AECR-ML FOR IOT ATTACK DETECTION IN EVS

Nguyễn Hữu Tài

[1] Trường ĐH Công Nghệ Thông Tin. ĐHQG TP.HCM

What ?

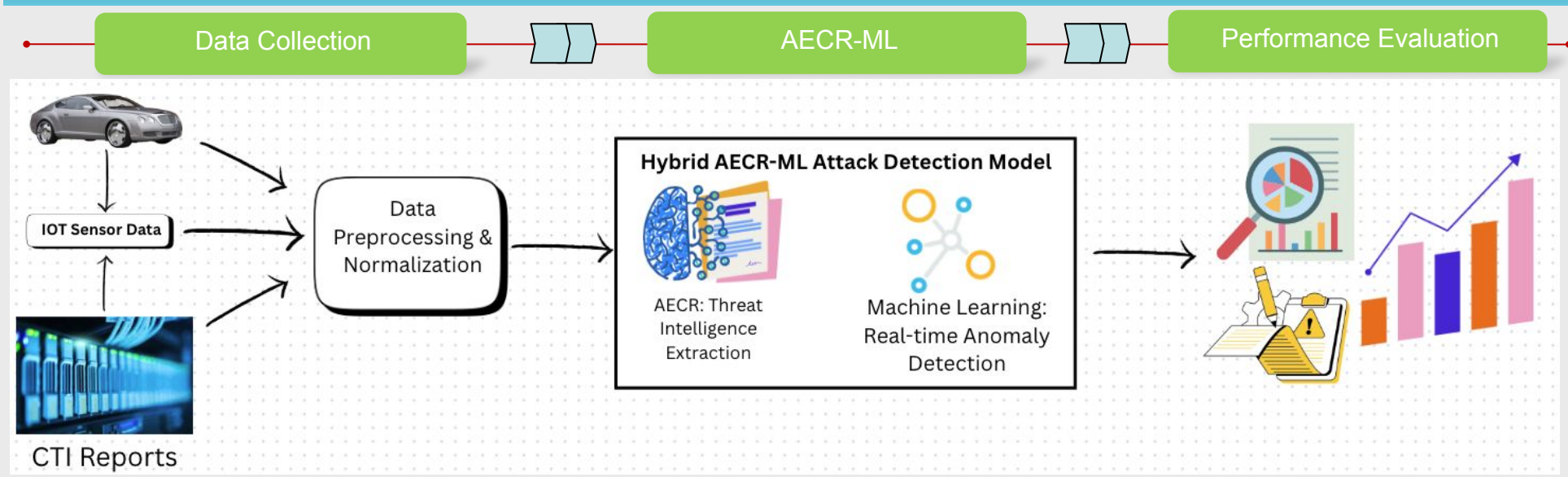
We propose AECR-ML, a hybrid framework to detect cyberattacks on electric vehicle (EV) IoT systems.

- AECR extracts technical attack intelligence from CTI reports using a fine-tuned language model.
- ML models (e.g., Random Forest, Deep Learning) detect real-time anomalies from sensor data.
- Fusion improves detection accuracy and responsiveness.

Why ?

- EVs are getting smarter but more exposed. As IoT grows in EVs, key systems like sensors and comms become prime targets for attacks (spoofing, DoS, MiTM), risking operation and safety.
- Existing solutions are reactive or narrow: Rule-based methods lack adaptability, and data-only models may miss new threats. Our model combines real-time sensor data and CTI insights for smarter, proactive defense.

Overview



Description

1. Data Collection

- Integrate IoT sensor data from EVs and intelligence from CTI reports to clean and normalize inputs for the model.

Details:

- Collect data from sensors (GPS, speed, environment,...) and CTI reports.
- Use AECR to extract attack knowledge from CTI reports.
- Normalize and synchronize data from both sources.

Figure 1. Sensor data and collection

2. AECR-ML Model

This step focuses on designing and training a hybrid machine learning model that detects cyberattacks by leveraging both sensor data and intelligence from AECR.

- **Model training:** Apply machine learning algorithms (e.g., Random Forest, SVM, Deep Learning) to identify anomalies in EV sensor data.
- **AECR feature integration:** Enrich the detection model with behavioral features extracted from CTI reports, improving detection of unknown or zero-day attacks.
- **Multi-source fusion:** Merge sensor-based features and AECR-derived insights using feature fusion strategies.
- **Optimization:** Perform hyperparameter tuning and cross-validation to ensure high accuracy, precision, and generalization.

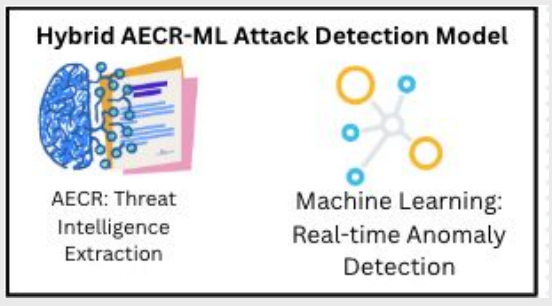


Figure 2. AECR-ML Model

3. Performance Evaluation

- Simulated Testbed: Build an EV IoT environment using Raspberry Pi and Arduino to emulate networks and sensors (e.g., CAN, MQTT).
- Attack Scenarios & Monitoring: Simulate spoofing, DoS, MiTM attacks and use the model for real-time anomaly detection.
- Model Evaluation: Measure detection accuracy, processing efficiency, and scalability across sensor types.

NII

Nguyen Huu Tai – Trường Đại học Công Nghệ Thông Tin. ĐHQG TP.HCM
Tel : 052296xxxx Email : tainh.19@grad.uit.edu.vn