Dataset Description – CICIDS2017

The dataset used in this project is the CICIDS2017 dataset, created by the Canadian Institute for Cybersecurity. It is widely regarded as one of the most comprehensive and realistic benchmarks for evaluating Intrusion Detection Systems (IDS).

◆ Key Features of the Dataset

- Captures both normal network traffic and multiple attack scenarios.
- Traffic was collected using real network configurations, including servers, clients, routers, and switches.
- Provides labeled data, meaning each record is categorized as either normal or a specific attack type.
- Includes more than 80 network traffic features, such as duration, protocol type, source/destination IP, flow information, and statistical features.

◆ Attack Categories

The dataset covers a wide range of contemporary cyberattacks, including:

- Denial of Service (DoS) / Distributed Denial of Service (DDoS)
- Port Scanning attacks
- Web Attacks (e.g., Brute Force, XSS, SQL Injection)
- Infiltration attacks
- Botnet traffic
- Normal user activity for baseline comparison

◆ Data Files Used in This Project

For experimentation, the dataset is divided into multiple CSV files corresponding to specific days and attack scenarios:

- **Monday-WorkingHours.pcap_ISCX.csv** – Contains only normal traffic.
- **Tuesday-WorkingHours.pcap_ISCX.csv** – Includes DoS attacks.
- **Wednesday-workingHours.pcap_ISCX.csv** – Contains Brute Force & Web attacks.
- **Thursday-WorkingHours-Morning-WebAttacks.pcap_ISCX.csv** – Focus on Web attacks.
- **Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX.csv** – Covers Infiltration attacks.
- **Friday-WorkingHours-Morning.pcap_ISCX.csv** – Mix of normal and suspicious traffic.
- **Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv** – Includes Port Scan attacks.
- **Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv** – Includes DDoS attacks.

Dataset Link:
https://drive.google.com/drive/folders/1Mko-LkUO7gEiaC-1ak6SomuLd3QC8OBY?usp=drive_link