**Comparison of CIC IoT-DIAD 2024, CIC APT IIoT 2024, CIC-BCCC-NRC TabularIoTAttack-2024, and CIC EV Charger Attack Dataset 2024 (CICEVSE2024)**

[**1. CIC IoT-DIAD 2024**](https://www.unb.ca/cic/datasets/iot-diad-2024.html)

1. **Purpose:**
   * Dual-purpose dataset for:
     + **IoT device identification**.
     + **Anomaly detection**.
   * Focused on improving security analytics for general IoT environments.
2. **Environment:**
   * **Traditional IoT network** with **105 devices**.
3. **Attack Types:**
   * **33 attack types**, grouped into 7 categories:
     + **DDoS**, **DoS**, **Recon**, **Web-based**, **Brute Force**, **Spoofing**, and **Mirai**.
4. **Data Collected:**
   * **Packet-based** and **flow-based feature extraction**.

[**2. CIC APT IIoT 2024**](https://www.unb.ca/cic/datasets/iiot-dataset-2024.html)

1. **Purpose:**
   * Designed for **Advanced Persistent Threat (APT)** detection in **industrial IoT (IIoT)** environments.
2. **Environment:**
   * **IIoT hybrid testbed** (real + simulated components).
   * Inspired by **APT29 attack group scenarios**.
3. **Attack Types:**
   * Focused on **APT campaigns**.
4. **Data Collected:**
   * **Provenance logs** and **network traffic data**.

[**3. CIC-BCCC-NRC TabularIoTAttack-2024**](https://www.unb.ca/cic/datasets/tabular-iot-attack-2024.html)

1. **Purpose:**
   * Created for training and testing **AI-powered IoT cybersecurity models**.
   * Focuses on **detecting and identifying IoT-specific cyberattacks**.
2. **Environment:**
   * Simulated **realistic IoT environments** with **real devices** and attack scenarios.
   * Combines data from **nine widely used datasets** for augmentation.
3. **Attack Types:**
   * Rich and diverse **labeled attack scenarios**.
4. **Data Collected:**
   * Augmented **IoT network traffic data**.

[**4. CIC EV Charger Attack Dataset 2024 (CICEVSE2024)**](https://www.unb.ca/cic/datasets/evse-dataset-2024.html)

1. **Purpose:**
   * Focused on cybersecurity research for **electric vehicle charging stations (EVSE)**.
   * Targets the identification of attacks in **idle** and **charging states** of EV chargers.
2. **Environment:**
   * **Operational EV charging station lab setup**:
     + Level 2 charging station (EVSE-A).
     + Raspberry Pi devices simulating the **Electric Vehicle Communication Controller (EVCC)**, **local CSMS**, and power monitoring.
     + Communication using **OCPP** and **ISO15118 protocols**.
3. **Attack Types:**
   * **Network Attacks**: Reconnaissance, Denial-of-Service (DoS).
   * **Host Attacks**: Backdoor, Cryptojacking.
4. **Data Collected:**
   * **Power consumption data**.
   * **Network traffic captures**.
   * **Host activities** under benign and attack conditions.
5. **Applications:**
   * **Behavioural profiling** and **anomaly detection**.
   * Binary and multi-class classification using machine learning.

**Key Differences**

|  |  |  |  |
| --- | --- | --- | --- |
| Feature | CIC IoT-DIAD 2024 | CIC APT IIoT 2024 | CIC-BCCC-NRC TabularIoTAttack-2024 |
| Purpose | IoT device identification & anomaly detection. | Detecting APTs in IIoT environments. | Training/testing AI cybersecurity models. |
| Environment | Traditional IoT network (105 devices). | IIoT hybrid testbed (real + simulated). | Realistic IoT environments (real + simulated). |
| Attack Types | 33 attacks (7 categories). | APT campaigns. | Diverse IoT-specific attack scenarios. |
| Data Collected | Packet and flow-based features. | Provenance logs, network traffic. | Augmented network traffic. |
| Special Features | Focus on general IoT anomalies. | APT29-inspired scenarios. | Combines data from 9 datasets for robustness. |

**Summary**

* **CIC IoT-DIAD 2024**: Best for general IoT device identification and anomaly detection.
* **CIC APT IIoT 2024**: Focused on APT detection in industrial IoT settings.
* **CIC-BCCC-NRC TabularIoTAttack-2024**: Comprehensive for training/testing AI models in IoT security.
* **CIC EV Charger Attack Dataset 2024**: Specialized for EV charger security, combining power consumption and network data under various conditions.