A diagram of a car

AI-generated content may be incorrect.

A diagram of a charging station

AI-generated content may be incorrect.

A car charging at a charging station

AI-generated content may be incorrect.

A car with a computer connected to it

AI-generated content may be incorrect.

Yes, there are now publicly available datasets specifically designed for detecting DDoS and other cyberattacks on Electric Vehicles (EVs) and EV charging infrastructure. These datasets are well-suited for developing and evaluating adaptive federated deep learning models for cybersecurity in EV ecosystems.

**🔐 Recommended Datasets for EV Cybersecurity Research**

**1. CICEV2023 – DDoS Attack Dataset for EV Authentication**

* **Focus**: Simulates DDoS attacks targeting EV authentication processes within charging infrastructure.
* **Features**:
  + Four attack scenarios: Correct EV ID, Wrong EV, Wrong EV Timestamp, and Wrong Charging Station (CS) Timestamp.
  + Includes system performance metrics such as CPU cycles, branch instructions, and timing differences.
  + Data collected using a custom simulator in a Linux environment.
* **Use Case**: Ideal for training and testing classifiers aimed at detecting DDoS attacks during EV authentication.
* **Access**: CICEV2023 Dataset[University of New Brunswick+2ResearchGate+2CoLab+2](https://www.researchgate.net/publication/375855013_DDoS_Attack_Dataset_CICEV2023_against_EV_Authentication_in_Charging_Infrastructure?utm_source=chatgpt.com)[University of New Brunswick+1GitHub+1](https://www.unb.ca/cic/datasets/cicev2023.html?utm_source=chatgpt.com)

**2. CICEVSE2024 – EV Charger Attack Dataset**

* **Focus**: Comprehensive dataset capturing both network and host-based attacks on EV charging stations.
* **Features**:
  + Attack types include Reconnaissance, Denial-of-Service (DoS), Backdoor, and Cryptojacking.
  + Data encompasses power consumption, network traffic (pcap files), and host activities (e.g., hardware performance counters).
  + Collected from a real-world testbed using Level 2 charging stations and Raspberry Pi-based monitoring systems.
* **Use Case**: Suitable for behavioral profiling, anomaly detection, and developing intrusion detection systems (IDS) for EV charging infrastructure.
* **Access**: CICEVSE2024 Dataset[University of New Brunswick+1GitHub+1](https://www.unb.ca/cic/datasets/evse-dataset-2024.html?utm_source=chatgpt.com)[MDPI+2GitHub+2University of New Brunswick+2](https://github.com/CrashedBboy/ML-NetworkAttack-Detection?utm_source=chatgpt.com)

**🧠 Applying Adaptive Federated Deep Learning**

These datasets are particularly valuable for exploring adaptive federated learning approaches in EV cybersecurity. For instance, the CICEVSE2024 dataset has been utilized to develop a Federated Averaging Learning Classifier (FALC), enabling decentralized training of intrusion detection models without sharing raw data. This approach enhances privacy and scalability in distributed EV charging networks. [ACM Digital Library+4PubMed Central+4MDPI+4](https://pmc.ncbi.nlm.nih.gov/articles/PMC11920061/?utm_source=chatgpt.com)[MDPI](https://www.mdpi.com/2227-7390/13/5/712?utm_source=chatgpt.com)

**📝 Suggested Paper Structure**

To structure your paper on "An Adaptive Federated Deep-Learning Model for Cybersecurity Attacks Detection on Electric Vehicles," consider the following outline:

1. **Introduction**
   * Overview of cybersecurity challenges in EV ecosystems.
   * Importance of DDoS attack detection in EV and charging infrastructure.
   * Motivation for using federated deep learning approaches.[ResearchGate](https://www.researchgate.net/publication/375855013_DDoS_Attack_Dataset_CICEV2023_against_EV_Authentication_in_Charging_Infrastructure?utm_source=chatgpt.com)
2. **Related Work**
   * Review of existing intrusion detection systems in EV contexts.
   * Discussion of federated learning applications in cybersecurity.
3. **Datasets**
   * Detailed description of CICEV2023 and CICEVSE2024 datasets.
   * Justification for their selection in your study.[MDPI+8CoLab+8University of New Brunswick+8](https://colab.ws/articles/10.1016/j.iot.2024.101343?utm_source=chatgpt.com)[University of New Brunswick](https://www.unb.ca/cic/datasets/cicev2023.html?utm_source=chatgpt.com)
4. **Methodology**
   * Design of the adaptive federated deep learning model.
   * Implementation details, including model architecture and training procedures.
   * Federated learning setup and communication protocols.
5. **Experimental Setup**
   * Data preprocessing steps.
   * Evaluation metrics (e.g., accuracy, precision, recall, F1-score).
   * Baseline models for comparison.
6. **Results and Discussion**
   * Performance analysis of the proposed model.
   * Comparison with baseline models.
   * Discussion on the adaptability and scalability of the model.[ScienceDirect+27Siemens Blog Network+27arxiv.org+27](https://blogs.sw.siemens.com/ee-systems/2021/04/13/firewalling-cybersecurity-threats-for-connected-cars/?utm_source=chatgpt.com)[illuminei.com](https://www.illuminei.com/blog/charging-up-how-innovative-design-is-revolutionizing-ev-charging-stations-design?utm_source=chatgpt.com)[PubMed Central+5MDPI+5MDPI+5](https://www.mdpi.com/1996-1073/15/11/3931?utm_source=chatgpt.com)
7. **Conclusion and Future Work**
   * Summary of findings.
   * Limitations of the current study.
   * Directions for future research, such as real-world deployment and integration with other security mechanisms.[Nano NTP+29MDPI+29MDPI+29](https://www.mdpi.com/1424-8220/23/15/6716?utm_source=chatgpt.com)

If you need assistance with implementing the federated learning framework or further guidance on model selection and evaluation, feel free to ask!