# Common Features

|  |  |  |  |
| --- | --- | --- | --- |
| Feature | [CIC APT IIoT Dataset 2024](https://www.unb.ca/cic/datasets/iiot-dataset-2024.html) | [CIC-BCCC-NRC-TabularIoTAttacks-2024](https://www.unb.ca/cic/datasets/tabular-iot-attack-2024.html) | [CIC IoT-DIAD 2024 dataset](https://www.unb.ca/cic/datasets/iot-diad-2024.html) |
| Flow Duration | flow\_duration | Flow Duration | Flow Duration |
| Source IP | Source IP | Src IP | Src IP |
| Source Port | Source Port | Src Port | Src Port |
| Destination IP | Destination IP | Dst IP | Dst IP |
| Destination Port | Destination Port | Dst Port | Dst Port |
| Protocol | Protocol Type | Protocol | Protocol |
| Timestamp | ts | Timestamp | Timestamp |
| Flow Bytes/s | Rate | Flow Bytes/s | Flow Bytes/s |
| Flow Packets/s | Flow Packets/s | Flow Packets/s | Flow Packets/s |
| FIN Flag Count | fin\_flag\_number | FIN Flag Count | FIN Flag Count |
| SYN Flag Count | syn\_flag\_number | SYN Flag Count | SYN Flag Count |
| RST Flag Count | rst\_flag\_number | RST Flag Count | RST Flag Count |
| PSH Flag Count | psh\_flag\_number | PSH Flag Count | PSH Flag Count |
| ACK Flag Count | ack\_flag\_number | ACK Flag Count | ACK Flag Count |
| URG Flag Count | urg\_flag\_number | URG Flag Count | URG Flag Count |
| CWR Flag Count | cwr\_flag\_number | CWR Flag Count | CWR Flag Count |
| ECE Flag Count | ece\_flag\_number | ECE Flag Count | ECE Flag Count |
| Active Mean | flow\_active\_time | Active Mean | Active Mean |
| Idle Mean | flow\_idle\_time | Idle Mean | Idle Mean |

# Type of Attacks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attacks | [CIC APT IIoT Dataset 2024](https://www.unb.ca/cic/datasets/iiot-dataset-2024.html) | [CIC-BCCC-NRC-TabularIoTAttacks-2024](https://www.unb.ca/cic/datasets/tabular-iot-attack-2024.html) | [CIC IoT-DIAD 2024](https://www.unb.ca/cic/datasets/iot-diad-2024.html) | |
| 1. collection 2. cleanup 3. discovery 4. credential access 5. command and control 6. persistence 7. exfiltration 8. lateral movement   total sampling for all : 1004 | 1. DDoS ICMP Flood 2. DDoS UDP Flood 3. DoS ICMP Flood 4. DoS UDP Flood 5. MITM ARP Spoofing 6. MQTT DDoS Publish Flood 7. MQTT DoS Connect Flood 8. MQTT DoS Publish Flood 9. MQTT Malformed 10. Recon OS Scan 11. Recon Ping Sweep 12. Recon Port Scan 13. Recon Vulnerability Scan | In paper description | In dataset 2024 |
| 1. DDoS 2. Brute Force 3. Spoofing 4. DoS 5. Recon 6. Web-based 7. Mirai | 1. Vulnerability Scan 2. DDoS-HTTP\_Flood 3. DDoS-ACK\_Fragmentation 4. DDoS-ICMP\_Flood 5. DNS\_Spoofing 6. Mirai-greeth\_flood 7. MITM-ArpSpoofing 8. SqlInjection |