

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

Chapter	Title	Page
	CERTIFICATE	ii
	DECLARATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	TABLE OF CONTENTS	vi
	LIST OF FIGURES	viii
	LIST OF TABLES	ix
	LIST OF ABBREVIATIONS	x
1	INTRODUCTION	1
1.1	Overview	1
1.2	DDoS Attack Taxonomy	2
1.3	Motivation	4
1.4	Problem Statement	5
1.5	Objectives	6
1.6	Scope and Limitations	7
1.7	Organization of Report	8
2	LITERATURE SURVEY	9
2.1	Traditional DDoS Mitigation Approaches	9
2.2	Machine Learning-Based Detection	11
2.3	Kernel-Level Mitigation Systems	14
2.4	eBPF/XDP in Network Security	16
2.5	Comparative Analysis of Existing Systems	18

Chapter	Title	Page
2.6	Research Gap	20
3	SYSTEM ARCHITECTURE & DESIGN	21
3.1	Overall System Architecture	21
3.2	Data Plane Design (eBPF/XDP)	23
3.3	Control Plane Design (User Space)	26
3.4	ML Module Architecture	28
3.5	Dashboard and Monitoring	30
3.6	Integration Design	32
4	METHODOLOGY & IMPLEMENTATION	34
4.1	Development Environment	34
4.2	Dataset Preparation	35
4.3	Feature Engineering	37
4.4	ML Model Training	40
4.5	eBPF/XDP Implementation	43
4.6	User Space Components	46
4.7	System Integration	49
5	EXPERIMENTAL SETUP & RESULTS	51
5.1	Testbed Configuration	51
5.2	Attack Simulation Methodology	53
5.3	Performance Metrics	55
5.4	Experimental Results	57
5.5	Analysis and Discussion	63
6	COMPARATIVE ANALYSIS	66
6.1	Comparison with Traditional Firewalls	66
6.2	Comparison with Rate Limiting	67
6.3	Comparison with ML-Only Approaches	68
6.4	Performance Benchmarking	69
7	DISCUSSION	71
7.1	Key Findings	71
7.2	Trade-offs and Design Decisions	72

Chapter	Title	Page
7.3	Challenges Encountered	73
7.4	Lessons Learned	74
8	CONCLUSION & FUTURE WORK	75
8.1	Conclusion	75
8.2	Contributions	76
8.3	Future Enhancements	77
	REFERENCES	79
	APPENDICES	82
A	Source Code Listings	82
B	Configuration Files	85
C	Test Results	87

LIST OF FIGURES

Figure No.	Title	Page
1.1	DDoS Attack Taxonomy	3
1.2	Volumetric Attack Impact	4
3.1	Overall System Architecture	22
3.2	eBPF/XDP Data Plane Architecture	24
3.3	Packet Processing Flowchart	25
3.4	Control Plane Components	27
3.5	ML Detection Pipeline	29
3.6	Technology Stack Layers	31
3.7	System Integration Diagram	33
4.1	Feature Extraction Process	38
4.2	ML Model Training Workflow	41
4.3	eBPF Map Structure	44
4.4	XDP Hook Points	45
5.1	Testbed Network Topology	52
5.2	Attack Simulation Setup	54
5.3	Detection Latency Graph	58

Figure No.	Title	Page
5.4	Throughput Comparison	59
5.5	CPU Utilization Graph	60
5.6	ML Model Accuracy	61
5.7	False Positive Rate	62
6.1	Performance Comparison Chart	70

LIST OF TABLES

Table No.	Title	Page
2.1	Literature Survey Summary	19
2.2	Research Gap Analysis	20
4.1	CIC-DDoS-2019 Dataset Statistics	36
4.2	Feature Set Description	39
4.3	ML Model Hyperparameters	42
5.1	Hardware Specifications	51
5.2	Software Configuration	52
5.3	Attack Scenarios	56
5.4	Performance Metrics Summary	64
6.1	Comparative Analysis Table	69

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.