicts whether the traffic is normal or an attack. If an attack is detected, the system takes action by dropping harmful packets, blocking ports and sending alerts.
- Thus it provides a simple, effective solution for detecting and mitigating DDoS attacks, ensuring smooth and secure network performance.



MODULES AND TECHNOLOGY STACK

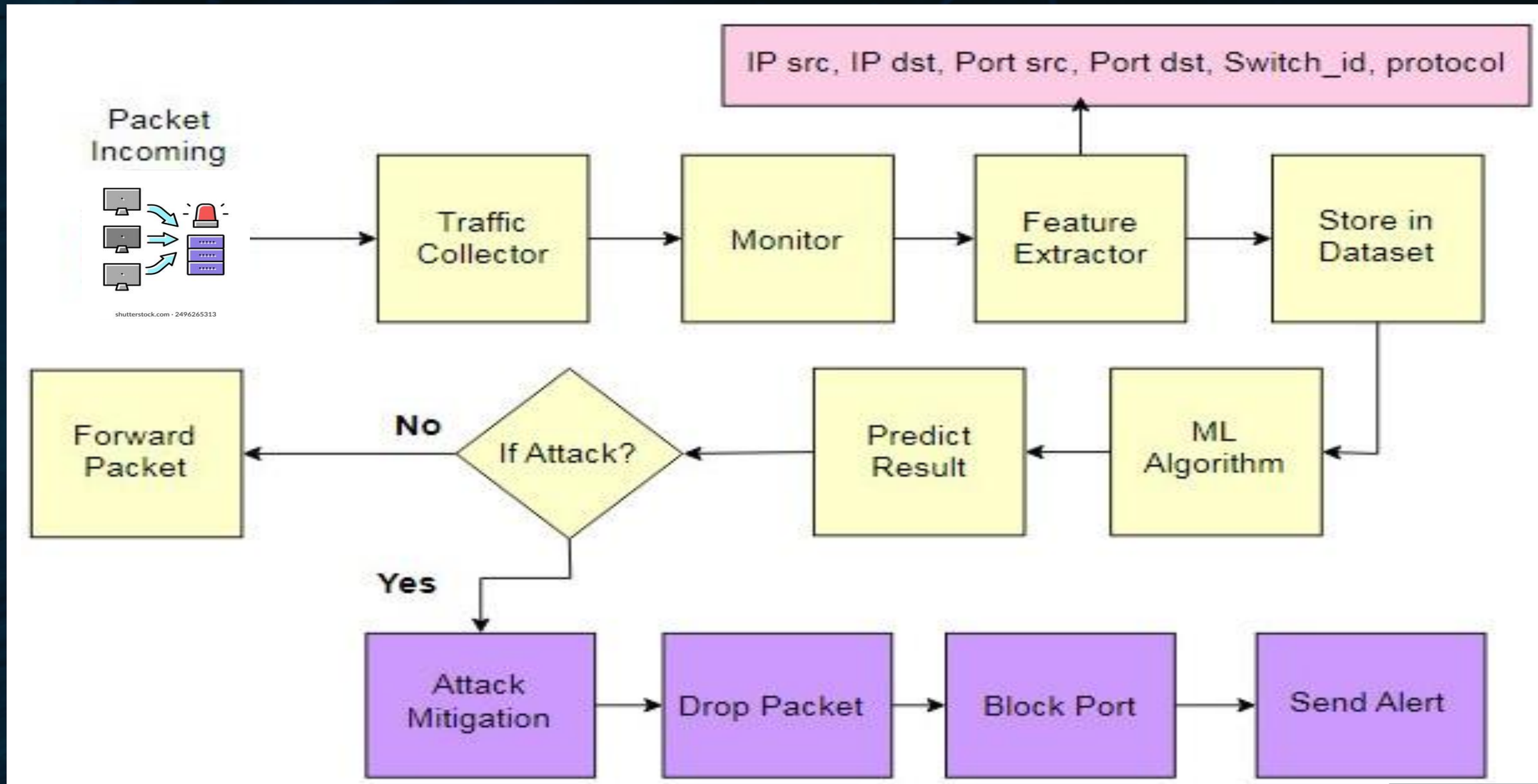
Development Tools :

- Ubuntu 20.04 OS
- OpenFlow Protocol for SDN
- Ryu controller – Python Based

Simulation Tools :

- Mininet
- Hping3
- Iperf

WORK FLOW


IP src, IP dst, Port src, Port dst, Switch_id, protocol
Packet Incoming
shutterstock.com · 2496265313
Traffic Collector
Monitor
Feature Extractor
Store in Dataset
Forward Packet
No
If Attack?
Predict Result
ML Algorithm
Yes
Attack Mitigation
Drop Packet
Block Port
Send Alert

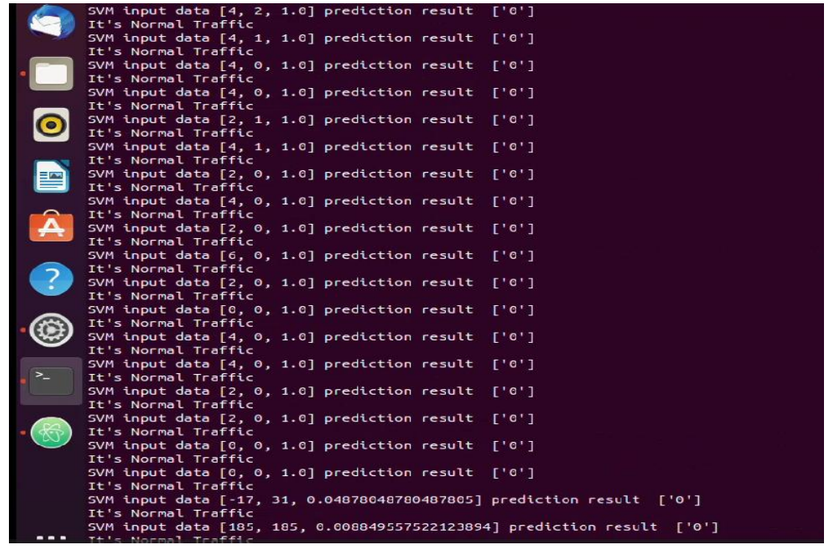
METHODOLOGY

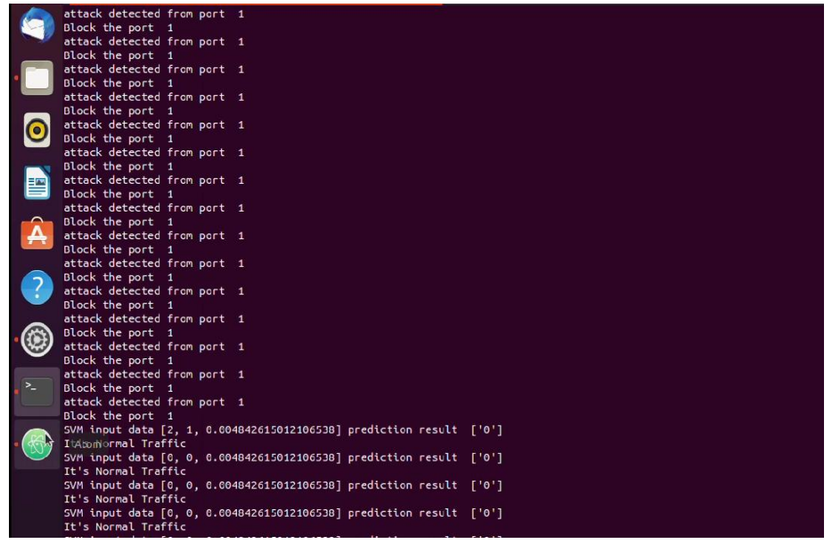
1. It starts with system design, where key components like packet monitoring, traffic collection, feature extraction, machine learning, and attack prevention methods are planned. After that, data collection takes place using tools like Open Flow Switch to capture both normal network traffic and DDoS attack patterns.

2. Next is feature extraction, where the IP addresses, ports, and protocols are gathered and organized into a dataset. Then, in the model development phase, machine learning algorithms like SVM or Decision Tree are used to analyze the data. The data is split into training and testing sets so the model can learn to recognize DDoS attacks.

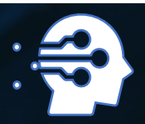
3. Finally, it is added to the system for real-time monitoring, allowing it to continuously analyze incoming traffic and detect DDoS attacks. If an attack is detected, the system takes action by blocking harmful packets or closing vulnerable ports also send the alert to the network security management .

```
singh@ubuntu:~/Final codes$ ryu-manager controller.py
loading app controller.py
loading app ryu.controller.ofp_handler
instantiating app controller.py of SimpleSwitch13
instantiating app ryu.controller.ofp_handler of OFPHandler
SVM input data [1, 0, 1.0] prediction result  ['0']
It's Normal Traffic
SVM input data [172, 172, 0.0] prediction result  ['0']
It's Normal Traffic
SVM input data [186, 186, 0.0] prediction result  ['0']
It's Normal Traffic
SVM input data [185, 185, 0.0] prediction result  ['0']
It's Normal Traffic
SVM input data [172, 172, 0.0] prediction result  ['0']
It's Normal Traffic
SVM input data [67, 67, 0.0] prediction result  ['1']
Attack Traffic detected
Mitigation Started
attack detected from port  2
Block the port  2
attack detected from port  2
Block the port  2
attack detected from port  2
Block the port  2
attack detected from port  2
Block the port  2
attack detected from port  2
Block the port  2
attack detected from port  2
Block the port  2
attack detected from port  2
Block the port  2
attack detected from port  2
Block the port  2
attack detected from port  2
```





USE CASES AND BENEFITS

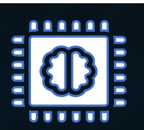


Dynamic Traffic Steering

- This system protects various sectors, including businesses, cloud services, online stores, banks, telecom companies, and government agencies, from DDoS attacks.

Adaptive Mitigation

- The system adapts to evolving attack techniques by continuously learning from new attack patterns and updating mitigation policies.



Reduced Downtime and Cost Efficiency

- By effectively blocking DDoS attacks, the system keeps services running smoothly, minimizing downtime and the financial losses that come with it.

Real-Time Threat Detection

- With its ability to detect DDoS attacks in real time, It enables immediate action, significantly minimizing the impact of attacks and ensuring network resilience etc ..,

FUTURE DEVELOPMENT

1. **Integration with Advanced AI Models:**

Implement more sophisticated machine learning algorithms like deep learning for enhanced attack detection accuracy.

2. **Cross-Validate Across Multiple Datasets:**

Perform cross-validation on diverse datasets to ensure the robustness and generalization of the model across different scenarios.

3. **User-friendly Interface:**

Develop a graphical user interface (GUI) for easier network monitoring and attack mitigation management.

CONCLUSION

- This project uses Software Defined Networking (SDN) to detect and mitigation DDoS attacks.
- Once the system is set up, the SDN Controller automatically handles the detection and prevention of attacks.
- If someone tries to flood the network with traffic, like through port scanning, the system detects it and blocks the attack.
- The OpenFlow (OF) Switches play a key role by dropping harmful packets based on traffic rules.
- Overall, this solution provides a simple and effective way to improve network security and protect against DDoS threats.