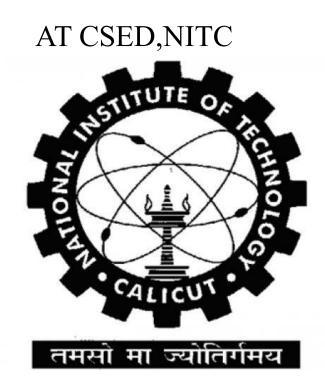
# INTERNSHIP REPORT

UNDER GUIDANCE OF DR.ARUN RAJ KUMAR P.



# BY MUMMANA SANJAY

BTECH MAJOR - MECHANICAL ENGINEERING [NITK] MINOR - COMPUTER SCIENCE [NITK]

# TASK 3 ASSIGNED ON 3<sup>RD</sup> JUNE:

Title: Analysis of Network Traffic Datasets: CIC DDoS 2019 and CSE-CIC-IDS2018

## Task:

- Determine the total dimensions (mxn) of each dataset.
- Count the number of genuine and malicious traffic samples in each dataset.
- Calculate the percentage of malicious samples that consume TCP SYN Flood attacks for both datasets.
- Identify the top features by information gain for each dataset.
- Present the dataset statistics, including total dimensions, genuine samples, malicious samples, and TCP SYN Flood percentage.
- Explore the distribution of label types within each dataset.

#### NOTE:

- TABLE 1 gives general info of both datasets.
- TABLE 2 gives general info of information gains.
- TBALE 3 [2018] and TABLE 4 [2019] are giving info regarding the types of attacks in both datasets.

#### TABLE1:

| Dataset                             | CIC DDoS 2019  | CSE-CIC-IDS2018  |
|-------------------------------------|--|--|
| Total Dimensions<br>(mxn)           | 1,874,788 x 88   | 607,012 x 80   |
| Genuine Samples                     | 26,222   | 0  |
| Malicious Samples                   | 1,848,566  | 607,012  |
| TCP SYN Flood %                     | 8.61%  | 0.00%  |
| Top Features by<br>Information Gain | Average Packet Size, Packet Length Mean, Fwd<br>Packet Length Mean, Avg Fwd Segment Size, Max<br>Packet Length | Fwd Pkts/s, Flow IAT Max, Dst<br>Port, Flow Pkts/s, Flow<br>Duration |

## TABLE 2:

| Rank | CIC DDoS 2019<br>(Feature) | Information<br>Gain | Rank | CSE-CIC-IDS2018<br>(Feature) | Information<br>Gain |
|------|----------------------------|---------------------|------|------------------------------|---------------------|
| 1    | Average Packet Size        | 1.562453            | 1    | Fwd Pkts/s                   | 1.003015            |
| 2    | Packet Length Mean         | 1.550324            | 2    | Flow IAT Max                 | 1.001102            |
| 3    | Fwd Packet Length<br>Mean  | 1.539658            | 3    | Dst Port                     | 1.000434            |
| 4    | Avg Fwd Segment Size       | 1.539144            | 4    | Flow Pkts/s                  | 0.997708            |
| 5    | Max Packet Length          | 1.536757            | 5    | Flow Duration                | 0.986621            |

## TABLE 3 [2018]:

## **Label Types**

Benign, Bot, nan, DoS attacks-SlowHTTPTest, DoS attacks-Hulk, Brute Force -Web, Brute Force -XSS, SQL Injection, Label, DoS attacks-GoldenEye, DoS attacks-Slowloris, FTP-BruteForce, DDOS attack-LOIC-UDP, DDOS attack-HOIC

## TABLE 4[2019]:

| Day        | Attack Types   |
|------------|--|
| First Day  | PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN                             |
| Second Day | NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, TFTP |

----THANK YOU-----