**Internship Project: DDoS Attack Detection Using Entropy-Based Analysis**

horizontal line

# Introduction

During my internship, I worked on a project focused on detecting Distributed Denial of Service (DDoS) attacks, a prevalent and dangerous cyber threat that overwhelms servers with excessive traffic, making them inaccessible to legitimate users. The project aimed to develop a method using Node.js to detect DDoS attacks through entropy-based analysis of network traffic, and to integrate this method into a MERN stack application.

## Project Overview:

The project involved the following key components:

* **Simulating Network Traffic:**
* **Normal Traffic:** Generated from a wide range of IP addresses, resulting in higher entropy due to the diverse distribution.
* **Attack Traffic:** Simulated by concentrating traffic from a smaller set of IP addresses, leading to lower entropy.
* **Entropy Calculation:**
* Entropy, a concept from information theory, was used to measure the randomness in the distribution of IP addresses.
* The Shannon entropy formula was applied to calculate the entropy of the traffic data.
* **Threshold Setting:**
* A threshold entropy value was established by averaging the entropy values from normal and attack traffic.
* This threshold served as the basis for classifying incoming traffic as either normal or indicative of a potential DDoS attack.
* **Detection and Accuracy Measurement:**
* The system classified traffic based on whether its entropy was above or below the threshold.
* Detection accuracy was assessed by running multiple test scenarios, comparing the results to expected outcomes.
* **Integration with MERN Stack:**
* The DDoS detection logic was integrated into a MERN stack application, using an Express.js backend to handle the detection process and providing an API endpoint for interaction with a frontend React.js application.

**Implementation Details:**

1. **Traffic Simulation:**

* **Function:** sendPackets(numPackets, numIps, attack = false)
* **Purpose:** Simulates network traffic by generating IP addresses.
  + **Normal Traffic:** IP addresses are evenly distributed, representing legitimate traffic.
  + **Attack Traffic:** Traffic is concentrated from a smaller set of IP addresses, simulating a DDoS attack.

1. **Entropy Calculation:**

* **Function:** computeEntropy(traffic)
* **Purpose:** Calculates the Shannon entropy of the simulated traffic.
  + **Entropy Formula:** H=−∑(p(i)⋅log⁡2(p(i)))H = -\sum (p(i) \cdot \log\_2(p(i)))H=−∑(p(i)⋅log2​(p(i))), where p(i)p(i)p(i) is the probability of packets originating from IP address iii.

1. **Traffic Classification:**

* **Function:** detectDdos(traffic, thresholdEntropy)
* **Purpose:** Classifies the traffic based on its entropy.
  + **Classification:** Traffic is classified as normal if the entropy is above the threshold and as a DDoS attack if it is below the threshold.

1. **Detection Accuracy:**

* **Function:** findAccuracy(numTests, numPackets, numIps, thresholdEntropy, verbose = false)
* **Purpose:** Measures the accuracy of the DDoS detection method.
  + **Method:** Runs multiple test scenarios to compare the detection results against expected outcomes.

1. **Express.js Integration:**

* **API Endpoint:** /api/detect-ddos
* **Purpose:** Provides an interface for the frontend to trigger the DDoS detection process.
  + **Request Handling:** The API accepts parameters for the number of packets, IPs, and tests, and returns the detection results in JSON format.

**Results:**

The entropy-based detection method successfully identified DDoS attacks by distinguishing between normal and attack traffic. Normal traffic exhibited higher entropy, while DDoS attack traffic showed lower entropy. The integration into the MERN stack application enabled real-time monitoring and interaction.

**Conclusion:**

This project effectively demonstrated the use of entropy-based analysis for detecting DDoS attacks. The integration into a MERN stack application provided a practical and scalable solution for real-time network traffic monitoring. Future work could involve enhancing the system with machine learning techniques to improve detection accuracy further.