Cyber Threat Detection and AI/ML-Driven Response Strategies in Electric Vehicle Charging Stations

VESTEL MOBILITY

Sabancı Üniversitesi
FACULTY OF ENGINEERING AND NATURAL SCIENCES

Students

Havva Aylin Günay
Mert Can İldem
Dilara Şentürk

Faculty Members

Albert Levi
Orçun Çetin

Company Advisors

Kaan Kahraman
Barış Mehmetoğlu

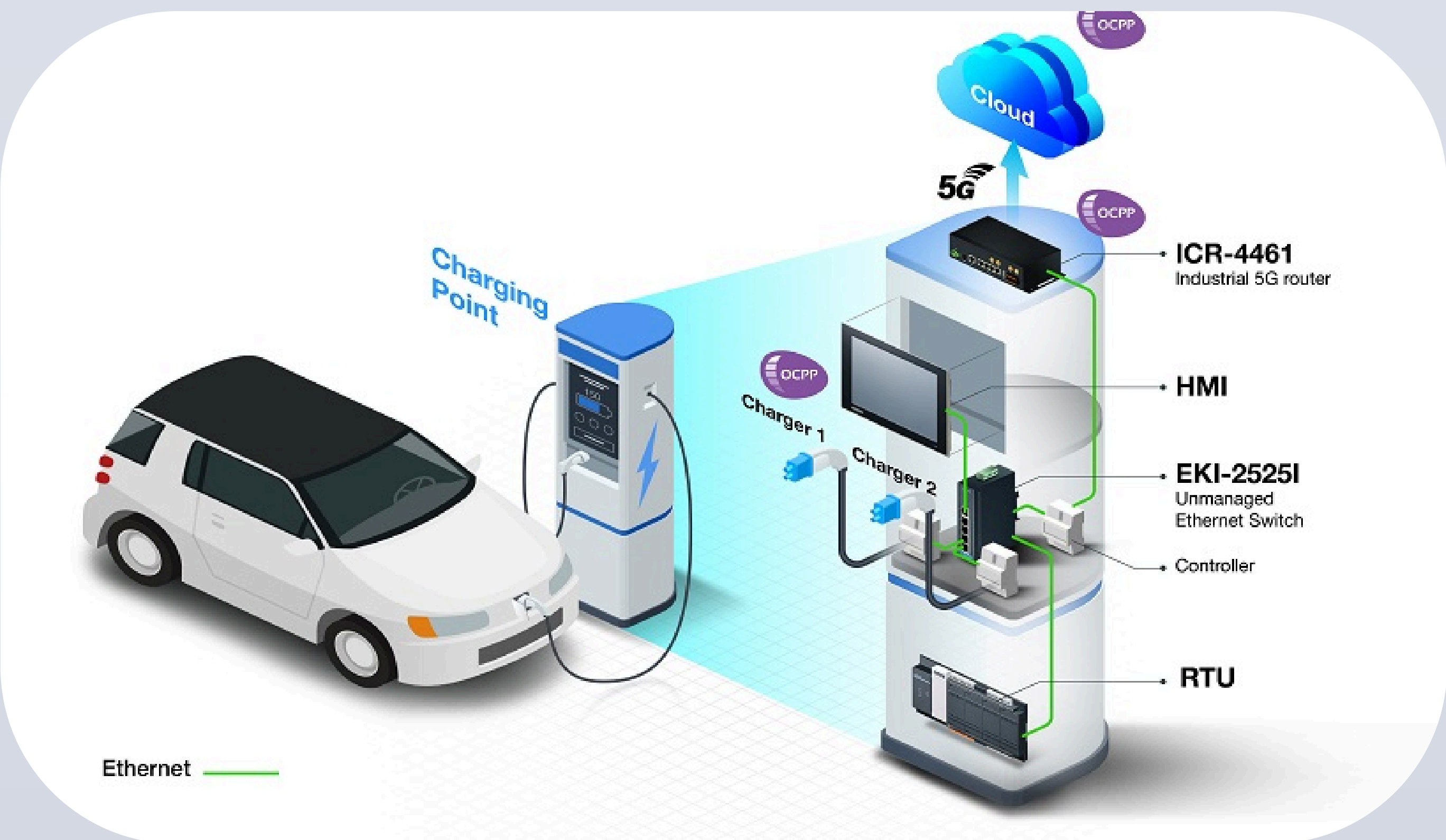
ABSTRACT

As Electric Vehicle Charging (EVC) systems expand, ensuring cybersecurity is essential. This project, in collaboration with Vestel Mobility, applied threat modeling, penetration testing, and traffic analysis to assess the security of a representative EVC system in a controlled lab environment. A custom dataset from real charger interactions was used to train lightweight machine learning models for edge deployment, laying the foundation for scalable cybersecurity in electric mobility.

OBJECTIVES

- Assess the cybersecurity posture of an Electric Vehicle Charging (EVC) system
- Perform threat modeling, penetration testing, and traffic analysis
- Identify real-world vulnerabilities in web, API, and protocol layers
- Capture and label traffic data to build a custom dataset
- Train lightweight machine learning models for real-time anomaly detection
- Design scalable and edge-compatible cybersecurity solutions for future EV infrastructure

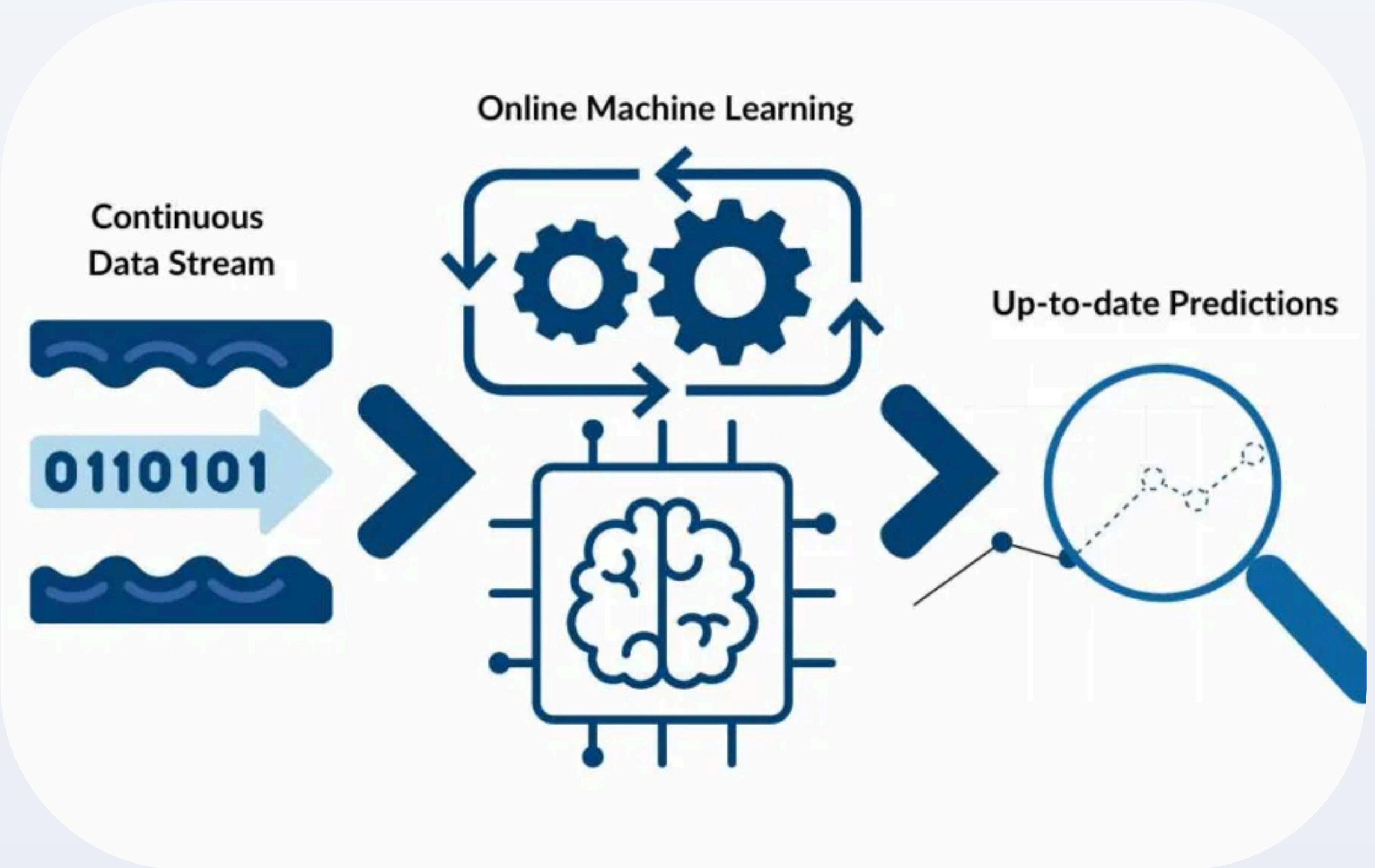
PROJECT DETAILS



Advantech, EV Charging Data Management Case Study, 2024.

- Applied a systematic methodology to assess the security of a representative EVC system developed in collaboration with Vestel Mobility.
- Built a STRIDE-based threat model to identify assets, attack vectors, and trust boundaries
- Mapped system exposure using passive (Nmap) and active (ZAP, Nessus) scanning

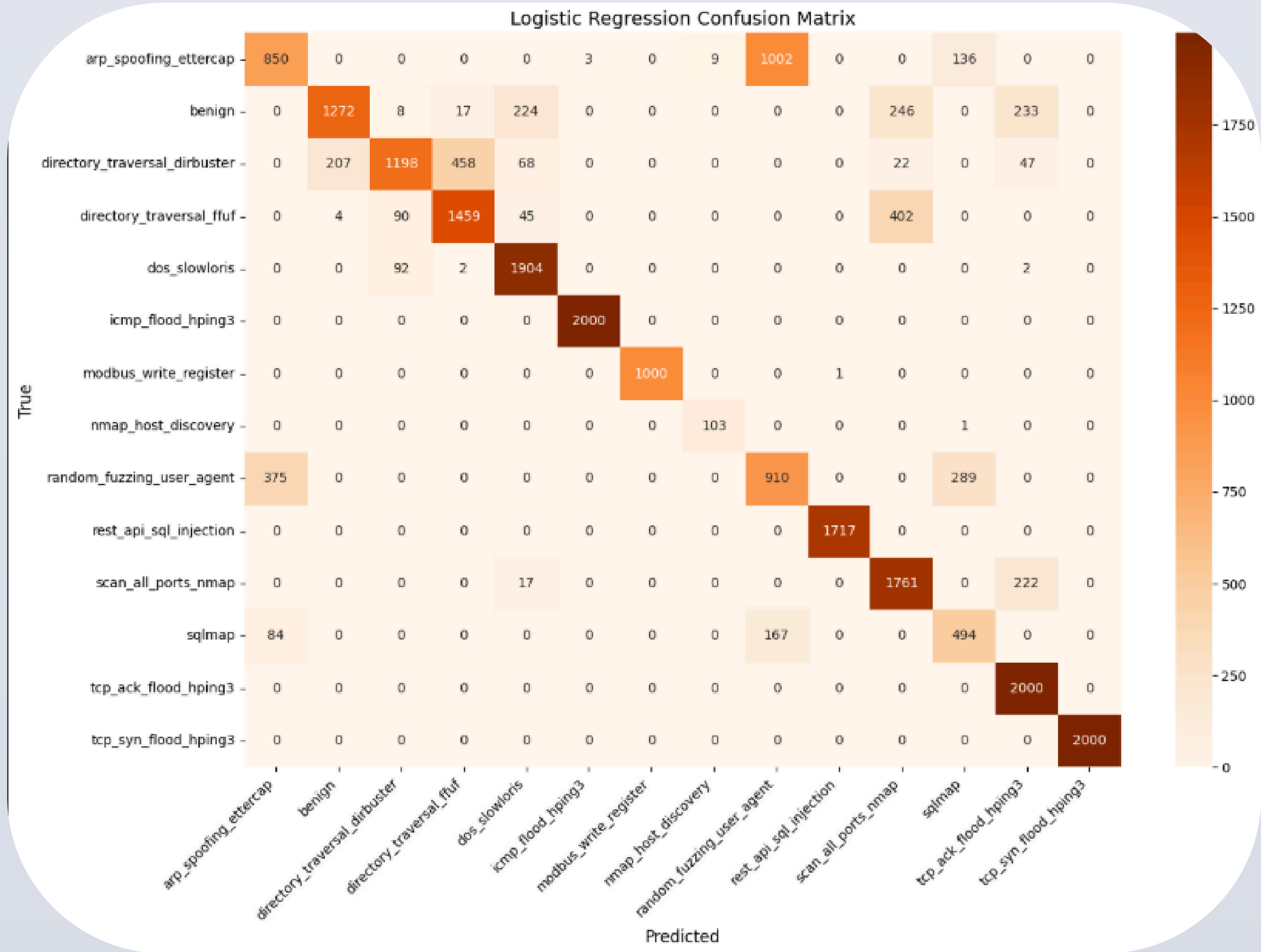
PROJECT DETAILS-II



Spot Intelligence, Online Machine Learning – A Beginner's Guide, 2024.

- Performed penetration testing in a controlled lab environment
- Testbed included the charger, backend server, and tools like Wireshark and Burp Suite
- Captured traffic was labeled to create a benign vs. attack dataset
- Extracted network and protocol features for ML processing
- Trained lightweight ML models for intrusion detection on edge devices
- Ongoing evaluation of models (e.g., decision trees, neural networks) for real-time detection

CONCLUSIONS


Logistic Regression Confusion Matrix

True \ Predicted	arp_spoofing_ettercap	benign	directory_traversal_dirbuster	directory_traversal_ffuf	dos_slowloris	icmp_flood_hping3	modbus_write_register	nmap_host_discovery	random_fuzzing_user_agent	rest_api_sql_injection	scan_all_ports_nmap	sqlmap	tcp_ack_flood_hping3	tcp_syn_flood_hping3
arp_spoofing_ettercap	850	0	0	0	0	3	0	9	1002	0	0	136	0	0
benign	0	1272	8	17	224	0	0	0	0	0	246	0	233	0
directory_traversal_dirbuster	0	207	1198	458	68	0	0	0	0	0	22	0	47	0
directory_traversal_ffuf	0	4	90	1459	45	0	0	0	0	0	402	0	0	0
dos_slowloris	0	0	92	2	1904	0	0	0	0	0	0	0	2	0
icmp_flood_hping3	0	0	0	0	0	2000	0	0	0	0	0	0	0	0
modbus_write_register	0	0	0	0	0	0	1000	0	0	1	0	0	0	0
nmap_host_discovery	0	0	0	0	0	0	0	103	0	0	0	1	0	0
random_fuzzing_user_agent	375	0	0	0	0	0	0	0	910	0	0	289	0	0
rest_api_sql_injection	0	0	0	0	0	0	0	0	0	1717	0	0	0	0
scan_all_ports_nmap	0	0	0	0	17	0	0	0	0	0	1761	0	222	0
sqlmap	84	0	0	0	0	0	0	0	167	0	0	494	0	0
tcp_ack_flood_hping3	0	0	0	0	0	0	0	0	0	0	0	0	2000	0
tcp_syn_flood_hping3	0	0	0	0	0	0	0	0	0	0	0	0	0	2000

- Potential vulnerabilities were successfully identified in a representative EVC system under controlled lab conditions
- Built and labeled a comprehensive attack vs. benign traffic dataset
- Trained lightweight ML models for anomaly detection on edge devices
- Logistic Regression model achieved strong classification on several attack types
- Lays the foundation for scalable, edge-compatible cybersecurity in smart mobility

Note: *All security assessments in this project were conducted using a specially prepared test version of the EVC system software, which was intentionally designed by Vestel for training and academic purposes. This version includes controlled vulnerabilities and does not reflect the security status of any commercial products.*