Synopsis: AI-Powered Intrusion Detection System for Cloud Networks

Name-Harsh Sandesh Kathe

Class-MSc IT(Part 2)

Seat no.31031424015

1. Introduction

With the rapid adoption of cloud computing, cyber threats have become more sophisticated and harder to detect using traditional security mechanisms. Intrusion Detection Systems (IDS) play a crucial role in monitoring and identifying malicious activities within networks. However, conventional IDS solutions often struggle with high false alarm rates and poor adaptability to evolving attack patterns. This research aims to develop an AI-powered intrusion detection system that leverages machine learning algorithms to automatically detect and classify network intrusions in cloud environments with high accuracy and minimal false positives.

2. Objectives

- To analyze existing IDS techniques and identify their limitations in cloud-based infrastructures.
- To design and implement a machine learning-based IDS for real-time detection of network intrusions.
- To compare performance metrics such as accuracy, precision, recall, and F1-score across different ML algorithms.
- To deploy and test the system using benchmark intrusion datasets such as CICIDS2017 and NSL-KDD.

3. Methodology

The project will follow the following approach:

1. Data Collection & Preprocessing:
   - CICIDS2017 Dataset: https://www.unb.ca/cic/datasets/ids-2017.html
   - NSL-KDD Dataset: https://www.unb.ca/cic/datasets/nsl.html
   Data will be cleaned, normalized, and key features extracted for analysis.
2. Model Training: Implement and train models like Random Forest, Decision Tree, SVM, and Neural Networks using Python (Scikit-learn, TensorFlow).
3. Model Evaluation: Evaluate models using metrics such as accuracy, precision, recall, and F1-score.

4. System Implementation: Integrate the best-performing model into a simulated cloud environment (using tools like Wireshark or CloudSim).
5. Visualization: Develop a dashboard to monitor network activity and visualize detected anomalies.

4. Expected Outcome

A prototype IDS capable of detecting various types of network intrusions in real time, with improved detection accuracy compared to traditional systems. The system will demonstrate how AI can strengthen cloud network security through intelligent automation.

5. Tools & Technologies

Programming: Python
Libraries: Scikit-learn, TensorFlow, Pandas, NumPy
Simulation Tools: Wireshark, CloudSim
Datasets:

- CICIDS2017 (https://www.unb.ca/cic/datasets/ids-2017.html),
- NSL-KDD (https://www.unb.ca/cic/datasets/nsl.html)