NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY

School of Electrical Engineering and Computer Sciences

Data Structures & Algorithms – CS – 250

Project Proposal

Title of the Project:
AI – Intrusion Prevention and Detection System

SUBMITTED TO: **Dr. Ayesha Hakim**

SUBMITTED BY: (Name + CMS ID)

1. **Samrah Mumtaz 502346**
2. **Nabiha Adnan 507288**

CLASS + SECTION: CS-14 A

Date of Submission: 14/11/2025

Problem Statement:

Today, networks face many types of cyberattacks, and it’s getting harder for traditional security tools to catch everything. Attack patterns change quickly, so relying only on fixed rules or signatures isn’t enough. Our project aims to solve this problem by creating an IDPS that uses AI to detect suspicious traffic and help prevent attacks. The goal is to make a system that can understand patterns from real network data and identify threats more accurately.

Problem Description:

Our system will work in two ways. First, we will use offline datasets (like NSL-KDD or captured pcap files) to train and test our model. This lets us experiment safely and understand the patterns of normal and malicious traffic.

Second, we will add live traffic capturing, where we collect packets from our own device using tools like Wireshark/tshark or Python’s scapy. These packets will be analyzed in real-time. If the system detects something suspicious, it will generate an alert and simulate a prevention action (such as blocking an IP). This helps us show how an actual IDPS would behave.

Chosen Data Structures and Algorithms:

We are using simple and efficient data structures to manage network data.

- Queues will hold live packets temporarily before they are processed.
- Hash tables will store known suspicious IPs or patterns for fast checking.
- Lists/arrays will be used to store features from each packet.

For detection, we will use basic AI/ML algorithms like Decision Trees, k-NN, and Naive Bayes to classify traffic as normal or malicious. We may also use simple pattern matching for known attacks.

The system’s workflow is:
Capture packets → extract features → classify using AI → alert or simulate prevention.

Conclusion:

By combining AI with basic data structures and both offline and live data, our project will create a simple but effective IDPS that can detect threats and demonstrate how prevention works. This serves as a clear starting point for building a more advanced real-time security system in the future.