Domain: Systems and Software Security

Problem Statement: DDoS Mitigation System

Description

Develop a machine learning based DDoS mitigation system capable of distinguishing legitimate traffic spikes from malicious floods, providing adaptive and automated defenses against hyper volumetric attacks.

Exact Deliverables

- Traffic shaping proxy implementation with fast BPF filters and auto signature generation.
- ML-based anomaly detection module to differentiate real traffic surges from attacks.
- Simulation framework to test floods and chart mitigation latency vs. packet-rate peaks.
- Comparative benchmarking report vs. traditional appliance-based solutions.

Relevance

DDoS attacks are surging in scale and complexity. Cloudflare reported 5.6 Tbps attacks in late 2024, and by 2025 attacks reached 6.5–7.3 Tbps+, with year-on-year increases of 358%. IoT botnets and hyper-volumetric attacks are stressful legacy appliances beyond capacity.

For India, where digital financial infrastructure (UPI, banks), e-governance platforms, and telecoms form national backbones, DDoS resilience is a critical requirement. Globally, automated and anycast-enabled mitigation is a necessity for ensuring uninterrupted digital services.

Business Case

A DDoS mitigation framework built by students could evolve into enterprise-ready systems that serve ISPs, data centers, cloud providers, and government CERTs. These systems would reduce downtime, prevent reputational damage, and safeguard critical services like banking and e-commerce.

Commercially, adaptive DDoS defense systems can be offered as cloud SaaS solutions, modular proxies, or integrated into national-level internet exchange defenses. The demand is massive, and India can contribute to this global challenge by innovating locally.

Dataset(s)/Benchmarks

CICDDoS2019 dataset, CAIDA Anonymized Internet Traces, UNSW-NB15 Network Dataset, DDoS-DB 2020, DARPA Intrusion Detection Dataset

Milestones, Evolution Parameters

- Phase 1: Implement baseline traffic anomaly detection.
- Phase 2: Add ML-based classification for attack vs. legitimate surges.
- Phase 3: Deploy traffic shaping proxy and validate on large, simulated floods.

Additional Information

- Focus on real-time mitigation capabilities.
- Lightweight ML models are preferred to ensure high speed packet filtering.
- Prototypes should be benchmarked against attack scales relevant to India’s internet exchanges.