Survey on Electric Vehicle Charging Stations: System and Security Perspectives*

Seungbin Lee, Kyeong A Kang, Soowang Lee, Joo Hyeon Lee, and Jiyoon Kim†

Department of Computer Science and Engineering, Gyeongsang National University
{dltmdqls1526, kka2418, id0311sw, wngysl12, jykim92}@gnu.ac.kr

Abstract

The proliferation of electric vehicles (EVs) is shifting the paradigms of transportation and energy, and electric vehicle charging infrastructure (EVCS) is emerging as a key element for achieving sustainable mobility. From a systems perspective, EVCS consists of heterogeneous components, including power electronics, communication controllers, and cloud-based management platforms, interconnected via standard protocols such as ISO 15118 and OCPP. However, technical challenges persist, including grid instability, lack of interoperability, and high deployment costs. From a security perspective, EVCS, as a cyber-physical interface connecting vehicles and the grid, presents a broad attack surface, with threats such as CMA, DDoS, FDI, and MitM being reported. To address these challenges, various AI-based security techniques, such as machine learning-based anomaly detection, transfer learning, federated learning, and TCN-based IDS, are being studied. However, practical application is limited due to limited datasets, computational resource constraints, and hardware compatibility issues. This paper comprehensively examines EVCS from both a systems and security perspective, analyzing the latest charging technology trends, grid integration strategies, standardization issues, and key security vulnerabilities and countermeasures. Through this, it proposes research directions for building more efficient, reliable, and secure EVCS.

1 Introduction

As vehicles increasingly use electricity as fuel, not just oil, the proliferation of electric vehicles (EVs) is transforming the global transportation and energy sectors. Electric vehicle charging infrastructure is becoming a key element in achieving sustainable mobility. As governments and industries around the world pursue decarbonization goals, establishing accessible, reliable, and safe charging stations is becoming a critical challenge (Carlton et al., 2024).

A systems perspective, EVCS consists of diverse components such as Power electronic devices, communication controllers, and cloud-based management platforms, interconnected via standard protocols such as ISO 15118 and OCPP (Pamulapati et al, 2024). These systems require integration with smart-grid, renewable energy, and bidirectional power exchange frameworks. However, although infrastructure design and optimization have been a core of systematic research, persistent challenges remain, including grid instability, lack of

*Proceedings of The 2025 IFIP WG 8.4 International Symposium on E-Business Information Systems Evolution (EBISION 2025), Article No. 10, December 16-18, 2025, Sapporo, Japan.

†Corresponding Author

interoperability, and high construction costs(Yousuf et al., 2024; Sarda et al., 2024). From a security perspective, EVCS presents a broad attack surface because it is implemented as a cyber-physical interface connecting vehicles and the power grid. Recent studies have reported various vulnerabilities, including charge manipulation attacks (CMA), denial-of-service attacks (DoS/DDoS), false data injection (FDI), and man-in-the-middle (MitM) attacks (Jahangir et al., 2024). These threats not only undermine service availability and payment integrity, but also seriously threaten grid stability and user trust. To address these challenges, machine learning-based anomaly detection, transfer learning techniques, and AI-powered IDS frameworks have been proposed. However, practical application is limited due to limited datasets, limited computational resources, and compatibility issues with various EVCS hardware (Dehrouyeh et al., 2024; Benfarhat et al., 2025).

Based on this background, this study comprehension considers the system and security perspective of EVCS. Concretely, our study organizes the state of the art of the trend in charging technology, power grid integration strategies, and standardization from a systemic perspective, and also organizes them from a security perspective, such as security vulnerabilities, attack models, and correspondence techniques.

Our study is structured as follows: Section 2 analyzes and organizes recent research from a systems and security perspective. Section 3 provides a discussion based on the analysis. Section 4 presents our conclusions and discusses future research directions.

2 Recent research

2.1 System perspective

Authors	Purpose	Technique	Pros	Challenges
(Yousuf et al., 2024)	- recognize EVCS as a complex system integrated with power and transportation infrastructure - Analyze obstacles such as quality degradation, demand uncertainty, and lack of standardization	- Harmonic filtering -power factor compensation - smart grid integration - battery management and recycling, -high-speed, mobile, and bidirectional charging stations.	- Comprehensive presentation of key elements - Increased efficiency through fast charging and battery swapping - Flexibility through diverse operating methods(such as fixed, mobile and bidirectional) - Energy optimization	- Real-World Application Gap - Lack of Economic Feasibility in Battery Recycling - Policy and Standard Uncertainty - Charging Demand Uncertainty and Investment Burden
(Sarda et al., 2024)	- Systematically analyze EVCS with a focus on charging technology, emphasizing its contribution to EV diffusion and energy and environment.	- Technical classification (AC/DC based, grid-connected, off-grid, hybrid) - Classification by level I to IV according to charging speed - Battery replacement method	- Comprehensive review of charging technology - operational structures, proposal of power quality - peak load mitigation measures - expected promotion of EV adoption.	- Establishing ultra-fast charging stations - Improving battery life - Advancing V2G/V2H connectivity - AI-based charging and price prediction techniques - Smart energy management
(Singh, A. et al., 2024)	- propose an ANN-based adaptive power management controller for V2G and G2V bidirectional power flow control.	- Build a mathematical model of each PV system, storage battery, EV battery, and grid	- Compensation for instability in solar power generation and battery charging status - Manages power flow stably - Supports efficient energy management in EVCS	- Establishing ultra-fast charging stations - Improving battery life - Advancing V2G/V2H connectivity - AI-based charging and price prediction techniques - Smart energy management
(Pamulapati et al, 2024)	- To ensure the security and reliability of EVCS, propose evciArch, an architectural and semantic model.	- Multi-layered structure modeling using ArchiMate based on literature, standards, and reports - Mapping CVE/CWE data with actual vulnerabilities	- Provides a common language for stakeholders - Serves as a foundational tool for security analysis, threat modeling, and policy development	- Early-stage model fails to fully encompass EVCS - Limited CVE/CWE mapping, lack of proven real-time threat detection and response

TABLE 1: Summary of System aspect

As the diffusion of EVs accelerates, recent research recognizes EVCS as a complex, multi-layered system and explores an integrated approach based on this.Table 1 presents a summary of recent research from a systems perspective.

(Yousuf et al., 2024) recongize EVCS as a complex system integrated with the power system and traffic infrastructure. The spread of EVs poses challenges to the development of EVCS, indicating obstacles such as deterioration of power quality, uncertainty in charging demand, complexity of battery technology, and lack of standardization. We review multifaceted approaches to address these challenges, including harmonic filtering, power factor compensation, smart grid integration, battery management, and recycling strategies. The authors comprehensively present the key components required for building an EVCS by analyzing existing studies and structuring them into a Challenges - Response Strategy - Optimization model. Consequently, the authors emphasize that a reliable and efficient charging infrastructure is essential, fast charging stations and battery swapping stations are key solutions to reduce driving range and increase charging efficiency. Also, depending on the operating approach of the charging station, it is divided into fixed, mobile, and bidirectional, suggesting flexible solutions that offer complementary utilization methods.

(Sarda, J et al., 2024) argue that EVs contribute to reducing carbon emissions in the transportation sector while also contributing to energy security, improving air quality, and expanding the use of renewable energy. The authors systematically analyze charging technology, focusing on this key perspective in the EVCS development process. Specifically, they comprehensively review the practical operational structure, including the technological classification of charging infrastructure (AC/DC-based, grid-connected, off-grid, and hybrid), classification by charging speed (Levels I to IV), and even battery swapping methods. Furthermore, to address grid integration issues, they address specific technical issues such as power quality, peak load, and voltage imbalance. To mitigate these challenges, they discuss power management systems, charging scheduling, demand response techniques, and renewable energy-based charging station operation, focusing on case studies. The next decade is expected to witness a significant increase in the adoption of EVs driven by technological advancements, improved charging infrastructure, and grid integration. Accordingly, key research topics include the construction of ultra-fast charging stations, enhanced V2G/V2H connectivity to improve battery life, AI-based charging and price prediction techniques, and smart energy management.

(Singh, A. et al., 2024) The authors address the AI-based power management problem in EVCS. Specifically, they propose an ANN-based adaptive power management controller for bidirectional V2G and G2V power flow control and model the EVCS as a distributed DC microgrid system. This controller optimizes power flow between PV, storage batteries, the grid, and EV batteries, enabling charging stations to function as bidirectional energy hubs (V2G/G2V) rather than simply loads. The authors construct mathematical models of the PV system, storage batteries, EV batteries, and grid, and simulate the performance of the ANN-based controller in a MATLAB/Simulink environment. The authors demonstrate that an ANN-based controller effectively compensates for the highly variable solar power generation and instability of battery charge levels, and effectively manages stable and efficient power flow in EVCSs. In particular, they demonstrate that bidirectional power exchange between EVs and the grid can contribute to the efficient utilization of distributed energy resources and grid stabilization beyond the simple function of charging stations.

(Pamulapati et al., 2024) propose evciArch, an architectural and semantic model, to ensure the security and reliability of EVCSs. Drawing on literature, standard documents, manufacturer reports, and industry reports, the model models the EVCS structure from a multi-layered perspective. Based on ArchiMate, it distinguishes between stakeholders, operational applications, and technology layers, expressing the service and data flow between each layer. Furthermore, utilizing a Common Vulnerabilities and Exposures (CVE, CWE) database, the authors link the architecture to reported security issues, such as OCPP command injection, privilege escalation, cross-site scripting (XSS), unauthorized network access, and HPGP vulnerabilities based on ISO 15118. The proposed model

can serve as a foundational tool for developing security analysis and threat modeling policies, providing a common language for EVCS stakeholders. However, the evciArch model is still in its initial stages and does not fully encompass the entire EVCS landscape. Consequently, CVE/CWE-based vulnerability mapping is limited, making it difficult to demonstrate real-time threat detection and response capabilities in real-world industrial settings. Future research will focus on expanding evciArch and developing a real-time security monitoring system, reflecting empirical data and diverse EVCS operating environments.

2.2 Security persepctives

Authors	Purpose	Technique	Pros	Challenges
(Jahangir et al., 2024)	- Presents a new threat model for EVCS, CMA (Charge Manipulation Attack). - Analyzes the effectiveness and impact of this attack and proposes a detection mechanism.	- Define 6 CMA scenarios that covertly manipulate user-defined charging start/end times and requested power - Simulations based on real-world datasets - Present a real-time monitoring framework based on unsupervised learning using a deep autoencoder (2D-CNN)	- Highlighting the feasibility of circumventing OCPP security features. - Demonstrating the effectiveness (experimental performance) of a deep learning-based detection framework.	- Detection performance deteriorates due to practical constraints such as communication failures and data noise; false positives increase during mixed attacks. - Exclusion of standards other than OCPP limits generalizability.
(Aljohani, T. et al, 2024)	- Recognizing EVCS as a core infrastructure within the smart grid - Identifying the threat of large-scale DDoS attacks through mathematical models	- Modeling attack occurrence and intensity using time-varying Poisson processes and Ornstein–Uhlenbeck stochastic processes - Analysis of server congestion and power grid disruption using M/G/1 queues	- Mathematically proven that attacks via EVCS can cause real-world power grid disruptions, including frequency fluctuations, voltage distortion, and generator instability. - Evidence supporting the need for cyber resilience.	- Lack of IDS-based advanced detection strategies - Failure to reflect gaps in actual communication networks - Absence of empirical, large-scale data validation
(Dehrouyeh et al., 2024)	- A security enhancement plan utilizing TinyML in resource-constrained environments of EVCS and IoT devices is presented.	- Consideration of ISO 15118 and OCPP protocols, as well as DoS, MitM, and malware attack scenarios - TinyML-based IDS and mitigation framework design - ESP32 experimental implementation and performance evaluation	- Real-time threat detection - Bandwidth savings - Energy efficiency - Enhanced privacy protection - Validated as an EVCI security alternative	- Lack of training data - Absence of a unified framework - Limited real-time adaptability - Lack of versatility
(Kesavan et al., 2025)	- Proposed an ML-based anomaly detection technique for detecting advanced attacks in EVCS and smart grid environments.	- Combining LSTM, Random Forest, SVM, and Autoencoder - Injecting DDoS and data tampering attacks in a smart grid protocol simulation - Applying distributed security updates using federated learning	- Ensures high detection accuracy and low latency - Demonstrates scalability and real-time adaptive security capabilities - Provides an intelligent, adaptive security system	- Simulation-based verification fails to reflect real-world variability. - Inadequate efficiency assessment in resource-constrained environments.
(Benfarhat et al., 2025)	- Proposed a lightweight, real-time TCN-based intrusion detection system (IDS) to address security vulnerabilities targeting OCPP.	- Application of Temporal Convolutional Networks - Learning long-term time series dependencies through causality and dilation, implementing real-time classification and detection	- Efficient long-term dependency learning - Low computational costs and latency, making it lightweight and suitable for real-time operations - Excellent performance in classifying various attacks (DoS, backdoors, data tampering, cryptojacking, etc.)	- Performance degrades due to network noise, data bias, and a lack of rare attack samples. - Training data acquisition and generalization remain challenges.
(Almadhor et al., 2025)	- Designing an IDS for EVCS that is robust	- Initialize with pre-trained DNN weights,	- Achieves detection accuracy exceeding 93%	- Real-time processing optimization required, lack of

	against unknown attacks and zero-day attacks using transfer learning to improve detection accuracy and scalability.	then apply fine-tuning (transfer learning) to the EVCS-specific dataset. - Reduce computational costs by reducing weight.	- Secures high generalization performance and scalability with low computational costs - Expected to improve practical applicability	large-scale, real-world data - Issues with compatibility with standards (e.g., OCPP) and diversity of operating environments

TABLE 2: Summary of Security aspects

EVCS is implemented as a cyber-physical interface that combines power grid and communication technology, presenting a wide attack surface. Research is underway to enhance this interface structure through vulnerability analysis and integration with IDS and AI technologies to ensure robust security. Table 2 presents a summary of recent research from a security perspective.

(Jahangir et al., 2024) proposed a new attack model, Charge Manipulation Attacks (CMA), targeting EVCS and presented a detection mechanism methodology. In contrast to existing attacks such as sudden surges in electricity demand or periodic switching-based strategies, CMA adopts a different approach. It covertly manipulates user-defined charging start and stop times as well as the requested power. As a result, CMA targets the power market rather than the electric grid, making it a distinctive type of attack. These attacks can be executed without bypassing OCPP's security functions, such as maximum charging speed limits or random delay execution, making them a realistic threat. The authors define 6 types of CMA scenarios and analyze them using real-world datasets. The result of the simulation, these attacks directly losses in profitability and market trust. To address against, the authors proposed a real-time monitoring framework utilizing deep autoencoder-based unsupervised learning (2D-CNN). They present a new threat model that can occur in EVCS environments and improve the effectiveness of a deep learning-based framework for detecting these threats. However, under realistic constraints such as data noise and communication disruptions, the approach exhibits reduced detection efficiency and an increased false positive rate against mixed attack types. Moreover, it reveals a limitation in that the analysis does not extend to standards beyond OCPP.

(Aljohani, T. et al, 2024) present a mathematical model of the threat of widespread DDoS attacks on EVCS, a cyber-physical system that combines cyber-physical systems and is considered a critical infrastructure within the smart grid. The authors point out that EVCS can be used as an attack vector, and argue that even small fluctuations in EV charging load can cause large disturbances in the power grid. The attacks were confirmed to cause rapid fluctuations in grid frequency, voltage profile distortion, generator output instability, and transient current oscillations. These results imply that securing cyber-resilience is essential as EVCS and smart grids are increasingly digitized and electrified. In conclusion, this study clarified the probabilistic characteristics of DDoS attacks targeting EVCS and the power grid disruption effect, thereby emphasizing the necessity of adaptive security mechanisms and real-time defense systems in smart grid environments. However, limitations include that the proposed model does not fully reflect the advanced detection strategies of IDS or the heterogeneous characteristics of actual communication networks, and that there is a lack of large-scale field verification based on empirical data.

(Dehrouyeh et al., 2024) present an Electric Vehicle Charging Infrastructure (EVCI) security solution utilizing TinyML, which operates in constrained environments such as EVCS and IoT devices. This study explores the role that TinyML contributes to enhancing cybersecurity. The authors proposed crucial challenges such as power, memories, and computational constraints, and solutions. They propose a detection and mitigation framework that considers standard communication protocols(ISO 15118, OCPP, etc) and attack scenarios (DoS, MitM, malware injection, etc). Additionally, they conducted a case study applying TinyML to an actual EVCI environment and verified its practicality through experimental implementation and performance evaluation based on the ESP32 microcontroller. Applying this method, they demonstrate that real-time IDS and response are possible in resource-constrained environments by integrating various methods such as energy harvesting, privacy-preserving learning, lightweight optimization, and transfer learning. The authors confirm that TinyML can be an effective alternative for EVCI security, offering real-time threat detection, bandwidth reduction, energy efficiency, and enhanced privacy.

However, challenges such as Insufficient data set, lack of an integrated framework, and real-time adaptability remain. Future work requires the development of a general-purpose TinyML-based security model that can overcome these limitations.

(Kesavan et al., 2025) proposed a machine learning-based anomaly detection technique based on the Grid Sentinel Framework (AD-GS). This technique addresses the limitations of existing statistical or rule-based methods, which fail to detect sophisticated attacks. The proposed technique combines various ML and DL models, such as LSTM, Random Forest, SVM, and Autoencoder, to achieve high accuracy and low latency.

Attacks such as DDoS and data tampering are injected in a simulated environment that mimics actual smart grid communication protocols, and the anomaly detection engine's ability to identify and respond to these attacks is evaluated. Furthermore, by dynamically reflecting security updates across a distributed charging station network through federated learning, the proposed technique demonstrates scalability and real-time adaptive security capabilities. This study contributes to enhancing reliability and resilience by proposing an intelligent adaptive security system in a converged environment of EVCS and smart grids. However, due to the large number of simulation-based verifications, it fails to adequately reflect real-world variability and its effectiveness in resource-constrained environments is inadequate.

(Benfarhat et al., 2025) proposed an IDS based on a Temporal Convolutional Network (TCN) to address the security vulnerabilities of OCPP. While existing deep learning techniques are limited by their inability to adequately reflect time-series dependencies and complex attack patterns or their high computational costs, TCN efficiently learns long-term dependencies through convolutional causality and dilation structures, achieving both lightweightness and real-time performance. This study presents a new standard for lightweight, high-performance security models capable of effectively detecting and classifying various cyberattacks targeting OCPP (DoS, backdoors, data tampering, cryptojacking, etc.). However, it demonstrates that detection performance can be degraded by network noise, data bias, and a lack of rare attack samples. (Almadhor et al., 2025) propose a transfer learning-based IDS to detect cyber-physical threats facing EVCS. Existing IDSs rely on signatures of known attacks, making them vulnerable to novel or zero-day attacks. To overcome these limitations, they combine deep learning and transfer learning to achieve higher accuracy and scalability. The proposed model achieves a detection accuracy of over 93% by initializing the model using the weights of a pre-trained DNN and then fine-tuning it using an EVCS-specific dataset. This study demonstrates that an IDS utilizing TL can effectively enhance security in real-world EVCS operating environments, demonstrating higher detection rates and generalization performance at lower computational costs than existing deep learning models. Future research will focus on optimizing real-time performance, securing large-scale/real-world datasets, and ensuring compatibility with standards.

3 Discussion

From a systems perspective, EVCS is being redefined as a complex system encompassing the power grid, transportation infrastructure, storage devices, and charging station operations. It faces technical and operational challenges such as degraded power quality, demand uncertainty, battery complexity, and a lack of standardization (Yousuf et al., 2024; Sarda et al., 2024). To address these challenges, harmonic filtering, power factor compensation, charging scheduling, smart grid integration, battery management/recycling, and AI-based power control techniques (Singh et al., 2024) are being proposed. Furthermore, the role of charging stations as bidirectional energy hubs (V2G/G2V) rather than mere loads is emphasized.

From a security perspective, EVCS, as a cyber-physical interface combining the power grid and communication infrastructure, presents a broad attack surface. Against this backdrop, new threat models such as CMA (Jahangir et al., 2024) and DDoS (Aljohani et al., 2024) have been proposed, and various AI-based detection techniques are being studied, including TinyML (Dehrouyeh et al., 2024), Federated Learning (Kesavan et al., 2025), TCN-based IDS (Benfarhat et al., 2025), and transfer learning-based IDS (Almadhor et al., 2025). However, limitations include a lack of datasets, lack of empirical validity, and limitations to protocols other than OCPP. Future research should move toward establishing a comprehensive security framework that includes securing empirical data, reflecting heterogeneous communication environments, responding to mixed attacks, and verifying policy and standard linkages.

System and security research requires a combination of these two areas in real-world EVCS operating environments. System research focuses on operational optimization, including charging efficiency, power quality, smart-grid integration, and battery management. Security research focuses on threat response, including attack model definition, IDS, and AI-based detection. However, in real-world EVCS environments, operational reliability is difficult to ensure unless efficient system design

and security assurance are simultaneously met. For example, while optimizing V2G/G2V bidirectional power flow is a systemic goal, communication vulnerabilities can also be exploited as attack vectors. Therefore, the need for an integrated framework that combines power management algorithms with IDS/AI-based security techniques is emerging.

4 Conclusion

This paper comprehensively analyzes and summarizes EVCS from a systemic security perspective. From a systemic perspective, EVCS is recognized as a complex, multifaceted architecture that redefines a complex, multi-layered structure encompassing the power grid, transportation infrastructure, storage devices, and charging station operations. Key challenges within this architecture include charging efficiency, power quality stabilization, smart grid integration, battery management, and recycling. Harmonic filtering, charging scheduling, and AI-based power control techniques have been proposed to address these challenges. Some papers argue that EVCS should function as a two-way energy hub, rather than simply a load.

From a security perspective, EVCS, as a cyber-physical interface CPS connecting vehicles and the strategic network, presents a broad attack surface, leading to reports of various threat models, including CMA, DDoS, FDI, and MitM. To address this, AI and ML-based security frameworks such as TinyML, transfer learning, federated learning, and TCN-based IDS have been proposed. However, these frameworks suffer from limitations such as limited datasets, resource constraints, and compatibility with heterogeneous environments.

In this context, real-world EVCS operational environments require both system and security requirements, highlighting the need for a framework that integrates power management algorithms with IDS/AI-based security techniques.

Therefore, future research should expand to design an integrated framework that includes empirical data-based validation, incorporating heterogeneous communication standards, hybrid attack response strategies, and economic and policy linkage analysis. Accordingly, this study aims to conduct a more comprehensive and in-depth analysis to explore the detailed design and practical feasibility of such an integrated framework.

Acknowlegement

This work was supported by the Glocal University 30 Project Fund of Gyeongsang National University in 2025.

References

Carlton, G. J., & Sultana, S. (2024). Electric vehicle charging equity and accessibility: A comprehensive United States policy analysis. Transportation Research Part D: Transport and Environment, 129, 104123.

Pamulapati, T., Walker, M., Adu-Duodu, K., Huraysi, T., Ranjan, R., & Shah, T. (2025, May). Architectural and Semantic Models for EV Charging Infrastructure. In 2025 IEEE 25th International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW) (pp. 117-124). IEEE.

Yousuf, A. K. M., Wang, Z., Paranjape, R., & Tang, Y. (2024). An in-depth exploration of electric vehicle charging station infrastructure: A comprehensive review of challenges, mitigation approaches, and optimization strategies. IEEE access, 12, 51570-51589.

Sarda, J., Patel, N., Patel, H., Vaghela, R., Brahma, B., Bhoi, A. K., & Barsocchi, P. (2024). A review of the electric vehicle charging technology, impact on grid integration, policy consequences, challenges and future trends. Energy Reports, 12, 5671-5692.

Jahangir, H., Lakshminarayana, S., & Poor, H. V. (2024). Charge manipulation attacks against smart electric vehicle charging stations and deep learning-based detection mechanisms. IEEE Transactions on Smart Grid, 15(5), 5182-5194.

Dehrouyeh, F., Yang, L., Ajaei, F. B., & Shami, A. (2024). On TinyML and cybersecurity: Electric vehicle charging infrastructure use case. IEEE Access.

Temporal convolutional network approach to secure open charge point protocol (OCPP) in electric vehicle charging. IEEE Access.

Singh, A. P., Kumar, Y., Sawle, Y., Alotaibi, M. A., Malik, H., & Marquez, F. P. G. (2024). Development of artificial Intelligence-Based adaptive vehicle to grid and grid to vehicle controller for electric vehicle charging station. Ain Shams Engineering Journal, 15(10), 102937.

Aljohani, T., & Almutairi, A. (2024). Modeling time-varying wide-scale distributed denial of service attacks on electric vehicle charging Stations. Ain Shams Engineering Journal, 15(7), 102860.

Kesavan, V. T., Hossen, M. J., Gopi, R., & Joseph, E. R. (2025). Anomaly detection with grid sentinel framework for electric vehicle charging stations in a smart grid environment. Scientific Reports, 15(1), 15774.

Benfarhat, I., Goh, V. T., Siow, C. L., Sheraz, M., & Chuah, T. C. (2025). Temporal convolutional network approach to secure open charge point protocol (OCPP) in electric vehicle charging. IEEE Access.

Almadhor, A., Alsubai, S., Bouazzi, I., Karovic, V., Davidekova, M., Al Hejaili, A., & Sampedro, G. A. (2025). Transfer learning for securing electric vehicle charging infrastructure from cyber-physical attacks. Scientific Reports, 15(1), 9331.