Intrusion Detection using Peer-to-Peer Distributed Context-Information for Electric Vehicle Supply Equipment

Julian Graf, Christoph Moser, Philipp Fuxen, Rudolf Hackenberg
Faculty of Computer Science and Mathematics
Ostbayerische Technische Hochschule Regensburg
Regensburg, Germany
e-mail: {julian.graf | christoph.moser | philipp.fuxen | rudolf.hackenberg}@oth-regensburg.de

***Abstract*—In this paper, we present a decentralized approach to securing charging infrastructure in the private and semi-public sector. The goal is strengthening the resilience of charging infrastructure through enhanced security mechanisms based on sharing context information. Therefore, an architecture was developed that combines concepts of data acquisition, information exchange and analysis methods to efficiently monitor Electric Vehicle Supply Equipment systems. The "Resiliente und Sichere Ladeinfrastruktur" research project architecture connects the interfaces between charging hardware, a highly scalable Peer-to-Peer cybersecurity mesh network and the static and Artificial Intelligence-supported analysis processes on the top layer. The most important tasks across the domains of detection, reaction, attribution and prevention are taken into account. A large information space, which aggregates the content of the individual domains, is created and made available in the network. The context data of the information space is obtained from the individual peers and used for the analysis. Context-based data regarding loading procedures, network communication parameters, system loads, Open Charge Point Protocol parameters, and other domain data clusters are recorded. The extended local and central analysis use the context information for monitoring and attack classification. The context information is transmitted via an InterPlanetary File System-based Peer-to-Peer mesh network.**

Keywords-EVSE; Charging Station; Security; Peer-to-Peer; P2P; Context Information; Resilience; Attack Detection; IDS; Security-Architecture.

I. INTRODUCTION

The increasing uptake of Electric Vehicles (EVs) is a crucial step towards sustainable mobility. Governments and organizations around the world are setting ambitious targets to reduce CO2 emissions, with the development of a nationwide charging infrastructure playing a central role [1]. A reliable, safe and efficient charging infrastructure is crucial to increase the adoption of electric vehicles and enable a sustainable transition to transportation. However, while charging infrastructure is growing exponentially, the security of these systems often falls short of requirements. Cyberattacks on charging stations can not only affect individual users but, in the worst case, destabilize the entire energy grid and cause significant economic damage [2]. The charging infrastructure for electric vehicles is complex and consists of a large number of components, including hardware, software and communication interfaces. This heterogeneity opens up numerous attack surfaces for cyber threats. Existing studies have already revealed serious security vulnerabilities in current systems. For example, the widely used Open Charge Point Protocol (OCPP) 1.6 has significant vulnerabilities that allow attackers to carry out Man in the Middle (MitM) attacks or energy theft [3]. Other threats include Denial of Service (DoS) attacks, inadequately protected interfaces and the risk of malware spreading via compromised charging stations [4][5]. Despite the existing security measures, a fundamental problem remains: Current protection mechanisms are mostly centralized and reactive, which leaves them vulnerable to coordinated attacks and makes it difficult to efficiently detect and defend against threats. To minimize security risks, we propose a new type of decentralized architecture with the ReSiLENT approach. An additional detection unit is integrated into an Electric Vehicle Supply Equipment (EVSE), which gathers local data, conducts a series of analysis on behalf of intrusion detection and connects the EVSE to the cybersecurity mesh (a network of many individual EVSE). This allows the charging stations to communicate securely with each other and exchange contextual information. This distributed structure enables faster detection of anomalies and attacks and improves the resilience of the overall system. By integrating a cybersecurity mesh based on the principles of the cybersecurity domains of prevention, detection, reaction and attribution, a scalable and economically viable security solution for EVSE is created. As this paper introduces the concept of the ReSiLENT approach, the following research questions focus on its theoretical foundations and possible implications:

- **RQ1:** How can a decentralized peer-to-peer architecture effectively contribute to the detection and prevention of cyberattacks on EVSE?
- **RQ2:** Can contextual information be used to improve the prevention, detection, response and attribution of attacks on the charging infrastructure?

Following this introduction, Section II analyzes the relevant literature and existing work on security problems in the charging infrastructure. Section III describes the current threat situation for EVSE and highlights specific attack scenarios. Section IV provides an overview of the ReSiLENT system and its architecture. The details of the peer-to-peer network technology and its security advantages are discussed in Section V. Section VI presents the Cybersecurity Mesh, which enables efficient threat detection and defense. Section VII describes the ReSiLENT cybersecurity stack with its four core

areas: Detection, Reaction, Prevention and Attribution. Finally, Section VIII discusses further research questions and future challenges.

II. Related Work

The security of EVSE is an increasingly relevant area of research as the number of connected charging stations continues to grow and potential attack vectors increase. Existing work is investigating various security-critical aspects, from vulnerabilities in communication and authentication to approaches for detecting and preventing cyberattacks. This section presents relevant studies that deal with security risks, attack detection and possible countermeasures in the charging infrastructure. It then discusses the extent to which existing solutions are sufficient and what research gaps still exist.

The security of EVSE is increasingly becoming a focus of research, as networked charging stations offer new opportunities for attacks. Existing work identifies vulnerabilities in communication, authentication and hardware. Skarga-Bandurova et al. [6] highlight various security vulnerabilities in charging stations, including lack of authentication for API access, insecure firmware updates and insufficiently protected data, and recommend secure communication, encryption and intrusion detection systems as countermeasures. Gottumukkala et al. [4] analyze vulnerabilities in the cyber-physical security of charging stations and identify attacks on network interfaces such as Bluetooth, Wi-Fi and wired connections, including spoofing, MitM, DoS and SQL injection. In addition, they show that physical access enables attacks on chip components, side-channel attacks and tampering. As a countermeasure, they propose a secure system design that includes a comprehensive assessment of threat vectors in hardware and software. Gottumukkala et al. [4] expand their recommendations on hardware and software security by focusing on the elimination of existing vulnerabilities and the preventive development of secure systems. Pratt et al. [5] address the growing threat to electric vehicle charging infrastructure and develop security paradigms to defend against potential cyberattacks. The large number of components, the heterogeneity of the systems and the decentralized distribution of critical infrastructures pose a particular security challenge. Although Pratt et al. [5] emphasize the independence of the various players in the charging system, they also point out the need for a coordinated exchange of information to defend against threats. They also emphasize the importance of continuous monitoring and diagnostics of all system components, focusing in particular on the role of EVSE monitoring from the provider's perspective. They classify key data such as billing information, location data and charging performance managed by a central entity. They also discuss mechanisms for checking the consistency between the physical and digital state of the charging infrastructure in order to detect deviations at an early stage. In the event of an attack, the response strategy should take into account both the security requirements of the affected component and the potential impact. Particularly critical incidents, such as attacks on the power grid, require differentiated measures compared to targeted attacks on individual units. Security is restored primarily through regular software and firmware updates of the vehicle and EVSE systems.

Securing charging infrastructure requires not only addressing existing vulnerabilities but also effective attack detection. Various research efforts have explored different methods to enhance security in this domain. While the integration of multi-layered intrusion detection system architectures [7] enables the analysis and evaluation of several AI-supported procedures by providing large information spaces and thus optimizes the results. Buedi et al. [8] contribute a multidimensional dataset containing charging information and its evaluation. Their study focuses on EVSE in both charging and idle states, analyzing power consumption, network traffic, and host activities to support anomaly detection. Similarly, Kim et al. [9] provide a DoS-specific dataset that includes four attack scenarios related to vehicle authentication. Another approach is introduced by Purohit and Govindarasu [10], who utilize data collected from charging infrastructure entities. Instead of sharing raw data, their method relies on exchanging model parameters, enabling a federated learning framework for enhanced security. Additionally, Mavikumbure et al. [11] propose Cy-Phy ADS, an anomaly detection framework that integrates CAN data with machine learning to identify potential threats in charging systems. While many studies focus on anomaly detection and machine learning-based models for attack identification, our approach takes a broader, more comprehensive security perspective on EVSE. While existing work mainly focuses on specific security domains, Fuxen et al. [12][13] focus on a decentralized, graph-based architecture for Cyber Threat Intellgence (CTI) analysis and privacy-preserving threat intelligence sharing. The ReSiLENT approach, on the other hand, deals specifically with the security-critical EVSE. The challenges in this area differ from those of classic IT systems, as EVSE offers not only digital but also physical attack vectors that can have a direct impact on the power grid and transportation infrastructure. While Fuxen et al. [12][13] focus on cross-organizational threat detection and networking, our focus is on the local, decentralized security architecture of charging stations and their resilience against coordinated attacks. Our approach integrates specific protection measures for EVSE, including secure communication between charging points, protection in the OCPP, and attack detection based on real EVSE usage data. In summary, the security of EVSE is becoming an increasingly important area of research as the number of connected charging stations rises, creating new attack vectors. Various studies have identified vulnerabilities in communication, authentication, and hardware, proposing countermeasures such as secure communication, encryption, and intrusion detection systems. While existing solutions provide valuable insights, there is still room for improvement, particularly in the development of secure, decentralized systems, as most solutions currently rely on centralized systems. Furthermore, existing research tends to focus on either detection or prevention of cyberattacks instead of taking a comprehensive approach including the domains of reaction and

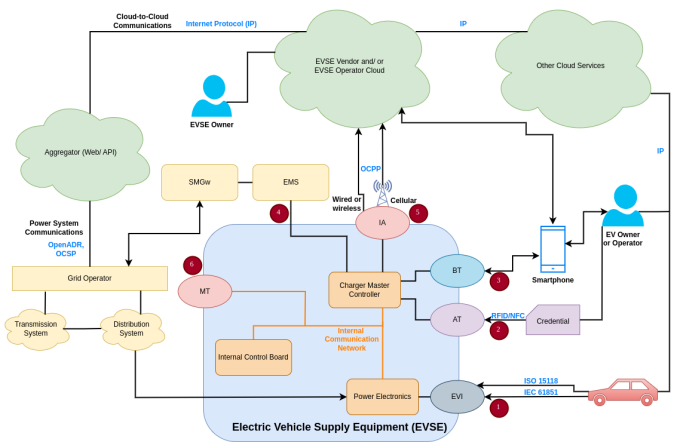

Figure 1. Electric Vehicle Infrastructure Landscape [15].

attribution.

III. EVSE Threat Landscape

EVSE faces numerous cybersecurity vulnerabilities that could compromise the integrity of the charging infrastructure and the power grids. These vulnerabilities include weak authentication mechanisms, unsecured communications, and potential exploits in connected systems [14]. Attacks on EVSE could lead to consequences ranging from localized disruptions to long-term national impacts [15]. The cyber-physical nature of EVSE systems, involving sensing, communication, and computational components, makes them susceptible to various threats [4]. As Electric Vehicle (EV) adoption grows, securing the charging infrastructure becomes crucial to prevent potential political, social, and financial consequences [16]. To address these challenges, researchers emphasize the need for comprehensive cybersecurity approaches, including threat modeling, risk assessments, and the development of effective countermeasures [14], [15]. Implementing Information Technology (IT) and Operational Technology (OT) cybersecurity best practices can help mitigate these risks and ensure the resilience of EVSE systems [15]. Before delving into the concepts and ideas that underlie the ReSiLENT project, it is essential to first establish the necessity of these efforts. Therefore, taking a look at current threats concerning Electric Vehicle Infrastructure (EVI) and especially EVSE.

ReSiLENT identifies attack vectors at a more granular level. As shown in Figure 1 designations 1-6, the interfaces EVI (ev-to-evse) via powerline communication, authentication (AT) via RFID / NFC, Bluetooth, EVSE Internet Access, SmartMeter Gateway (SMGw) and the maintenance terminal alone and in combination are identified as possible entry points. Effectively addressing each attack vector requires the identification, monitoring, and integration of countermeasures, ensuring an understanding of potential threats and the deployment of dedicated solutions to safeguard the resilience of the EVSE ecosystem.

IV. Overview of the ReSiLENT System

Given the current security landscape, there is a clear need to enhance EVSE cybersecurity. ReSiLENT introduces a novel architecture leveraging the distribution of cybersecurity information and assets across various actors and components within a connected charging infrastructure using a Peer-to-Peer (P2P) mesh network. Covering the domains detection, reaction, prevention, and attribution, the goal is to create a scalable and flexible security ecosystem for various e-mobility market segments, including private, commercial, and public high-power charging. Furthermore, our approach aims to ensure the economic viability of cybersecurity measures in low-cost charging infrastructure through automation.

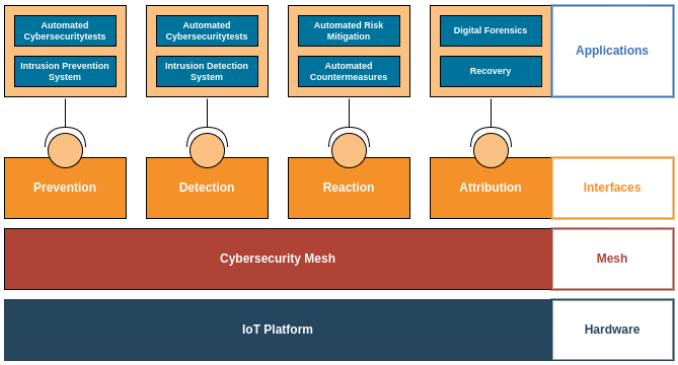

Figure 2. ReSiLENT High-Level Architecture.

As shown in Figure 2, the high-level ReSiLENT architecture consists of three core levels. Starting with the hardware level, which is mapped via the so-called IoT platform. The hardware level forms the interface to the firmware of the local charging controllers and to other hardware elements installed in the charging station. It enables the collection of information on specific system parameters, such as the current and voltage during a charging process or the utilization of the controller CPU. It also enables safety measures to be carried out on the charging station. Possible reactions here are, for example, canceling the charging process or closing communication connections. The second level, also known as the mesh level, is responsible for connecting the charging stations. A P2P mesh network is established at this level. Each charging station is considered a peer in this network and can provide and request information after authentication. The mesh network offers the possibility to share information in a decentralized manner. Charging stations can specifically request information that is required for local analyses. The creation, networking and distribution of a context-based information space is essential for advanced attack classification, derivation of response measures, prevention and attribution. The top level, also known as the application level, is supplied with the required data space via the domain-specific interfaces. It integrates the cybersecurity applications, which carry out certain analyses, measures or the provision of information depending on the domain. Through this architecture, we establish

a robust security system that enhances the resilience of EVSE against cyber threats while ensuring practical and cost-efficient implementation.

V. Peer-to-Peer Mesh-Network

The essence of the ReSiLENT project is to identify an effective method for distributing context information while simultaneously ensuring security. In the realm of Internet of Things (IoT) networks, application protocols such as Message Queueing Telemetry Transport (MQTT) have gained significant popularity due to their lightweight nature and efficiency in distributing data. MQTT is particularly well-suited for resource-constrained environments, offering publish-subscribe communication that minimizes bandwidth and computational overhead. However, its architecture relies on centralized brokers, which may introduce single points of failure and increasing complexity when scaled up [17]. Therefore, and because of the reasons mentioned below, a P2P approach was taken in the ReSiLENT-System. More specifically, the InterPlanetary File System (IPFS) protocol stack was chosen, as it combines peer-to-peer communication (via libp2p) with robust data storage capabilities, enabling distributed systems to share and store content without the need for centralized servers. The ReSiLENT P2P mesh network offers the following advantages:

- **Resilience Against Failures and Attacks:** ReSiLENT follows a security-by-design approach, prioritizing decentralization to enhance resilience. Unlike centralized models, where data is stored on a single server, ReSiLENT distributes data across multiple nodes. When a node requests data, it caches a copy and serves it to others, ensuring continued availability even if the original source goes offline.
- **Data Integrity and Tamper Resistance:** One of the key security aspects of ReSiLENT is ensuring data integrity and protection against tampering. In contrast to Hypertext Transfer Protocol (HTTP), data in IPFS is addressed by content rather than location. Instead of being found through a Uniform Resource Locator (URL), files are retrieved via their cryptographic hash. This ensures that each file is uniquely identified by its content rather than its address.
- **Secure and Reliable Data Distribution:** Traditional server-client models often experience performance degradation when too many users access a server simultaneously. In contrast, P2P networks such as IPFS allow nodes to retrieve files from the nearest available peers, optimizing data transfer efficiency.
- **Anonymity and Privacy Protection:** Privacy is a critical aspect of cybersecurity, and P2P networks offer inherent advantages in this regard. Depending on the protocol, P2P communication can provide a certain degree of anonymity, as data requests and transmissions are relayed through multiple nodes. This obfuscation makes it more difficult to trace data streams and provides an added layer of privacy protection. Within ReSiLENT, this feature can be leveraged for secure sharing of anonymized cyber threat intelligence, ensuring that sensitive data remains protected while enabling collaborative security efforts among distributed nodes.

VI. Context Distribution

With the possibility of distributing data, it is necessary to evaluate which data must be passed on and which node has an interest in receiving it. In the ReSiLENT-System, the contextual information disseminated through a private IPFS network enables each node to conduct a series of analytical processes. The goal is to determine which context information needs to be distributed to positively impact existing CTI processes and to develop new approaches based on this foundation.

A. Conventional Approaches vs ReSiLENT

Traditionally, cyber threat intelligence relies on a centralized server model, where all data is collected and processed in one location. This approach, while effective, introduces single points of failure, scalability limitations, and potential privacy concerns. ReSiLENT employs a hybrid P2P model, where each node contributes to CTI by analyzing and sharing context information. A specialized centralized node, with greater computational power, augments the P2P network by performing complex calculations. Figure 3 illustrates the context distribution and analysis in the ReSiLENT system. The nodes $P_1 - P_4$ represent individual charging stations, where the IoT platform within each EVSE gathers local hardware and network data, shares relevant information, and conducts analysis before publishing results back into the network. The central node P_M leverages additional information, e.g. from a Charging Station Managemant System (CSMS), for its analysis.

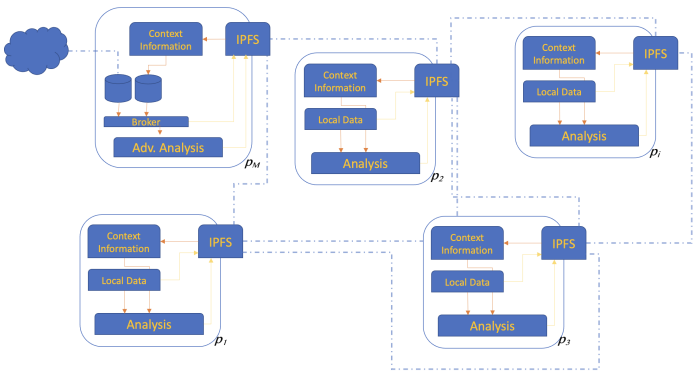

Figure 3. Overview of ReSiLENT P2P context distribution and analysis.

B. Distribution of Context Information

To effectively distribute context information within the network, ReSiLENT leverages a combination of IPFS functionalities:

- **Distributed Hash Table (DHT)** Enables efficient storage and retrieval of data.
- **PubSub Mechanism:** Facilitates real-time notifications about publication of files in the DHT.

- **Topic-based Channels:** Nodes subscribe to relevant topics, such as detection methods or threat reports, ensuring focused information exchange.

C. Types of Distributed Information

s shown in Table I, ReSiLENT distributes various forms of context information, including EVSE charging session data, network traffic, hardware status and threat reports generated by local analysis. This is not a comprehensive list yet, as further information can be relevant based on future development of CTI-Applications.

TABLE I. TYPES OF DISTRIBUTED INFORMATION IN RESILENT

Data Type	Description
Threat Reports	Periodically generated by each EVSE to document anomalies, vulnerabilities, and security states.
IPFS Metrics	Insights into neighboring peers, network traffic, detection of malicious nodes, and integrity verification.
EVSE Profiles	Summarizing charging behavior, station usage, and proximity relationships.
User Profiles	Capturing behavioral patterns, such as charging station preferences and consumption trends.

VII. RESILENT CYBERSECURITY-STACK

The ReSiLENT cybersecurity stack combines methods and procedures from the domains of **detection**, **reaction**, **prevention** and **attribution**, making efficient use of overarching synergy effects. Focused and classified attack detection makes it possible to generate targeted information that enables dedicated response measures to be activated and provides information on balanced preventive measures. Attributive operations can be efficiently identified based on the results of other domains.

A. Detection

To detect attacks on EVSE, it is necessary to combine different monitoring methods and systems. For the protection and detection of ReSiLENT, procedures from the following areas are to be included:

- Network traffic monitoring
- Intrusion Detection and Prevention System (IDS/P)
- Signature-based Intrusion Detection System (IDS)
- Behaviour-based IDS
- Firmware integrity checks, e.g. secure boot
- Secure updates, e.g. code signing
- Physical tamper detection
- Protocol and log analysis, e.g. correlation of events
- Authentication and access control
- Anomaly Detection using Artificial Intelligence (AI)
- Threat Intelligence, e.g. information sharing

In order to regularly monitor and evaluate the systems, it makes sense to carry out additional stress tests and penetration tests. Blackbox fuzzing attacks should also be included.

A crucial aspect of the ReSiLENT detection approach is the usage of context information shared by individual nodes and distributed over the IPFS mesh. The threat detection mechanisms specifically using this shared data fall into three categories:

- **Complementary**: Using data and results from multiple nodes in order to gain a broader view of the whole system, even on single nodes.
- **Consensus-Oriented**: Cross-verifying results from different nodes to increase detection reliability.
- **Comparative**: Analyzing deviations from normal behavior based on historical data and comparing results of multiple nodes.

B. Reaction

With regard to response measures, a distinction must be made between automated measures and manual or person-controlled measures.

Automated measures:

- Segmentation or isolation of components
- Automated blocking, e.g. IP- / MAC-addresses or traffic
- Rollbacks to previous firmware or software versions
- Automated lockouts, e.g. failed authentication

Manual interventions:

- Security incident response teams
- Forensic investigations
- Replacing hardware and software

A structured evaluation should be carried out after each prevented or successful attack. Based on that, security guidelines should be updated and findings should be incorporated into the ongoing security strategy.

C. Attribution

Attribution is often a major challenge in the field of cybersecurity. The same applies to attacks on charging stations for electric vehicles: Although technical traces can be collected, a clear attribution to specific actors is usually only possible with considerable effort and probability statements. Nevertheless, there are various measures and methods to support the best possible attribution. Attribution benefits from the most accurate attack classification possible, which includes, among other things, information gathering methods with or for digital forensics. The use of synergy effects of the ReSiLENT cybersecurity stack based on context information plays a central role here.

D. Prevention

While detection, response and attribution tend to intervene when a security event has already taken place or is actively underway, prevention starts before the actual incident. Prevention refers to all measures aimed at preventing attacks from the outset or significantly reducing their chances of success. The aim is to reduce the attack surface, minimize vulnerabilities and make access as difficult as possible for attackers A basic distinction is made between three preventive measures: technical, organizational and process-related preventive measures:
Technical prevention measures:

- Secure system and software architecture
- Security aspects during development phase

- Use of secure configurations
- Secure key management
- Encrypted communication
- Authentication and access controll
- Network segmentation
- Patch and update management
- Physical safety

VIII. Conclusion and Future Work

The security system for hardening the resilience of charging infrastructure presented in this paper demonstrates technology-based, modern approaches for collecting, distributing and analyzing EVSE-relevant data. In addition to recording Vehicle-to-EVSE transmissions, the interface between the IoT platform to the charging station also enables the monitoring of relevant charging process data, back-end communication, as well as the hardware status. The cybersecurity mesh network that builds on this enables the collected context information to be distributed securely, quickly and in a scalable manner. The extended analysis methods can integrate complex context-based analyses through the decentralized networking of the charging stations and thus also their data. Attacks can be detected and classified via the detection domain with your applications. Dedicated security measures can be selected, implemented and transmitted to the prevention applications for further preventive steps using the methods and procedures of the reaction domain. And finally, the decentralized distributed information space can be used for attributive measures.

In the future, it is intended to further expand the collection of context information and thus enlarge the information space. This will increasingly include EVSE-related communication patterns from Vehicle-to-EVSE. Furthermore, the response measures will be cyclically adapted and expanded in line with the progress made in the development of detection analyses. An automated derivation of preventive security measures is to be integrated on the basis of the information space of the detection and response domains and visualized for users. In addition, attributive measures are to be finally integrated based on the results of the three preliminary domains. The developments will be accompanied by tests using a laboratory test setup and the integration of the software into real charging stations to evaluate the functionality.

References

[1] E. Parliament, "'fit for 55' legislative package: Strengthening the co2 emission performance standards for new passenger cars and new light commercial vehicles," [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/694249/EPRS_BRI(2021)694249_EN.pdf (visited on 12/13/2024).

[2] S. H. Ahmed and F. M. Dow, "Electric vehicle and charging station technology as vulnerabilities threaten and hackers crash the smart grid," 2016.

[3] C. Alcaraz, J. Lopez, and S. Wolthusen, "Ocpp protocol: Security threats and challenges," *IEEE Transactions on Smart Grid*, 2017. DOI: 10.1109/TSG.2017.2669647.

[4] R. Gottumukkala *et al.*, "Cyber-physical system security of vehicle charging stations," in *2019 IEEE Green Technologies Conference(GreenTech)*, 2019. DOI: 10.1109/GreenTech.2019.8767141.

[5] R. M. Pratt and T. E. Carroll, "Vehicle charging infrastructure security," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019. DOI: 10.1109/ICCE.2019.8662043.

[6] I. Skarga-Bandurova, I. Kotsiuba, and T. Biloborodova, "Cyber security of electric vehicle charging infrastructure: Open issues and recommendations," in *2022 IEEE International Conference on Big Data (Big Data)*, 2022. DOI: 10.1109/BigData55660.2022.10020644.

[7] J. Graf, K. Neubauer, S. Fischer, and R. Hackenberg, "Architecture of an intelligent intrusion detection system for smart home," in *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2020, pp. 1–6. DOI: 10.1109/PerComWorkshops48775.2020.9156168.

[8] E. D. Buedi, A. A. Ghorbani, S. Dadkhah, and R. L. Ferreira, "Enhancing ev charging station security using a multi-dimensional dataset: Cicevse2024," in *Data and Applications Security and Privacy XXXVIII*, 2024. DOI: 10.1007/978-3-031-65172-4_11.

[9] Y. Kim, S. Hakak, and A. Ghorbani, "Ddos attack dataset (cicev2023) against ev authentication in charging infrastructure," in *2023 20th Annual International Conference on Privacy, Security and Trust (PST)*, 2023. DOI: 10.1109/PST58708.2023.10320202.

[10] S. Purohit and M. Govindarasu, "Fl-evcs: Federated learning based anomaly detection for ev charging ecosystem," in *2024 33rd International Conference on Computer Communications and Networks (ICCCN)*, 2024. DOI: 10.1109/ICCCN61486.2024.10637543.

[11] H. S. Mavikumbure *et al.*, "Cy-phy ads: Cyber-physical anomaly detection framework for ev charging systems," *IEEE Transactions on Transportation Electrification*, 2024. DOI: 10.1109/TTE.2024.3363672.

[12] P. Fuxen *et al.*, "Mantra: A graph-based unified information aggregation foundation for enhancing cybersecurity management in critical infrastructures," in *Open Identity Summit 2023*, Bonn: Gesellschaft für Informatik e.V., 2023, pp. 123–128, ISBN: 978-3-88579-729-6. DOI: 10.18420/OID2023_10.

[13] P. Fuxen, M. Hachani, R. Hackenberg, and M. Ross, "Mantra: Towards a conceptual framework for elevating cybersecurity applications through privacy-preserving cyber threat intelligence sharing," *IARIA Cloud Computing 2024*, 2024. DOI: 10.18420/OID2023_10.

[14] G. Vailoces, A. Keith, A. Almehmadi, and K. El-Khatib, "Securing the electric vehicle charging infrastructure: An in-depth analysis of vulnerabilities and countermeasures," in *Proceedings of the Int'l ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet '23, New York, NY, USA: Association for Computing Machinery, 2023, pp. 31–38. DOI: 10.1145/3616392.3623424.

[15] J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses," *Energies*, vol. 15, no. 11, p. 3931, May 26, 2022, ISSN: 1996-1073. DOI: 10.3390/en15113931.

[16] J. Johnson, "Securing vehicle charging infrastructure," SAND–2020-11971R, 1706221, 691697, Nov. 6, 2020, SAND–2020–11971R, 1706221, 691697. DOI: 10.2172/1706221.

[17] M. A. Spohn, "On MQTT scalability in the internet of things: Issues, solutions, and future directions," *Journal of Electronics and Electrical Engineering*, p. 4, Oct. 19, 2022, ISSN: 2972-3280. DOI: 10.37256/jeee.1120221687.