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

Julian Graf, **Christoph Moser**, Philipp Fuxen, Prof. Dr. Rudolf Hackenberg

Contact: **christoph.moser@oth-regensburg.de**

Introduction

Christoph Moser

About Me

- **B.Sc. in Computer Science**, Technische Hochschule Ingolstadt (2022)
- **M.Sc. in Computer Science** with a focus on **Computer Engineering**, Ostbayerische Technische Hochschule Regensburg (2024)
- Since **June 2024**, working as a **Scientific Assistant** at the **Automotive Security Laboratory** at OTH Regensburg, contributing to the **ReSiLENT Project** on secure EV charging infrastructure
- My **research interests** include **Peer-to-Peer Networks**, **Security Engineering**, and **e-mobility infrastructure security**

Introduction

Aims and contributions of our paper

Aims:

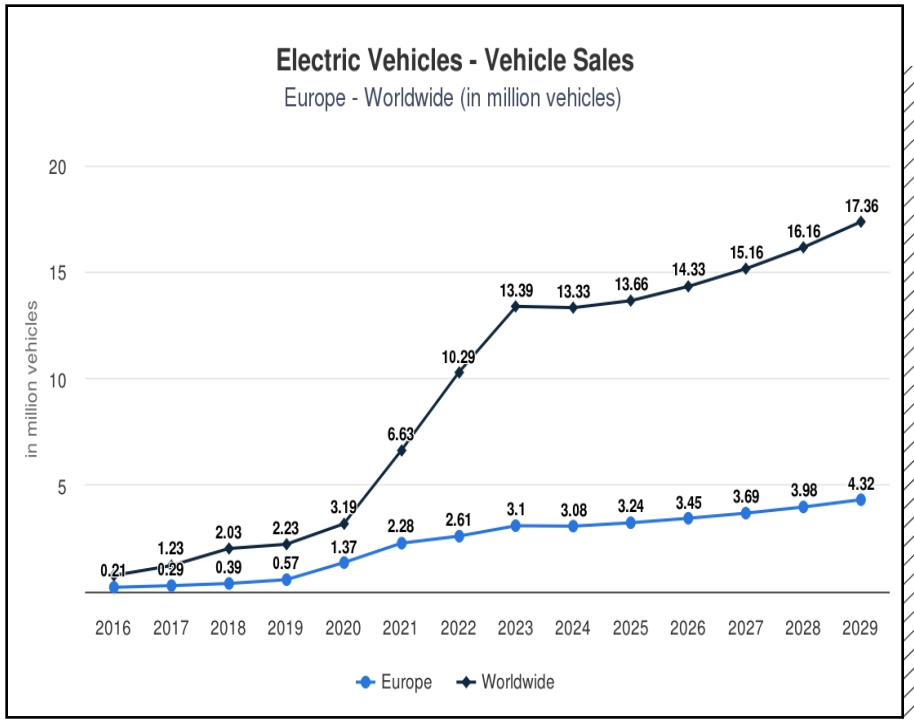
- Develop a cost-effective system designed for seamless integration into charging stations and wallboxes, enhancing inherent security features.
- Contribute to the long-term resilience of e-mobility infrastructure by securing Electric Vehicle Supply Equipment (EVSE) against emerging threats.

Contributions:

- Introduction of a novel system architecture specifically engineered to meet the outlined security and integration objectives.

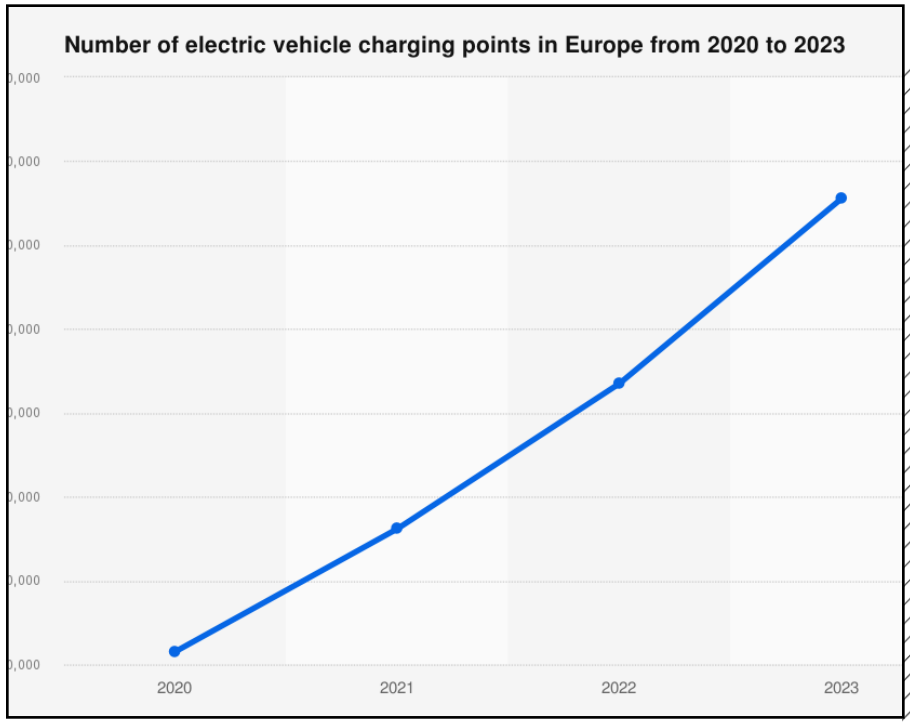
Introduction

Current trends in E-Mobility



Electric Vehicle Sales

Source: https://www.statista.com/outlook/mmo/electric-vehicles/europe#unit-sales



Charging Points in Europe

Source: https://www.statista.com/statistics/1537841/public-ev-charging-points-installed-worldwide-by-power-rating/

Threat Landsape

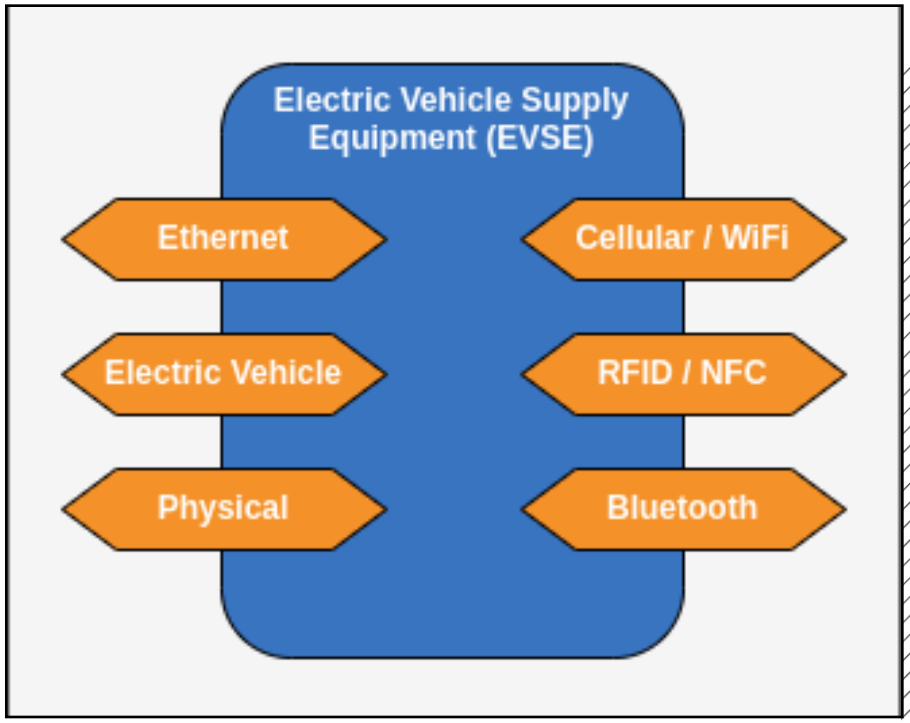
Attacks on charging infrastructure

Key Vulnerabilities

- Weak authentication & unsecured communication channels [14]
- Exploitable connected systems (IT/OT) [14], [15]
- Physical access interfaces (e.g., maintenance ports, RFID, Bluetooth) [4]
- Protocol-specific flaws (e.g., OCPP, MQTT) [16]

Potential Threats & Risks

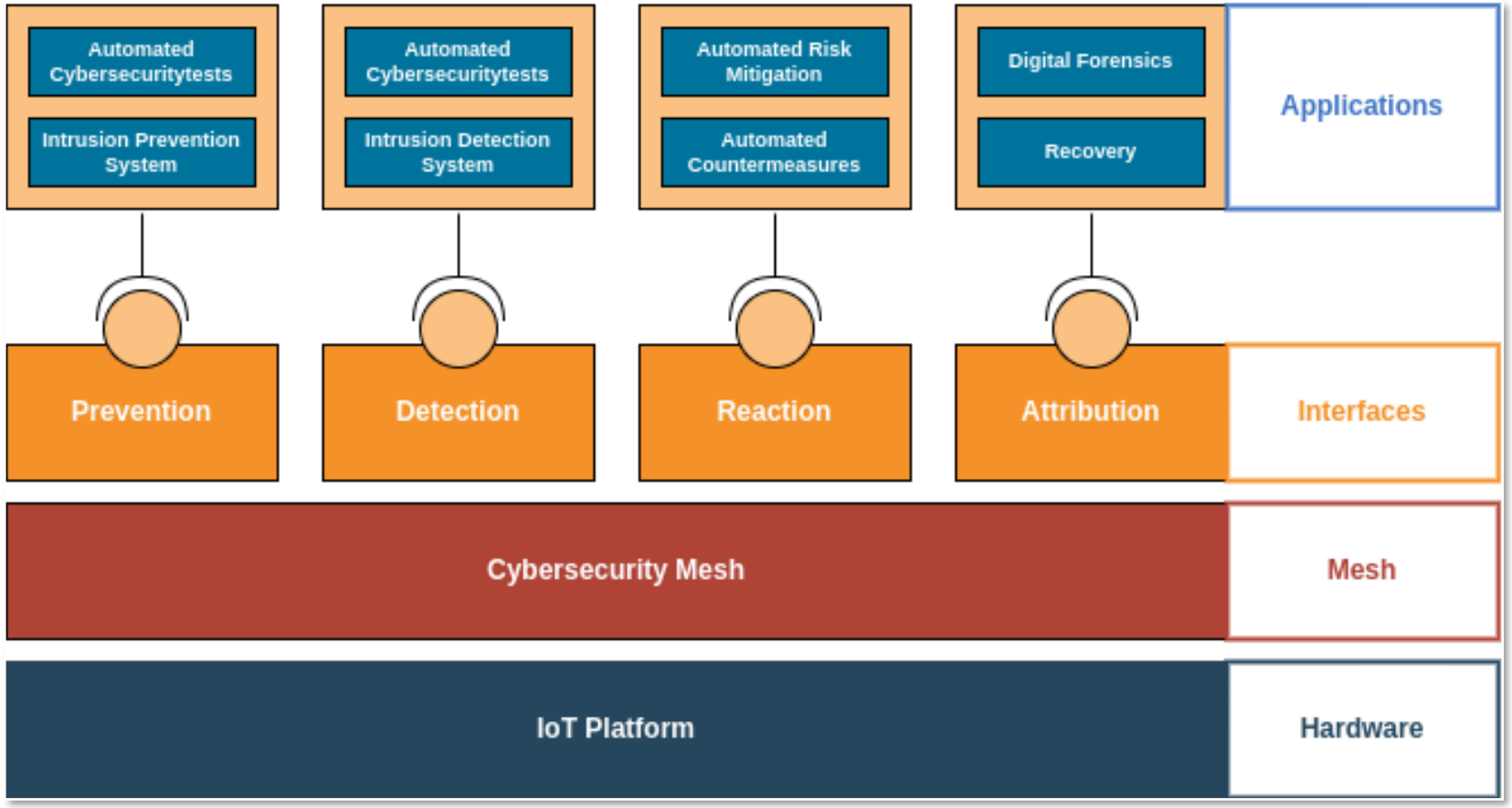
- Data theft, fraud, and ransomware [16]
- Denial-of-Service attacks [14]
- Power grid destabilization (local → national scale) [15]



EVSE Interfaces

System Architecture

ReSiLENT System Overview



System Architecture

IoT Platform

Modular Hardware Unit

- Embedded directly into the EVSE
- Hosts software responsible for core EVSE functionalities:
  → Communication with electrical components, Charge Point Management System (CPMS), and Electric Vehicle (EV)

ReSiLENT System - bidirectional communication between EVSE software and the ReSiLENT security system:

- **System observability** (logs, network traffic, etc.) for anomaly detection and threat monitoring
- **Response mechanisms**, enabling real-time countermeasures

Cybersecurity Mesh

Concept for improved threat detection

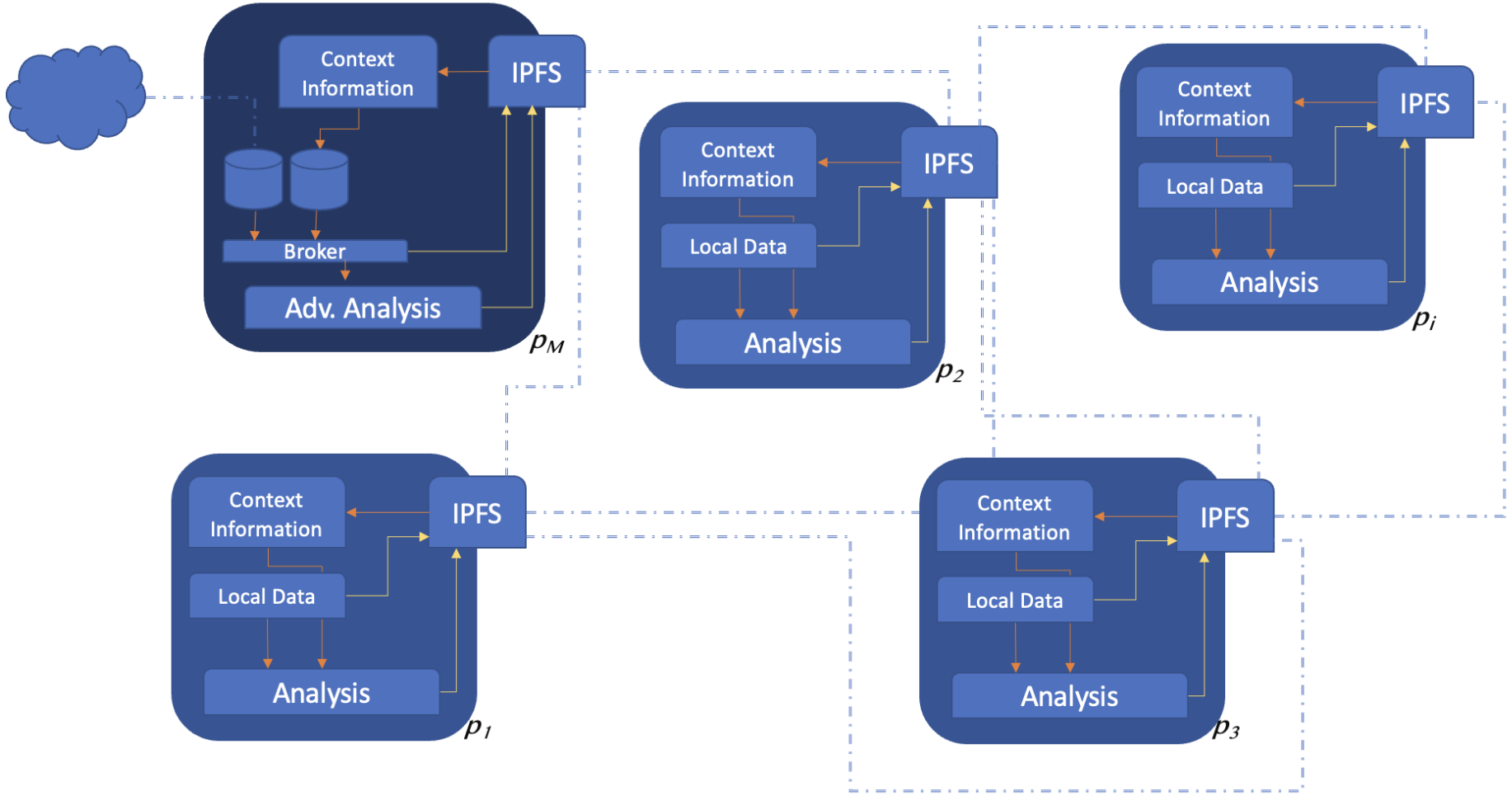
Our Approach: A Cybersecurity Mesh for EVSE

- ReSiLENT introduces a **Cybersecurity Mesh Architecture**
- Links individual EVSE units as **nodes** in a distributed, collaborative security network
- Each node collects, processes, and **shares context-aware data**

Goal: **Leverage collective intelligence** to improve threat detection and resilience

Cybersecurity Mesh

Peer-to-Peer Communication using the InterPlanetary File System (IPFS)



Cybersecurity Mesh

InterPlanetary File System (IPFS)

IPFS Protocol Stack

- Enables **P2P communication** *and* resilient, distributed data access
- Decentralized file storage: files are stored on each node and retrieved by **hash**, not URL (content addressability)
- No centralized server required

Data sharing with Pub/Sub Model

1. Nodes subscribe to topic-based channels (e.g., network-traffic, threat-reports)
2. After publishing a file, the node **sends a lightweight notification**
3. Interested nodes pull the file if subscribed to that topic

Cybersecurity Applications

Security Domains

Distributed data usage for enhancing security applications in the following domains:

- Detection
- Reaction
- Prevention
- Attribution

Goals: Enhance security by utilizing **contextual insights** from distributed nodes

Cybersecurity Applications

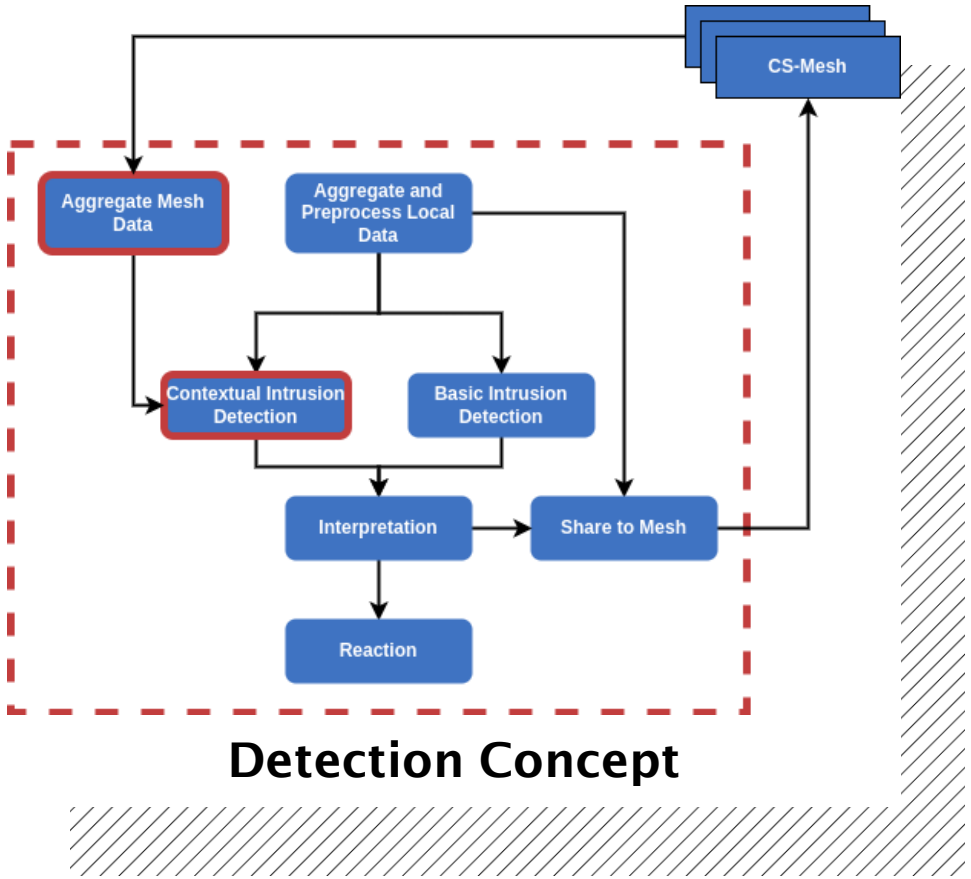
Detection

Basic Intrusion Detection

- Signature- and behaviour-based intrusion detection for system, network, and charging sessions

Contextual Intrusion Detection

- Complementary
- Consensus-Oriented
- Comparative



Detection Concept

Conclusions and Future Work

Ongoing implementation and validation

- **Implementation** of detection and reaction mechanisms is in progress
- Metrics and results will be measured to assess the efficacy of the system
- Objective: **Validate improvements in threat detection** and refine based on observed results

Contact

Feel free to contact us

OTH REGENSBURG

KONTAKT

-

Seybothstraße 2

93053 Regensburg

christoph.moser@oth-regensburg.de

Department of Computer Science and Mathematics – Laboratory for Automotive Security

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.

References

[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.