21AIE302 ADVANCED COMPUTER NETWORKS

IMPLEMENTATION OF FIREWALL IN SDN NETWORKS USING MACHINE LEARNING

THE TEAM

GROUP 14

Sai Varun

amenu4aie21120@am.students.amrita.edu

Mohit Yadav

amenu4aie21128@am.students.amrita.edu

Shiva Shankara

amenu4aie21122@am.students.amrita.edu

Sai Nikhil M

amenu4aie21142@am.students.amrita.edu

PROBLEM STATEMENT

Create a firewall to enhance network security by swiftly identifying and blocking malicious IP addresses using advanced threat intelligence and behavior analysis. Implement predictive capabilities for rerouting suspicious IPs, utilize machine learning for continuous improvement, refining our defense against evolving cyber threats.

ABSTRACT

This abstract presents a novel approach to network communication using Software Defined Networking (SDN) and a machine-learning-based firewall. The goal is to enhance network security by integrating a firewall using the K-Nearest Neighbors (KNN) algorithm within the SDN system. The approach was tested on the RYU SDN controller in a basic setup, aiming to simplify network management and improve security.

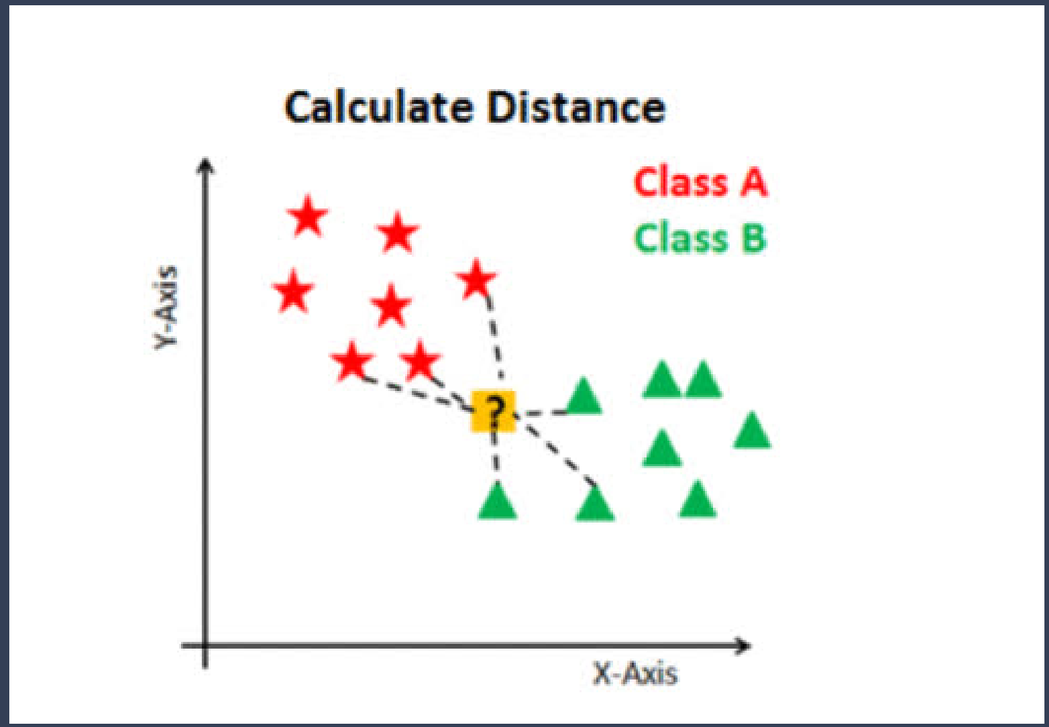
BRIEF EXPLANATION OF THE PROJECT

The project aims to create an effective machine learning-based firewall that can classify IPs with malicious intent and prevent the entry of packets from these sources into the network. The use of KNN and validation processes ensures the reliability of the model in identifying and blocking malicious traffic. The project employs Mininet for simulating SDN networks and evaluates its methodology through simulation results. The primary objective is to block or drop packets from malicious hosts, identified based on their IP addresses. The approach involves using the K-Nearest Neighbors (KNN) algorithm to classify IPs as malicious (0) or non-malicious (1).

KNN

- A supervised-classification Algorithm which works on the nearest neighbour policy and labels the data based on the nearest neighbours of the data

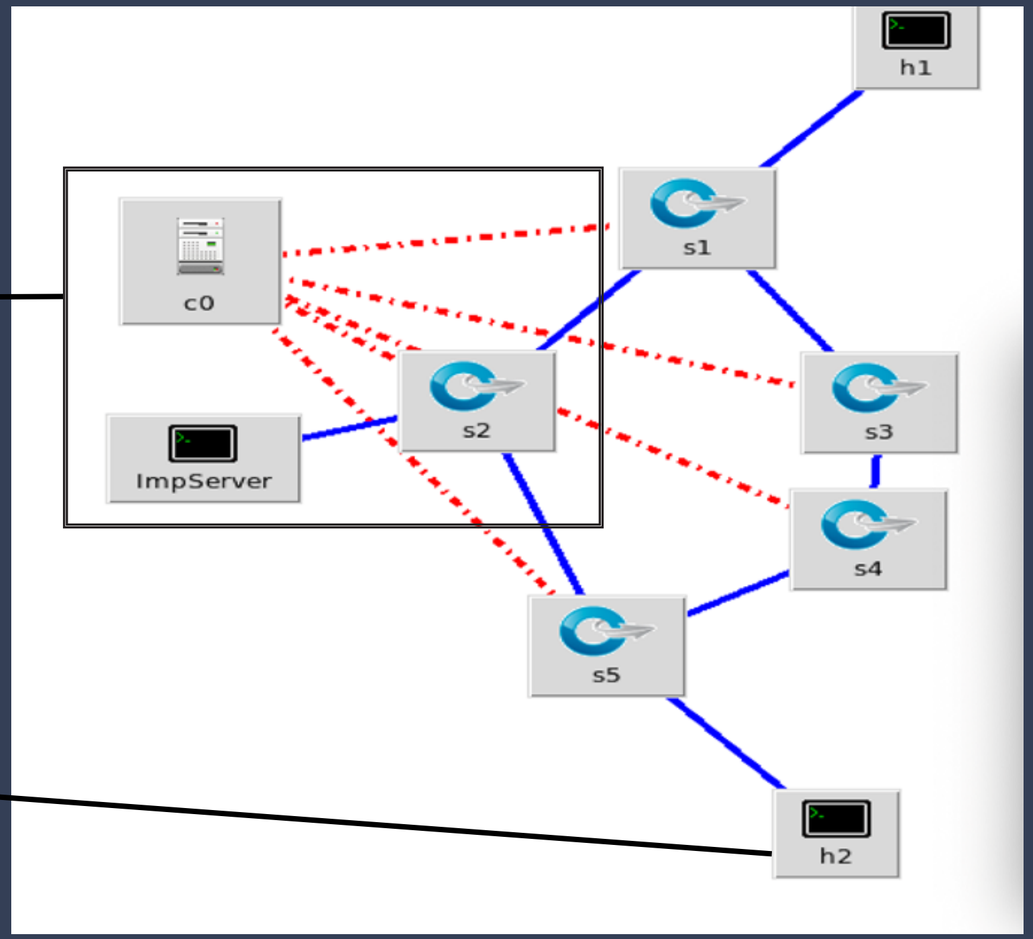
- The data used here is IP address and they have been converted into a 32 bit unique integer using the “IPaddress” module in python.

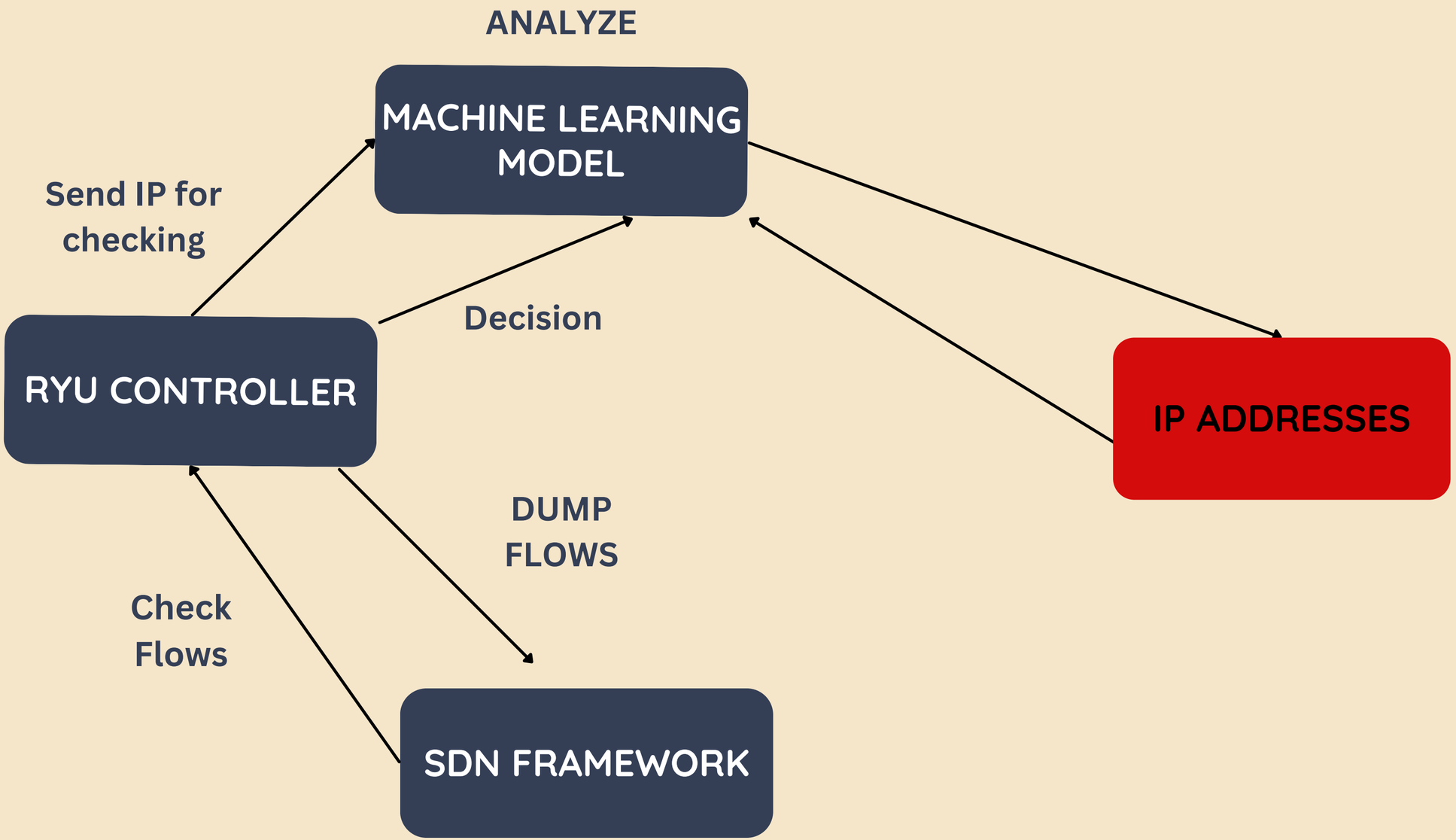


TOPOLOGY USED

SECURED SERVER AREA

Here we could see that there are two paths to H2 where multipath-routing has been enabled but one part is more vulnerable to attacks than the other.




ANALYZE
MACHINE LEARNING MODEL
Send IP for checking
Decision
RYU CONTROLLER
IP ADDRESSES
DUMP FLOWS
Check Flows
SDN FRAMEWORK

Project Timeline

4 Jan 2024

Researching various papers and selection of topics.

11 Jan 2024

Research for various ML models and controllers which will fit our project

15 Jan 2024

Developing ML Model

21 Jan 2024

Integrating the ML Model with SDN controller

23 Jan 2024

Testing and Reviewing the final revision.

Member Contributions

A Sai Varun
installation of paths between specified source and destination

B Shiva Shankara
Building Topology and KNN model

G Mohit yadav
Adding flows handling incoming packets

M Sai Nikhil
Testing code for RYU controller and finding optimal paths

ACCOMPLISHMENTS

- INNOVATIVE APPROACH TO NETWORK SECURITY
- MALICIOUS PACKET DETECTION USING KNN
- EFFICIENT IP CLASSIFICATION AND GENERALIZATION
- SIMULATION USING MININET AND VALIDATION
- OPTIMAL PATH DETECTION FOR THE PACKETS

THANK YOU