FINAL PROJECT REPORT

Real-Time DDoS Mitigation System using Machine Learning and eBPF/XDP

FINAL REVIEW

Project Type: Major Project
Semester: VIII
Academic Year: 2025-2026

Submitted by:
[Your Name]
[Roll Number]
[Department]

Under the Guidance of:
[Guide Name]
[Designation]

[Your College Name]
[University Name]
[Month, Year]

CERTIFICATE

This is to certify that the project entitled **"Real-Time DDoS Mitigation System using Machine Learning and eBPF/XDP"** is a bonafide work carried out by **[Student Name]** in partial fulfillment of the requirements for the award of **Bachelor of Technology** in **Computer Science and Engineering** at **[College Name]** during the academic year **2025-2026**.

Project Guide:
[Name]
[Designation]

Head of Department:
[Name]
Professor & Head
Department of Computer Science and Engineering

External Examiner:
[Name]

DECLARATION

I hereby declare that the project work entitled **"Real-Time DDoS Mitigation System using Machine Learning and eBPF/XDP"** submitted to **[College Name]** is a record of original work done by me under the guidance of **[Guide Name]**, and this project work has not been submitted elsewhere for the award of any degree or diploma.

Place:
Date:

Signature of Student
[Your Name]
[Roll Number]

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my project guide **[Guide Name]** for their invaluable guidance, continuous support, and encouragement throughout this project. Their expertise in network security and machine learning has been instrumental in shaping this work.

I am grateful to **[HoD Name]**, Head of the Department of Computer Science and Engineering, for providing the necessary facilities and resources to complete this project.

I extend my thanks to all faculty members and lab staff who supported me during the implementation and testing phases.

Finally, I thank my family and friends for their constant support and motivation.

[Your Name]

ABSTRACT

Distributed Denial of Service (DDoS) attacks pose a critical threat to modern network infrastructure, causing service disruptions and financial losses. Traditional mitigation approaches suffer from high latency, limited scalability, and inability to distinguish legitimate traffic surges from malicious attacks.

This project presents a **real-time DDoS mitigation system** that combines **lightweight machine learning models** with **eBPF/XDP-based packet filtering** to achieve high-speed threat detection and mitigation. The system operates at the kernel level using Extended Berkeley Packet Filter (eBPF) and eXpress Data Path (XDP) for ultra-fast packet processing, while employing a Random Forest classifier trained on the CIC-DDoS-2019 dataset for intelligent attack classification.

The proposed hybrid detection mechanism integrates statistical anomaly detection with machine learning inference, achieving detection latency under 1 second while maintaining throughput exceeding 5 million packets per second. The system was implemented on Linux (Ubuntu 22.04, Kernel 5.15+) and evaluated against multiple attack scenarios including SYN floods, UDP floods, and DrDoS attacks.

Experimental results demonstrate:

- Detection accuracy: 95.3%
- Packet processing latency: <1 microsecond (kernel level)

- ML inference time: <10 milliseconds
- False positive rate: <2%
- CPU overhead: <20% at 5M pps

The system successfully mitigates volumetric attacks while preserving legitimate traffic, offering a practical solution for real-world deployment in enterprise networks and cloud infrastructure.

Keywords: DDoS Mitigation, eBPF, XDP, Machine Learning, Random Forest, Network Security, Anomaly Detection

---

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Full Form
DDoS	Distributed Denial of Service
eBPF	Extended Berkeley Packet Filter
XDP	eXpress Data Path
ML	Machine Learning
NIC	Network Interface Card
PPS	Packets Per Second
BPS	Bytes Per Second
BCC	BPF Compiler Collection
TCP	Transmission Control Protocol

Abbreviation	Full Form
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
HTTP	Hypertext Transfer Protocol
DrDoS	Distributed Reflection Denial of Service
DNS	Domain Name System
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
SYN	Synchronize
ACK	Acknowledge
IAT	Inter-Arrival Time
CIC	Canadian Institute for Cybersecurity
CPU	Central Processing Unit
API	Application Programming Interface
JSON	JavaScript Object Notation
REST	Representational State Transfer

[Continue to Chapter 1...]

Note: This is the front matter of the Final Review Report. The complete chapters will be provided in separate files for better organization.