An AI-Driven Digital Twin Framework for Cyber-Attack Detection and Mitigation in Electric Vehicle Charging Infrastructure

Vinoth Kumar J[1], Dr. V. Kumar[2]

[1]*Department of Computer Science and Engineering Knowledge Institute of Technology (Autonomous), Salem Anna University, Chennai, India*

[2]*Ph.D, Department of Computer Science and Engineering Knowledge Institute of Technology (Autonomous), Salem Anna University, Chennai, India*

***Abstract*—The widespread deployment of electric vehicles is driving a new demand for advanced cybersecurity in charging infrastructure, where interconnected networks create new targets for cyber threats. This work introduces an artificial intelligence-based Digital Twin framework aimed at instantly detecting and responding to cyber-attacks on electric vehicle charging systems. By combining dynamic simulation, machine learning models, and automated defense mechanisms, the framework strengthens the resilience and security of charging operations against an evolving threat landscape, helping to ensure reliable EV usage even as cyber risks continue to grow.**

***Index Terms*—Cybersecurity, Digital Twin, Electric Vehicle, Anomaly Detection, AI, EV Charging Infrastructure, Machine Learning, Critical Infrastructure.**

I. INTRODUCTION AND MOTIVATION

The transportation industry is undergoing a major shift as electric vehicles rapidly rise in global market share and are forecasted to account for a large proportion of vehicles by the end of this decade. As public and private investment in EV charging networks climbs, the integration of Internet of Things devices and system interconnectivity continues to grow, which unfortunately also expands the attack surface for cyber threats. Modern charging infrastructure faces an array of security concerns, such as ransomware incidents, unauthorized firmware modifications, fraudulent billing, distributed denial-of-service (DDoS) attacks, and malicious attempts to disrupt grid balance.

Conventional defensive strategies, which often rely on static threat signatures and post-incident responses, are not effective against emerging vulnerabilities or sophisticated coordinated attacks. The new generation of risks calls for real-time data analysis, coordinated oversight across both operational and digital layers, and proactive, automated security mechanisms. Digital twin technologies—high-fidelity digital counterparts of physical infrastructure—offer a promising solution by enabling ongoing monitoring, simulation, and dynamic safeguarding of these critical EV charging assets.

II. LITERATURE REVIEW AND RELATED WORK

Table I surveys key studies and highlights gaps our work addresses.

TABLE I
SUMMARY OF RELATED WORK

Reference	Focus	Gaps
Sun et al. (2022) [2]	Survey of CAV security	Lacks focus on EVCI
Chattopadhyay et al. (2021) [1]	Security by design for AVs	Minimal for EV charging
Mun et al. (2022) [6]	V2V privacy in 5G-V2X	Detection, not mitigation
Khan et al. (2020) [10]	Attack mitigation in smart cars	No digital twin context
Kim et al. (2023) [7]	Federated, blockchain in V2X	Not EVCI-centric

Recent reviews [3], [5] emphasize that digital twins and ML-driven defense mechanisms are underexplored in EV charging networks.

III. ENABLING TECHNOLOGIES

A. *Digital Twin Platforms*

A digital twin creates a dynamic virtual counterpart of an electric vehicle charging station, constantly updated to reflect the real-world system's status and behavior. This setup al- lows for uninterrupted monitoring, live performance tracking, early detection of issues, and even advanced forecasting of maintenance requirements or cyber incidents. In the developed framework, real-time data collected through physical sensors is continuously transmitted to the digital twin, while the virtual model is flexibly used to simulate both standard operations and potential cyber-attack scenarios with a combination of typical and intentionally abnormal data.

B. *AI/Machine Learning for Security*

Both supervised and unsupervised machine learning ap- proaches—including models like LSTM networks, support vector machines, isolation forests, and deep autoencoders—are leveraged to detect anomalies within time series data, net- work flows, and system event logs. By continuously adapting through retraining, these algorithms remain effective as attack techniques evolve, helping to uncover new or previously unseen security threats [8]

C. *Anomaly Detection and Response*

Detecting anomalies in real time is essential for uncovering incidents such as credential abuse, unusual communication patterns, or the introduction of unauthorized hardware. Au- tomated security workflows are designed to translate these detections directly into mitigation steps, allowing the system to isolate affected devices or activate emergency shutdown procedures without manual intervention [9].

IV. PROPOSED SYSTEM ARCHITECTURE

As depicted in Figure 1, the complete system workflow begins with raw data being collected by physical sensors and fed into the central digital twin engine. This core module is responsible for analyzing incoming information, making threat predictions, and executing timely responses. Simultaneously, cloud-based monitoring dashboards provide operational teams with real-time visibility into both network health and detected security events.

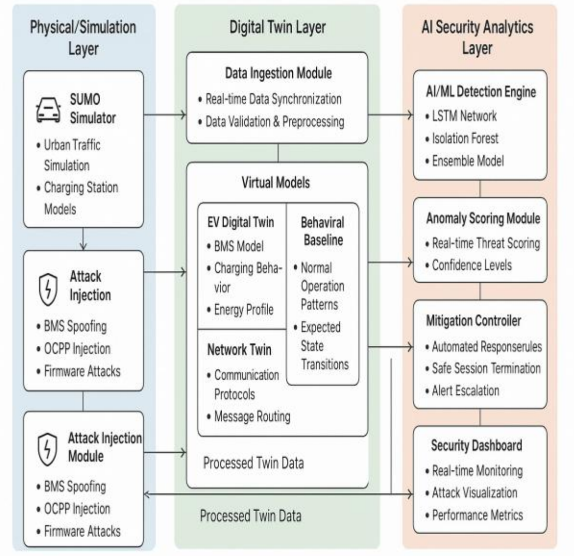

Fig. 2. High-Level Architecture of the Proposed Digital Twin Framework

VI. IMPLEMENTATION PLAN AND CASE STUDY

Our iterative methodology:

1) Model Creation: Build digital twin models of represen- tative EVCI using SUMO, Simulink, and custom IoT interfaces.
2) Data Collection: Gather baseline and attack event data from testbeds and public datasets.
3) AI Training: Develop, test, and evaluate classical and deep learning models for anomaly and intrusion detec- tion.
4) Twin Synchronization: Connect real-time feeds from simulation/physical layer into the ML evaluation loop.
5) Incident Mitigation: Validate automated response (alerts, network segmentation, etc.) upon test attacks.

A case study will simulate targeted malware/ransomware, protocol tampering, and billing fraud to evaluate system re- sponse.

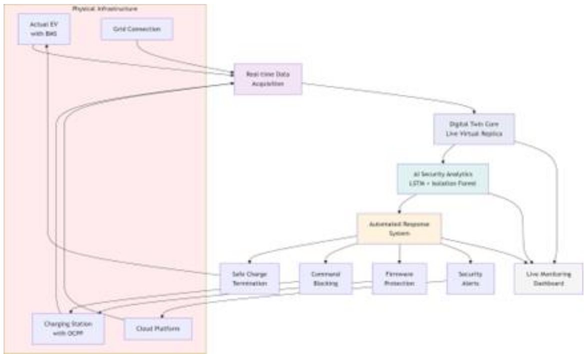
Physical Infrastructure
Actual EV with BMS
Grid Connection
Real-time Data Acquisition
Digital Twin Core Live Virtual Replica
AI Security Analytics LSTM + Isolation Forest
Automated Response System
Safe Charge Termination
Command Blocking
Firmware Protection
Security Alerts
Live Monitoring Dashboard
Charging Station with OCPP
Cloud Platform

Fig. 1. Real-World Implementation Architecture of the AI-Driven Digital Twin Framework

V. HIGH-LEVEL DIGITAL TWIN ARCHITECTURE

Figure 2 illustrates the core workflow and structural components within the digital twin system. Key subsys- tems—including data gathering, state synchronization, ma- chine learning-based anomaly detection, management dash- boards, and automated response mechanisms—are intercon- nected to create a seamless, adaptive security environment. This architectural abstraction supplements the physical system perspective and underscores the modularity and scalability essential for deploying the platform effectively in real-world and expanding infrastructure contexts.

VII. EVALUATION AND DISCUSSION

Evaluation measures:

- Detection rate, false positive/negative rates for unseen attacks.
- System latency—can the platform respond in real-time?
- Resilience: Recovery time and isolation efficiency.
- (Optional) Usability: Admin/operator acceptance. Discussion topics can include scalability to city-scale infrastructures and adaptability as threat models evolve.

VIII. LIMITATIONS AND FUTURE DIRECTIONS

Key obstacles include limited access to authentic attack datasets, significant variability across hardware platforms, and the challenge of retrofitting advanced monitoring into older charging systems. Looking ahead, the project plans to roll out demonstration systems in smart campus or partnership- based grids, experiment with distributed ledger technologies to authenticate peer transactions, and build comprehensive digital twin simulation environments that allow for large-scale adversarial testing and iterative security development.

IX. CONCLUSION

The adoption of an AI-enhanced digital twin framework stands to greatly strengthen the cybersecurity foundations of electric vehicle charging systems. By integrating continuous analytics, detailed simulations, and rapid automated defense, this strategy establishes a robust, flexible, and scalable means of safeguarding EV networks—ensuring their reliability and resilience as they become essential elements of modern trans- portation.

ACKNOWLEDGMENT

The author thanks Dr. V. Kumar, Ph.D., and the Department of Computer Science and Engineering, Knowledge Institute of Technology, for their guidance and support.

REFERENCES

[1] A. Chattopadhyay, K.-Y. Lam, and Y. Tavva,” Autonomous Vehicle: Security by Design,” IEEE Trans. Intell. Transport. Syst., vol. 22, pp. 7015–7029, 2021.

[2] X. Sun, F. R. Yu, and P. Zhang,” A Survey on Cyber-Security of Con- nected and Autonomous Vehicles (CAVs),” IEEE Trans. Intell. Transport. Syst., vol. 23, pp. 6240–6259, 2022.

[3] S. Parkinson, P. Ward, K. Wilson, and J. Miller,” Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges,” IEEE Trans. Intell. Transport. Syst., vol. 18, pp. 2898–2915, 2017.

[4] I. Chowdhury and R. Hasan,” Security Analysis of Connected Au- tonomous Vehicles (CAVs): Challenges, Issues, Defenses, and Open Problems,” in Proc. IEEE World Forum Public Safety Tech. (WFPST), Herndon, VA, USA, 2024.

[5] M. A. Shahid, A. Jaekel, C. Ezeife, Q. Al-Ajmi,

and I. Saini,” Review of Potential Security Attacks in VANET,” in Proc. Majan Int. Conf. (MIC), Muscat, Oman, 2018.

[6] H. Mun, M. Seo, and D.H. Lee,” Secure Privacy-Preserving V2V Com- munication in 5G-V2X Supporting Network Slicing,” IEEE Trans. Intell. Transport. Syst., vol. 23, pp. 14439–14455, 2022.

[7] M. Kim, I. Oh, K. Yim, M. Sahlabadi, and Z. Shukur,” Security of 6G Enabled Vehicle-to-Everything Communication in Emerging Federated Learning and Blockchain Technologies,” IEEE Access, vol. 12, pp. 33972–34001, 2023.

[8] A. Hankins, T. Das, S. Sengupta, and D. Feil-Seifer,” Eyes on the Road: A Survey on Cyber Attacks and Defense Solutions for Vehicular Ad-Hoc Networks,” in Proc. IEEE 13th Annual Computing and Communication Workshop & Conf. (CCWC), Las Vegas, NV, USA, 2023.

[9] A. Sui and G. Muehl,” Security for Autonomous Vehicle Networks,” in Proc. IEEE 3rd Int. Conf. on Electronic Information and Communication Technology (ICEICT), Shenzhen, China, 2020.

[10] S.K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen,” Cyber- Attacks in the Next-Generation Cars, Mitigation Techniques, Anticipated Readiness and Future Directions,” Accident Anal. & Prev., vol. 148, p. 105837, 2020.