# Enhancing Intrusion Detection System using XDP with eBPF

**K.Geethika, G.Krishna Prathibha, G.Sneha**

Under the esteemed guidance of

**Mr. N. Anand**

Assistant Professor

VISHNU
UNIVERSAL LEARNING

Bachelor of Technology
Department of Information Technology
**BVRIT HYDERABAD college of engineering for Women**

November 15, 2023

# Overview

# Introduction

Network filtering is essential for securing computer networks, and there are various types of attacks that network filtering aims to mitigate. Here are some common network attacks:

- **DOS (Denial of Service) Attack:**
  Attackers flood a network or system with excessive traffic, causing it to become overwhelmed and unavailable to legitimate users.
- **DDOS (Distributed Denial of Service) Attack:** Similar to DoS but conducted from multiple sources, making it even more challenging to mitigate.

**Intrusion Detection System :**

IDS stands for Intrusion Detection System. It is a critical component of a cybersecurity strategy designed to detect and respond to unauthorized access or suspicious activities on a network. IDS is required for several reasons:

- **Security Threat Detection:** IDS helps in detecting and identifying security threats and unauthorized activities within a network or computer system.
- **Network Visibility and Risk Mitigation:** IDS offers insights into network traffic, aids in understanding normal network behavior, and helps reduce the attack surface by identifying vulnerabilities and deviations from the norm.

**What if we use general packet filters ? :**

- Detection Precision :
  This can lead to a higher rate of false positives or missed detections.
- Resource Efficiency :
  consuming more CPU and memory resources.
- Network Performance :
  may introduce more latency and could impact network performance.

# eBPF and XDP

**eBPF (extended Berkely Packet Filtering) :**

- eBPF is a revolutionary technology which origins in the Linux kernel.
- eBPF extends kernel capabilities without altering kernel source code or loading kernel modules.
- It operates as a bytecode-based virtual machine for running programs.
- A verifier assesses the safety of eBPF programs when loaded into the kernel and rejects them if found unsafe.

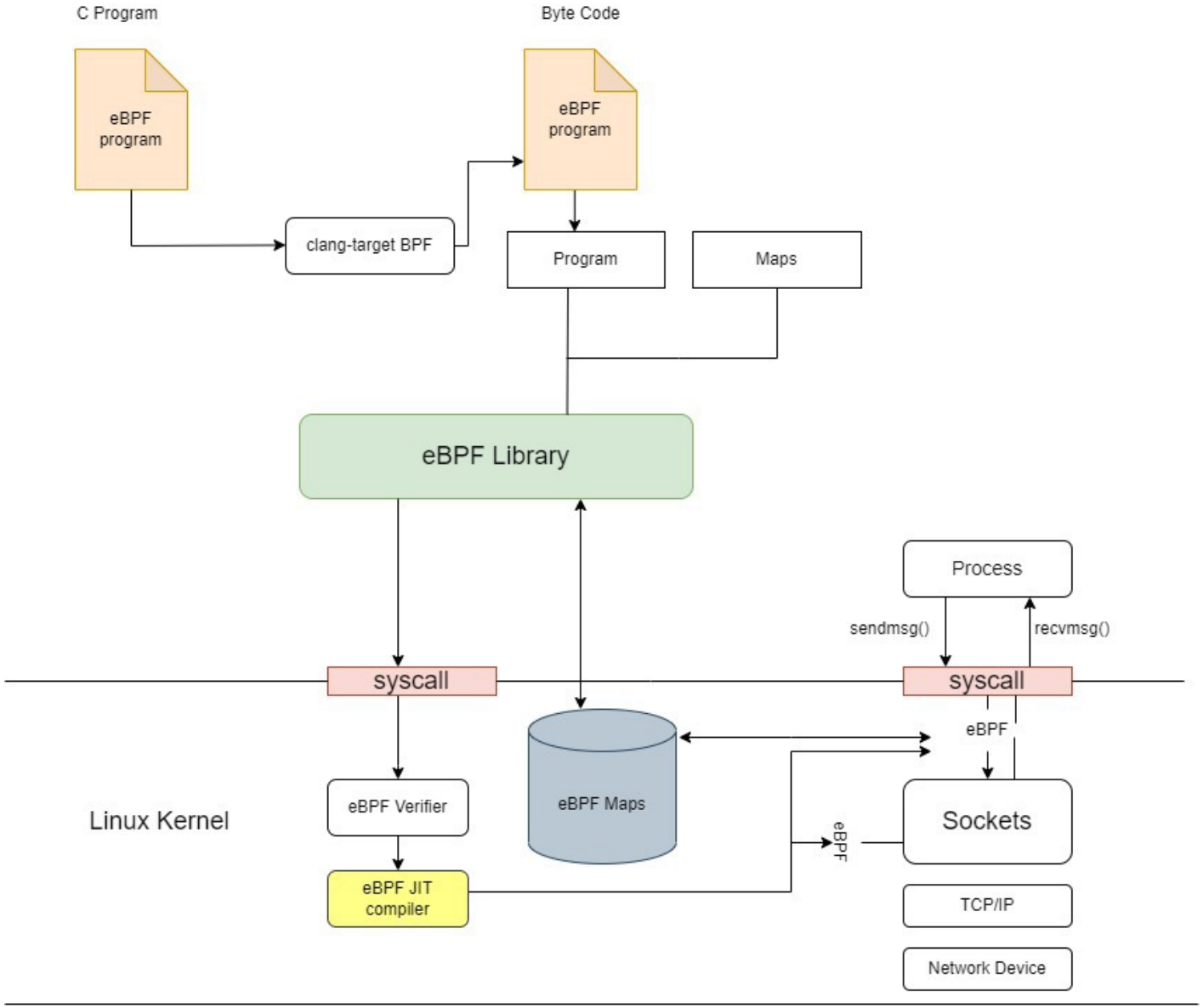



Figure: eBPF Architecture

## XDP (eXpress Data Path) :

- XDP (eXpress Data Path) is a high-performance data processing framework in the Linux kernel.
- It operates at an extremely low level, providing fast packet processing capabilities.
- XDP is commonly used for network filtering, load balancing, and DDoS mitigation.
- It allows for efficient packet handling with minimal overhead, making it ideal for high-speed networking applications.

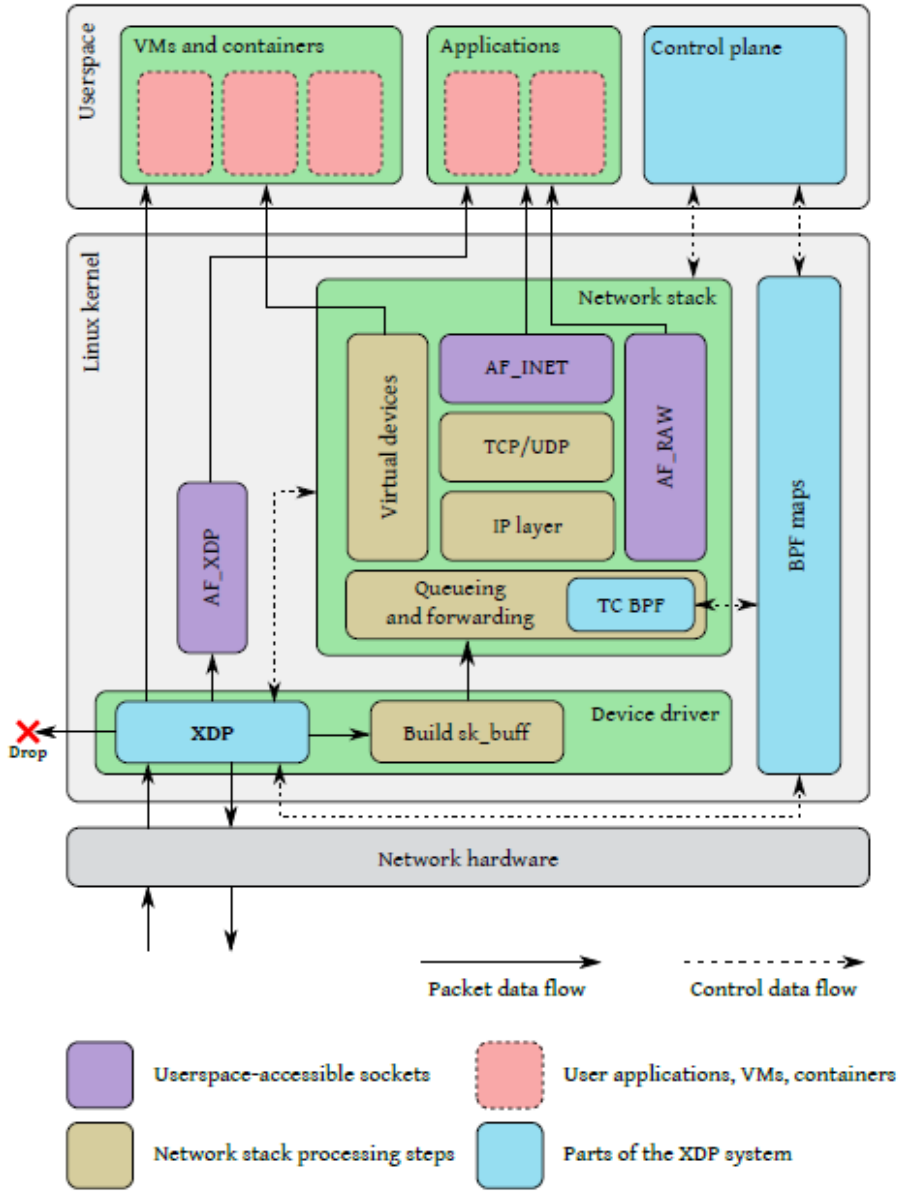



Figure: XDP Architecture

# Literature Survey

| Title | Author | Description | Comments | Year |
|---|---|---|---|---|
| High-performance Intrusion Detection System using eBPF with Machine Learning algorithms [1] | Nemalikanti Anand, Saifulla M A | Intrusion Detection system using eBPF | trained models with DT, RF, SVM, and TwinSVM, obtained low accuracies at userspace | 2023 |
| Intrusion Detection Systems, Issues, Challenges, and Needs [2] | Mohammad Aljanabi, Mohd Arfian Ismail | Machine Learning Algorithms like Decision Tree and Support Vector Machine | analysis of ML algorithms such as ANN, BN, DT, KNN, and SVM, and state weaknesses and strengths for each one that lead to choose SVM | 2021 |
| Fast Packet Processing with eBPF and XDP: Concepts, Code, Challenges and Applications [3] | MARCOS A.M.VIEIRA, MATHEUS S.CASTANHO, R.D.G. PACÍFICO | Resource for understanding and working with eBPF and XDP in the context of network packet | focused on eBPF and the XDP hook, providing examples and showing existing tools or allowing to provide new functionalities | 2020 |

| Title | Author | Description | Comments | Year |
|---|---|---|---|---|
| Design and implementation of an intrusion detection system by using Extended BPF in the Linux kernel [4][5] | Shie-Yuan Wang, Jen-Chieh Chang | The eBPF mechanism has great potential to be used as a framework to implement a high-performance IDS in the Linux kernel. | experimental results show that the maximum throughput of our IDS system can outperform that of Snort by a factor of 3 under many tested conditions. | 2021 |
| The eXpress Data Path: Fast Programmable Packet Processing in the Operating System Kernel [6] | Toke Høiland-Jørgensen, Jesper D. Brouer | XDP design and architecture and how it works is explained | XDP achieves impressive single-core packet processing rates, reaching up to 24 million packets per second. | 2018 |

# Problem Statement

- Attack detecting methods(like IDS, IPS, etc) can detect various application-level attacks (eg.HTTP attacks, DHCP attacks, etc) at network layer.
- In network layer, during packet filtering, there may be loss of data/useful information. (due to DOS attacks, Resource Limitations, Inadequate Throughput, etc ).
- Machine learning algorithms help to classify the normal data and attack data. So that the performance may increase compared to existing methods.

**"So, At what level can we filter the attacks ??"**

# Proposed Method

- The proposed solution is the eBPF (extended Berkely Packet Filtering) technology along with XDP (eXpress Data Path)
- eBPF technology with XDP is used to detect the attacks at kernel level without modifying the source code in the kernel
- Kernel-level packet filtering provides more efficiency in detecting and handling attacks by controlling packet flow at a lower system level ensuring robust security.
- eBPF with XDP analyzes target values from trained models and connects with network devices to make decisions on packet dropping or forwarding.

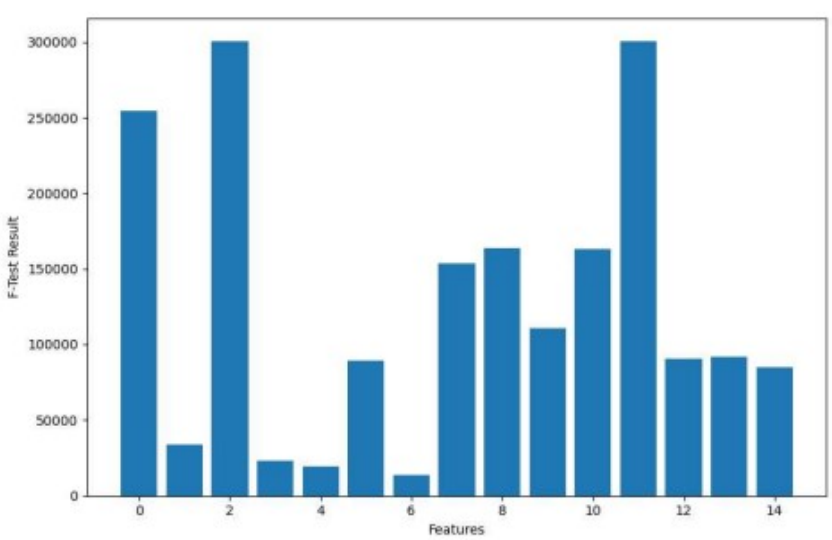
The steps involved in this process are:

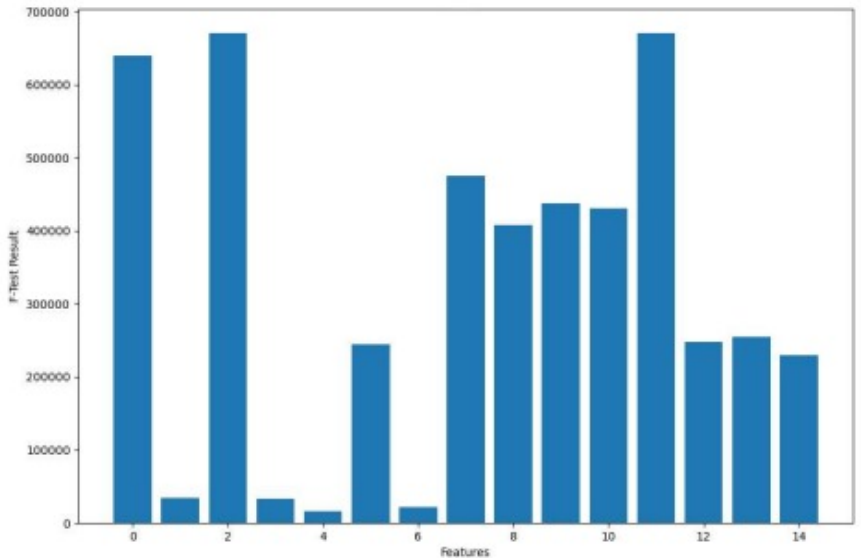
- Identify CIC-IDS-2017 dataset.
- The raw data is then pre-processed, that includes data transmission, cleaning (infinity, NULL values, etc.), and reduction (size).
- Apply ANOVA technique to find top rated features from the pre-processed data
- The extracted features are analyzed for intrusion detection, using ML algorithms (DT, RF, SVM, TwinSVM).
- write an eBPF program(C program) that is converted to bytecode which utilizes trained model parameters to detect attacks.
- write a XDP code with eBPF program that utilizes trained model parameters to detect attacks (filter packets) faster and accurate within the kernel.

# Implementation & Results

- Analyzed the dataset CIC IDS 2017
- Top 15 Features are Extracted from dataset using ANOVA F-test method.
- These features are destination port, total forward packets, total backward packets, minimum packet length, etc.
- All the preprocessed data is trained with Random Forest, Decision Tree, Support Vector Machine, Twin Support Vector Machine.
- The output parameters from trained model are given as input to the ebpf bytecode at kernal level.
- eBPF(extended Berkley Packet Filtering) Bytecode is executed and decide the packet is attack free or not.

# Implementation & Results




Anova F-Test features for DDOS-DOS dataset and CIC-IDS-2017 dataset

# Implementation & Results

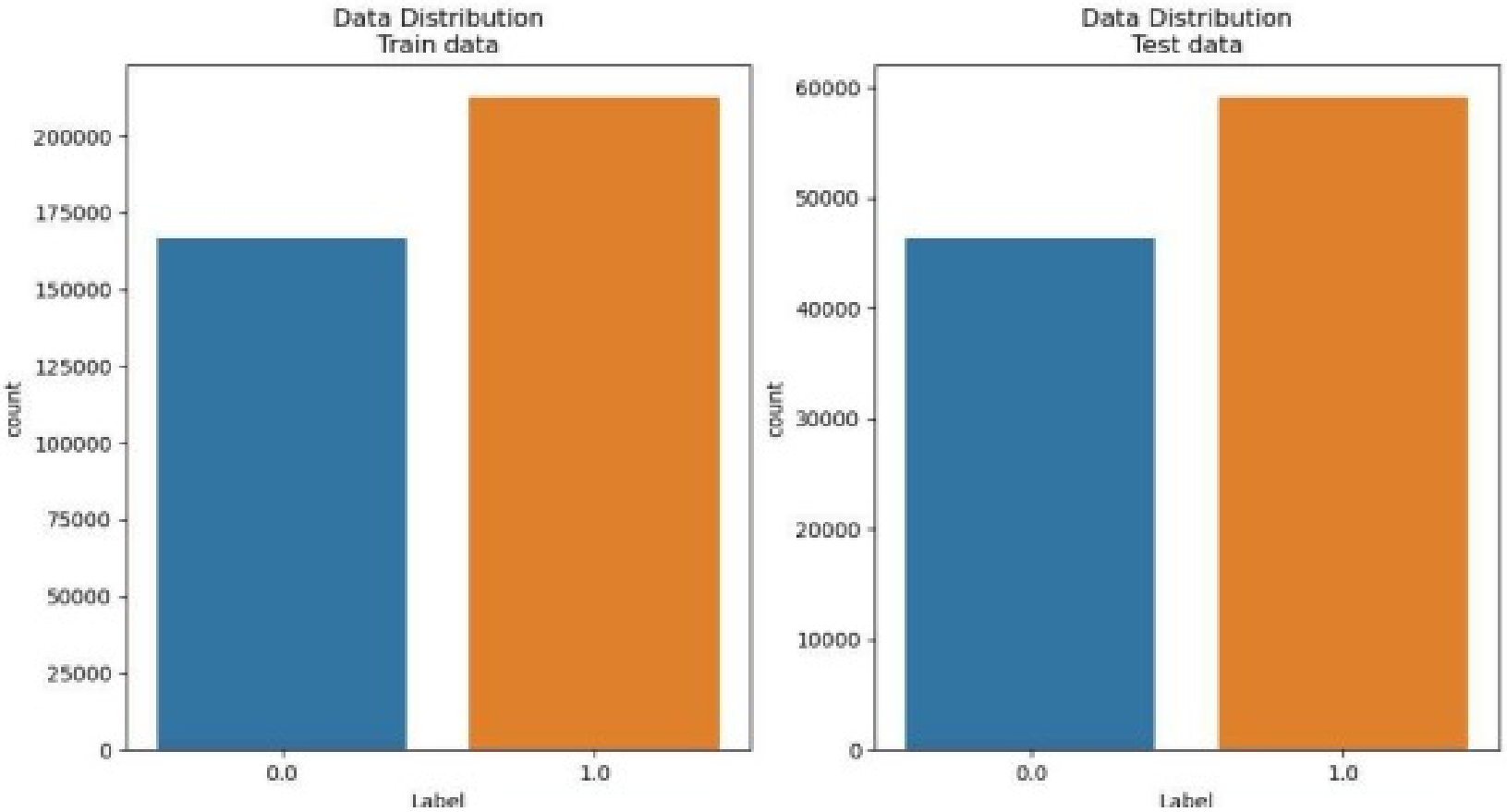
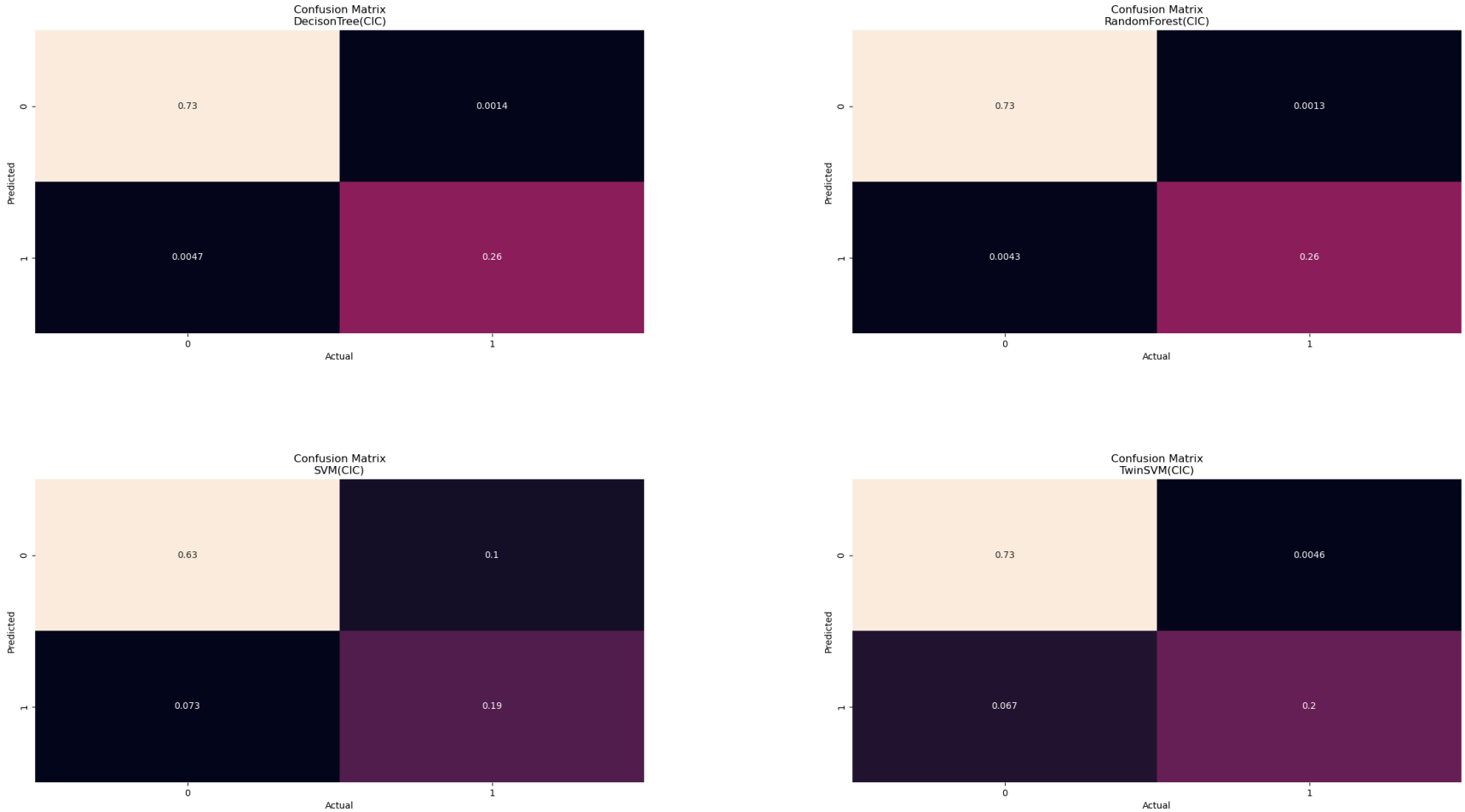



Figure: Data Distribution for DDOS-DOS dataset and CIC-IDS-2017 dataset

# Implementation & Results




Confusion Matrix for CIC-IDS-2017 dataset

# Implementation & Results

| Performance Parameters | Method | DT | RF | SVM | TwinSVM |
|---|---|---|---|---|---|
| Accuracy | Train | 99.52 | 99.59 | 88.77 | 93.87 |
| | Test | 99.38 | 99.44 | 88.74 | 93.82 |
| Precision | Train | 99.71 | 99.74 | 78.97 | 98.58 |
| | Test | 99.46 | 99.51 | 78.97 | 98.49 |
| Recall/ Sensitivity | Train | 98.49 | 98.72 | 73.41 | 75.9 |
| | Test | 98.21 | 98.37 | 73.26 | 75.78 |
| F1 Score | Train | 99.09 | 99.23 | 76.09 | 85.76 |
| | Test | 98.83 | 98.94 | 76.01 | 85.65 |
| Specificity | Train | 99.89 | 99.91 | 93.71 | 99.65 |
| | Test | 99.81 | 99.82 | 93.73 | 99.63 |

| Performance Parameters | Method | DT | RF | SVM | TwinSVM |
|---|---|---|---|---|---|
| Accuracy | Train | 99.73 | 99.82 | 84.43 | 88.49 |
| | Test | 99.57 | 99.58 | 84.43 | 88.42 |
| Precision | Train | 99.87 | 99.88 | 84.28 | 98.53 |
| | Test | 99.71 | 99.65 | 84.31 | 98.49 |
| Recall/ Sensitivity | Train | 99.65 | 99.80 | 86.74 | 79.42 |
| | Test | 99.52 | 99.60 | 86.70 | 79.33 |
| F1 Score | Train | 99.76 | 99.84 | 85.49 | 87.95 |
| | Test | 99.62 | 99.62 | 85.48 | 87.88 |
| Specificity | Train | 99.83 | 99.85 | 81.83 | 98.67 |
| | Test | 99.64 | 99.55 | 81.88 | 98.63 |

Figure: ML performance for cic ids dataset and ddos dos attacks dataset

# Implementation & Results

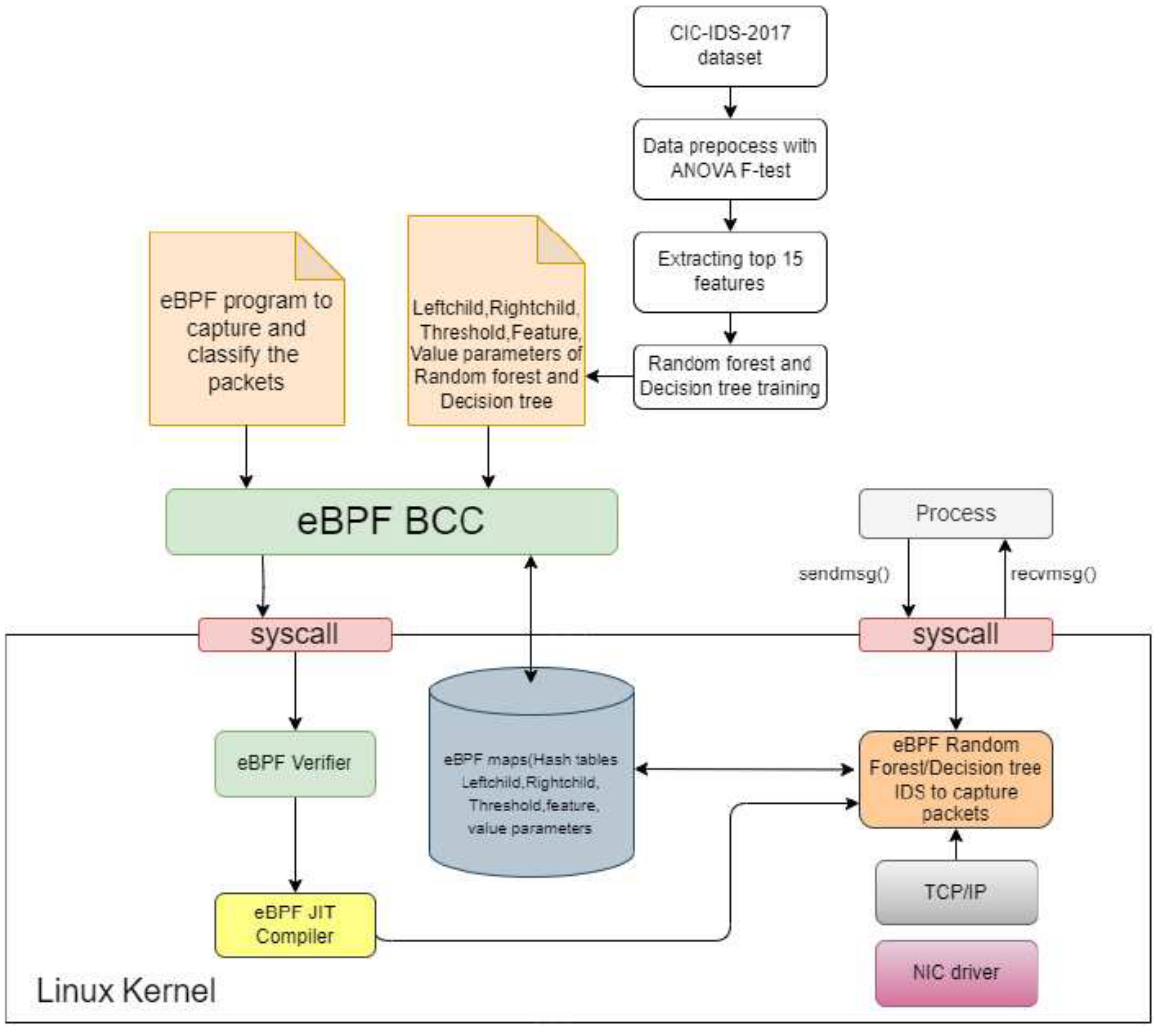



Figure: Proposed model using RF and DT algorithms

# Implementation & Results

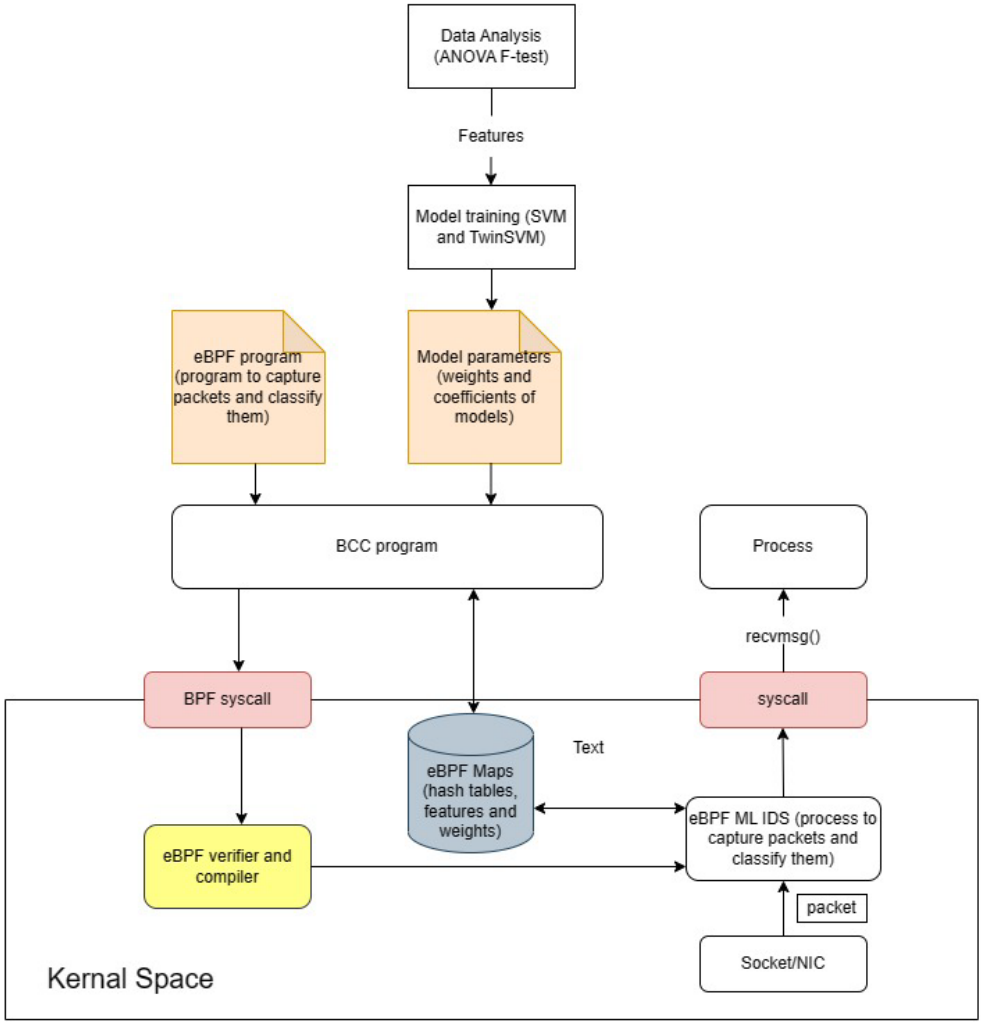



Figure: Proposed model using SVM and TwinSVM algorithms

# Implementation & Results

| Algorithms | Userspace (Mean) | eBPF (Mean) |
|---|---|---|
| Decision Tree packet/s | 46239 | 109691 |
| Random Forest packet/s | 45978 | 108534 |
| SVM packet/s | 45590 | 92978 |
| TwinSVM packet/s | 38430 | 109865 |

Figure: eBPF performance cic ids dataset

| Algorithms | Userspace (Mean) | eBPF (Mean) |
|---|---|---|
| Decision Tree packet/s | 42463 | 106421 |
| Random Forest packet/s | 41632 | 105245 |
| SVM packet/s | 49376 | 92581 |
| TwinSVM packet/s | 42487 | 117536 |

Figure: eBPF performance ddos dos attacks dataset

# Conclusion & Future Scope

- Packets at kernel level are filtered faster than userspace using eBPF technology.
- Using XDP, the arrived packets can be processed before even touching the network stack in the kernel.
- XDP can let the packets bypass the kernel to reach userspace for processing.
- Future scope is to attach XDP with eBPF with other Machine Learning Algorithms.


Nemalikanti Anand Pavan Kumar Aakula, Saifulla M A.
High-performance intrusion detection system using ebpf with machine learning algorithms.
pages 1–25, 2023.


Ahmed Hussein Ali Mohammad Aljanabi, Mohd Arfian Ismail.
Intrusion detection systems, issues, challenges, and needs.
14:560 – 571, 2021.


RACYUS D. G. PACÍFICO ELERSON R. S. SANTOS EDUARDO P. M. CÂMARA JÚNIOR MARCOS A. M. VIEIRA, MATHEUS S. CASTANHO and LUIZ F. M. VIEIRA.
Fast packet processing with ebpf and xdp: Concepts, code,challenges and applications.
53:1–36, 2020.


Jen-Chieh Chang Shie-Yuan Wang.
Design and implementation of an intrusion detection system by using extended bpf in the linux kernel.

page 1–17, 2021.

E Dumazet.
A jit for packet filters.
page 1–13, 2011.

Daniel Borkmann John Fastabend Tom Herbert David Ahern Toke Høiland-Jørgensen, Jesper Dangaard Brouer and David Miller.
The express data path: Fast programmable packet processing in the operating system kernel.
page 1–13, 2018.

# Thank you