**Motivation**

The total number of attacks increased by 75.60% in the first half of 2022 compared to the second half of 2021, according to Nexusguard INT (2022). According to Amazon's report Shield (2020), the DDoS attack rate hit 2.3 Tbps in the first quarter of 2020. These attacks also come at increased financial cost.

Internet Service Providers (ISP) and businesses use a variety of solutions and Scrubbing Centers, such as Radware DefensePro, Radware Cloud DDoS Protection Service, Cloudflare DDoS Mitigation Services, etc., as defenses against DDoS attacks. Multi-layered protection, real-time threat detection, reporting, and analytics are just a few of the features available with all of these solutions However, actual DDoS attacks are more advanced, faster, and occurring at rates never before seen. Botnets are much more secure and less centralized. An innovative strategy to improve the automation and accuracy of centers is the use of intelligent scrubbing centers. So-called Next Generation Scrubbing Centers (NGSC) are scrubbing facilities based on machine learning.

**Objective**

To enhance the IDS’s performance in the detection of the DDoS attack

**Solution**

The adversary model aims to generate DDoS attacks on the network traffic that remains undetected by the ML-based IDS. Therefore, the generator model should be able to control the value of the features that are used by the IDS to decide whether to block the traffic or forward it to the server. To accomplish this, we need a qualitative awareness of the relationship between the model’s

prediction and the attributes of the data instance used to make that prediction.

We investigate the effectiveness of the model in generating DDoS attacks data which follow the data distribution of the samples in the dataset

**Choice of algorithm**

We used to models Linear regression & SVM:

1. Linear-regression models have become a proven way to scientifically and reliably predict the future. Because linear regression is a long-established statistical procedure, the properties of linear-regression models are well understood and can be trained very quickly.
2. SVM is a supervised machine learning algorithm which can be used for classification or regression problems. It uses a technique called the kernel trick to transform your data and then based on these transformations it finds an optimal boundary between the possible outputs

**Summary**

DDoS detection is still a difficult issue in cybersecurity. DDoS detection using machine learning (ML) and deep learning (DL) algorithms has recently attracted more attention. Ironically, ML/DL techniques can be used to generate attack traffic in order to evade detection even though they can improve detection accuracy. Those facets of ML-based DDoS detection and anti-detection techniques are covered in this paper.

First, we collect data from “**CIC-DDoS2019 Dataset**”. Then we applied basic steps for preparing the data like cleaning (includes removing null values and duplicates) and balancing (using oversampling), featuring, and splitting the data into training and testing sets. After that we used the Linear Model and passed our data to it to find patterns and make predictions.

The detection method demonstrated a high level of accuracy in identifying DDoS attacks with a 94.3% accuracy rate while SVM model gave a higher accuracy with 99.9%.