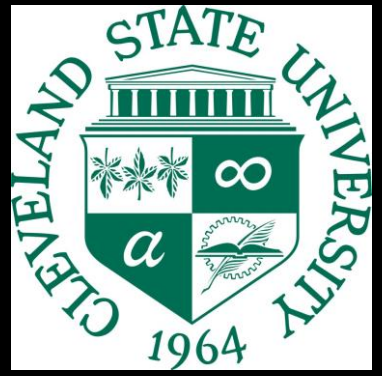
UNLEASHING THE POWER OF DDOS AND MITM ATTACKS ON A SOFTWARE DEFINED NETWORK

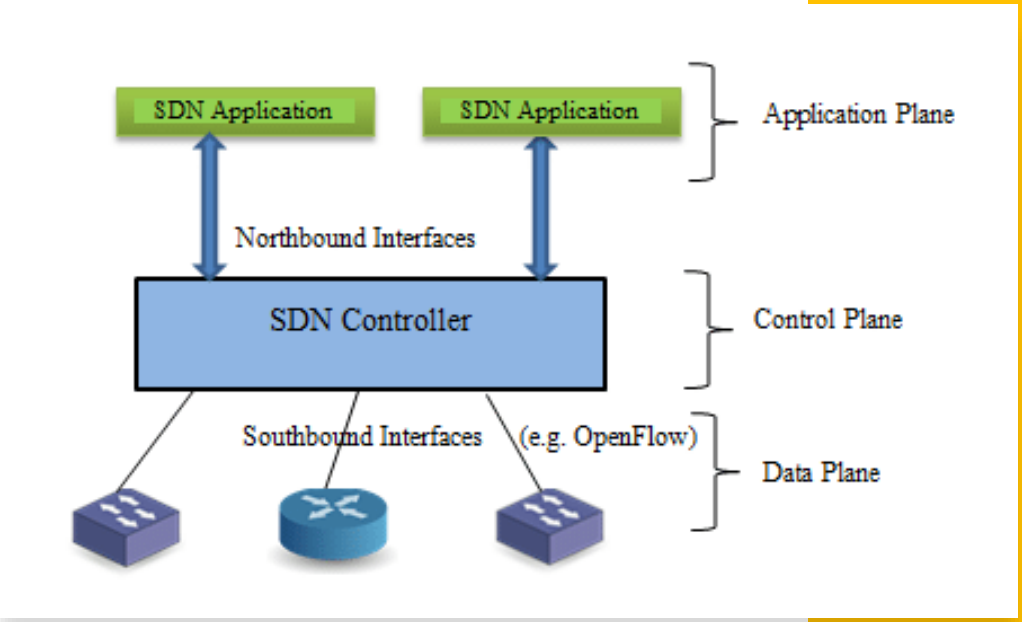


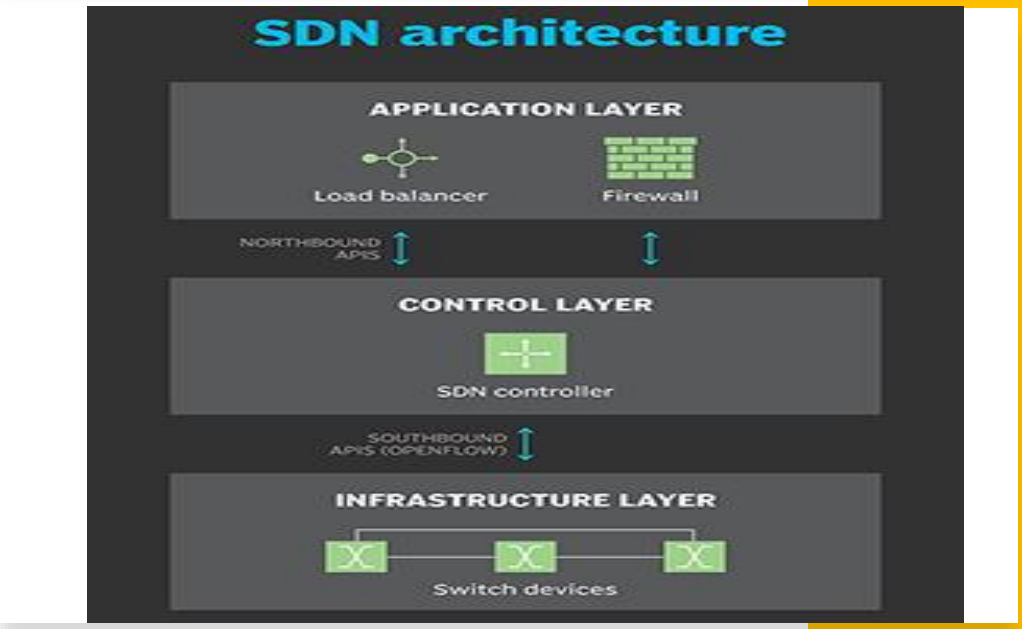
- CARMEN VILLALOBOS GARCIA
- PROFESSOR SATHISH KUMAR

INDEX

INTRODUCTION - SDN

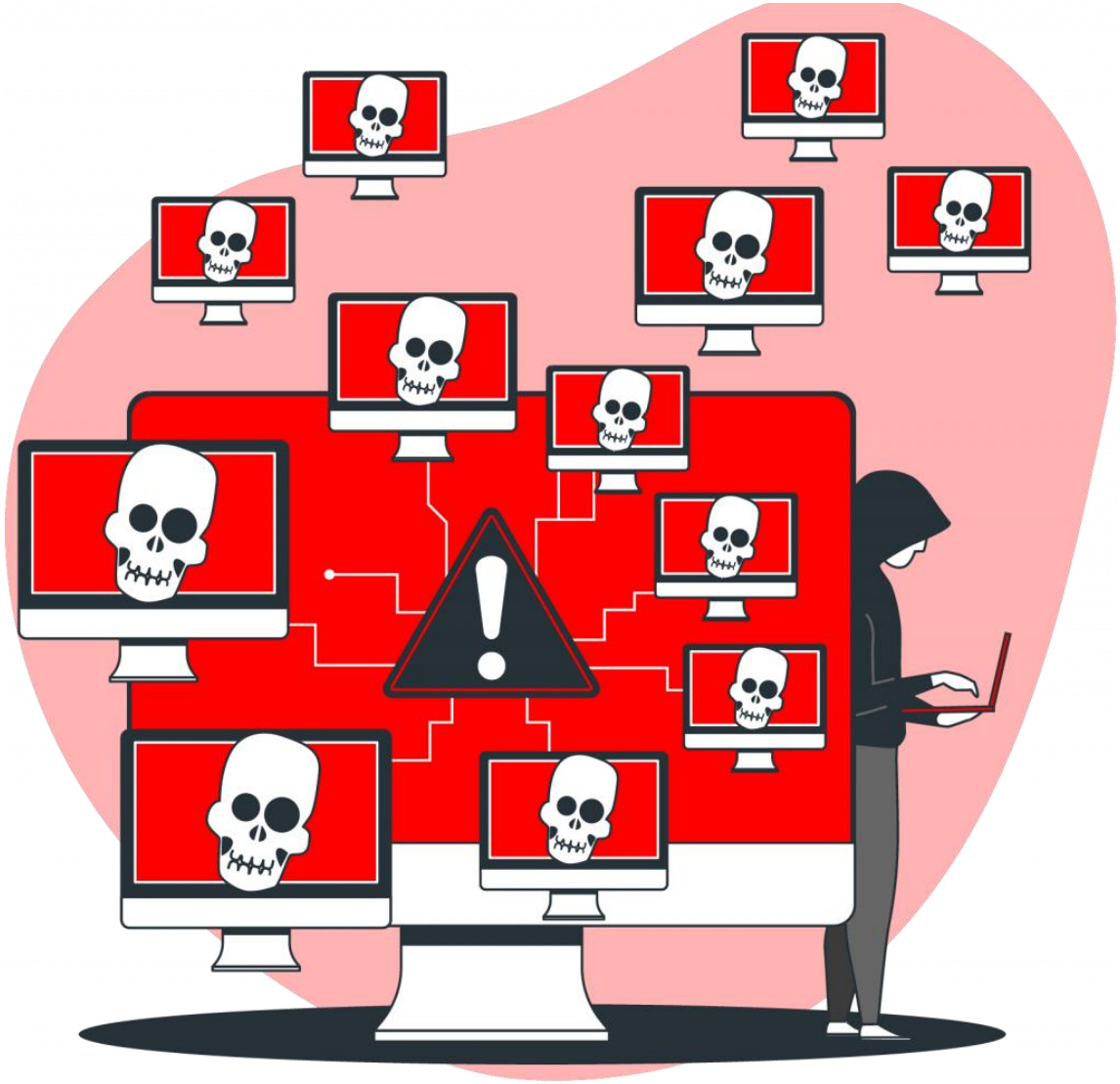
- SDN separates the control plane from the data plane, centralizing network management in a software-based controller.
- The controller acts as the "brains" of the network, making decisions on how to forward packets based on the information it has about the network topology, traffic conditions, and policies defined by administrators.
- Offers new level of flexibility and control.





INTRODUCTION - DDOS ATTACK

- Consists of a cyberattack that makes a computer unavailable. Disrupt the normal functioning of a computer network, service or website by overwhelming it with excess of traffic.
- Lanching a DDoS attack is extremely simple.
- Increasing latency and dropping legitimate packets can caused degradation of the SDN performance.



RESEARCH OBJECTIVE

Classify different types of DDos attacks.

Detect a MITM attack.

DATASET EXPLANATION

Benign and DDos Traffic is generated using four different files:

Generate_benign_traffic.py Collect_benign_traffic.py

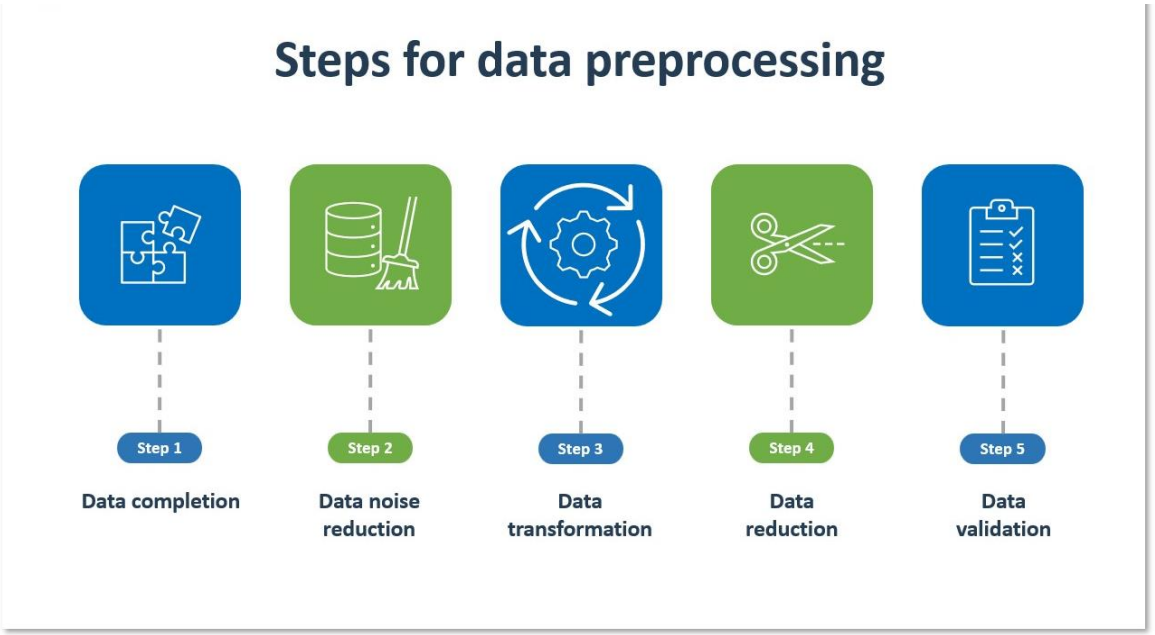
Generate_ddos_traffic.py Collect_ddos_traffic.py

We will collect all this traffic in the file FlowStatsfile.csv

Record these features:
timestamp,datapath_id,flow_id,ip_src,tp_src,ip_dst,tp_dst,ip_proto,icmp_code,icmp_type,flow_duration_sec,flow_duration_nsec,idle_timeout,hard_timeout,flags,packet_count,byte_count,packet_count_per_second,packet_count_per_nsecond,byte_count_per_second,byte_count_per_nsecond,label

The dataset contains 2667524 records, 906880 benign, 1760644 DDos

DATA PREPROCESSING

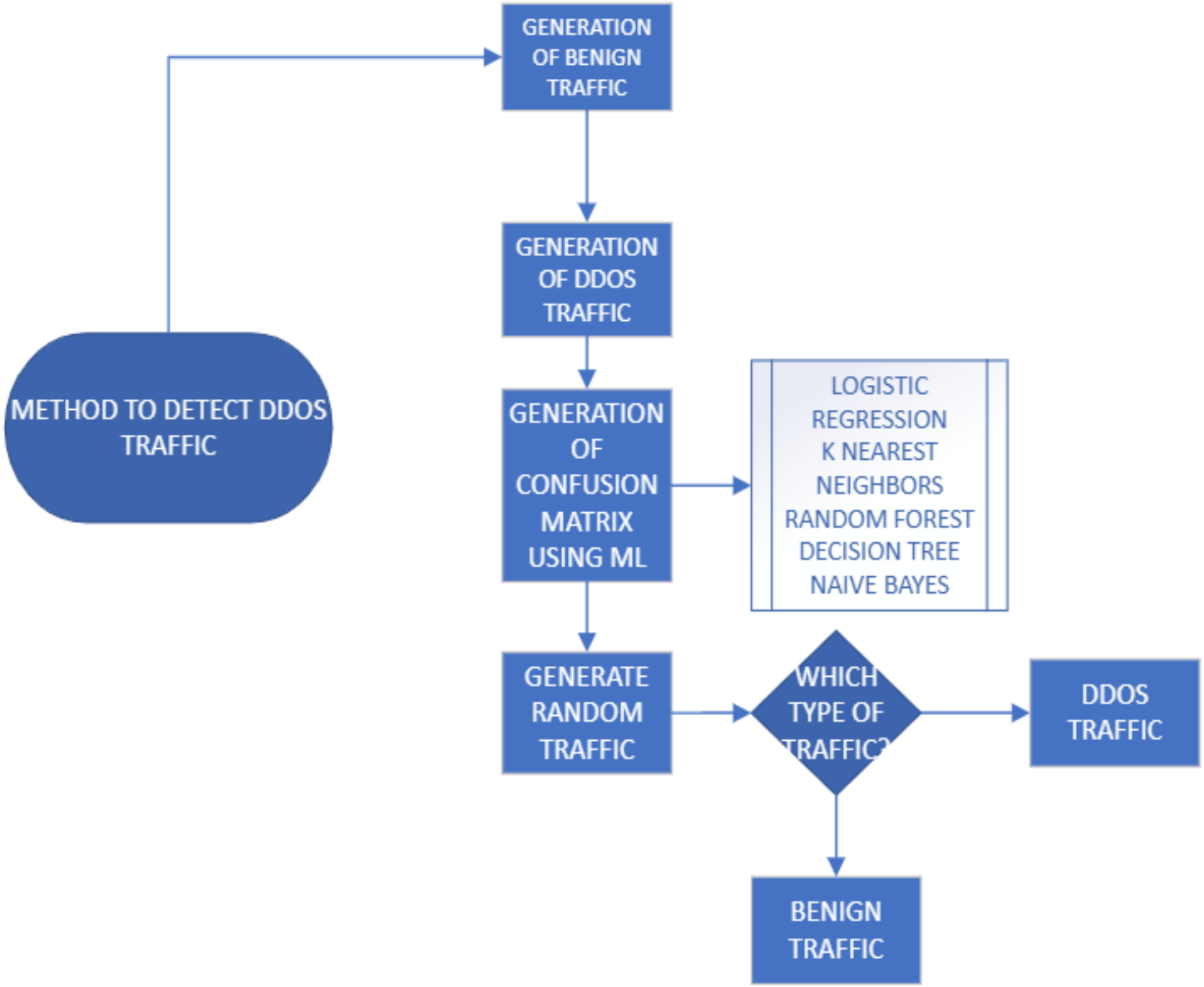


PRINCIPAL COMPONENT ANALYSIS

- After we obtain the variance of the dataset, we need to find the one with the least number of components and has the most similar value to the variance of the dataset.

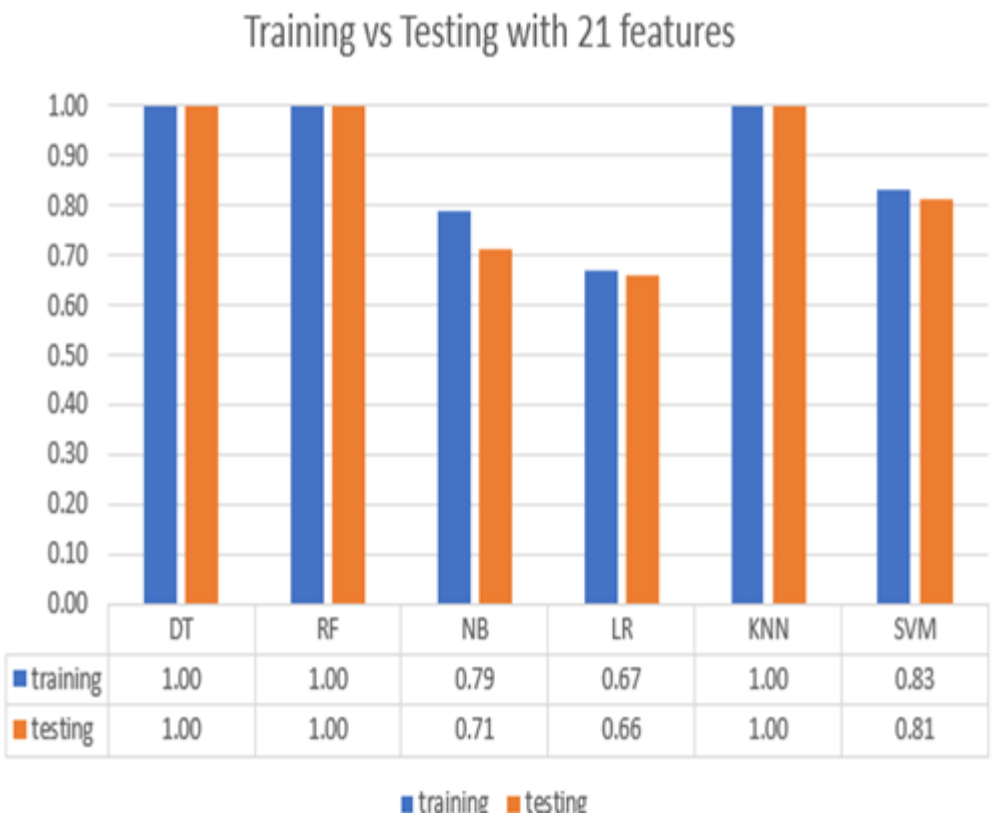
Components	Sum of Variances
21	1.262862
18	1.262862
15	1.262804
13	1.262262
12	1.259926
10	1.211322
8	1.136906

CLASSIFICATION PROCESS



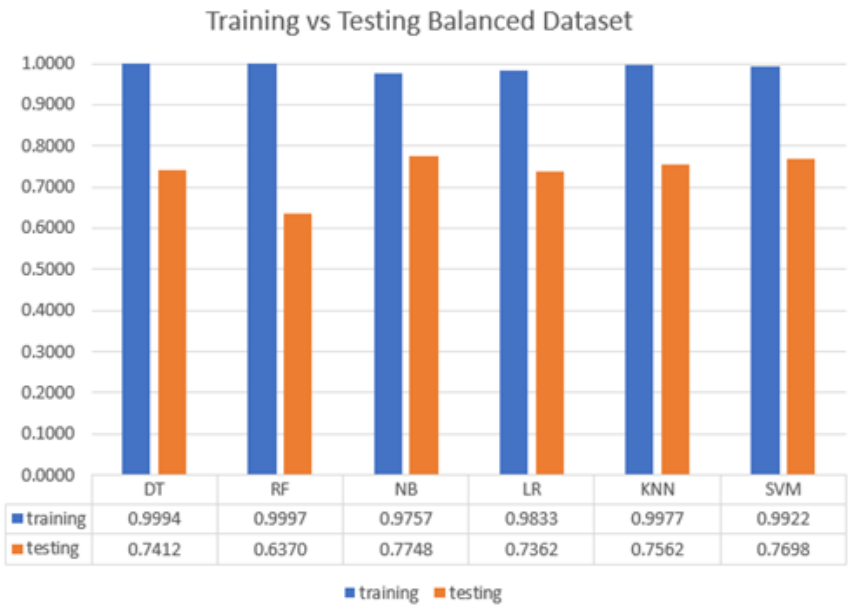
ANALYSIS RESULTS

TRAINING VS TESTING GRAPHS

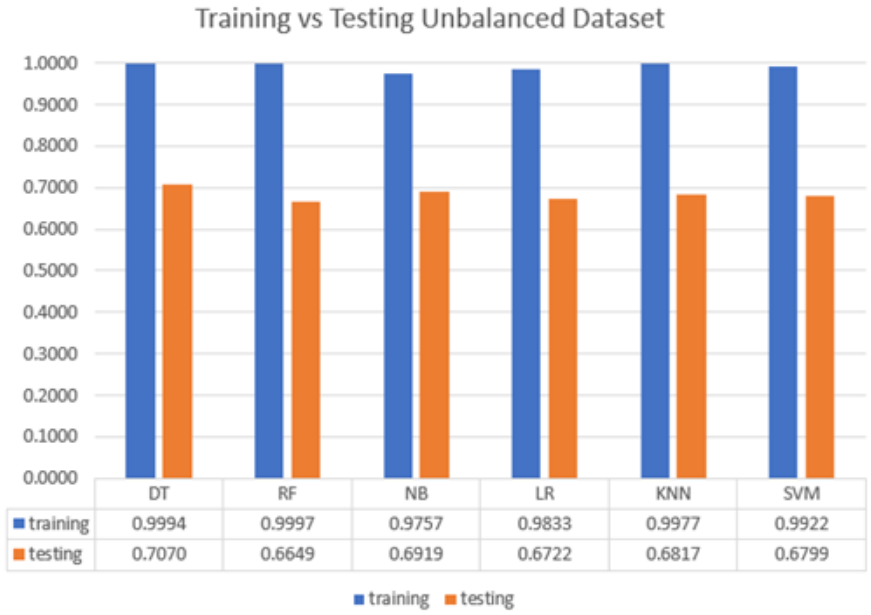


	DT	RF	NB	LR	KNN	SVM
training	1.00	1.00	0.79	0.67	1.00	0.83
testing	1.00	1.00	0.71	0.66	1.00	0.81

Balanced VS Unbalanced GRAPHS

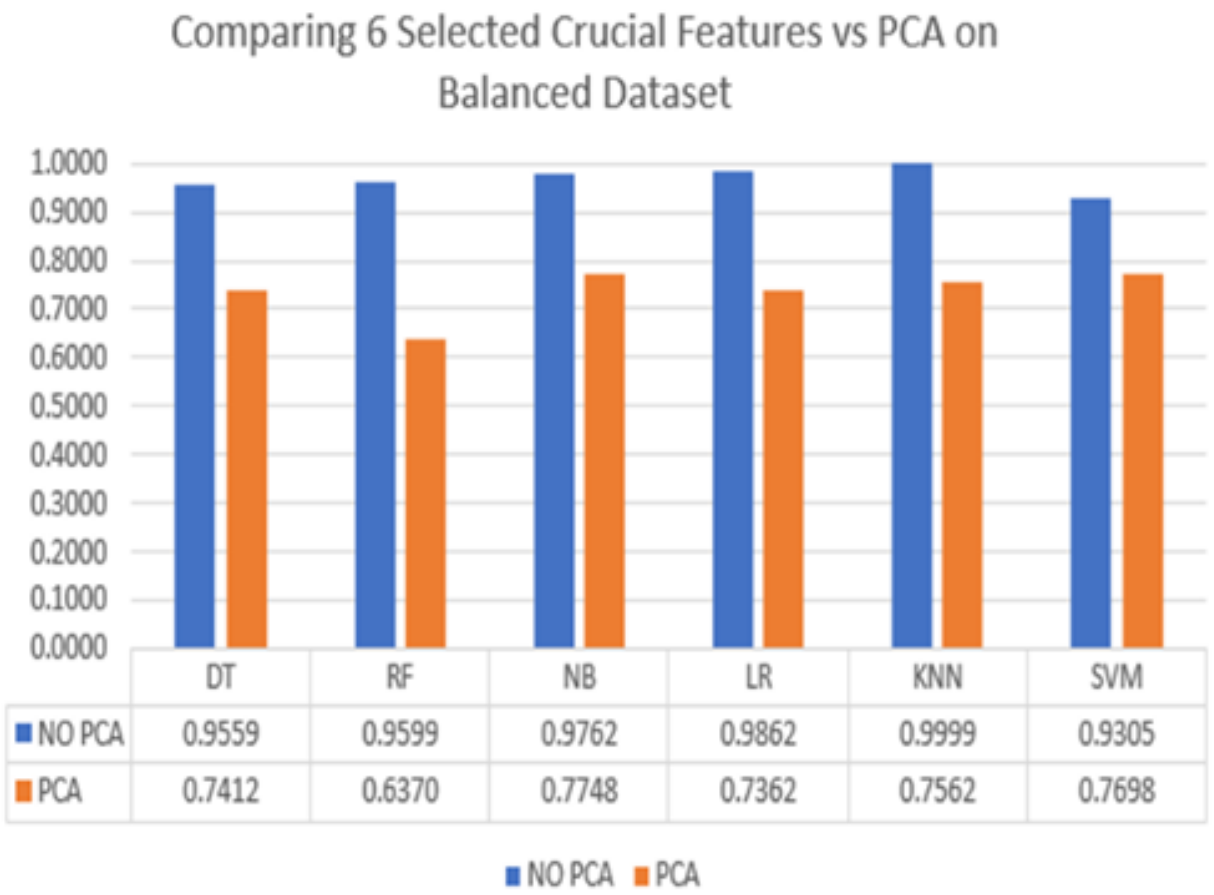


	DT	RF	NB	LR	KNN	SVM
training	0.9994	0.9997	0.9757	0.9833	0.9977	0.9922
testing	0.7412	0.6370	0.7748	0.7362	0.7562	0.7698



	DT	RF	NB	LR	KNN	SVM
training	0.9994	0.9997	0.9757	0.9833	0.9977	0.9922
testing	0.7070	0.6649	0.6919	0.6722	0.6817	0.6799

ACCURACY ON BALANCED AND UNBALANCED DATASET WITHOUT PCA USING 6 PARAMETERS



	DT	RF	NB	LR	KNN	SVM
NO PCA	0.9559	0.9599	0.9762	0.9862	0.9999	0.9305
PCA	0.7412	0.6370	0.7748	0.7362	0.7562	0.7698

DECISION TREE

Features	6 – Hand Picked	21	21	21
Normalization	Yes	Yes	Yes	Yes
PCA	Yes 3 components	Yes 12 components	Yes 18 components	No
UDP accuracy	1.0	0.25272	0.49852	1.0
ICMP accuracy	1.0	0.0	0.0	1.0
TCP accuracy	0.99999	0.0025	0.0141	1.0

RANDOM FOREST

Features	6 – Hand Picked	21	21	21
Normalization	Yes	Yes	Yes	Yes
PCA	Yes 3 components	Yes 12 components	Yes 18 components	No
UDP accuracy	0.00062	0.46258	0.57196	1.0
ICMP accuracy	1.0	0.0	0.0	1.0
TCP accuracy	1.0	0.00078	0.01116	1.0

NAIVE BAYES

Features	6 – Hand Picked	21	21	21
Normalization	Yes	Yes	Yes	Yes
PCA	Yes 3 components	Yes 12 components	Yes 18 components	No
UDP accuracy	0.14338	0.79954	0.79954	1.0
ICMP accuracy	0.16352	1.0	1.0	0.99998
TCP accuracy	0.15882	0.4003	0.4003	1.0

LOGISTIC REGRESSION

Features	6 – Hand Picked	21	21	21
Normalization	Yes	Yes	Yes	Yes
PCA	Yes 3 components	Yes 12 components	Yes 18 components	No
UDP accuracy	1.0	0.7367	0.7586	1.0
ICMP accuracy	0.0	0.88404	0.86374	1.0
TCP accuracy	1.0	0.76414	0.76838	1.0

K-NEAREST NEIGHBOR

Features	6 – Hand Picked	21	21	21
Normalization	Yes	Yes	Yes	Yes
PCA	Yes 3 components	Yes 12 components	Yes 18 components	No
UDP accuracy	1.0	0.83486	0.49378	1.0
ICMP accuracy	0.99996	1.0	1.0	1.0
TCP accuracy	0.99988	0.83746	0.53126	0.12288

- Once we detect that the traffic is DDos, we will need to check what type of protocol is.
- The IP protocol is the 7th feature that we collect.
  - DDos attack Performing **ICMP** (Ping) Flood -> IP_PROTO = 1

    hping3 -1 -V -d 120 -w 64 -p 80 --rand-source --flood {}".format(dst)
  - DDos attack Performing **UDP** Flood -> IP_PROTO = 6

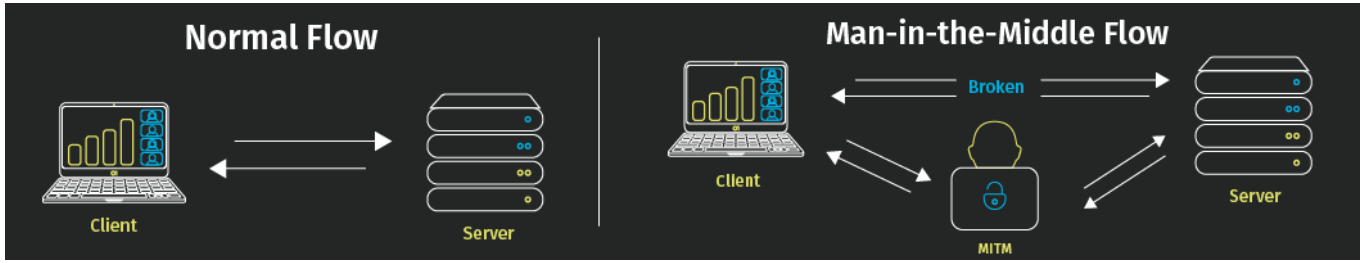
    hping3 -2 -V -d 120 -w 64 --rand-source --flood {}".format(dst)
  - DDos attack Performing **TCP-SYN** Flood -> IP_PROTO = 17

    hping3 -S -V -d 120 -w 64 -p 80 --rand-source --flood 10.0.0.1

- TRAINING: 400 000 rows for benign traffic and 300 000 rows for DDos traffic.
- For the DDos traffic:
  - 100 000 rows UDP.
  - 100 000 rows TCP.
  - 100 000 rows ICMP.

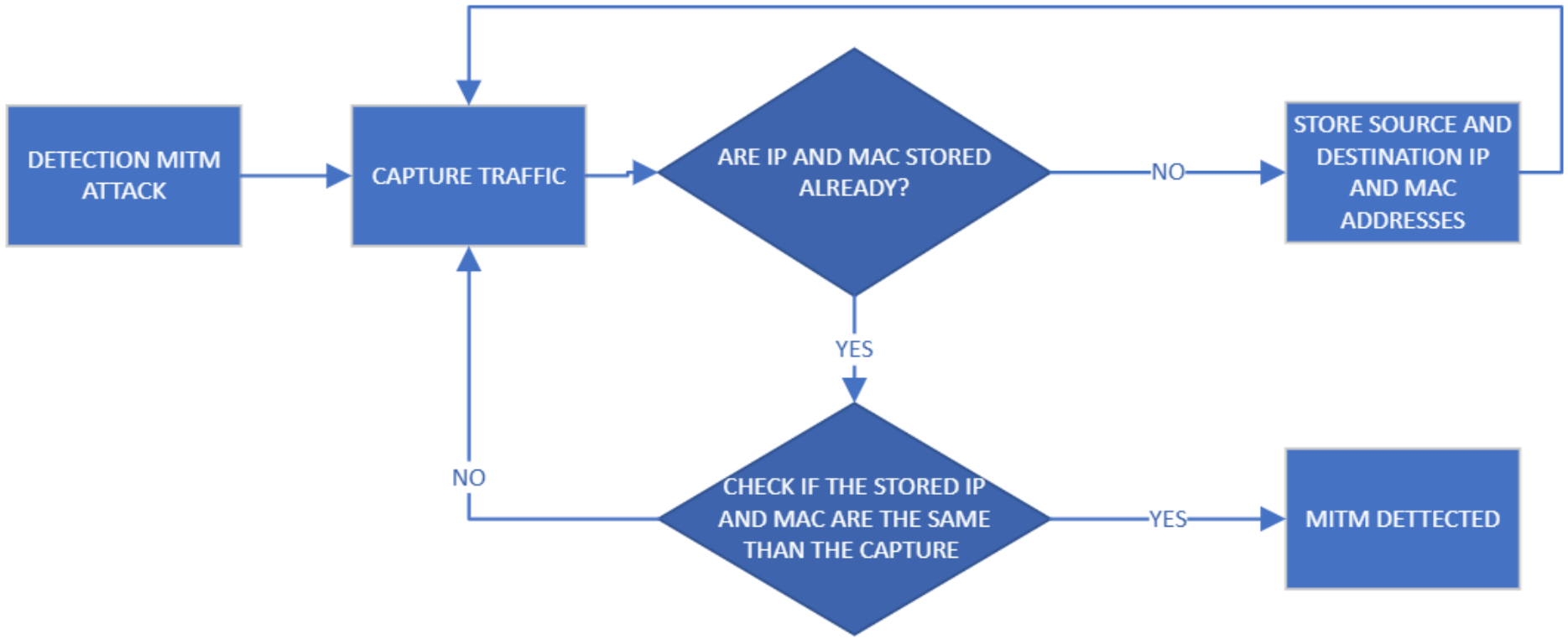
- TESTING: 150 000 rows for benign traffic and 150 000 rows for DDos traffic.
- For the DDos traffic:
  - 50 000 rows UDP.
  - 50 000 rows TCP.
  - 50 000 rows ICMP.

MAN IN THE MIDDLE ATTACK

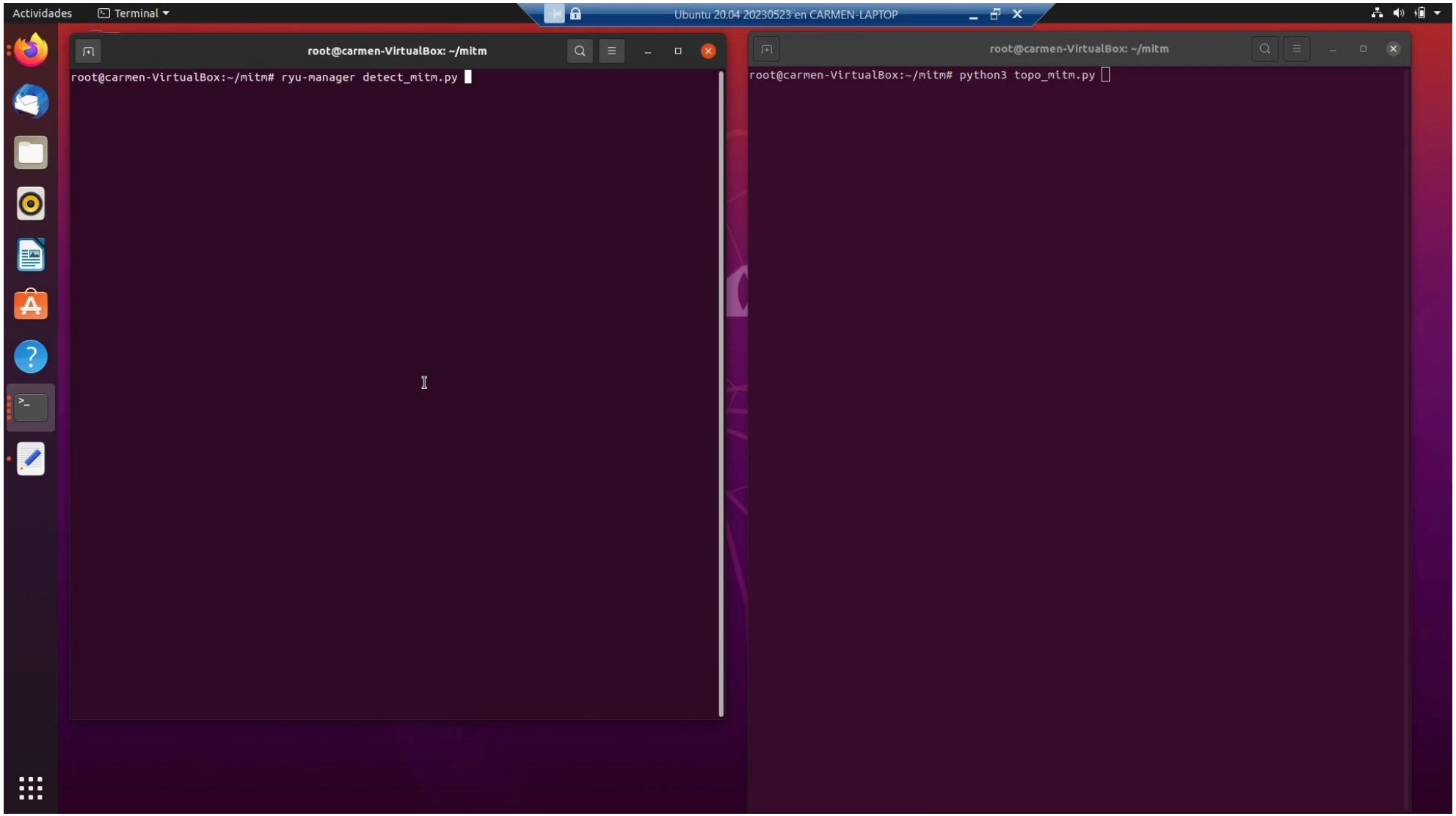


- MITM consists of a cybersecurity attack where a malicious actor intercepts and possibly alters communication between two parties who believe they are directly communicating with each other.
- ARP poisoning consists of manipulate an ARP packet so the man in the middle gets the traffic from the communication.
- To detect the MITM, the controller will capture the incoming traffic and get the source and destination IP and MAC addresses. We will store this tuple information so when we have new incoming traffic, we will compare the new tuple with the stored tuple.

CLASSIFICATION PROCESS

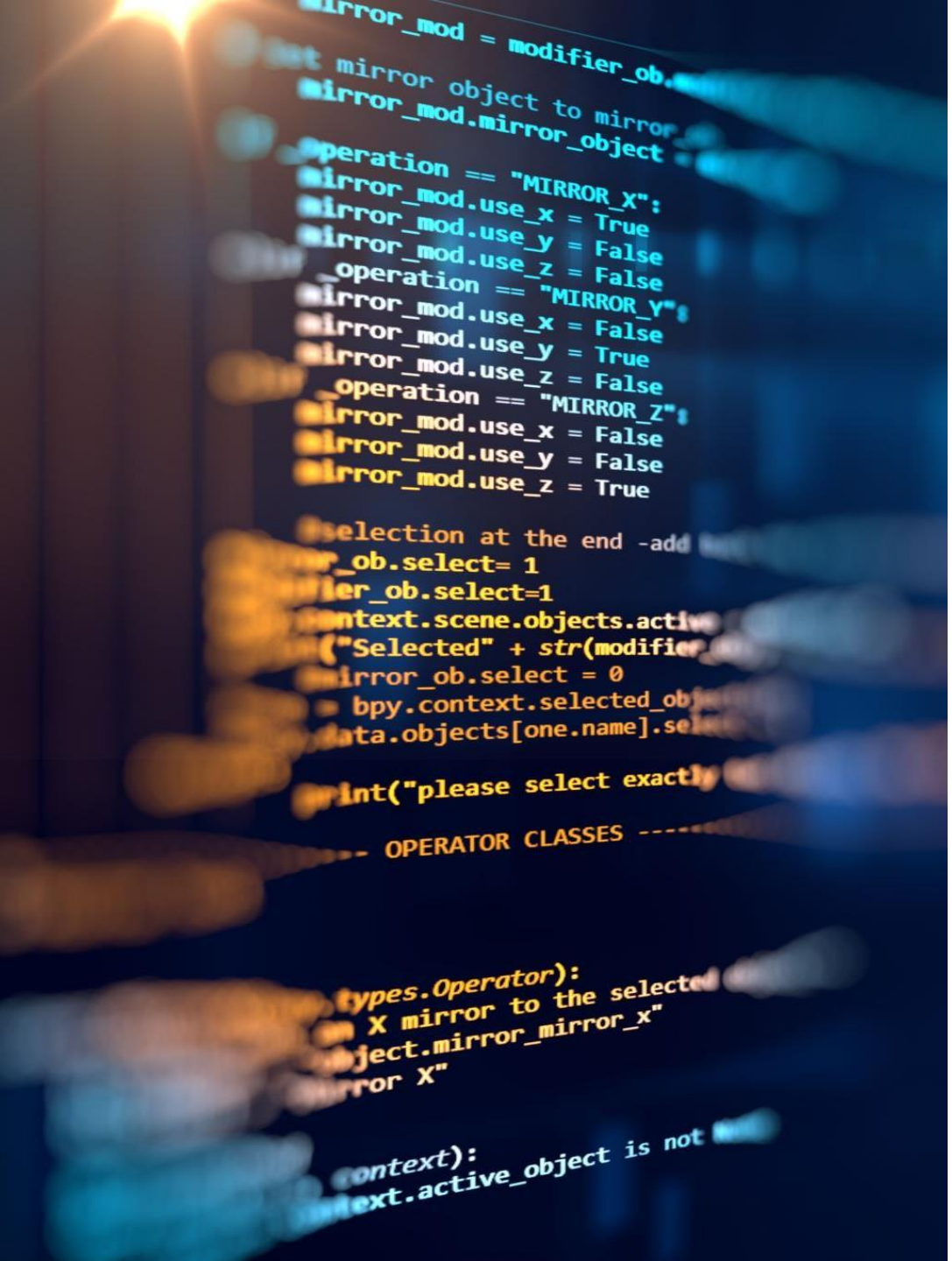


EXAMPLE DETECTING MITM ATTACK



CONCLUSION

- SDN offers a new level of flexibility because separates the control plane and the data plane in a network infrastructure.
- Generation and collection of benign and DDoS traffic in a dataset.
- It is important to study the features of the dataset because this will affect radically the accuracy.
- Accuracy improves using this 6 features ip source, packet_count, packet_count_per_second,packet_count_per_nsecond,byte_count_per_second,byte_count_per_nsecond.
- Each ML method will get a different accuracy based on how we want to study the data.
- Logistic Regression and K-Nearest Neighbors are the most constant methods to classify DDos attacks.
- MITM performs an ARP poisoning to get the traffic from a desire communication.
- MITM will attack a SDN but it is easy to detect it.



FUTURE WORK

- Generate different types of attack data in SDN other than DDoS from SDN simulator.
- Classify different type of attacks and identify top variables for each attack.
- Evaluate using different types of controllers for RYU, POX, OpenDaylight etc., for DDoS attacks and other different types of attacks.
- Mitigate DDos attack.

REFERENCES

- H. Bisht, M. Patra and **S. Kumar**, " Detection and Localization of DDoS attack during Inter-Slice Handover in 5G Network Slicing", 20th IEEE Internatonal Conference on Consumer Communications, January 2023
- Jeeva Chelladhurai, Pethuru Raj Chelliah and **Sathish A.P. Kumar**, "Securing Docker Containers from Denial of Service (DoS) Attacks" in 13th IEEE International Conference on Service Computing (IEEE SCC), pp. 856-859, 2016
- Kumari, K., Mrunalini, M. Detecting Denial of Service attacks using machine learning algorithms. J Big Data 9, 56 (2022). https://doi.org/10.1186/s40537-022-00616-0
- https://scikit-learn.org/stable/
- https://github.com/dz43developer/sdn-network-ddos-detection-using-machine-learning/blob/master/mininet/generate_benign_trafic.py
- https://www.freecodecamp.org/news/feature-engineering-and-feature-selection-for-beginners/
- https://mdh.diva-portal.org/smash/get/diva2:1741686/FULLTEXT01.pdf