PUNJAB UNIVERSITY COLLEGE OF INFORMATION TECHNOLOGY LAHORE

INFORMATION SECURITY

PROJECT PROPOSAL

DDoS Attack Detection System

SUBMITTED BY:

Muhammad Mujeeb

BITF22M024

1. Idea

The project aims to design and develop a real-time **DDoS (Distributed Denial of Service) detection and mitigation system** capable of identifying abnormal traffic patterns and automatically blocking potential attacks before they impact the network or service availability.

The core concept is to **continuously monitor incoming network traffic**, detect unusual spikes or anomalies that indicate a DDoS attempt, and then **execute automated mitigation steps** such as blocking attacker IPs or throttling their requests.

2. Scope

Real-time **traffic monitoring** using packet sniffing libraries such as **Scapy**, **socket**, or **pcapy**.

- **Traffic analysis** to identify anomalies such as:
    - Sudden increase in request rate.
    - Repeated requests from same IPs.
    - Abnormal packet sizes or SYN flood patterns.
- **Detection algorithms**, using:
    - Threshold-based methods (simple, rule-based approach).
    - Optionally, a lightweight ML classifier (like logistic regression or random forest) for improved accuracy.
- **Mitigation mechanism** that:
    - Automatically blocks malicious IPs using **iptables**, **firewall-cmd**, or a simulated blocking module.
    - Logs all blocking events for monitoring and analysis.
- **Visualization or logging interface** for real-time status of network traffic, detection alerts, and mitigation actions.

3. Deliverables

The following components will be developed and submitted:

1. **Traffic Capture Module**
2. **Detection Engine**
3. **Mitigation Module**
4. **Monitoring Dashboard / CLI Interface**
5. **Project Documentation and Demo**