Electric Vehicles and Charging Infrastructure Security

by

Soheil Shirvani

Bachelor of Engineering, University of Tehran, 2021

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Computer Science

In the Graduate Academic Unit of Computer Science

Supervisor(s):	Ali A. Ghorbani, Ph.D., Computer Science
Examining Board:	Wei Song, Ph.D., Computer Science, Chair
	Kalikinkar Mandal, Ph.D., Computer Science
	Liuchen Chang, Ph.D.,
	Electrical and Computer Engineering

This thesis is accepted by the
Dean of Graduate Studies

THE UNIVERSITY OF NEW BRUNSWICK

August 2023

Abstract

Electric Vehicles (EVs) have gained popularity in recent years due to their economic and environmental benefits. However, their growth has faced numerous technical challenges, with cybersecurity emerging as critical. To address security concerns, this thesis initially surveys the previous literature to find possible attacks and challenges of EVs. Then, it analyzes the security of all components that can transmit data or are connected to EVs, with the aim of identifying the critical elements in the ecosystem. Utilizing the proposed architecture, this study introduces a comprehensive risk assessment framework that identifies all possible attacks and challenges. These are then ranked based on impact, likelihood, and risk criteria, with subsequent countermeasures proposed. Furthermore, to demonstrate the applicability of our proposed methods, we identify a gap in the Electric Vehicle-Electric Vehicle Supply Equipment (EV-EVSE) system, specifically monitoring charging sessions. Consequently, we propose a five-step intelligent monitoring framework for charging sites to prevent fraudulent charging and malicious sessions.

Dedication

This thesis is warmly dedicated to my cherished parents and siblings, whose unwavering love and support have been my beacon of light in the journey of knowledge. Their relentless faith in my capabilities, coupled with their constant encouragement, has empowered me to chase my dreams. My deepest gratitude goes out to them for being my steadfast pillars of strength and for their invaluable contributions to my life. Thank you for your love and sacrifices.

Acknowledgements

My heartfelt appreciation goes out to my supervisor, Professor Ali Ghorbani, whose unwavering support, and expert guidance have been invaluable throughout this thesis journey. The privilege of working under his mentorship and collaborating with the esteemed Canadian Institute for Cybersecurity (CIC) has truly been an honor. Additionally, I would like to express my sincere acknowledgment of the diligent efforts made by my astute colleagues at the CIC, whose dedication has significantly contributed to my academic experience.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ADEV	Autonomous Driving EV
AV	Autonomous Vehicle
CAN	Controller Area Network (Bus)
C-V2X	Cellular Vehicle-to-Everything
DR	Demand Response
DSRC	Dedicated Short-Range Communications
ECU	Electronic Control Unit
EV	Electric Vehicle
EVCS	Electric Vehicle Charging Station
EVSE	Electric Vehicle Supply Equipment
EV-SP	Electric Vehicle Service Provider
EVSE-SP	Electric Vehicle Supply Equipment Service Provider
ICV	Intelligent Connected Vehicles
IoAV	Internet of AV
IoV	Internet of vehicles
LIN	Local Interconnect Network (Bus)
MOST	Media Oriented System Transport (Bus)
OTA	Over The Air (Update)
OBD	On Board Diagnostic (Monitoring)
OCPP	Open Charge Point Protocol
OTA	Over The Air (wireless)
OpenADR	Open Automated Demand Response (protocol)
PEV	Plug-In-Electrical-Vehicles
RSU	Road Side Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
TCU	Telematics Control Units
VANET	Vehicle Ad Hoc Network
V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2P	Vehicle to Pedestrian
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything

Chapter 1

Introduction

1.1 Introduction

Electric vehicles (EVs) represent a growing transportation industry poised to impact public life, making it more affordable and convenient. As the number of EVs increases, concerns about accidents, greenhouse gas emissions, and fossil fuel issues intensify. This rapid growth in EVs necessitates more trustworthy public and private Electric Vehicle Supply Equipment (EVSE) and EVs. Furthermore, many countries worldwide are investing in efforts to phase out gasoline vehicles, such as the UK's announcement to ban them by 2035 [117, 326]. Due to the advantages EVs offer for both the public and government economies, it is predicted that the number of EVs in use will reach around 125 million by 2030 [44]. However, the growth of the EV market is hindered by several challenges. In particular, EV security has emerged as a major concern for vehicle vendors, with cybercriminals using zero-day attacks to compromise EVs. In response, industry and academic researchers are working to overcome these challenges [86, 102].

The evolution of EVs and EVSEs technologies began a decade ago and continues today. As technologies such as the Internet of Things (IoT), Artificial Intelligence (AI),

complex communication networks and protocols, and smart grids evolved, researchers have leveraged these advancements for EVs and EVSEs to enhance their reliability and efficiency. While manufacturers are developing new vehicles with greater connectivity and autonomy, such as Intelligent Connected Vehicles (ICVs) and Autonomous Vehicles (AVs) [182,336], EVSE vendors are introducing more advanced charging stations. Networked chargers, Fast Chargers (FC), Extreme Fast Chargers (XFC), and Solar Chargers (SC) are examples of such innovations [248,298]. These advancements have gradually expanded charging stations and EVs usage in homes, public places, and commercial buildings, mitigating the social impacts of EV adoption [82,189].

However, the evolution and widespread adoption of EVs have presented countries with the significant challenge of securing their infrastructure and smart grids. EVs employ a variety of software components like applications, Electronic Control Units (ECUs) firmware, and cloud servers that offer functionalities and address technical challenges, but these also present potential security risks and privacy concerns [113]. The integration of EVs into the Internet of Vehicles (IoV) [152], termed ICVs, leverages technologies such as Dedicated Short-Range Communications (DSRC) and Cellular Vehicle-to-Everything (C-V2X) for communication, enhancing their efficiency but also introducing new security threats [20, 205]. Moreover, EVs are moving towards autonomy with the aid of advanced sensors and AI, leading to the emergence of AVs [168,170]. While AVs signify a transportation revolution, their cybersecurity, especially given the potential risk to human life, has emerged as a pressing research area [103].

As a result, researchers have begun to explore ways to secure the EV-EVSE infrastructure. The National Institute of Standards and Technology (NIST) was one of the pioneers in emphasizing EV security, and according to NIST's cybersecurity guidelines for intelligent grids [240], EVs are considered part of the smart grid due to critical communications between EVSEs and smart grids, such as participation in Demand

Response (DR) [126] and energy transfers. In 2020, the same organization brought together prominent researchers to work on charging infrastructure security [190]. Additionally, as more companies enter the EV market, ensuring a secure infrastructure is becoming increasingly demanding, requiring more effort to establish reliable electrified transportation.

This thesis aims to develop methods to bridge existing gaps and establish a more secure EV-EVSE ecosystem. In order to achieve this, it is essential to first comprehend the EV-EVSE ecosystem, which comprises communication protocols, interfaces, components, and data and power flows. This thesis introduces a unique Data Flow Diagram (DFD) that delineates all the data and power flows within each EV and EVSE and between them. Examination of this ecosystem can shed light on potential vulnerabilities and points where adversaries might initiate an attack. Although the proposed ecosystem covers all major components, it is not sufficient to fully understand the security aspects surrounding the EV-EVSE ecosystem. Hence, this thesis investigates vulnerabilities and security measures separately to identify all possible attacks and challenges.

EVs face many cybersecurity risks like hacking, malware, data breaches, and supply chain attacks. Ensuring their security necessitates a comprehensive risk assessment to identify vulnerabilities. This thesis concentrates on risk assessment, a crucial aspect of the risk management process outlined by NIST [35], and employs the STRIDE threat model to categorize attacks and challenges. The assessment involves breaking down the EV-EVSE system's security into different aspects, each comprising attack surfaces, attack subsurfaces, and vulnerabilities. Attack surfaces refer to abstract threats to the system, while attack subsurfaces represent the specific targets that adversaries can exploit. Vulnerabilities are the weaknesses in the subsurfaces that adversaries can use to launch attacks. This thesis leverages the STRIDE model to categorize attacks and challenges. Based on the categorized surfaces, the paper

proposes possible solutions to mitigate those attacks. The study addresses all possible security vulnerabilities threatening EVs in the following sections.

While understanding the architecture of the EV-EVSE ecosystem and its related security profiling helps identify the system's security flaws, it is not a solution in itself. Numerous proposed solutions primarily rely on AI and Machine Learning (ML) techniques to address specific security aspects of the architecture. For instance, [297] proposes an intrusion detection system for in-vehicle CAN bus security, and [112] suggests using statistical analysis to detect anomalies in charging stations. Other solutions include securing EV's V2X communication [279], protecting sensitive data privacy [84], scheduling charging sessions [321], and balancing the charging load across an area [211]. Each study focuses on a single part of the entire EV-EVSE architecture. By examining previous studies and extracting the security flaws of the EV-EVSE system through the proposed architecture and profiling, monitoring and maintaining reliable charging sessions emerge as ongoing security challenges that require greater focus, particularly as the number of EVs increases.

Aiming to address this challenge, this thesis proposes a five-stage framework, focusing on securing the charging sessions at sites that could be home-based, private, or public stations. Unlike traditional gasoline stations, these stations involve the exchange of time-sensitive and personal user information during EV charging, increasing vulnerability to malicious activities such as misinformation or compromise of the EVSE. To ensure safety, security, and prevent financial fraud, monitoring of all EVSE sessions, similar to Security Information and Event Management (SIEM) or Network Intrusion and Detection Systems (IDS) in network companies, is proposed [115, 307]. This thesis suggests a SIEM-like AI-enabled EV charging session monitoring system, following a hybrid five-stage approach, each building on the previous stage for full functionality. This process starts with analyzing the behaviour at the charging site and sessions, then setting up a rule-based detection system, followed by training a

supervised ML model, developing an anomaly detector, and finally determining the cause of anomalous sessions using prior stages' ML models. This system can identify malicious sessions at any charging site and provide explanations for any abnormal session activities. Figure 1.1 illustrates the mentioned stages.

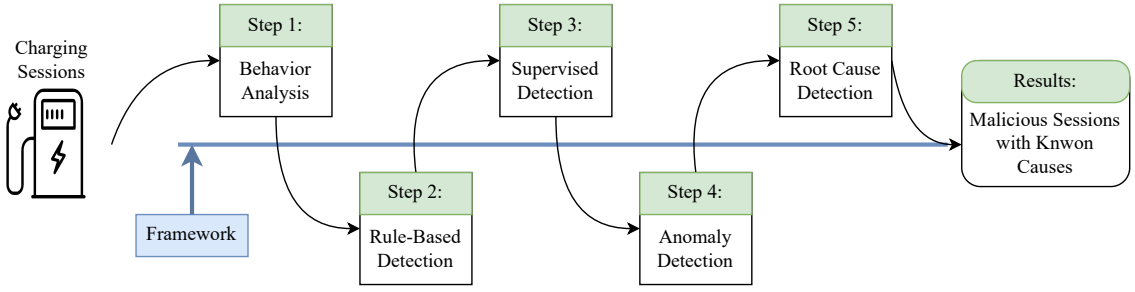

Figure 1.1: Steps of the proposed for EV charging sessions security

1.2 Motivation and Objectives

Thus far, this thesis has underscored the importance of EV and EVSE security, especially given the substantial investments countries are making to foster the widespread adoption of these technologies. The aim is to explore all security aspects of EVs and EVSEs and propose corresponding solutions. To this end, we first conduct a comprehensive literature review to understand all facets of EVs and EVSEs. This step is crucial for identifying security vulnerabilities and ensuring all elements are taken into consideration. We then present a unique DFD architecture of EV and EVSE, encompassing all major components and systems. This DFD aids in understanding communication pathways, identifying vulnerable components, and pinpointing potential sources of attacks. However, the DFD provides only a snapshot of the security landscape and potential vulnerabilities. We propose a risk assessment framework based on NIST guidelines and the STRIDE threat model to truly identify attacks and risks associated with the architecture. This framework aims to evaluate and identify all risks linked to this system. We suggest universal profiling for EVs en-

compassing five different aspects that will assist in understanding risks, identifying attacks and challenges, and assessing the impact and likelihood of various attacks. To rank the risks within each profile aspect, we develop our own set of criteria for impact and likelihood. Moreover, to illustrate the application of the proposed risk assessment framework, we apply its steps to assess and identify the risks of eight real-world EV attacks. To develop a solution and demonstrate how researchers can use the proposed architecture and risk assessment framework, we delve deeper into one of the emerging challenges in EV charging - EVSE charging session monitoring. After identifying this challenge through a literature review, we propose a SIEM-like intelligent monitoring framework for charging sites. This will help monitor all incoming charging sessions, preventing charging fraud and vehicle impersonations. This intelligent framework represents just one part of the larger picture and serves as a model for developing real solutions. In future work, we will discuss additional problems and demonstrate how the proposed architecture can be leveraged to identify more security issues surrounding EVs and EVSEs.

1.3 Summary of Contributions

The primary purpose of this thesis is to investigate the security aspects of EVs and EVSEs and to develop security solutions for this ecosystem. In summary, our contributions are listed as follows:

1. Demonstrating the components and communications of a generic EV and EVSE based on existing studies and surveying existing security solutions based on ML, AI, and SIEM-like software.

2. Conducting a comprehensive analysis of the various security aspects of EVs and providing detailed information regarding attack vectors that can compromise EVs. This analysis involves classifying EV security into five categories and iden-

tifying possible attack surfaces/subsurfaces, vulnerabilities, threats, challenges, and attacks. For each attack, we present possible countermeasures based on categorization to mitigate the risks associated with the attacks.

3. Profiling the EV-EVSE ecosystem with all components, data flows, power flows, and communication protocols. This architecture can provide insight for anyone working on EV-EVSE infrastructure.

4. Providing a risk assessment framework and threat modelling of EVs and EVSEs with STRIDE, the most mature threat model, to map the identified vulnerabilities to STRIDE areas to analyze the risk associated with each security aspect using the identified aspects and their detailed analysis by applying custom criteria.

5. Conducting a detailed analysis of real-world attacks on EVs to demonstrate how researchers can use our proposed framework to identify vulnerabilities and risks and describe their attack scenarios.

6. Proposing a five-stage SIEM framework for EV charging sessions' security based on AI and publicly available datasets, ACN-data, evaluating the proposed framework's results, and explaining the anomalies detected.

1.4 Thesis Organization

The remainder of this thesis is organized as follows. Chapter Two summarizes the literature review of security concerns and challenges of EVs, generic components of EVs and EVSEs, risk assessment analysis surrounding smart grids and EVs, and analysis of EV charging session's security. Then Chapter Three discusses the proposed DFD ecosystem of EV-EVSE based on the literature review. Chapter Four proposes a risk assessment framework based on previous chapters' identified attacks and challenges.

This chapter also adopts the framework for real-world EV attacks as a use case of the framework. Chapter Five proposes an intelligent monitoring framework for EV charging sessions that combines and showcases one usage of the proposed ecosystem and risk assessment framework. Finally, the conclusion and future work are presented in Chapter Six.

Chapter 2

Literature Review

2.1 Electric Vehicle and Charging Station Security

In recent years, public interest in EVs has increased. However, this fast-growing market requires studies involving the security of EVs [313]. Finding vulnerabilities in EVs is only possible through a comprehensive literature review, which we present in this section. We have divided EV security into five categories. The following subsections demonstrate the background and related works of each category. Later in this thesis, we will use them to categorize EV security vulnerabilities, extract security layers, and propose a risk framework.

2.1.1 Electric Vehicle Charging Stations Security

EVCSs are essential components of the electric vehicle ecosystem, especially for Plug-in Electric Vehicles (PEVs) [350]. Researchers have identified various cyber and physical vulnerabilities. The ISO/IEC 15118 standard defines the interface for charging EVs, but it has vulnerabilities in data exchanges, as described in attacks by authors in [116]. In [241], the ecosystem of EVSEs was determined, and various cyber vulnerabilities of EVSEs were demonstrated. EVSEs constantly communicate with smart

grids, so vulnerabilities in EVSEs can also affect the entire smart grid. A collaboration of multiple US departments, including the US transportation department and the US Department of Energy Office in [130], provided a detailed technical report regarding cyber security issues of EVSEs and EVs. Researchers have examined the cybersecurity issues of EVSEs from the perspective of the power grid and provided standards for mitigating these cyber vulnerabilities. Therefore, it is crucial to address these security issues to ensure the efficient and secure mass adoption of electric vehicles. Authors in [4] examined charging stations from the power grid perspective and analyzed cyber security issues. Consequently, EVSE cyber security and physical safety are crucial for EVs.

2.1.2 Electric Vehicle Information Privacy

Considering the rapid growth of EVs, user privacy has become a critical issue. The bottleneck of information exchange is when the vehicle is charging or when users use software to interact with their vehicles. Vehicle actuators gather sensitive data, and compromising this information compromises user privacy. Information leaks, such as location, identification, payments, and driving habits, can endanger privacy. For instance, in [129], the authors surveyed existing techniques that address various privacy issues in EVs and smart grids. In [276], the authors conducted an innovative study regarding the privacy challenges affecting EVs and EVSEs. Some studies tried to solve the privacy of users' payments. For example, in [222], the authors presented a privacy-preserving authentication and payment scheme, which is proven to have a secure way of payment to preserve user identification and privacy while making it feasible to trace the vehicle in case of vehicle theft. Another critical privacy issue is user location, examined in [195]. Some studies also concern an authentication scheme for EVs connecting to power stations, such as [227] and [184]. Thus, EV information privacy requires assessment.

2.1.3 Electric Vehicle Software Security

EVs rely on software to interact with users. Secure and reliable software is essential for managing EV's rapid growth [24]. EV applications, such as monitoring EVs [43], analyzing charging infrastructure [177], or vendors software such as Nissan or Ford applications, are available for public use. Firmware of ECUs and other embedded hardware control various functionalities in EVs, making them safety critical [51]. Firmware updates, especially Over-the-Air (OTA) updates, code injections, and malware, are security challenges that threaten EV software and hardware, as described in [271]. A comprehensive literature review of techniques for testing embedded software in transportation systems and EVs is provided in [55]. EV and EVSE vendors also rely on their cloud servers to maintain a reliable product, and compromising them can have devastating financial and reputation consequences, as described in [154]. Therefore, software security in EVs is an important part.

2.1.4 Connected Electric Vehicle Security

To navigate unpredictable real-world situations, EVs became part of a complex network of connected entities, Vehicular Ad-hoc Networks (VANET) [178]. These new ICVs can connect to other vehicles, infrastructure, and pedestrians via various communication modes, including V2X (includes V2N, V2V, V2I, V2P) and DSRC. However, ICVs face several complexity and security issues [78]. For instance, in [131], the authors describe DSRC and C-V2X technologies and their architectures for V2X communication. Meanwhile, [358] discusses the evolution of communication technologies for V2X and ICVs and demonstrates an emerging IoV technology. Other attacks on ICVs include those targeting traffic light infrastructure [110], attacks on the communication channel and sensor tampering [21], and the security and privacy concerns of C-V2X and DSRC communication technologies [200]. V2X communication security is crucial, and many studies have examined the flaws in this type of transportation.

However, the cyber-physical nature of ICVs introduces more vulnerabilities to their communications [259]. Adversaries can compromise the vehicle's power system or controllers and endanger pedestrians by injecting malicious code, malware, arbitrary code execution, and vandalizing the battery or controllers [206]. Hence, considering both the physical and communication aspects of ICVs to maintain a secure transportation system is critical in EVs.

2.1.5 Autonomous Driving Security

The growth of Autonomous Driving EVs (ADEVs), also known as AVs, requires robust detection and computer vision methods, such as lane and pedestrian detection, especially under real-world scenarios. However, recent studies have shown vulnerabilities of AVs to adversarial attacks, particularly in the sensor system, which can compromise AVs' driving decisions [273]. With new adversarial machine learning attacks rising, AVs are in great danger [245]. These attacks include lane detection adversarial or trajectory adversaries, as discussed in [351]. AVs rely on multi-sensor perception rather than a single camera, LiDAR, and telemetry services to make them more secure. Such sensors introduce new vulnerabilities to compromise the ADEVs. For instance, authors in [331] designed spoofing attacks towards a Tesla Model S ultrasonic sensor in autonomous driving mode, causing total blindness of the vehicle and resulting in wrong decisions. Authors in [48] examined multi-sensor-fusion security-based perception AV. [224] explored the new Internet of Autonomous Vehicles (IoAV) and its security needs and challenges, similar to authors in [334], which investigated different issues and cyber vulnerabilities that threaten AVs. Another crucial vulnerability for AVs is in-vehicle communications. Authors in [263] investigated vulnerabilities in AV in-vehicle protocols, including CAN, LIN, MOST, and FlexRay buses. The CAN bus is responsible for all ECU communication and can easily be modified and monitored through the On-Board Diagnostic (OBD) port. Examples of

CAN bus and other bus attacks are explained in papers [26,148]. this thesis will assess in detail AV vulnerabilities, including sensors, assistant drivers, telemetry services, and in-vehicle buses.

2.2 Electric Vehicle and Charging Station Ecosystem

This section presents a literature review of other studies related to EVs, EVSEs, and security solutions for EVSE sessions. The primary goal of the literature review is to identify the critical components of EVs and EVSEs within their ecosystem, their communications, and the proposed security solutions for each component. Additionally, a literature review of security solutions for EVSE sessions helps to understand the problem and propose a reliable framework as part of the ecosystem.

2.2.1 Electric Vehicle and Charging Station Communications

Today, there are numerous solutions for securing the EV infrastructure. Understanding the various components and their interactions can reveal potential vulnerabilities and weaknesses that attackers could exploit. By nature, EVs and EVSEs heavily rely on communication with each other, the smart grid, and cloud networks. These communication requirements have made the EV-EVSE ecosystem a complex interconnected system of different components. Examples of such communications include Vehicle-to-Everything (V2X) [20], encompassing Vehicle-to-Pedestrian (V2P), Vehicle to Network (V2N), and Vehicle to Infrastructure (V2I), Vehicle to Grid (V2G); Vehicle to EVSE (charging); connected ECUs and in-vehicle buses (CAN, The Local Interconnect Network or LIN, FlexRay, and MOST buses) [39]; EVSE to the smart grid (V2G); EVSE to Vendor or other EVSEs using Open Charge Point Protocol (OCPP) [235]; and EV or EVSE to Software (V2S) [336]. Additionally, numerous

smaller components, such as the battery, ECU, Telematics Control Units (TCU), and IoT actuators, are connected to form the physical parts of EVs and EVSE. All these components work simultaneously to achieve functional, reliable, and efficient transportation. However, maintaining a reliable and secure system with many complex building blocks can be erroneous and require significant effort. Figure 2.1 provides an abstract view of these communications, and Figure 2.2 presents a conceptual view of the layers within the EV-EVSE ecosystem. this thesis aims to offer insight into how these components function as a system and provide detailed information regarding these elements.

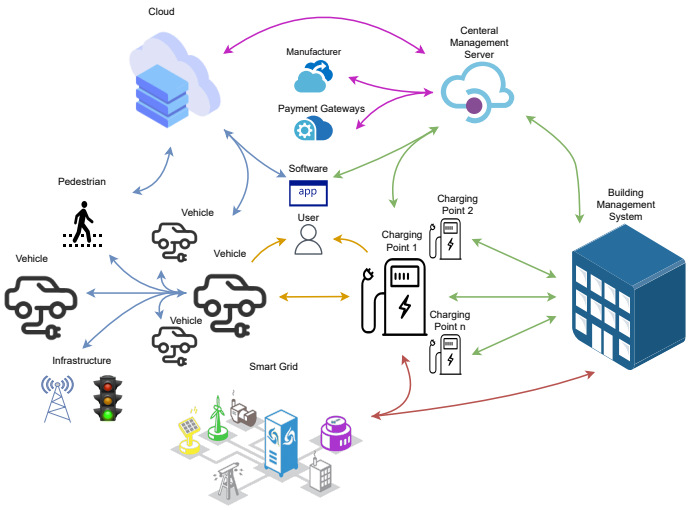

Figure 2.1: Abstract overview of communications between EVs and EVSEs

2.2.2 Generic Electric Vehicle

Authors in [255] demonstrate the design and communications of the CAN bus in EVs. The CAN bus enables ECUs to communicate and transfer data. There are two types of CAN buses: low-speed and high-speed CAN buses. The high-speed CAN bus is the main bus in EVs, while the low-speed CAN bus is often used for telemetry services in EVs [327]. Other types of buses in EVs include the MOST, LIN, and FlexRay bus. Authors in [51] studied the usage of FlexRay in EVs, and its purpose is for

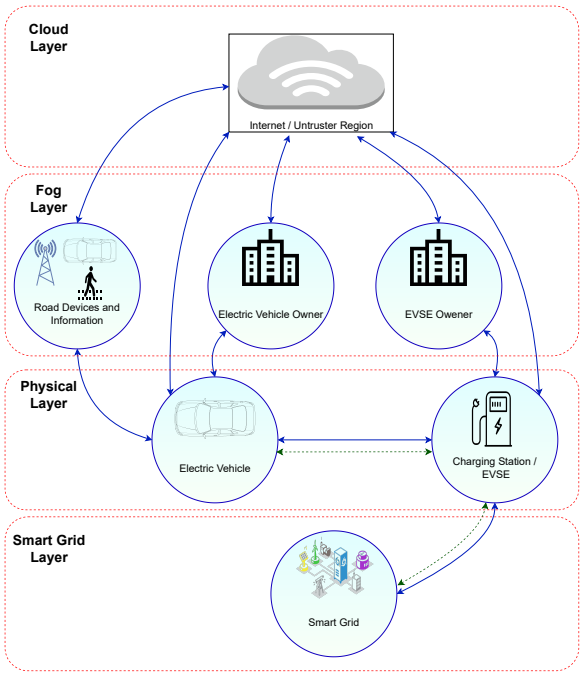

Figure 2.2: Abstract overview of different layers in EV-EVSE relationships

control, such as safety control. The MOST bus is used in media systems in EVs, as it has relatively low speed, as described in [62]. LIN bus connects less complex networks where bandwidth is not required, such as seats or window control [320]. In addition, the authors in [292] did a great job demonstrating the components of EVs. However, their study does not include one of the buses and other major components like autonomous systems; thus, their design could be more precise. According to this literature review and completing the design in [292], Figure 2.3 shows how generic EV (both AV and ICV) components work.

2.2.3 Generic Electric Vehicle Charging Station

As for charging points or EVSEs, authors in [329] study smart charging points and how to develop or simulate one. They demonstrate the components required in a generic EVSE, such as power lines and communication lines. [256] studies a generic AC charger and illustrates how they communicate with other EVSEs and the cloud using OCPP. They also develop an interface for their chargers and discuss its components.

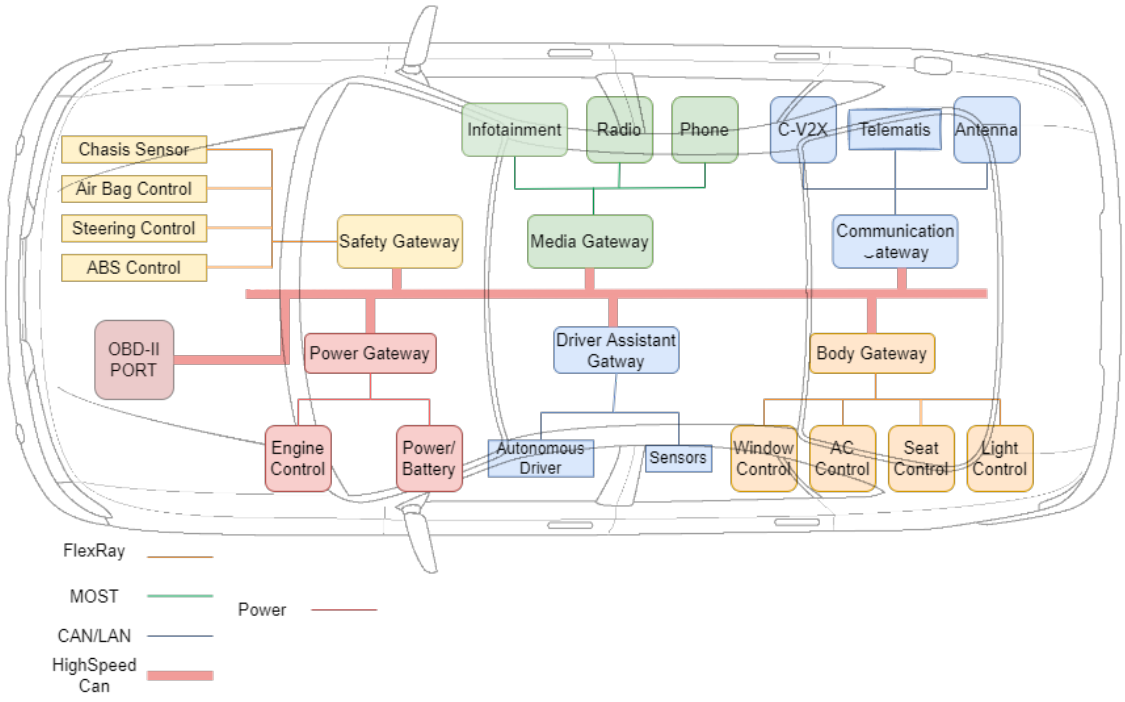

Figure 2.3: Generic overview of EV components

Authors in [7] study different types of chargers and connectors used in the US and their differences. Authors in [100] provide a great design of a generic EVSE and its components. They also include safety requirements for a single EVSE. However, these works are incomplete. For instance, the battery or power system of an EVSE or telemetry service is not shown in their figures. Based on this literature, a generic EVSE design is proposed by this thesis and is shown in Figure 2.4 to fill this gap.

2.3 Electric Vehicle Risk Assessment

Risk assessment, as a critical component of providing a secure environment, is instrumental in identifying vulnerabilities, ranking them along with challenges, and implementing countermeasures. As the fourth step in risk management, risk assessment was first discussed in NIST risk management guidelines [266]. NIST also outlined a risk assessment process in [267], a framework many researchers have since adopted

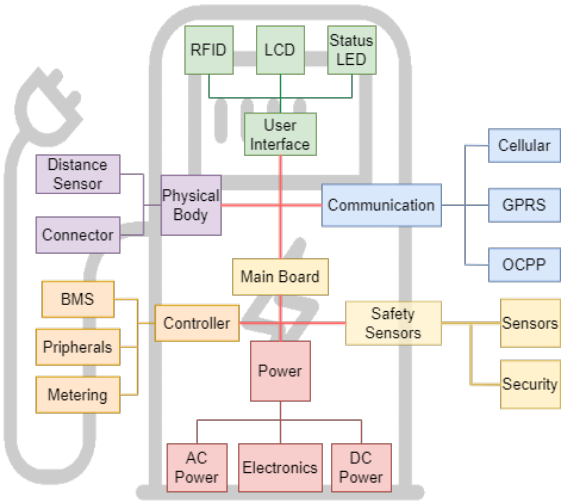

Figure 2.4: Generic overview of EVSE components

across numerous domains. Authors in [232], for instance, carried out a comprehensive risk assessment of the IoT environment, underscoring the importance of such assessments given the unique ecosystem of IoT. However, their study necessitates a robust threat model to pinpoint all vulnerabilities inherent in such systems. Furthermore, authors in [249] proposed and applied a risk strategy model to the IoT environment, emphasizing the need for such a model to secure the IoT landscape. A number of studies also examine risks in cyber-physical systems and smart grids; for example, a risk assessment for smart grids was conducted in [99], addressing potential challenges and attacks in these systems. While risk assessment is essential for secure EV and EVSE systems, no comprehensive system risk assessment currently exists. Several studies, such as [49], which explores risks in EV integration, and [183], which delves into the risks of EV battery and power systems, all necessitate a thorough threat model and risk assessment to uncover all potential vulnerabilities. this thesis intends to bridge this gap by proposing a risk assessment framework for EVs and EVSEs that takes into account all vulnerabilities in these systems. One significant challenge with EV systems is the extensive domain and the integration of EVs, smart grids,

networks, autonomous functions, and in-vehicle sensors, details of which will be elaborated on in Chapter Four. Figure 2.5 illustrates the NIST risk assessment framework and a simple risk matrix to be used later in this thesis.

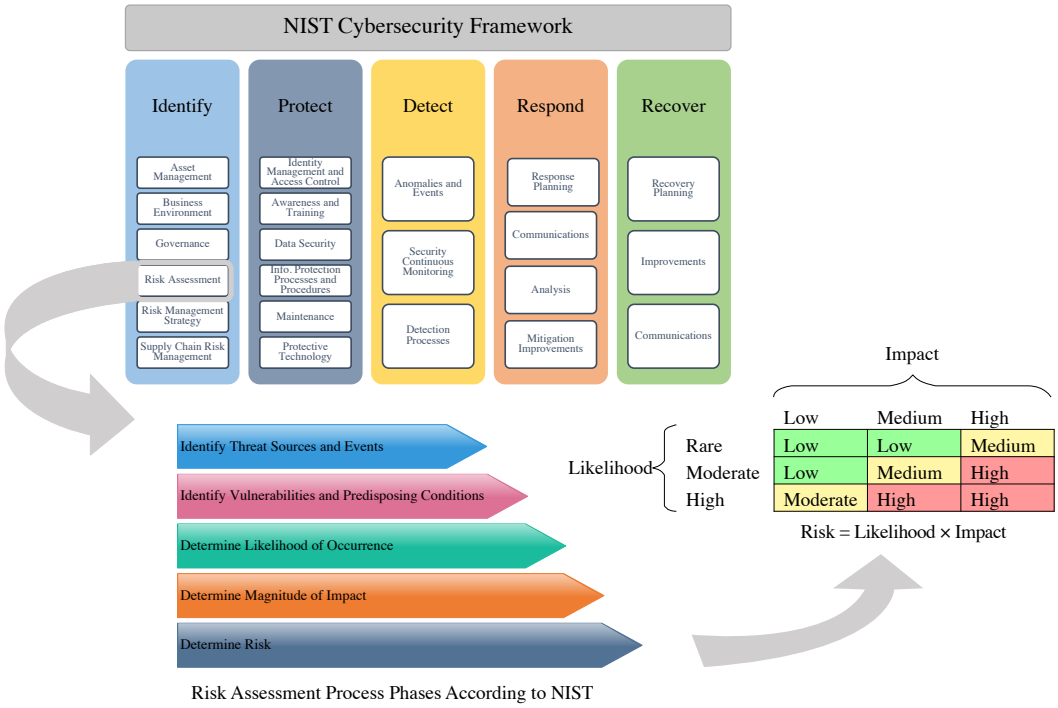

Figure 2.5: Cybersecurity Risk Assessment

2.4 Electric Vehicle Charging Sessions

EV charging sessions represent one of the critical challenges in ensuring the trustworthiness of EVSEs. As the popularity of EVs continues to surge, the number of public and private charging sites is expected to follow suit. Therefore, it becomes increasingly crucial to monitor these charging sites and sessions for potentially fraudulent activity and impersonation. Each charging session encompasses a wealth of time-sensitive information such as connection and disconnection times, charging duration, user-sensitive data including user IDs, payments, and passwords, as well as power-sensitive details such as the total energy delivered and current signal during charging.

Given the sensitivity and importance of this information, ensuring secure charging sessions is paramount. This section offers a review of the existing literature on EV charging sessions. this thesis aims to propose a security framework for monitoring these charging sessions, a subject that will be addressed in greater detail in Chapter Five.

2.4.1 Intelligent Electric Vehicle Charging Sessions Security

AI is an effective solution for the security of EVs and EVSEs. In [353], the authors propose an architecture for collaborative intrusion detection through distributed machine learning. The solution uses the alternating direction method of multipliers to a class of empirical risk minimization problems and detects intrusions in VANETs. Similarly, authors in [340] apply federated learning for Vehicle Edge Computing (VEC) and propose a selective model for image processing in connected vehicles. There are many more studies in which authors suggested AI models detecting DDoS, ransomware, or malware attacks towards EV and EVSEs in papers [31, 34, 352] respectively. SIEM software is another security solution for EVs and EVSEs. For instance, authors introduce SPEAR-SIEM [251] for smart grids. Their SIEM platform can detect events through both signatures and ML models. A similar method is in [328], where authors discuss a monitoring system for various network attacks.

2.4.2 Electric Vehicle Charging Sessions Analysis

The second part of this thesis aims to adopt a SIEM-like solution to address a challenge that hasn't been a focus in recent years: the security of charging sessions and real-world charging sites that require both AI solutions and behaviour analysis of the charging site sessions. There are studies on EVSEs that predict, schedule, or balance loads and energy transfers. For instance, authors in [359] survey different load forecasting methods using deep learning for EVSEs, and [344] proposes a deep

learning model for demand forecasting in EVSEs. this thesis analyzes the behavior of charging session events and predicts anomalies and malicious sessions. Aside from security, behavior analysis is also a focus regarding EVSEs and charging sessions. Examples of such works are [247] and [332], where authors used statistical analysis and data visualization techniques for charging sessions and weather data to understand the behavior and characteristics of critical times, energy transfers, loads, and users. Also, in [79], authors studied the behaviour of charging sessions and EVs based on large-scale power transfer data. Although the mentioned studies provide solutions for energy balancing and statistical analysis of charging sessions, they have yet to tackle the security of the sessions. Providing trustworthy charging sessions can be crucial for charging sites, EVSE owners, and users charging their vehicles. This gap is one of the aims of this thesis and will be discussed in the following sections.

2.4.3 Electric Vehicle Charging Sessions Datasets

There are different datasets available for EVSE sessions. Authors mostly use simulated charging session datasets for their work or have a charging site in their hometown where they can obtain data. These datasets are often private and operated by the same authors for multiple research projects. Examples of such datasets can be found in [77, 79]. Furthermore, there are some charging session datasets publicly available. These datasets include ACN and Elaad data [63, 180, 269]. More information on various EV and EVSE datasets is gathered in a survey [45]. this thesis uses the Caltech ACN data [180], real-world charging sessions derived from Caltech charging sites, to train the hybrid security method. More information on the dataset is discussed later in this thesis.

2.5 Concluding Remarks

In this chapter, we have summarized previous works focusing on the security of EVs and EVSEs, the EV-EVSE ecosystem and communications, and the security of EV charging sessions. We have discussed numerous security challenges surrounding EVs and EVSEs, including the security of charging stations, information privacy, software security, connected vehicle security, and autonomous vehicle security. Moreover, we have emphasized the importance of risk assessment and management for security and discussed how other studies have proposed risk strategies in different domains, such as the IoT. We have identified the components of a typical EV and EVSE, including power and communication aspects, and compiled all the communications in the EV-EVSE ecosystem. Furthermore, we have pinpointed a crucial challenge - monitoring charging sessions - which EVSEs must overcome to ensure a trustworthy charging site. We also gathered security solutions based on AI and SIEM for such challenges. In summary, we have identified a gap in risk assessment for EVs, produced a DFD of the EV-EVSE ecosystem to highlight vulnerabilities and challenges, and recognized the need for effective charging session monitoring as part of the EV-EVSE ecosystem. In the subsequent sections of this thesis, we aim to address these issues by proposing a unique ecosystem, a risk assessment framework, and an intelligent monitoring framework.

Chapter 3

Proposed EV-EVSE Ecosystem Architecture

3.1 Motivation

Until now, we have discussed the rapid growth of EVs and the various challenges they pose, encompassing social, technical, and security aspects. Through an exhaustive literature review, we have identified several unresolved issues, including the security of EVSE, EV and EVSE information privacy, software security, ICV security, and autonomous vehicle security. We have explored how each segment can compromise an EV and emphasized the necessity of a risk assessment framework. However, to pinpoint all the challenges prior to conducting a risk assessment, we need comprehensive insights into all the components that are integral to the EV-EVSE ecosystem. It is necessary to understand these components because adversaries will exploit them for attacks, and the most effective way to mitigate these attacks is prevention at the source. In the literature review, we addressed the internal components of a generic EV and an EVSE, but their ecosystem also encompasses external elements, such as the EV owner or cloud services. By gaining a clear understanding of the EV-EVSE

ecosystem, researchers and industrial companies can devise mitigation strategies that cover certain, if not all, potential starting points for attacks on EVs. Hence, this chapter aims to thoroughly comprehend all these components; their data flows and protocols, power flows, and any third parties that communicate with or exchange data with EVs or EVSEs. Key components include smart grids, cloud services, EV and EVSE owners, and internal parts of EV and EVSE. The following sections will propose an architecture for the EV-EVSE ecosystem and subsequently identify all components within the proposed architecture. Using the insights from this chapter, the next chapter will propose a risk assessment framework to better identify all potential vulnerabilities.

3.2 Ecosystem Components

Up to this point, we have surveyed related works to find a generic view of a single EVSE and EV. While generic ideas help to understand the necessary components and how they communicate within an EV or EVSE, they lack many critical features. Two NIST publications, funded projects for charging stations [190], and security guidelines for smart grids [240] are used as baselines to draw a schematic of the EV-EVSE ecosystem in this section. [190] includes six different projects regarding charging station design. However, its first project contains an exemplary schematic of the EV-EVSE system. Although their schematic includes many more components than the generic design in the previous section, it still lacks some essential components, such as the smart grid, EV network, and cloud. For the smart grid part, the second NIST publication [240] demonstrates the design of the smart grid and its connection to EVs. Using both designs and adding missing EV-EVSE-specific components, we present an architecture using a DFD for the EV-EVSE system in Figure 3.1.

As shown in the figure, "blue" lines indicate data flows, while "green" ones indicate

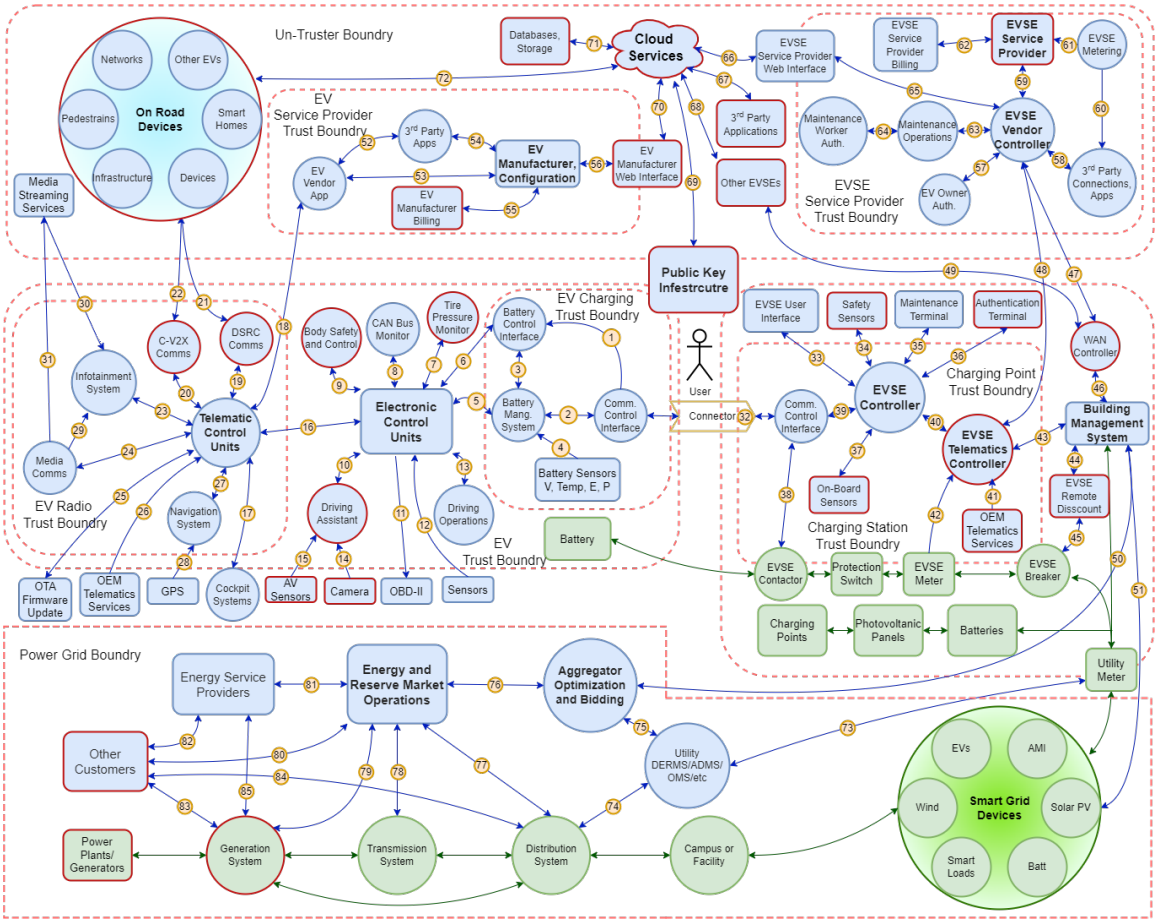

Figure 3.1: Overview of EV-EVSE Ecosystem Architecture

power flows. Additionally, those entities with a "red" outline are the extra components added by the authors of this thesis to the figures shown in NIST publications. All data flows are numbered and have communication direction. Numbers are used in the following sections and tables to summarize the data flow detail, protocols, and data type communicated between the entities. This architecture includes six trusting regions, indicating six main layers in the EV-EVSE system. These six regions are: 1) EV trusting region, 2) EV service provider trusting region, 3) EVSE trusting region, 4) EVSE service provider trusting region, 5) power grid or smart grid region, 6) untrusted region, internet, or cloud. Sections 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, and 3.2.6 show the details of each region respectively.

3.2.1 EV Trusting Boundary

EVs have three primary parts, including 1) the battery section (EV charging trusting boundary), 2) the ECUs section, and 3) the TCU section (EV radio trusting boundary). The battery section is responsible for powering all other components, charging protocols, and handshaking while connected to an EVSE [212]. Connected ECUs are primary parts responsible for all vehicle control, safety, planning, and perception [51]. The TCU or radio part is responsible for all communications, actuators, and media in the vehicles. ICVs can communicate with other cars, pedestrians, infrastructure, and networks using C-V2X or DSRC technologies [90]. Keep in mind that the architecture is showing a general-purpose EV. However, not all EVs have all the components shown in the figure. For instance, not all vehicles have autonomous driving parts or sensors. Table 3.1 shows all the data flows within EVs with their protocols and type of data transferred.

Table 3.1: Components of Electric Vehicle Trusting Boundary

Section	Component	(Number) Data Flow	Data Type	Protocols
Electric Vehicle	BMS	(1) Battery Comm. Control Interface	PWM Control	Wire
		(2) Comm. Control Interface	Battery Data, Charge Commands	Wire
		(32) Connector	Charge Commands	CHAdeMO, ISO 15118, Tesla
		(3) Battery Control Interface	Send Battery status and Sensors, Set Charge Rate/Duration	Wire
		(4) Battery Sensors	Read Battery Data	Wire
		(5) ECUs	Battery Information to other ECUS	CAN
	ECUs	(5) Battery Mang. System	ECUs Information to Battery System	CAN
		(6) Battery Control Interface	Battery Can Traffic	CAN
		(7) Tire Pressure Monitor	Read Tire Data	CAN
		(8) Can Bus Monitor	CAN Bus Data	CAN
		(9) Body Safety and Control	Send Control Signals for Safety/-Hazards	Wire
		(10) Driving Assistant	Send/Receive Assistant Commands	CAN
		(14) (15) Camera and Sensors	Read AV Sensors Data	Wire Wireless IoT,
		(11) OBD-II	Diagnose Can Bus	CAN
		(12) Sensors	Read Sensors Data	Wire
		(13) Driving Operations	Send/Receive Driving Commands	CAN
		(16) TCU	TCU/ECU Can Data	CAN
	TCU	(16) ECUs	ECU/TCU Can Data	CAN
		(17) Cockpit System	Send TCU Data for Personalized Features	Wire, CAN, Wireless IoT
		(18) EV Vendor App	Send Chrg/ Battery/ User Request Data	Wireless, API
		(19) (21) DSRC Comms.	Send DSRC packets for V2V and V2I	DSRC
		(20) (22) C-V2X	Send Cellular packets for V2X Connection	Cellular, 3G, LTE, 5G
		(23) (30) Infotainment	Send/Receive Media Control/-Data	Wire, Wireless (API)
		(24) (31) Media Comms.	External Telematics	Wi-Fi, Bluetooth, Cell
		(25) OTA Firmware Update	Send/Receive Firmware Updates	API, Telematics, Remote Unlock
		(26) OEM Telematics	OEM Telematic Commands	RFID, Alert (API), Infrared
		(27) (28) Navigation System	Send/Receive Navigation Data	GPRS, GPS, Wire
		(29) Infotainment	Send Signal Strength	Wire

3.2.2 Electric Vehicle Service Provider Trusting Boundary

The EV service provider (EV-SP) or EV vendor is the manufacturer of the EV. Although an EV-SP is untrusted by any other entities in the system or other EVs, EVs trust their own SP. Manufacturers require vehicle access for maintenance and over-the-air (OTA) updates [127]. Also, some third-party applications may require EVs' location or status information to provide services such as smart parking, charging site scheduling, or status monitoring, which requires accessing the vehicles through the EV-SPs. Most EV-SPs provide web interfaces and APIs for other applications or EV users to communicate with their EVs [320] and they are responsible for secure user payments [52]. EV-SPs are critical actors in the EV-EVSE system. All data flows with protocols and data types transferred are shown in Table 3.2.

Table 3.2: Components of Electric Vehicle Service Provider Trusting Boundary

Section	Component	(Number) Data Flow	Data Type	Protocols
EV Vendor	EV Manufacturer Configuration	(52) (53) (54) EV Vendor / 3rd Party Apps	Send /Receive EV Data (Status, Operations, Updates, Features)	API, Internet
		(55) EV 3rd Party Billing	Send / Receive Billing Data	API, Internet
		(56) EV Vendor Web Interface	Send / Receive User Interface Data	API, Cloud Internet

3.2.3 EVSE Trusting Boundary

Functional EVs require trustworthy EVSEs. To this end, different types of charging sites are proposed in other papers such as [349], categorizing them into three types: residential, commercial or building, and public charging sites. Each charging site can have one or more charging points referred to as EVSEs, charging spaces, or charging stations. A general public charging site has multiple EVSEs and a management building [318]. An EVSE consists of three main parts: power, EVSE safety controller, EVSE telematics or radio controller, sensors, and user interface [22]. EVSEs can communicate with other EVSEs or cloud (through OCPP), smart grids (through

V2G and openADR), EVs (through CHAdeMO, ISO 15118, or EEBus) or building management for various purposes such as scheduling, maintenance, or DR [212]. Also, many types of EVSEs exist, such as fast chargers, AC, or DC chargers [98]. EVSEs, as part of the smart grid, participate in DR and energy transfers to make a stable grid and are crucial parts of EV-EVSE systems. All data flows with protocols and data type transferred are shown in Table 3.3.

3.2.4 Electric Vehicle Supply Equipment Service Provider Trusting Boundary

Like EV-SP, EVSE Service Providers (EVSE-SP) operate EVSEs. Like EV-SP, EVSE-SP provides web interfaces and APIs for third-party application services such as charging monitoring, scheduling, and payments [33]. Also, customers can use web interfaces for authentication or payments [262]. In addition to these functionalities, EVSE-SP should monitor and maintain their EVSEs for both smart grids (reporting energy transfers, measuring energy, etc.) and maintenance of their physical states. EVSE-SPs can communicate with their EVSEs directly through OCPP or the management building [348]. All data flows with protocols and data types transferred are shown in Table 3.4.

3.2.5 Cloud, Internet, or Untrusted Boundary

All other regions can communicate with each other or external entities, such as infrastructures and applications, through the Internet. The internet is untrusted in all regions mentioned; therefore, entities must implement secure communications, private information exchanges, and authentication mechanisms [321]. When an EV connects to an EVSE for a charging session, a TLS channel opens for handshaking. This communication and all other protocols that require security urge the requirement of a

Table 3.3: Components of Electric Vehicle Supply Equipment Trusting Boundary

Section	Component	(Number) Data Flow	Data Type	Protocols
Charging Station	EVSE Controller	(32) (39) Comm. Control Interface	Charge Commands	CHAdeMO, ISO 15118, Tesla
		(33) EVSE User Interface	Charge Status / Authentication Data	Wire, RFID
		(34) Safety Sensors	Read Sensors Data	Wire, Wireless IoT Wireless
		(35) Maintenance Terminal	Diagnose Charging Point Terminal	Wire, LAN
		(36) Authentication Terminal	Read Authenticate Users / Workers	Wire, RFID
		(37) On-Board Sensors	Read Sensors Data (Distance, Temp)	Wire, Wireless, IoT Wireless
		(40) EVSE Telematics	Send/Receive Telematic/Control Data	Wire, LAN
	EVSE Telematics Controller	(40) EVSE Controller	Send/Receive Telematic/Control Data	Wire, LAN
		(41) OEM Telematics	Receive Telematics Data	OCPP, RFID, LAN, Cellular
		(42) EVSE Metter	Read Metter Data	Wire
		(43) (49) Building Mang. System	Demand-Response Data, Control Data, Configuration	OCPP, Wire, Wireless IoT
		(48) EVSE Vendor Controller	Send/Receive EVSE Operations	Wireless, LAN, OCPP, API
	Building Management System	(43) EVSE Telematics	Demand-Response Data, Control Data, Configuration	OCPP, Wire, Wireless IoT
		(44) (45) EVSE Remote Disconnect	Send Control Signal	Wire, Wireless IoT
		(46) (47) EVSE Vendor Controller	Send/Receive EVSE Operations, Billing, Maintenance	Wireless, LAN, OCPP, API
		(46) (49) Other EVSEs	Send / Receive Pricing/Scheduling	Wireless, LAN, OCPP, API
		(50) Aggregator Optimization and Bidding	DER, Nameplates, Ratings, SOC, Market Commitments	LAN, Wireless (API)
		(51) Utility	DER, Market Commitments, Energy Transfer Configuration	LAN, Wireless (API)

Table 3.4: Components of Electric Vehicle Supply Equipment Service Provider Trusting Boundary

Section	Component	(Number) Data Flow	Data Type	Protocols
EVSE Owner	EVSE Vendor Controller	(57) EV Owner Authentication	Receive Auth. Of EV and its manufacturer	API, RFID, Auth. Terminal
		(58) 3rd Party Apps	EVSE Monitoring/ Charging Apps	API, Internet
		(59) EVSE Service Provider	Send / Receive Energy-Related or Metering Data/ Price	API, Cloud Internet
		(63) (64) EVSE Maintenance	Receive Auth. of Maintenance workers and operations	API, RFID Internet, Cloud
		(65) EVSE Owner Web Interface	Send / Receive User Interface Data	API, Cloud Internet
	EVSE Service Provider	(59) EVSE Controller	Send/Receive EVSE Operations	API, Cloud Internet
		(61) EVSE Metering	Receive EVSE Metering Data	OCPP, API, Cloud, Internet
		(62) EVSE 3rd Billing	Send / Receive Billing Data	API, Internet

Public Key Infrastructure (PKI) that various EVSE-SPs use to communicate with EVs of various EV-SPs [193]. The cloud is an essential part of an effective EV-EVSE ecosystem. Additionally, EV-to-EVSE communication while charging requires secure and mutual authentications that can only be available through a trusted key infrastructure. All data flows with protocols and data types transferred are shown in Table 3.5.

3.2.6 Smart Grid Trusting Boundary

The power grid is responsible for providing sufficient power to EVSEs. Smart grids are complex networks of entities involved in generating, distributing power, and providing services to manufacturers, service providers, and customers. EVSEs and EVSE-SPs must measure their energy transfer and participate in DR to form a stable grid. Due to its complexity and as the smart grid is not the focus of this thesis, no table exists for its data flows. All components in the smart grid region shown in Figure 3.1 are explained in the NIST smart grid guideline [240].

Table 3.5: Components of Cloud or Untrusted Boundary

Section	Component	(Number) Data Flow	Data Type	Protocols
Cloud Networks	Cloud Services	(66) EVSE Web Interface	Send / Receive User Interface Data for EVSE	API, Cloud, Internet
		(67) 3rd Party Apps	Send / Receive Data for EVSEs and EVs (Monitoring)	API, Cloud, Internet
		(68) Other EVSEs	Send / Receive EVSEs Pricing, Request, Data	API, Cloud, Internet
		(69) Public-Key Infrastructure	Send / Receive Auth. Data and Security Keys	API, Cloud, Internet
		(70) EV Vendor Web Interface	Send / Receive User Interface Data for EV	API, Cloud, Internet
		(71) Database and Storage	Send / Receive Storage Data	API, Cloud, Internet
		(72) On-Road Devices	Send / Receive Data from Road Devices (EVs, Networks, ...)	API, Cloud, Internet

3.3 Concluding Remarks

In conclusion, the rapid growth of EVs introduces many challenges, notably those concerning security, technical and social. We have identified these challenges via an extensive literature review, highlighting issues such as EVSE security, data privacy concerns for both EVs and EVSE, software security, ICV security, and the security of autonomous vehicles. It has become evident that a comprehensive risk assessment framework is necessary for mitigating these issues. An in-depth understanding of all components of the EV-EVSE ecosystem, both internal and external, is crucial as adversaries can potentially exploit these components to launch attacks. By having a comprehensive understanding of this ecosystem, which includes elements like the EV owner, EVSE owner, cloud services, smart grids, and EV and EVSE components, we can facilitate the development of robust and efficient mitigation techniques. These techniques can be designed to address a wide range of possible attack points. In this chapter, we have endeavoured to dissect and understand these components; their data flows and protocols, power flows, and third parties involved in communication or data exchange with EVs or EVSEs. In the following chapter, we will propose a risk assessment framework based on the insights gained here, aiming to better identify

and address the vulnerabilities within the EV-EVSE ecosystem. Our ultimate goal is to enhance the security and reliability of EVs and their associated infrastructure, contributing to a safer, more sustainable future in transportation.

Chapter 4

Electric Vehicle and Charging Station Risk Assessment

4.1 Motivation

So far, we have discussed numerous challenges related to the adoption of EVs and EVSEs. Academia, governments, and industry are all striving to surmount these obstacles to pave the way for a more efficient and beneficial transportation system. We have identified cybersecurity as one of the critical issues facing EVs and EVSEs, necessitating detailed analysis. Consequently, we have conducted a thorough survey of previous literature regarding the security of EVs and EVSEs, aiming to identify all potential attacks and challenges.

To enhance our analysis, we have sketched a possible EV-EVSE ecosystem architecture encompassing all data flows, power flows, and protocols. This design has been instrumental in helping us understand the critical points within this ecosystem. However, to improve EV and EVSE security, it is imperative that we conduct a comprehensive risk assessment. Such an assessment can help us identify all possible vulnerabilities and attacks and their impacts, thus enabling organizations to rank

vulnerabilities and propose mitigation techniques for the ecosystem.

In this chapter, we divide EVs and EVSEs into five different aspects previously identified as potential challenges in our literature review: charging station security, information privacy, software security, connected vehicle security, and autonomous vehicle security. We then propose attack surfaces, abstract starting points to exploit an attack, sub-surfaces, sub-categories where attackers can compromise, and vulnerabilities for each category that could be compromised by adversaries. Using this categorization, we propose a set of criteria for the likelihood and impact of attacks. We then employ the STRIDE threat model, a mature threat model, to identify vulnerabilities and potential challenges in an EVs and EVSEs attack taxonomy.

Subsequently, using a risk matrix and applying the proposed criteria, we rank all the attacks and propose countermeasures for each attack after categorizing them using the five-aspect attack surfaces and sub-surfaces. At the end of this chapter, we apply our proposed risk assessment framework to eight real-world EV attack scenarios and rank these attacks. Our objective is to demonstrate how this framework can be practically adopted to enhance EV and EVSE security.

4.2 Risk Management and Risk Assessment

this thesis uses a risk assessment methodology to evaluate security risks associated with EVs. Following the guidelines proposed by NIST [35], the risk assessment consists of four stages: preparation, conducting the assessment, communication of results, and maintenance. The thesis primarily focuses on the second stage of conducting the assessment, which involves identifying risk factors such as threat, vulnerability, likelihood, impact, and risk, using a qualitative approach among the three assessment approaches: quantitative, qualitative, or semi-quantitative. The forth aspect of the risk assessment methodology is risk analysis, which can be threat-oriented, asset-oriented,

or vulnerability-oriented. For this thesis, we use STRIDE as a threat-oriented analysis. Figure 2.5 summarizes the risk assessment.

4.2.1 Prepare for Risk Assessment

The first step in the risk assessment process is identifying initial variables and establishing assumptions, including the purpose, scope, considerations, information sources, and risk model. The purpose of the risk assessment framework described in this thesis is to identify and prioritize risks associated with the five security aspects of EVs, identify the weakest point in EV systems, and guide organizations on where to look for cyber threats. The study's scope covers the entire EV lifecycle, including modern ones, and considers the five security aspects surrounding the EV ecosystem. The assessment assumes that general modern EV threats exist across the five aspects and that manufacturers are trustworthy. Previous cybersecurity studies serve as sources of threats and vulnerabilities, and the STRIDE threat model is used to identify threats. The risk model used in this thesis is qualitative and utilizes a threat-oriented analysis to determine the impact, likelihood, and risk of vulnerabilities. A risk matrix is created to illustrate the final results of the proposed framework.

4.2.2 Conduct the Risk Assessment

The second step of the risk assessment process involves five tasks: identifying threat sources and events, identifying vulnerabilities, determining the likelihood and impact of vulnerabilities, and calculating risk. The second image in Figure 2.5 provides a summary of conducting the assessment step.

Task 1. Identify Threat Sources and Events: Identifying threats involves identifying sources and events that can cause security issues. Attackers can use different methods to exploit vulnerabilities in EVs, and these attacks can vary in their goals, ranging

from personal gain to information theft or organizational damage. The threats can be categorized into security aspects, each with attack surfaces, subsurface, and potential threat events. Exploiting any of these threats can lead to a threat event, which can cause varying levels of impact.

Task 2. Identify Vulnerabilities and Predisposing Conditions: In each security aspect, there are several vulnerabilities that attackers can exploit to compromise an EV. These vulnerabilities have been identified from previous research and will be discussed in the following sections. By analyzing vulnerabilities, we can determine the source of the threat event and potentially propose mitigations to prevent future attacks.

Task 3. Determine Likelihood of Occurrence: We propose a set of criteria to assess the likelihood of vulnerabilities identified in the literature review, focusing on the EV ecosystem and its associated threats. Adopting a qualitative approach, we utilize orders of magnitude for likelihood instead of specific numeric values. We define three levels of likelihood: Rare (R) for infrequent events, Medium (M) for events that occur occasionally, and High (H) for events that are likely to happen. The criteria for determining likelihood levels can be found in Table 4.1.

Task 4. Determine Magnitude of Impact: Similar to the likelihood evaluation, we established criteria for assessing the impact of threat events. Our qualitative approach uses orders of magnitude for impacts instead of specific numeric values. The orders of magnitude for impacts are classified as Low (L) for benign attacks, Medium (M) for attacks with minor consequences, and High (H) for severe attacks. The criteria for determining impact levels are presented in Table 4.2.

Task 5. Determine Risk: Finally, we want to determine the risk of each threat. Risk is a function of likelihood and impact and often integrates with the risk matrix. In this thesis, we use three levels of risk: High (H), Medium (M), and Low (L). A high level of risk means a threat has multiple harms or catastrophic consequences for

Table 4.1: Established Criteria for Risk Likelihood Levels

Likelihood	High	• Adversary is highly likely to initiate the threat event, and in case of happening, mitigation techniques are not sufficient to prevent the adverse impact. Threat event is almost certain to have an adverse impact. • Known vulnerabilities exist and can be launched remotely from the Internet or untrusted parties. Highly exposed to the Internet or other open systems. • Highly exploitable if insider (driver or passengers) is exercising threat event. • Can easily be accessed remotely or physically by an adversary with limited resources and expertise.
	Medium	• Adversary is somewhat likely to initiate the threat event, and in case of happening, mitigations are placed to impede the successful exercise of the threat event. Threat event is somewhat likely to have an adverse impact. • Known vulnerabilities exist, but adversaries need high-privilege access to exercise the Moderate vulnerability. Mediumly exposed to the Internet or other open systems. • Mediumly explosible if insider (driver or passengers) is exercising threat event. • Adversary requires moderate resources, expertise, and opportunities to support multiple successful attacks.
	Low	• Adversary is unlikely to initiate the threat event, and in case of happening, mitigations are placed to prevent the threat event. Threat event is unlikely to have an adverse impact. • Vulnerabilities are mostly unknown or new. The adversary needs administrative access to exercise a vulnerability. Slightly exposed to the Internet or other open systems. • Not explosible if insider (driver or passengers) is exercising threat event. • Adversary needs sophisticated expertise and well-resourced to make successful and coordinated attacks.

Table 4.2: Established Criteria for Risk Impact Levels

Impact	High	• Threat event can cause the loss of human lives, • Threat event can cause widespread power outages, • Threat event can cause damage to infrastructure or smart grid, • Threat event can cause the loss of sensitive consumer data, • Threat event can cause significant financial damage to assets, • Threat event can cause the whole system to become unstable or result in dangerous functionality, • Adversary seeks to severely impede or destroy the core or critical function of the system and is highly concerned about minimizing attack detection.
	Medium	• Threat event can cause failure in the real-time operation of the vehicle, • Threat event can cause unwanted functionality, • Threat events can cause significant dissatisfaction among clients, • Threat event can cause a loss of events (logs) occurring within the system, • Threat event can cause a violation of integrity or availability of actions or information in the system, • Threat event can cause disclosure of network connectivity, power network information, or system network information, • Threat event can cause medium fines or penalties for consumers or organizations, • Adversary seeks to obtain or modify sensitive or critical functions or information and disrupt services and is concerned about minimizing attack detection.
	Low	• Threat event can cause delay or failure in vehicle noncritical systems or services, • Threat event can cause the disclosure of non-critical information, • Threat event can cause minor damage to vehicles and minor financial loss, • Threat event can cause minor harm to individuals, • Threat event can cause a negligible adverse effect, • Threat event can cause temporary instability in the system, • Adversary seeks to obtain or modify critical information and disrupt services while he/she is not concerned about attack detection.

assets or individuals, while medium risk means a threat has severe results with fewer effects. A low-level risk shows the threat has a limited or negligible adverse effect. This thesis's function to classify the risk score levels combines likelihood and impact levels according to Figure 4.1.

		Impact		
		Low	Medium	High
Likelihood	Rare	Low	Low	Medium
	Moderate	Low	Medium	High
	High	Medium	High	High

Figure 4.1: Risk Assessment: Evaluating Risk (R) from Likelihood (L) and Impact (I) Levels

4.2.3 Risk Analysis Based on STRIDE Threat Model

We prepared a risk assessment process and established criteria to evaluate the likelihood and impact of threat events. In this section, we demonstrate a well-known threat model called STRIDE. Researchers have developed frameworks called threat models to find and rank the most severe vulnerabilities [289]. While threat models identify threats and vulnerabilities, risk assessment techniques can rank risks related to those threat events. There are several available threat models on the Internet, including STRIDE, PASTA, and attack trees [286]. STRIDE is one of the most mature and used threats modelling system-centric frameworks that evaluates system design and is a software threat-oriented approach. In STRIDE, the system's entities, events, and boundaries are first designed in DFD [294]. Then, the second step is to identify the threats domain based on STRIDE, which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. STRIDE is adopted to model threats in a variety of domains such as energy systems [361], automotive systems [158], and industrial control systems [150]. this thesis uses the

STRIDE threat model to map vulnerabilities in the STRIDE domain for the EV-EVSE ecosystem, determine all possible attacks, and identify their countermeasures.

4.3 Taxonomy of Attacks and Challenges in Electric Vehicles

To better assess the risks in the EV system, we gathered all possible attacks and challenges by surveying previous studies. We used the architecture presented in the previous chapter of this thesis to gain insights into possible initial points and identified those attacks from the literature review. We then categorized each attack based on its security category in EVs and STRIDE threats. Using this taxonomy, our aim is to assess the risks of different security aspects of EVs by categorizing these attacks into the surface and subsurfaces of each category. This will help us determine the correct impact, likelihood, and risk, along with the set of criteria mentioned before. The taxonomy of attacks on each component of the EV ecosystem, along with their STRIDE security aspects, is presented in Figure 4.2.

4.4 Electric Vehicle Security Profiling and Taxonomy of Attacks and Challenges in Electric Vehicles

This thesis proposes a universal security profile for EVs to address the need for a more comprehensive security approach for this new technology. The proposed profile covers five major components of the EV ecosystem: charging station security, information privacy, software security, connected vehicle security, and autonomous driver security. Figure 4.3 visualizes the universal profiling for EVs, including their attack surfaces

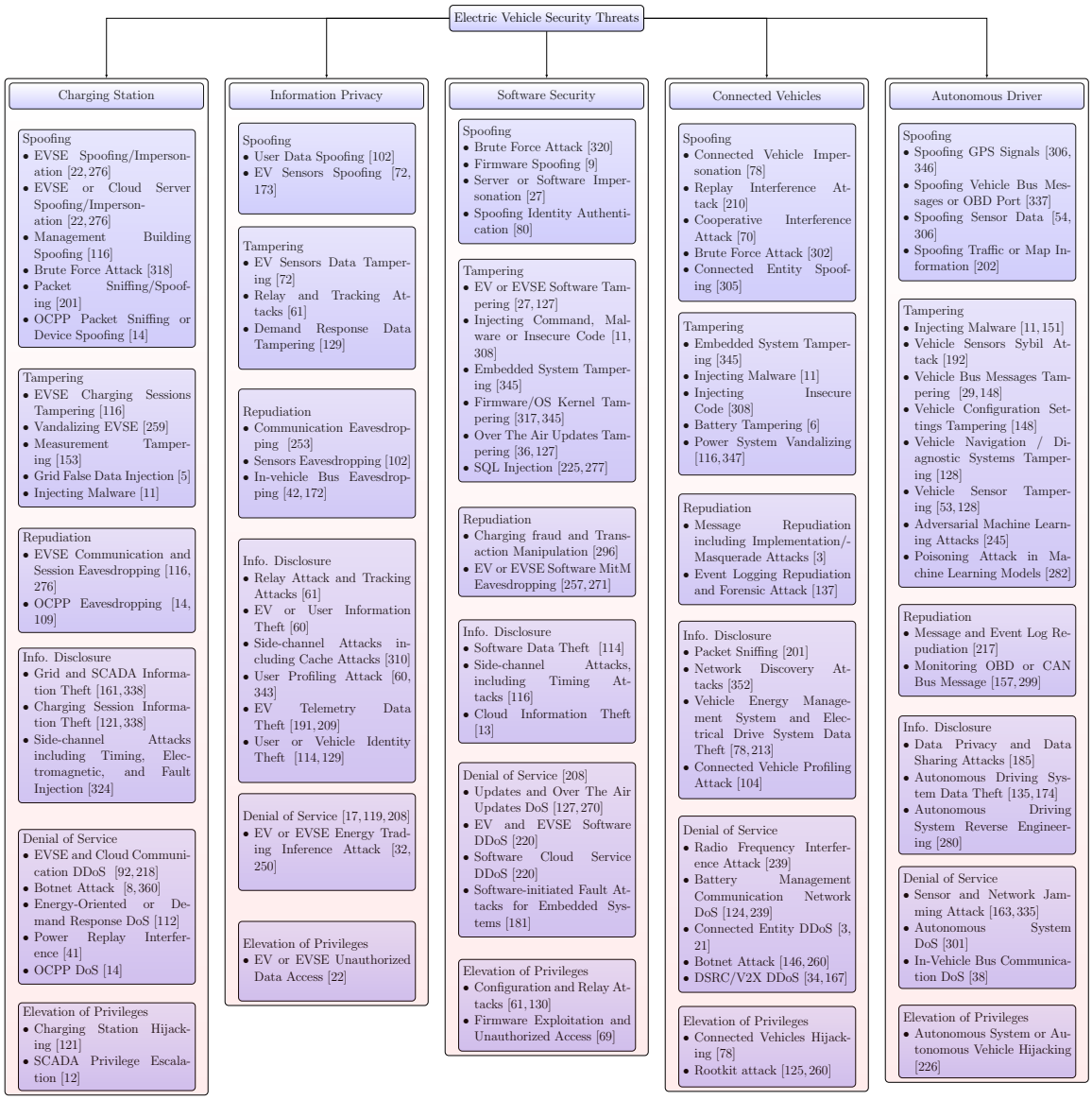

Figure 4.2: Taxonomy of Attacks Threaten Electric Vehicle Security

(green layer) and attack subsurfaces (blue layer). This thesis also describes each security aspect of EVs, maps them to STRIDE domains, identify possible attacks, applies a risk assessment framework to analyze their risk, and proposes countermeasures for attacks in the following sections.

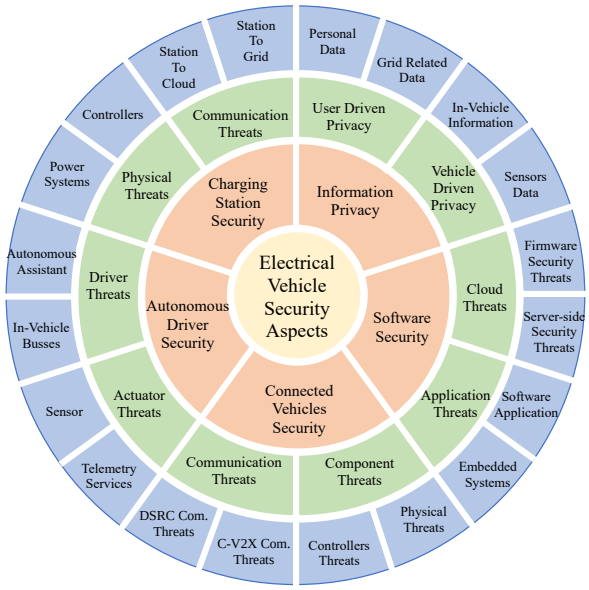

Figure 4.3: Electric Vehicle Security Profiling (A General Overview)

4.4.1 Electric Vehicle Charging Station Security Profiling

The security concerns surrounding the cyber-physical nature of EV charging stations are a top priority for the mass adoption of EVs, as charging stations connect the power grids to EVs [254]. Charging stations are vulnerable due to their public access and continuous communication with the grid, which can endanger the entire power grid [4, 22]. Two critical issues make charging stations vulnerable: communication security and physical security. Charging stations use ISO 15118 and Open Charge Point Protocol (OCPP) for communication [30, 278], which are vulnerable attack

surfaces for attackers. The vulnerabilities, challenges and attacks, STRIDE mapping, risk assessment, and possible countermeasures for electric vehicle charging stations security are summarized in Table 4.3.

A.1. Communication Threats

Two types of EVSE communication are communications to a power grid and communications to a cloud. In addition, EVSE vendors monitor their stations using SCADA. Each category creates attack surfaces that can compromise charging stations, making EVs or power grids vulnerable to further attacks. The vulnerabilities identified in these attack surfaces include the following.

A.1.1. Station-to-Grid Communication

Since charging stations are responsible for the maintenance and distribution of power to vehicles, it is in continuous communication with the grid. This communication can compromise the grid or the stations. First, we must understand the component's roles in grid communication to demonstrate and classify threats to this system. We divide this type of communication into station-to-grid communication and station-to-cloud communication.

A.1.1.1. Station-to-Vehicle Communication

PEVs constantly communicate with charging stations during the authentication and authorization process and throughout the charging session for handshake and heartbeat purposes [264]. Station-to-vehicle communication follows the security standard ISO 15118, but it is still vulnerable to attacks that can compromise the station or the vehicle. For example, Man-in-the-Middle (MitM) attacks, masquerade attacks, and repudiation attacks can be launched against this communication channel, potentially resulting in vehicle, information, or energy theft, as discussed in previous studies [30]. The likelihood, impact, and risk associated with these vulnerabilities are analyzed in the summary table.

A.1.1.2. Station-to-Grid Monitoring Communication

Another type of station-to-grid communication is grid monitoring. Supervisory Control and Data Acquisition (SCADA) is a system for supervisory control and surveillance of automation systems widely used in systems connected to smart grids [37]. It is necessary for charging stations to communicate to the SCADA system for every event within the station, such as connecting or disconnecting a vehicle, payments, and energy trades for security purposes. Even though SCADA is widely used, it creates security vulnerabilities [315]. Attacks on SCADA range from eavesdropping and sniffing of SCADA messages, data injection, jamming, and insider attacks [87, 122, 123]. For instance, injecting false data into the SCADA system can endanger the station, or jamming messages can cause security events. Because SCADA is accessible and the impact of a successful attack can cause devastating results, its risk is measured as high. The summary table shows more information about the risk assessment.

A.1.1.3. Station-to-Grid Power Communication

One more type of communication to the grid is for power demand and response. As a part of the smart grid, charging stations must participate in demand response. It means stations should demand energy from the grid in case of need, and the grid should respond to stations with power [126]. OpenADR [133] is the protocol most charging stations use for demand response communication to the grid. This unique communication type can be targeted by attackers, which can be a hazard for the grid [187]. An attack targeting demand response can have devastating consequences, such as disturbing the grid, information theft, or remote communication attacks [277]. For instance, by blocking messages to the grid in response, charging stations will demand more and more power from the grid, which causes the grid to enter an unstable phase. This case can have a low impact on a few charging stations but have a ruinous effect if more stations are compromised. Because compromising multiple stations requires skill and resources, its likelihood is medium instead of high. Thus,

medium impact and medium likelihood result in medium risk. The summary table shows more information about the risk analysis.

Table 4.3: Electric Vehicle Charging Stations Security Profiling and Risk Assessment

Aspect	Surface of Threat	Sub-Surface	Vulnerability	Challenges and Attacks	Threats	Criteria	Possible Countermeasures	L	I	R
Charging Station Security	Communication Threats	Station to Grid	Station to Vehicles, ISO 15118 [30, 96, 97]	• EVSE Charging Sessions Tampering, • EVSE Communication and Session Eavesdropping, • Charging Session Information Theft, • Side-channel Attacks.	• Tampering, • Repudiation, • Info. disclosure.	Charging stations communicate with vehicles after handshaking, according to ISO 15118. They exchange vital information, which may lead to information disclosure, and vehicles are subject to tampering while charging. Threat source is motivated, but adversaries require direct physical access while the vehicle charges. A successful attack can cause delay or failure in noncritical services or minor harm to individuals	• To detect and prevent EVSE charging sessions tampering: Session verification Anomaly detection, Encryption, Authentication [166], • To prevent EVSE communication and session eavesdropping: Identity verification and authentication (Encryption), Intrusion detection system, Physical layer security [116], • To avoid charging session information theft: Privacy policies, Differential privacy, Encryption, Intrusion detection system [68, 166], • To prevent side-channel attacks: Masking communication pattern, Randomized delay elements [108].	R	L	L
			Station to Grid, SCADA [87, 122, 123]	• SCADA Information Theft, • Grid False Data Injection, • SCADA Privilege Escalation.	• Tampering, • Info. disclosure, • Elevation of Privileges.	Stations are monitored in SCADA as part of the smart grid. SCADA contains sensitive information regarding users, payments, and station status, making it a good target for information disclosure. Also, attackers with high privileges can erase track of attacks in monitoring systems or impersonate valid assets to exercise further attacks. Threat source is highly motivated and requires a certain skill level to perform an attack. The adverse impact of a successful attack targeting SCADA can lead to catastrophic consequences causing damage to the smart grid, destroying critical information, or even causing a widespread power outage.	• To prevent SCADA information theft: Privacy Policies, Differential privacy, Intrusion detection system [161], • To detect grid false data injection: Authentication, Message integrity check, Intrusion detection system [23, 196], • To prevent SCADA privilege escalation: Identity verification and authentication (Encryption), Firewalls, Intrusion detection system [12, 171].	M	H	H
			Station to Grid, OpenADR [246, 354]	• Brute Force Attack, • Demand Response Information Theft, • Demand Response DoS.	• Spoofing, • Info. disclosure, • DoS.	Stations as part of the smart grid contribute to demand response. This participation makes them vulnerable to the disclosure of grid information and attackers who impersonate valid endpoints within the grid to attack stations. There are known vulnerabilities in OpenADR, but specific mitigations are placed to impede the attacks. Adverse effects of attacks targeting demand-response can cause failure in real-time operation or disclosure of network connectivity or power network information.	• To prevent brute force attack: Identity verification and authentication (Encryption), Rate limiting [318], • To detect and prevent demand response information theft: Authentication, Encryption, Digital signature [19, 338], • To prevent Demand Response DoS: Intrusion detection system, Load balancing, Blockchain, Software-defined networking [311].	M	M	M
		Station to Cloud	Station to Station, Scheduling [81, 116, 219]	• EVSE or Cloud Server Spoofing or Impersonation, • EVSE and Cloud Communication DDoS, • Botnet Attack.	• Spoofing, • DoS.	Stations communicate with other stations for price and status exchange. Spoofing as a valid station or denying communication of a station are common attacks. This communication can be remotely accessed and is highly exposed to the Internet. Mitigation techniques are usually not in place to impede such attacks. Adverse effects of a successful attack can cause delay or failure in station services, and while adversaries seek to disturb station services, they are not concerned with being detected.	• To prevent EVSE or cloud server spoofing or impersonation: Authentication, Secure connection (TLS), Intrusion detection system, Redundant verification [22], • To prevent EVSE and cloud communication DDoS: Rate limiting, Intrusion detection system, Firewalls, Traffic scrubbing and DDoS prevention services [92, 116], • To prevent Botnet Attack: Network segmentation, Intrusion detection system, Antivirus and anti-malware software, Behavioral analysis and anomaly detection [8].	H	L	M
			Station to Server, OCPP [14, 22]	• OCPP Packet Sniffing or Device Spoofing, • Management Building Spoofing, • OCPP Eavesdropping, • OCPP DoS.	• Spoofing, • Repudiation, • DoS.	Similar to scheduling, stations constantly exchange information with manufacturers' servers using the OCPP protocol. Common attacks are impersonating a valid station to obtain information from a server or denying one station's connection to the server. This communication is highly exposed to the Internet and external systems, and also limited mitigations are in place to impede the attack. The adverse impact of exercising attacks toward OCPP can cause station availability violations, network connectivity disclosure, or medium fines for stations.	• To prevent OCPP Packet Sniffing or Device Spoofing: Authentication, Physical layer security, Intrusion detection system, Redundant verification [109], • To avoid management building spoofing: Identity verification and authentication (Encryption), Digital Signatures [116], • To prevent OCPP Eavesdropping: Authentication, Intrusion detection system, Redundant verification, Encryption [109, 218], • To evade OCPP DoS: Secure connections (TLS), Network segmentation, Intrusion detection system, DoS prevention systems [218].	H	M	H
	Physical Threats	Power Systems	Power, Transformers, Power Cable, etc.	• Vandalizing, • Power Replay Interference.	• Tampering, • DoS.	Tampering with the power system of stations is a common attack and requires skill and resources to access the components physically. Adversaries are unlikely to initiate the threat event, and in case of a successful attack, impacts can have medium fines for the station or failure in real-time operation of the system	• To prevent vandalizing: Tamper-proof hardware, Physical layer authentication [259], • To avoid power replay interference: Hardware-based Security including Geo-Fencing and Distance bounding, Redundancy and Fingerprinting [41].	R	M	L
		Controllers	ECUs, TCUs, Embedded Systems, Measurements, etc	• Measurement Tampering, • Injecting Malware, • Charging Station Hijacking.	• Tampering, • Elevation of Privileges.	Tampering with controllers in stations using malware or code injection, which later can erase the tracks of the attacks, is a common attack. Like power systems, controllers need physical access, and adversaries require resources to exercise attacks. The adverse impact of the attacks can cause a loss of events occurring within the system. Adversaries seek to disturb the normal operation of the stations.	• To block measurement tampering: Tamper-proof hardware, Data verification, Intrusion detection system, physical layer security [153], • To avoid and detect Injecting Malware: Malware detection, Firmware updates, Physical layer security [243], • To prevent charging station hijacking: Identity verification and authentication (Encryption), Intrusion detection system [121].	R	M	L

A.1.2. Station-to-Cloud Communication

Charging stations communicate with cloud servers and other stations for scheduling, authentication, payment, and user interactions. Both types of communication need extra attention as known vulnerabilities exist and are exposed to third-party appli-

cations. Here, we will demonstrate them along with their potential vulnerabilities.

A.1.2.1. Station-to-Station Communication

Charging stations communicate with other stations via a cloud server mainly for scheduling and pricing [355]. Charging stations can implement pricing strategies with other stations to maximize their profit [355]. Charging stations also communicate with each other to establish ground rules or dynamic pricing regarding the cost of electricity [323]. This pricing communication type is also necessary for demand response. Attackers can compromise charging stations by communicating with other charging stations to gain advantages for pricing information or even compromise the grid, forcing it to enter an unstable status. Studies such as [81, 116, 219] provide further details of various attacks towards charging station communication. Compromising charging station scheduling can damage the system or cause fraud and client dissatisfaction for companies. The risk associated with this vulnerability in our framework is low as the impact of the damage is mostly limited and predictable, and many mitigation techniques exist to impede these attacks. The summary table shows more information about the risk assessment.

A.1.2.2. Station-to-Server Communication

Another type of communication with the cloud in charging stations is between a station and a cloud server. Stations need to stay in discussion with servers for security and updates, such as authentication of the user, user payments, and other user activities, such as a user asking for vehicle information [155]. Cloud communication security has always been a hot topic among researchers because of its known vulnerabilities [16]. Studies inform these vulnerabilities such as [275, 356]. OCPP is the protocol that works as a standard for charging stations to communicate to any cloud server or manufacturer [278]. OCPP and any cloud communication are targets for attackers to compromise a charging station. Examples of attacks targeting such communications include DoS attacks, Data disruption, information blocking,

and modifications. More information regarding such attacks is presented in [14, 22]. Affecting cloud communication can result in fraudulent payments or vehicle theft, which causes severe damage to users. Because of known vulnerabilities, researchers proposed many mitigations to limit the attacks to cloud servers, but a successful attack can cause severe results. Thus, the risk associated with cloud communication vulnerability is medium. The summary table shows more information about the risk analysis.

A.2. Physical Threats

One major challenge differentiating charging stations from most IoT devices is the physical accessibility [15]. Public physical access to stations for interface and billing purposes increases vulnerabilities [116]. In this thesis, we divide the physical access attack surface into two types: vulnerabilities that threaten the power system of a station and the controller part.

A.2.1. Power Systems

All charging stations have power systems to demand power from the grid and generate or transfer it to the vehicle [75]. Reviewing the load demand of charging stations is a must for countries before placing them in local areas since it may cause load errors for the grid. Authors in [76] review strategies for placement of the stations. Because charging stations are physically accessible, vandalizing and damaging the power system are critical issues. An example of an important physical attack is physical side-channel attacks in charging stations [22, 116] that may result in information disclosure or fraud. Although the probability of physical vandalism or connecting a USB to the stations for side-channel attacks is low, the impact of successful physical attacks can be severe, leading to fire hazards or station malfunctioning. Thus, the risk associated is low. The summary table shows more information about the risk analysis.

A.2.2. Controllers

Charging stations are controlled by embedded controllers, ranging from a single board controller to more advanced PLC controllers like those in Siemens' stations [291]. These controllers need to be physically accessible for technicians to address any issues, which creates a physical attack surface for attackers to inject malicious code, malware, or vandalize the ECU [91]. Similar to the power system part, although the probability of physical tampering is low, the impacts can be severe as they can destroy a whole charging station. Therefore, the risk associated with physical access to controllers is medium. The summary table provides more information about the risk analysis.

4.4.2 Electric Vehicle Information Privacy Profiling

Table 4.4: Electric Vehicle Information Privacy Profiling and Risk Assessment

Aspect	Surface of Threat	Sub-Surface	Vulnerability	Challenges and Attacks	Threats	Criteria	Possible Countermeasures	L	I	R
Information Privacy	Vehicle Driven Privacy	Vehicles Data	Sensors Data [141, 272]	• EV Sensors Spoofing, • EV Sensors Data Tampering, • Relay and Tracking Attacks, • Sensors Eavesdropping, • EV Telemetry Data Theft.	• Spoofing, • Tampering, • Repudiation, • Info. disclosure.	Sensors and actuators in EV systems contain sensitive information, that disclosure of those data can cause disastrous consequences. Threat source is highly motivated, but accessing these data requires specific skills. Data threats can cause the loss of sensitive consumer data, resulting in vehicle theft or significant financial damage to the asset.	• To avoid EV Sensors Spoofing: Data correlation and validation, Encryption, Anomaly Detection [72], • To prevent EV Sensors Data Tampering: Data validation checks, Secure communication, Anomaly detection, Blockchains [194], • To block Relay and Tracking Attacks: Fingerprinting, Distance bounding, Frequency hopping, Blockchain [61, 258], • To avoid sensors eavesdropping: Access controls, Physical layer security, Encryption [102], • To stop EV Telemetry Data Theft: Privacy policies, Encryption, Authentication, Differential privacy [191, 209].	M	H	H
			In-Vehicle Information [107, 141, 319]	• In-vehicle Bus Eavesdropping • Vehicle Identity Theft, • Side-channel Attacks including Cache Attacks, • Vehicle Communication DoS.	• Repudiation, • Info. disclosure, • DoS.	Each vehicle stores sensitive data that are derived from vehicle events. Adversaries with high privilege can access information, erase vehicle security events, or steal vehicle information for further attacks. The threat source is motivated, and the adversary requires a certain skill level. Performing such an attack often requires adversaries to have physical access with high privileges. The adverse impact of exercising the attack is loss of events or logs and loss of information.	• To avoid in-vehicle bus eavesdropping: Access controls, Physical layer security, Encryption, Authentication, Moving target defense [42, 172], • To prevent vehicle identity theft: Privacy policies, Access controls and Physical layer security [114], • To block side-channel attacks, including cache attacks: Masking, Redundant execution, Machine learning [310, 324], • To prevent vehicle communication DoS: Rate limiting, Flow control, DoS prevention services [88, 120].	R	M	L
	User Driven Privacy	Users Data	Personal Data [228, 319]	• User Data Spoofing, • User Identity Theft, • Communication Eavesdropping, • EV or User Information Theft, • User Profiling Attack, • EV or EVSE Unauthorized Data Access.	• Spoofing, • Info. disclosure, • Repudiation, • Elevation of Privileges.	Personal data stored within clouds, software, or vehicles are considered sensitive to users. Information such as payments and addresses can cause dangerous outcomes. Threat source is motivated to exercise attack. Adversaries require skills, and known vulnerabilities exist within the software, but mitigation techniques are placed to limit the attacks. The adverse impact of successful information loss can cause slight dissatisfaction among users.	• To prevent user data spoofing: Data validation checks, Anomaly and fraud detection [102], • To avoid user identity theft: Privacy policies, Differential privacy, Access control [114, 129], • To prevent communication eavesdropping: Secure connections (TLS), Intrusion detection system, Channel hopping [102, 253], • To block EV or user information theft: Privacy policies, Encryption, • To avoid user profiling attacks: Privacy policies, Encryption, Data minimization and privacy by design [60, 343], • To prevent EV or EVSE unauthorized data access: Access controls and physical layer security, Intrusion detection system [22].	M	L	M
			Grid Related Data [290]	• Demand Response Data Tampering, • EV or EVSE Energy Trading Inference Attack, • EVSE Unauthorized Data Access.	• Tampering, • Info. disclosure, • Elevation of Privileges.	Vehicles constantly communicate with smart grids, especially during charging, and often exchange energy-related information. Drivers should be aware of devices connected to the vehicle and their information exchange. This information is subject to adversaries' attacks to compromise users' privacy. Adversaries often require physical access, and successful attacks can result in the loss of non-critical information. Threat source is slightly motivated and is often in pursuit of personal gains, but mitigations are in place to control the attacks.	• To prevent demand response data tampering: Encryption, Intrusion detection system, Blockchain [65, 129], • EV or EVSE Energy Trading Inference Attack: Differential privacy, Encryption, Intrusion detection system [32, 285], • EV or EVSE Unauthorized Data Access: Access controls and physical layer security, Intrusion detection system [22].	R	L	L

Different types of information must be kept private to ensure privacy in EVs. The first

type is driver information stored in the vehicle's internal memory. This information includes personal details such as the driver's name, addresses, phone numbers, and preferences such as driving habits and routes. The second type of information is sensor data that can potentially reveal users' locations or other sensitive details, such as a camera. Third parties can use this data to track users' movements and habits, which can severely breach privacy. To mitigate these risks, manufacturers must implement measures to protect user data and establish data handling and storage regulations. Studies such as [141, 272] provide additional details. The likelihood of an attack on information privacy is considered high, and its impact can also be severe. Therefore, its risk is evaluated to be high. The summary table provides more information on the risk analysis.

The data within communication with the cloud server, other vehicles, or charging stations are also vital. This information varies from sensitive information for users, such as passwords and payments, to information usually used in software, such as authentication tokens and vehicle status [25]. Another type of private information that needs protecting is the information that users are unaware of, but vehicle uses. One example of this type is vehicle grid communication when the vehicle is charging. Information such as connected devices and visited charging stations are transmitted to the grid for authentication and power demand. Other confidential information is information related to the vehicle, for example, Vehicle Identification Number (VIN) can be used for transmision [290, 319]. This information is vital to users, and companies must ensure their privacy. A summary of this information, its related vulnerabilities, challenges and attacks, STRIDE mapping, possible countermeasures, and the associated risk can be found in Table 4.4.

4.4.3 Electric Vehicle Software Security Profiling

This section of the thesis discusses the importance of software security in EVs. There are two types of software systems in the EV ecosystem: software that connects to the EV (manufactured by EV manufacturers or third-party software providers) and software or firmware of embedded systems that make the EV functional [85,284]. Software vulnerabilities can cause EV failures, which can propagate a malicious event to the grid or users. Software vulnerabilities are divided into two categories: application-level security and cloud-level security. Failure of security countermeasures in each category can impact the entire EV system. This section provides a detailed discussion of software security categories, their risks, vulnerabilities, challenges and attacks, STRIDE mapping, and possible countermeasures, which can be found in Table 4.5.

C.1. Application Threats

Almost every modern product comes with a software application that interacts with users, monitors a device, or is part of the product's functionality. EVs often come with software for various purposes, such as monitoring the vehicle's status and history of travel routes or providing access to autonomous driving, as seen in Tesla [93]. Moreover, embedded systems code is vulnerable, and attackers can inject malicious malware if physically accessed. In this section, we define each application's vulnerabilities and associated risks.

C.1.1. Software Applications

Vehicles have mobile and desktop applications that allow users to interact with them. These applications vary from iOS, Android, and desktop applications to other third-party monitoring applications such as [85, 284]. If an attacker compromises such applications, users can be affected. For instance, an attacker can show false data about the status of the battery and make the user believe the vehicle is in good condition, causing future failures. An example of a software attack that can have severe

outcomes is directed against an autonomous driver application. AV software usually waits for commands, and if an attacker injects a malicious command, it can cause devastating consequences such as vehicle theft or brake failure [268]. Because known vulnerabilities exist and can sometimes be compromised by limited resources, the likelihood of such attacks is high, but their associated risk is medium. Vulnerabilities and their associated risks can be found in the summary table.

C.1.2. Embedded Systems

Each EV has embedded systems that perform various functions to enable the vehicle to operate. These embedded systems include controller ECUs, infotainment systems, telemetry services, and management systems such as battery management systems. While most embedded systems are only accessible to manufacturers, some are vulnerable due to their physical accessibility. Anyone capable of opening the car's front hood can introduce vulnerabilities such as malware injection or physical tampering [165]. Additionally, EVs have an interface that allows users to access critical in-vehicle information and diagnostics called OBD, which is vulnerable to unauthorized access and needs to be secured [333]. Compromising a vehicle's embedded systems requires skill and resources, so the probability of such an attack is medium. Also, attacking these components may cause failure in certain vehicle parts, and manufacturers often design backup systems for their ECUs to reduce the impact of an attack. Therefore, the impact of compromising embedded systems is classified as medium, and the associated risk is medium. Please refer to the table for more information about vulnerabilities and their associated risks.

C.2. Cloud Threats

EVs require continuous communication with backend servers to exchange information regarding the vehicle's status, obtain user information and queries from the server, and perform firmware updates or patches. Cloud threats can be categorized into

Table 4.5: Electric Vehicle Software Security Profiling and Risk Assessment

Aspect	Surface of Threat	Sub-Surface	Vulnerability	Challenges and Attacks	Threats	Criteria	Possible Countermeasures	L	I	R
Vehicles Software Security	Application Threats	Software Application	Mobile and Desktop Application [47, 165]	• Brute Force Attack, • Spoofing Identity Authentication, • EV or EVSE Software Tampering, • EV or EVSE Software MitM Eavesdropping, • EV and EVSE Software DDoS, • Software Data Theft, • Side-channel Attacks, including Timing Attacks.	• Spoofing, • Tampering, • Reputation, • Info. disclosure, • DoS,	Information theft from applications and bypassing authentication to log in as valid users are common attacks. Such systems are highly exposed to the Internet, and often vulnerabilities exist. Attackers may obtain information about clients or attempt to modify them later.	• To prevent brute force attack: Identity verification and authentication (Encryption), Rate limiting [223], • To avoid spoofing identity authentication: Authentication, Captcha or similar mechanisms, Anomaly detection [80], • To block EV or EVSE software tampering: Code signing, Regular software updates, Two-factor authentication [27, 127], • To evade EV or EVSE software MitM eavesdropping: Secure connections (TLS), Intrusion detection system, Channel hopping [257, 271], • To prevent EV and EVSE software DDoS: Intrusion detection system, Behavioral analysis and anomaly detection, DoS-prevention services [220], • To avoid software data theft: Privacy policies, Regular security testing, Encryption [114], • To evade side-channel attacks, including timing attacks: Delay execution, Redundant execution [116, 162].	H	M	H
		Embedded Systems	Hardware Vulnerabilities [165, 295]	• Injecting Command, Malware or Insecure Code, • Embedded System Tampering • Firmware/OS Kernel Tampering. • Over The Air Updates Tampering, • Side-channel Attacks, • Configuration and Relay Attack,	• Tampering, • Info. disclosure, • Elevation of Privilege	Onboard diagnostic issued for troubleshooting and tampering with it can cause erasing tracks of an attack. This vulnerability exists, and some mitigations are placed to limit the damage. The system is exposed only to adversaries with a particular skill level. The impact of a successful attack can vary from malfunctioning of the vehicle in real-time or loss of events and security logs.	• To prevent injecting commands, malware, or insecure code: Malware detection, Firmware updates, Access control and physical layer authentication [11, 308], • To avoid embedded system tampering: Tamper-proof hardware, Hardware-based Security including Geo-Fencing and Distance bounding [345], • To evade firmware/OS kernel tampering: Tamper-proof hardware, Intrusion detection system, Secure boot [317, 345], • To block over-the-air updates tampering: Code signing and secure boot, Intrusion detection system, Redundant verification [127], • To detect and prevent side-channel attacks: Redundant Execution, Masking, Randomized delay elements [116, 310], • To block configuration and relay Attack: Intrusion detection system, Encryption, Tamper-proof hardware [61, 130].	M	M	M
	Cloud Threats	Firmware Security Threats	Firmware Vulnerabilities [231, 341]	• Firmware Spoofing, • Updates and Over The Air Updates DoS, • Software-initiated Fault Attacks for Embedded Systems, • Firmware/OS Kernel Exploitation.	• Spoofing, • DoS, • Elevation of Privilege	Tampering and injecting codes or malware into firmware while updating is a typical attack, as the firmware is core to the system. Threat sources are highly motivated, and OTA updates are often exposed to the Internet. Attacks can cause a violation of the availability of the system and medium fines to the asset. The dissatisfaction of the client is also another possible impact.	• To prevent firmware spoofing: Code signing, Firmware encryption, Physical security [134], • To evade updates and over-the-air updates DoS: Intrusion detection system, Behavioral analysis and anomaly detection, Software-defined networking [127, 270], • To avoid software-initiated fault attacks for embedded systems: Code and data integrity checks, Intrusion detection system, Tamper-proof software [181], • To block firmware/OS kernel exploitation: Runtime verification and memory protection, Firmware signing and Encryption [50, 345].	H	M	H
		Server-Side Security Threats	Server Vulnerabilities [138]	• Server or Software Impersonation, • SQL Injection, • Injecting Command, Malware or Insecure Code, • Charging fraud and Transaction Manipulation, • Cloud Information Theft, • Software Cloud Service DDoS, • Firmware Exploitation and Unauthorized Access.	• Spoofing, • Tampering, • Info. disclosure, • DoS • Elevation of Privilege	Cloud security and attacks against it are in Denial of service and elevation of privileged areas of focus in STRIDE. Clouds are highly exposed to the Internet and external systems. Threat sources are highly motivated. Known vulnerabilities exist within the cloud, but mitigations are placed to impede the attacks. There is a possibility of information disclosure, and if adversaries manage to get high-privilege access to the server, loss of critical information is possible	• To prevent server or software impersonation: Authentication, Secure connection (TLS), Intrusion detection system, Redundant verification, Blockchain [27, 140], • To avoid SQL injection: Access control, Parameterized queries, Encryption, Authentication [225, 277], • To evade injecting commands, malware, or insecure code: Malware detection, Firmware updates, Intrusion detection system [11, 308], • To block charging fraud and transaction manipulation: Authentication, Encryption, Payment gateways, Blockchain [164, 303], • To prevent cloud information theft: Differential privacy, Privacy policies, Encryption [13], • To resist software cloud service DDoS: Intrusion detection system, Behavioral analysis and anomaly detection, Content delivery networks [220]. • to prevent firmware exploitation and unauthorized access: Secure boot, Firmware signing, Encryption, Access control [69, 317].	H	L	M

two main security concerns: vehicle firmware and server-side security. Firmware provides low-level control for specific hardware, such as ECUs and management systems. However, the firmware is a vulnerable point for attackers to exploit as it may contain bugs or vulnerabilities [64]. On the other hand, server-side or backend codes are also vulnerable to attacks due to the millions of lines of code included in their application. Securing servers is a crucial topic among researchers, and several mitigation and defense strategies have been proposed [156]. In an EV ecosystem, compromised servers can send malicious information to vehicles, making them susceptible to further attacks.

C.2.1. Firmware Security Threats

The firmware on ECUs and embedded systems enable various functionalities in EVs. As attackers continuously use new tools and software to compromise systems, it is necessary to provide new patches and updates to ensure the complete security of systems. Vehicle manufacturers need to send updates, but it is not feasible to access vehicles physically one by one, so updates are done Over The Air (OTA). OTA updates open new doors for adversaries to compromise EVs [64]. ECUs firmware and direct updates are also susceptible to attacks, but a successful attack against them is much less likely. Another type of vulnerability that needs attention is EVSEs firmware as they are more likely to be targeted as they are physically available compared to built-in vehicle ECUs [231, 341]. The impact of compromising an EV firmware can be severe because if a malicious code injects into the EV's firmware, it can go undetected for weeks or months. The risk associated with firmware security is medium. Vulnerabilities and their associated risks can be found in the table.

C.2.2. Server-side Security Threats

Much information is exchanged during server communication, making it easier for attackers to eavesdrop on or modify messages. EVs are also constantly exchanging

information with backend servers, vulnerable to threats such as database attacks, cloud services attacks, and REST-API vulnerabilities [138]. Energy management microservices are a component of the EV ecosystem vulnerable to server-side attacks. Manufacturers have various APIs for vehicles to communicate and set management policies. If an attacker compromises the energy management system and sends modified messages, it can cause an unstable phase resulting in dangerous consequences such as a battery explosion. Attacking servers and clouds requires high skill and can happen remotely, so the likelihood of such an attack is high. However, developers continuously develop backend codes with security in mind and try to design resilient, resistant, and tolerant servers, minimizing the threats and results caused by vulnerabilities. Thus, the impact of these kinds of attacks is low. The risk associated with server-side security is medium.

4.4.4 Connected Electric Vehicles Security Profiling

As IoT emerged, ICVs became a growing area of study. Studies examined the impact of ICVs on routine tasks, such as [234]. While this new type of transportation can make road travel safer and more comfortable, it also opens doors for attackers, making them vulnerable and extremely dangerous if security fails [199]. ICV security is vital because the whole platoon becomes insecure if an attacker manages to compromise one. A major issue that makes such a system vulnerable is the cyber-physical nature of ICVs [236]. Thus, security requirements in ICVs include communication and component threats security. This section categorizes attack surfaces, subsurfaces, vulnerabilities, challenges and attacks, STRIDE mapping, risk assessment, and possible countermeasures in ICVs. Table 4.6 summarizes this information.

D.1. Component Threats

Component-level security or physical security of ICVs includes physical and controller parts security. According to a newly published book on ICVs [103], an EV has fifteen

Table 4.6: Connected Electric Vehicle Security Profiling and Risk Assessment

Aspect	Surface of Threat	Sub-Surface	Vulnerability	Challenges and Attacks	Threats	Criteria	Possible Countermeasures	L	I	R
Connected Vehicles Security	Component Threats	Physical Threats	Vehicle Power System [300, 341]	• Embedded System Tampering, • Power System Vandalizing, • Battery Tampering, • Vehicle Energy Management System and Electrical Drive System Data Theft. • Battery Management Communication Network DoS	• Tampering, • Info. disclosure, • DoS.	Physical tampering with the power system and information theft of the energy management system (often physical connection) are common STRIDE attacks. Because the physical body of the vehicle and power system are safeguarded, it is not exposed to external systems. The impact of such attacks can cause failure in the real-time functionality of the vehicle and slight financial damage to the asset.	• To prevent embedded system tampering: Tamper-proof hardware, Tamper-proof firmware, Physical security [345], • To avoid power system vandalizing: Tamper-proof hardware, Tamper-proof firmware, Redundant transformers, Physical security [116, 347], • To evade battery tampering: Secondary battery, Tamper-proof hardware, Physical security, Blockchain [6, 139], • To resist vehicle energy management and electrical drive system data theft: Encryption, Code obfuscation, Intrusion detection system [78, 213], • To prevent battery management communication network DoS: Network segmentation, Access control, Encryption, Secondary Battery, Blockchain [124].	R	M	L
		Controllers Threats	Main Controller [101, 261]	• Connected Vehicle Impersonation, • Brute Force Attack, • Connected Entity Spoofing, • Connected Vehicle Profiling Attack, • Message Repudiation including Implementation/Masquerade Attack, • Connected Vehicles Hijacking.	• Spoofing, • Tampering, • Info. disclosure, • Repudiation, • Elevation of Privileges.	Physical tampering with control systems and ECUs are common STRIDE attacks. Because the physical body of the vehicle and power system are safeguarded, it is not exposed to external systems. The impact of such attacks can cause failure in real-time functionality of the vehicle, or in case of malware injection, it can slightly damage vehicles ECUs.	• To prevent connected vehicle impersonation : Redundant authentication, Secure communication (TLS), Intrusion detection system, Physical layer security, Blockchain [78], • To avoid brute force attack: Identity verification and authentication (Encryption), Rate limiting [302], • To evade connected entity spoofing: Encryption and digital certificates, Redundancy, Intrusion detection system, Blockchain [305], • To resist connected vehicle profiling attack: Encryption and anonymization, Privacy policies, Authentication [104], • to prevent message repudiation, including implementation/masquerade attack: Timestamps, Digital signatures and message authentication, Intrusion detection system, Forensic detection system [3, 137], • to block connected vehicles hijacking: Intrusion detection and prevention system, Physical layer security, Redundant authentication and identity verification, machine learning [78, 226].	M	M	M
			Embedded Systems [59, 89]	• Brute Force Attack, • Injecting Malware, • Injecting Insecure Code, • Event Logging Repudiation and Forensic Attack, • Botnet Attack, • Rootkit attack,	• Tampering, • Repudiation, • DoS, • Elevation of Privileges.	Tampering with embedded systems and electric boards in the vehicle is another type of STRIDE area focus. Electric parts of the vehicle are safeguarded within the body and are not exposed to external systems. The threat source is not motivated, and such attacks can cause a delay in functionality or minor adverse effects.	• To avoid brute force attack: Identity verification and authentication (Encryption), Rate limiting [302], • To prevent injecting malware: Malware detection, Firmware updates, Physical layer security [11], • To evade injecting insecure code: Code obfuscation, Firmware updates, Intrusion detection system [83, 308], • To resist event logging repudiation and forensic attack: Tamper-evident logging, Secure time synchronization, Encryption [137], • to prevent botnet attack: Network segmentation, Intrusion detection system, Antivirus and anti-malware, Machine learning [146, 260], • to block rootkit attack: Intrusion and malware detection system (rootkit detection software), Network segmentation, Machine learning [125, 260].	R	L	L
	Communication Threats	DSRC Communication Threats	DSRC Com. and Network Vulnerabilities [18, 21, 111, 149, 160, 357]	• Packet Sniffing, • Network Discovery Attacks, • Radio Frequency Interference Attack, • DSRC DDoS.	• Info. disclosure, • DoS.	DSRC is mainly used for V2V and V2I communications. Spoofing and impersonating a valid vehicle in the platoon or road infrastructure can cause dangerous effects for an EV. Another attack is denying safety-critical messages from valid vehicles, causing malfunctioning in the compromised EV. Known vulnerabilities exist for this technology. However, DSRC was designed with security in mind to impede many of these attacks. DSRC communication is exposed to anyone within its range of communication, and threat sources are motivated. Attackers can cause loss of events and dissatisfaction among clients.	• To avoid packet sniffing: Secure connections (TLS), Network segmentation, Intrusion detection system [201], • To prevent network discovery attacks: Intrusion detection and prevention system, Network Segmentation [352], • To evade radio frequency interference attack: RF shielding, Frequency hopping, Signal filtering [239, 302], • To resist DSRC DDoS: Intrusion detection system, Anomaly detection, Traffic scrubbing and DDoS prevention services [34, 167].	H	M	H
		C-V2X Communication Threats	C-V2X Com. and Network Vulnerabilities [21, 131], [18, 111, 149, 357]	• Replay Interference Attack, • Cooperative Interference Attack, • V2X DDoS, • Connected Entity DDoS.	• Spoofing, • DoS.	Impersonating as other valid entities to compromise C-V2X enabled vehicles or denying communication services of those vehicles are common attacks. Various known attacks are identified. Hacking through V2X can result in total vehicle failure, but carmakers often provide methods to limit the attack and turn the vehicle into manual mode in case of danger. C-V2X communication is highly exposed to external systems, and threat sources are motivated. Attackers can cause loss of events and dissatisfaction among clients.	• To avoid replay interference attack: Flow control, Timestamp, Intrusion detection system [210], • To prevent cooperative interference attack: Channel hopping, Cooperative intrusion detection system [70], • To resist V2X DDoS: Intrusion detection system, Anomaly detection, Traffic scrubbing, and DDoS prevention services [34, 167]., • To block connected entity DDoS: Rate limiting, Flow control [3, 21].	H	M	H

hackable parts. In [203], the authors demonstrate how different physical layer security measures can address these issues. Controllers and embedded systems within an EV are also prone to malware and physical side-channel attacks. Failure to meet security requirements can have dangerous consequences, as discussed in this subsection.

D.1.1. Physical Threats

The physical components of EVs vary from the body to replaceable parts. Here, we categorize the physical component as the power system because almost every attack targets the power system, which can have a severe impact, as opposed to any other physical component with almost no impact.

D.1.1.1. Vehicle Power System

Examples of power systems in EVs include the vehicle body, Energy Management System (EMS), and Electrical Drive System (EDS) [300, 341]. Attacks on these systems can severely impact the power grid or the vehicle. For instance, compromising the EMS and forcing it to demand more power from the grid than it should cause an energy outbreak. Physical attacks can also cause accidents if undetected, but they typically require significant resources and physical access. Therefore, the likelihood of such attacks is rare. However, the risk associated with power system security is medium because of the impacts.

D.1.2. Controllers Threats

EV controllers include main controllers and several embedded systems. Manufacturers try to physically protect controllers by hiding most embedded systems from being visible [261]. However, these hardware devices are accessible and can be points of interest for attackers looking to inject malware or tamper. This section discusses which parts of the vehicle controller systems are vulnerable to compromise.

D.1.2.1. Main Controller

One vital part of an EV is the main controller. Some examples of controllers are TCU, ECU, and the computation units that work with different ECUs and TPUs using trusted computations [101, 261]. Another type of controller is the battery controller [314]. Unlike other physical parts in EVSEs and EV power systems, the probability of someone getting physical access to controllers is medium as it requires almost no resources. Also, if an attacker successfully tampers with a controller, it can spread the malicious code to other connected vehicles or EVSEs, causing a botnet attack.

Thus, the magnitude of this vulnerability is also medium, which results in medium risk. The summary table shows more information about these attacks and their associated risks.

D.1.2.2. Embedded Systems

Failure in an embedded system can cause ECU failures, such as failure in actuators and autonomous driver assistants [207]. Although most embedded systems are hidden, some are vulnerable points to target, such as vehicle sensors, ultrasonics, and cameras. Two critical embedded systems are primary and secondary controllers [59, 89]. Another part that needs security attention is the vehicle battery charging system [322] and braking system [242], which are also physically embedded systems at risk of being tampered with by an attacker. The likelihood of physical attacks is low because the attacker requires direct physical access to the vehicle and enough knowledge about the vehicle's architecture. The impact is a real-time failure and dissatisfaction of clients. Thus, the risk associated with firmware security is low. The summary table shows more information about these attacks and their risks.

D.2. Communication Threats

There are four main types of communication in ICVs: V2V, V2I, V2N, and V2P [105]. With the growth of IoT technologies and new communication types, V2X communication has been introduced [57]. V2X uses two communication technologies: DSRC, a one or two-way wireless communication channel designed specifically for vehicular networks, especially in V2V, and C-V2X or LTE-V2X. LTE (Long-Term Evolution) is a standard for wireless broadband communication that enables high-speed data transfer, and C-V2X is a more comprehensive communication technology that encompasses LTE-V2X and expands upon it by incorporating 5G capabilities [160, 312]. Relying solely on DSRC is not viable since features such as low communication latency, rapid network connectivity, and security can differ [111]. Through V2X, compatible ve-

hicles can receive alerts regarding hazardous road conditions, traffic light statuses, changing work zones, platoon formation, lane changing, and more [73]. However, an ICV network can also create a highly vulnerable surface for attackers. Although the numerous security solutions proposed for V2X communication, such as [40], more detailed risk analysis is required to ensure its security.

D.2.1. DSRC Communication Threats

DSRC communication technology, developed from the IEEE802.11 standard, is widely used in EV communication, primarily for V2V and V2I communication [160]. However, DSRC faces several limitations, including unbounded delays, scalability issues, and lack of deterministic Quality of Service (QoS) support, which makes it challenging to use in V2X communication [111]. As a result, researchers have evolved cellular technologies for V2X communication [2]. RSUs and DSRC-enabled vehicles can send safety messages to an ICV, but this communication also creates a vulnerable attack surface. Therefore, researchers have looked into security issues in DSRC, such as jamming and DoS attacks. This section describes some of these issues and the associated risks with DSRC.

D.2.1.1. DSRC Communication and Network Vulnerabilities

DSRC has primarily developed for V2V and V2I communication but has also created a vulnerable surface for compromising DSRC-enabled vehicles. Some known attacks include message reply attacks, session hijacking, and DDoS [111]. Since attacks targeting ICV communication often target one of these two types of communication, researchers have developed mitigation and detection techniques, such as those in [293, 339], to prevent false safety messages from being sent throughout a platoon and causing dangerous decisions. Due to the known vulnerabilities and exposure of DSRC to the external network, its risk is considered high. More information about these attacks and their associated risks can be found in the summary table.

D.2.2. C-V2X Communication Threats

Cellular V2X (C-V2X) is a communication technology used in ICVs. It was introduced as 3GPP C-V2X in Release 14 of the LTE standard [1] and is enabled with LTE and 5G. C-V2X enhances communication over the previous DSRC technology due to its lower latency. In [283], the authors present a comprehensive study on the architecture and security of LTE-V2X and 5G-V2X. Since V2X refers to the communication of vehicles with anything, such as devices, pedestrians, other vehicles, infrastructures, networks, and sensors, C-V2X can gather more information about its surroundings, resulting in better decision-making and a higher level of autonomy. However, this also creates a vulnerable surface for attackers to compromise EVs or users' privacy. This type of communication requires extra security attention, and this section describes some security issues.

D.2.2.1. C-V2X Communication and Network Vulnerabilities

V2X is a vehicle's communication with any other entity that may be affected. V2X communication often includes V2V, V2I, V2N, and V2. Communications with devices and sensors can also be categorized as V2X [204]. V2V communication is for exchanging information within a platoon of vehicles, such as road traffic, lane changing, and platoon control messages [71, 188]. V2I is the vehicle for infrastructure communication, such as with road infrastructures, traffic lights, and road conditions. V2N is the communication of vehicles with the cloud server [106], and V2P is communication with pedestrians [143]. More information on the security and challenges of V2X communication can be found in [2, 83]. Many papers studied the security of these communication technologies, such as [111, 149, 357]. Adversaries can target the cellular architecture of the C-V2X, such as attacks targeting 5G or LTE core networks [283], or target the messages and responses within the communication. Since V2X is highly exposed to the Internet and third-party networks, it is vital to maintain C-V2X communication security. Although manufacturers design their enabled C-V2X

vehicles with security in mind, they must deliver OTA updates and patches as new attacks appear. The risk associated with C-V2X is similar to DSRC communication as they share common features, except that more mitigations are in place to impede a successful attack. Thus, it has a medium impact. The summary table shows more information about these attacks and their associated risks.

4.4.5 Autonomous Driving Security Profiling

Table 4.7: Autonomous Driver Electric Vehicle Security Profiling and Risk Assessment

Aspect	Surface of Threat	Sub-Surface	Vulnerability	Challenges and Attacks	Threats	Criteria	Possible Countermeasures	L	I	R
Autonomous Driver Security	Driver Threats	Autonomous Assistant	Learning Models [48, 56, 274]	• Spoofing Traffic or Map Information, • Vehicle Configuration Settings Tampering, • Injecting Malware, • Adversarial Machine Learning, • Poisoning Attack in Machine Learning, • Message and Event Log Repudiation, • Autonomous Driving System Data Theft.	• Spoofing, • Tampering, • Info. disclosure.	Machine learning model's adversarial attacks by tampering with learning/testing data and DoS attack against decision-making assistants and actuators. It can cause catastrophic damages such as loss of control or loss of human lives. This system is impossible, and the threat source is motivated to initiate the attack.	• To avoid spoofing traffic or map information: GPS and map verification, Intrusion detection system [202], • To prevent vehicle configuration settings tampering: Intrusion detection system, Configuration verification, Physical security [128], • To evade injecting malware: Malware detection, Encryption, Firmware updates, Machine learning, Physical layer authentication [11, 151], • To resist adversarial machine learning: Intrusion detection system, Data augmentation and verification, Adversarial training and model verification [145, 245], • To block poisoning attack in machine learning: Data augmentation and verification, Secure data sharing [67, 282], • To prevent message and event log repudiation: Secure logging, Timestamp, Redundancy, Blockchain [217, 233], • To avoid autonomous driving system data theft: Physical security, Privacy policies and data retention policies, Intrusion detection system [135, 174].	M	H	H
		In-Vehicle Bus Communication	Vehicle Buses Vulnerabilities [39, 62, 94, 136, 144, 221, 230, 244, 304, 330]	• Spoofing Vehicle Bus Messages or OBD Port, • Vehicle Bus Messages Tampering, • Monitoring OBD or CAN Bus Messages, • In-Vehicle Bus Communication DoS.	• Tampering, • Repudiation, • DoS.	Tampering in-vehicle busses data to vandalize the functionality of certain ECUs or trying to erase security logs (repudiation attack) are typical for in-vehicle communication. Tampering the buses can cause malfunction of certain ECUs and loss of events. Although the vulnerability exists, the attack requires experience, and mitigations are in place. The system is slightly exposed to external systems.	• To avoid spoofing vehicle bus messages or OBD port: Intrusion detection system, CAN message authentication, Finger printing Encryption [29, 337], • To prevent vehicle bus messages tampering: Intrusion detection system, CAN message authentication, Redundancy [148, 252], • To block monitoring OBD or CAN bus messages: Intrusion detection system, Access control and physical security, Encryption [157, 299], • To resist in-vehicle bus communication DoS: Rate limiting, Intrusion detection and prevention system [38, 159].	M	M	M
	Actuator Threats	Sensors	Sensors Vulnerabilities [48, 202]	• Spoofing Sensor Data, • Vehicle Sensors Sybil Attack, • Vehicle Sensor Tampering, • Sensor and Network Jamming Attack, • Autonomous System DoS.	• Spoofing, • Tampering, • DoS.	Physical tampering with sensors or denying their functionalities by vandalizing can cause disastrous effects such as loss of human lives. Threat sources are highly motivated, and systems are highly exposed to external systems. Adversaries can destroy critical functions of the vehicle.	• To avoid spoofing sensor data: Intrusion detection system, Encryption, Physical layer security, Multi-sensor correlation [54, 306], • To prevent vehicle sensors Sybil attack: Digital signatures, Multi-sensor data correlation, Intrusion detection system [192], • To block vehicle sensor tampering: Intrusion detection system, Redundant sensors, Sensor data encryption [53, 128], • To resist sensor and network jamming attack: Frequency hopping, Redundancy, Signal attenuation and anti-jamming technology [163, 335], • To resist autonomous system DoS: Network segmentation, Rate limiting, Intrusion detection system [301].	H	H	H
		Telemetry Services	Telemetry Services Vulnerabilities [88, 107, 309]	• Spoofing GPS Signals, • Vehicle Navigation / Diagnostic Systems Tampering, • Data Privacy and Data Sharing Attacks, • Autonomous Driving System Reverse Engineering.	• Spoofing, • Tampering, • Info. disclosure. • Elevation of Privilege	Denying telemetry services (DoS, DDoS attacks) is common and in conjunction with spoofing as adversaries can impersonate themselves as other valid vehicles or trusted third parties. Such attacks can destroy the functionality of vehicles in real-time, but although vulnerabilities exist, mitigations are in place to limit the attacks. Threat sources are highly motivated, and telemetry services are highly exposed to external systems and the Internet.	• To avoid spoofing GPS signals: Intrusion detection system, Encryption, Secure communication [306, 346], • To prevent vehicle navigation / diagnostic systems tampering: Intrusion detection system, Enhanced and resilient OBD system, Reputation-detection systems, Blockchain [128, 216], • To block data privacy and data sharing attacks: Secure data sharing, Privacy policies and data retention policies, Data encryption and anonymization [185], • To resist autonomous driving system reverse engineering: Firmware protection, Code obfuscation, Physical security [280].	H	M	H

The popularity of smart devices and IoT led to an increase in the use of intelligent vehicles, including Autonomous Vehicles (AVs). AVs can provide safety, comfort,

and economic benefits, but security is crucial for their adoption [95]. Although security flaws and solutions are studied [308], comprehensive security analysis and risk assessment are missing. AV vulnerabilities can be categorized as those threatening the driver system, and those threatening the AV system, including AV assistant, in-vehicle buses, sensors, and telemetry sensors and vehicle services [46, 74]. Currently, five levels of vehicle autonomy exist, and this section assumes a general AV [66]. A summary of AV vulnerabilities, challenges and attacks, STRIDE mapping, risk assessment, and possible countermeasures can be found in Table 4.7, and this section will provide detailed information on AV vulnerabilities.

E.1. Driver Threats One attack surface that threatens the AV system is driver threats. Here, the driver means both the person and the driver assistant model. Two critical issues that threaten the driver are autonomous assistant driver and in-vehicle busses threats [263]. A driver assistant is an AI software that runs on EV embedded system as an ECU. In-vehicle buses are often in charge of information exchange [325]. More information on these vulnerabilities is in the following sections.

E.1.1. Autonomous Assistant

The decision-making process in AVs presents a significant security challenge. Autonomous driving requires vast amounts of information from inside and outside the vehicle. Communication between ICVs and the sensors and services in an AV system allows machine learning models to make decisions while driving [325]. These AI models are trained on extensive data to make hundreds or thousands of decisions during a road trip. In [281], the authors demonstrate a simulation of an AV system, including the ECU and the AI firmware. This section will discuss how machine learning models can be vulnerable to AV systems.

E.1.1.1. Learning Models

Researchers developed machine learning and deep learning models to create intelligent

AVs with different autonomy levels [66]. State-of-the-art learning models are accurate in making correct decisions. However, in real-world scenarios, attackers try to disturb the models and force them into dangerous choices. For instance, attackers can tamper with the object detector in an AV system using a laser [56]. Adversarial machine learning attacks are highly effective against these models [198]. Such attacks are life-threatening as passengers may not be aware of the presence of an attack before it happens. Other examples of attacks toward AV systems include attacking vehicle lane change, navigation, and adversarial object detection [48, 274]. Since attackers require skills to attack the models, their likelihood is medium, but their impact is high. The summary table shows more information regarding attacks, countermeasures, and associated risks.

E.1.2. In-Vehicle Communication and Busses

Four types of physically wired buses exist in AV systems: CAN, LIN, FlexRay, and MOST [330]. These buses allow different components in the system to communicate with each other through wire bus communication. However, this type of communication creates new avenues for attackers to compromise AV systems [54]. This section will describe each bus, its vulnerabilities, and countermeasures. An attack on any of these buses can cause moderate to severe damage to the vehicle and passengers, as these attacks often go undetected until they happen.

E.1.2.1. In-Vehicle Bus Communication

Four buses existing in EVs are Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, and Media Oriented Systems Transport (MOST). These buses exchange information between different vehicle ECUs [39]. CAN bus has two forms: high-speed, used in telemetry services, engine control, and airbag control, and low-speed is used in wiper control and lighting control [342]. The LIN bus is often in charge of assembly units such as seats, steering wheels, and doors in vehicles [304], and it is slower than the CAN bus. FlexRay is a time-trigger bus invented after the

CAN bus. FlexRay is becoming more popular for companies to use in AV systems. The MOST bus [62] is less common among researchers and is in charge of vehicle media transfer. Academics investigated different attacks and mitigations. For instance, authors in [144] study spoofing attacks on the CAN bus, and authors in [94] study LIN bus security. For FlexRay, authors in [244] simulated attacks to show its security. In [94], authors worked on the security of MOST. Furthermore, researchers proposed different mitigation and detection techniques for the cyber security of in-vehicle busses, such as works in [263, 342]. The likelihood of these buses becoming a target is medium since attackers require skills and often physical or limited-range access to the bus. The impact, however, can be catastrophic as a compromised bus can go undetected until exercised. The summary table shows more information regarding the in-vehicle bus risks.

E.2. Actuator Threats

In the growth of sensor technology, sensors, and services have become integral features of Autonomous Vehicle (AV) systems, enabling them to gather information from their surroundings and make accurate decisions [168]. AV systems utilize ultrasonic, camera, lidar, and GPS sensors to obtain information about their environment [46]. Additionally, telemetry services in AV systems, such as Bluetooth, Wi-Fi, and RFID, facilitate communication with other vehicles and infrastructures and are sometimes employed for intra-vehicle communication between components like Bluetooth [169]. These sensors and services represent vulnerable points that attackers can exploit to compromise AVs, as sensors are typically located on the outer layer of the vehicle, making them physically visible. Also, telemetry services can act as gateways that readily accept modified packets in the network [10]. Analyzing the security of sensors and telemetry services in AVs is crucial to ensure attackers cannot compromise them. This section describes attacks on sensors and telemetry services.

E.2.1. Sensors

Sensors are essential for AVs, gathering information from their external surroundings [168]. Various attacks specifically target sensors to disrupt the decision-making process of AVs. For instance, some attacks aim to compromise AV cameras and lidar systems to blind the AV system [274]. Other attacks may exploit location and GPS sensors to track a vehicle, potentially leading to vehicle theft [202]. Lidar and camera systems in AVs detect objects and obstacles, and attackers can render the AVs blind, increasing the likelihood of accidents [48]. Consequently, physical and software security of sensors is crucial, which often necessitates regular inspections and secure firmware updates [54]. These sensors are particularly vulnerable targets, as attackers need more skills or resources to disrupt the vehicle. The impact can be catastrophic, as a vehicle with a compromised sensor can make dangerous decisions. The summary table shows more information on the challenges, risks, and countermeasures.

E.2.2. Telemetry Services

Telemetry services serve as the means of communication in ICVs and AVs. AVs collect information from other vehicles and their surroundings to make informed decisions [238]. Attackers target telemetry services directly to gain unauthorized access or compromise vehicle components, resulting in malfunctions. For instance, the RFID sensor represents a vulnerable point of attack, with researchers having already outlined its vulnerabilities [107]. Moreover, attacks on cellular network communication can render vehicles incapable of communication, leading them to transmit erroneous messages [309]. Many known vulnerabilities exist in telemetry services, such as Wi-Fi or RFID, and they typically do not require significant skill to exploit. Conversely, security teams implement various mitigation measures to thwart such attacks, making a successful attack's magnitude moderate. The summary table shows more information on the challenges, risks, and countermeasures.

4.5 Case study: Real World Cyber Attack Scenarios

To illustrate the application of the proposed framework for risk assessment, security categorization, and STRIDE domain analysis, this section presents an analysis of real-world cyberattacks on EVs. Attack scenarios from various references, organized by the date of occurrence, are compiled in Table 4.8. Cyber analysts can follow the same structure to determine risk and security categories for emerging threats. This section aims to assist organizations in identifying related attack surfaces and managing their resources based on risk levels classified using the framework.

4.6 Concluding Remarks

As the modern world transitions to connected cities and becomes more conscious of environmental issues such as climate change, eco-friendly technologies like EVs are gaining attention. Despite significant investments in EV development, obstacles and drawbacks to mass adoption persist, with cybersecurity being a critical concern. This thesis identified a need for comprehensive security analysis and risk assessment in the EV domain. We explored five major security categories: charging station security, information privacy, software security, connected vehicle security, and autonomous driving security. We identified challenges and attacks from previous studies, mapped them to a threat model STRIDE, and analyzed each category's attack surfaces, sub-surfaces, vulnerabilities, challenges and attacks, and potential countermeasures. We proposed a risk assessment framework using custom criteria and the STRIDE threat model to understand better and address the five security aspects. Our framework helps security researchers and analysts identify threats and risks in the EV ecosystem and develop mitigation strategies to tackle the issues discussed in this thesis.

Table 4.8: Risk Assessment of Real World Cyber Attack Scenarios on EVs

Year	Target Vehicle	Attack Scenario	Security Aspect	Threat	Vulnerabilities	L	I	R
2012	Toyota Prius 2010, Ford Escape 2010 [215]	Two cyber security white hatters named Miller and Valasek published a white paper on hacking two automobiles, including a Toyota Prius 2010 with a parking assistant and a Ford Escape 2010 with an intelligent parking assistant. Authors managed to hack into the automobile and take control of the steering, braking, acceleration, and display by injecting malicious code and hacking CAN bus communication through the vehicles' On-Board Diagnostic (OBD). Their paper fully demonstrated how they managed to do so, and detailed analysis of CAN protocol within the vehicle and the tools used to perform the attack. The only limitation of this attack was that attackers had to access the vehicle to inject CAN commands physically.	Connected Vehicles Security	Controllers	Embedded Systems	R	L	L
			Autonomous Vehicles Security	In-Vehicle Communication	In-Vehicle Bus Communication	M	M	M
2015	Jeep Cherokee 2014 [118, 214]	The same duo of white hatters, Miller and Valasek, performed another attack and published a white paper. The previous attack needed physical access, and companies like Toyota did not take the vulnerability seriously. This time the same duo performed a remote attack on Jeep Cherokee with Cyber-Physical Features, including 10 Adaptive Cruise Control (ACC), Forward Collision Warning-Plus (FCW+), Lane Departure Warning (LDW+), Park Assist System (PAM). The attack exercised over 15 kilometers from the vehicle while driving on the highway through its Internet connection. The authors exploited the Uconnect feature within the vehicle, which let attackers access the vehicle IP address. The authors accessed speed, brake, display, heating system, and GPS. Also, they have mentioned that this attack applies to many other automobiles. Companies forced 1.4 million vehicles to recall that were vulnerable to this attack. The wired magazine, a famous technological magazine, later narrated this attack.	Autonomous Vehicles Security	Actuators Threats	Telemetry Service	H	M	H
2016	Mitsubishi Outlander 2016 [197]	Another real-world attack occurred by PenTestPartners to hack a 2016 Mitsubishi Outlander PHEV. Unlike most vehicles, Mitsubishi Outlander used Wi-Fi instead of GSM to allow users to interact with the vehicle while they were out, probably to reduce the cost of the GSM module and the total vehicle cost. This module exchange put the vehicle at great risk of being compromised. PenTestPartners exploit this vulnerability by hacking Wi-Fi Pre-Shared Key (PSK) and cracking the SSID of the vehicle. They found the geolocation of all the Mitsubishi Outlanders. Furthermore, as an authorized mobile device connected to the vehicle, attackers managed to take control of the communication using a man-in-the-middle (MitM) attack to crack the messages and send malicious commands. PenTestPartners managed to lock/unlock the doors and then set the security alarm off in the vehicle, making it extremely vulnerable to further attacks. They also determined some fixes to the vulnerabilities and published the exploit afterward.	Software Security	Applications Threats	mobile and desktop application	H	M	H
2016	Nissan Leaf and Nissan eNV200 [142]	Another real-world attack occurred in the same year as Mitsubishi Outlander that affected Nissan software for its electric vehicles, including Nissan Leaf and Nissan eNV200. In the "NissanConnect" application, users were only asked to provide the Vehicle Identification Number (VIN) to connect to the vehicles, control the air conditioning, and see the location of their vehicles. With the initial characters of the VIN referring to the manufacturer, model of car, and country of the carmaker, attackers need to guess only the five last digits of the VIN to access the vehicle through the application. Hackers could turn the heating and cooling system on to drain the vehicle's battery or observe its geolocation. Nissan turned the app off after the vulnerability was discovered.	Software Security	Applications Threats	mobile and desktop application	H	M	H
2017	Tesla Model S P85, P75 [229]	Keen Security Lab of Tencent remotely hacked Tesla Model S P85 and P75 from wireless to CAN bus communication. They proved that it is possible to hack into a Tesla Model S vehicle through Wi-Fi/Cellular and inject CAN bus commands. Detail of the attack is provided in their white paper, and they also introduce three different mitigation for browser security enhancement, kernel security improvements, and code signing protection.	Autonomous Driver Security	Actuators Threats	Sensors	H	H	H
				Actuators Threats	Telemetry Services	H	M	H
2017	Tesla Fleet [176]	A hacker found a bug in the Tesla fleet's central server. Where every command or diagnostics is sent to, which is called "Mothership". The attacker impersonates a valid Tesla vehicle in the fleet and could get any information about the vehicles or send commands to them. The attacker later sent the Tesla fleet a "summon feature" command. The Tesla vehicle could remotely start traveling forward without anyone in it, and all the adversary needed was the VIN of one vehicle in the fleet. Tesla responded to the vulnerability within ten days and rewarded the attacker with a huge amount of 50,000$, which was the highest income from a bug.	Software Security	Cloud's Threats	Back-end Server	R	M	L
2018	Multiple BMW Vehicles [175]	Keen Security Lab did a security analysis on multiple BMW models. In their experiments, they implemented different attack chains, including local and remote attack chains. They found fourteen different physical and remote vulnerabilities, and later, in 2019, they released details of these attacks. These vulnerabilities include physical connection to execute an arbitrary command in diagnostic service through the OBD (physical), arbitrary code execution in navigation update service through USB port (physical), exploiting and intercepting vehicle browser (remote), injecting CAN messages (remote), compromising telemetry services (remote), and compromising gateway (physical). More detail can be found in the references. All the vulnerabilities are telemetry services, OBD physical ports, or vehicle communications.	Connected Vehicles Security	Controllers Threat	Embedded Systems	R	L	L
				Controllers Threat	Main Controllers	M	M	M
				Comm. Threat	Vehicle to infrastructure	H	M	H
			Autonomous Driver Security	In-Vehicle Communication	In-Vehicle Bus Communication	M	M	M
				Actuators Threats Threat	Telemetry Services	H	M	H
2020	Ford Focus, Volkswagen Polo	Volkswagen Polo had been found to have a vulnerability in the infotainment system, which allowed attackers to gain access to traction control and review the driver's data. The same method was used as a Man-in-the-Middle (MitM) attack in Ford Focus to intercept the tire pressure monitoring system to obtain personal data. Later, the Volkswagen "We Connect" app has found to request many permissions from users before use. The Ford "Pass" app allows sharing of travel routes and vehicle locations at any time needed, which may endanger users' privacy. After publishing the report to Ford and Volkswagen companies, Ford ignored it because they thought the attack required too much effort, whereas Volkswagen started implementing countermeasures. Although vulnerabilities were found only for two vehicles, others were susceptible to the same attack.	User Privacy	Vehicle Driven Information	In-Vehicle Information	R	M	L
				User Driven Information	Personal Data Services	M	L	L

Chapter 5

Intelligent Electric Vehicle Charging Session Monitoring: Combining Proposed EV-EVSE Architecture and the Risk Assessment

5.1 Motivation

So far, we have examined the architecture of the EV-EVSE, including all the components that play roles, using a DFD. This architecture helps the academic community understand the building blocks related to EV-EVSE. Using this architecture, we extracted all possible attacks and challenges in this system, categorized them, and proposed a risk assessment framework. In this section, our goal is to present a use case of the previous architecture and risk assessment by proposing an AI-enabled solution for security. Researchers often focus on specific elements, layers, or regions of

this ecosystem for further analysis. this thesis continues with an analysis of charging session security, which is a crucial aspect of EV security.

To provide trustworthy EVSEs, physical security, security of charging sessions, and security of communications in EVSEs are crucial. this thesis aims to analyze the application layer of EV-EVSE charging, specifically the EV charging sessions (EVCS). To achieve this, we present an intelligent monitoring framework (adopted from the SIEM monitoring solution in Section 2.4.1) for EV charging sessions in this section. To the best of our knowledge, we are the first to suggest a security mechanism for EV charging sessions to detect malicious sessions, EVSEs, and charging sites. Although the proposed framework evaluation is based on a single publicly available dataset of real-world charging sessions, charging sites can follow the same steps to build their specific intelligent monitoring system. The following section discusses the proposed framework.

5.2 Monitoring Framework

The proposed framework consists of five stages. It begins with a behavior analysis of the charging sites, EVSEs, and sessions. Each available charging site's and EVSE's characteristics and energy usage habits are determined through this stage. The second stage is Rule-Based detection, where the framework uses the first stage, behavior analysis, to establish rules, thresholds, or signatures to detect unusual, malicious, or misuse sessions. Rules can target a single session, EVSE, or charging site. The third stage is complementary to stage two, using Supervised Machine Learning Based detection to detect sessions close to malicious sessions from stage two in real-time. The results of the best-supervised model predict malicious sessions by comparing a couple of models as the final results. Stage four is Unsupervised Machine Learning detection. Like stage three, various anomaly detection algorithms are tested to find the best

model that detects all malicious sessions. Also, tuning and measuring the efficiency and robustness of stages three and four are in the following sections. The last step is to determine the cause of abnormal sessions. While the reasons for malicious sessions in the supervised and rule-based detection stages are known from the rule-based stage results, predicting the root cause for anomaly sessions in the unsupervised stage is yet to be specified. To this end, we develop two approaches: clustering and semi-supervised machine learning techniques to detect causes for all anomalous sessions. Figure 5.1 shows the steps of this framework.

Even though this thesis uses Adaptive Charging Network (ACN) data [180] to test and verify the proposed framework, the framework is data independent, and any charging session dataset or charging site can adapt it with slight differences in algorithms and rules. More information on the ACN dataset characteristics is in the next section.

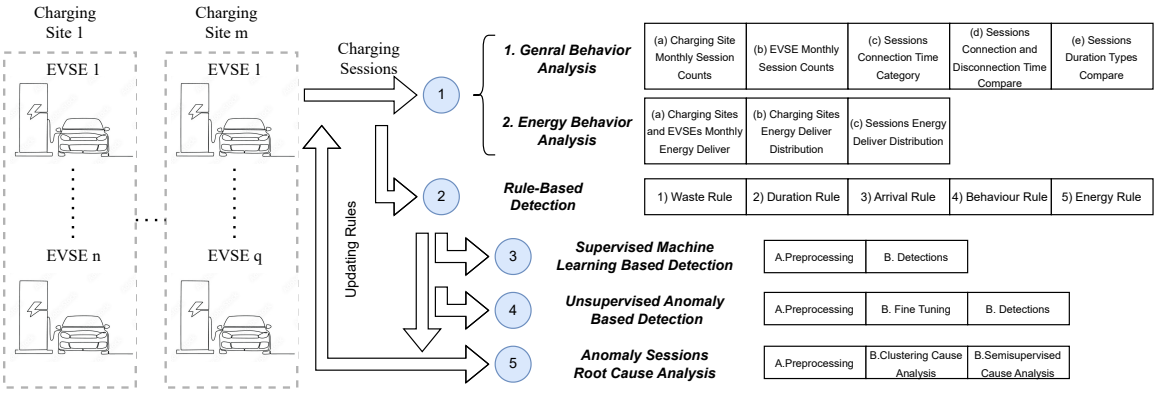

Figure 5.1: Intelligent EV charging sessions monitoring framework steps

5.2.1 Dataset and Characteristics

The proposed framework uses a publicly available dataset for EV charging sessions named ACN-Data. Authors in [180] have demonstrated the dataset's interesting characteristics of three available charging sites. They have also modeled the user behaviors using a Gaussian mixture model. For the sake of this thesis, since the behavior of the EVSEs, charging sites, and users are essential to the framework, we

briefly discuss some of the characteristics. ACN-Data contains three charging sites, all of which are located in Los Angeles. The Caltech site, often used by non-Caltech drivers, has 54 EVSEs and is open to the public. The JPL site includes 52 EVSEs, and only employees can access the site. The Office site consists of 8 EVSEs that only an office's employees can use. ACN data includes many features, including time series, date time, categorical, and numerical data [180]. However, in this thesis, only a proportion of features are used. Due to many null values, the time series features for energy delivery, user IDs, and user inputs are dropped. Table 5.1 shows this thesis dataset's features, descriptions, and types. In the following sections, these features will be used to demonstrate the behavior of the sites, place rules, and detect anomalies.

Table 5.1: Features of ACN-Data Used In this thesis

Feature	Description	type
connectionTime	Date and Time of which session started	DateTime
disconnectTime	Date and Time of which session ended	DateTime
doneChargingTime	Date and Time of which session stopped charging	DateTime
deltaConnectionDisconnet	Duration between connection and disconnection	Numeric
deltaConnectionDone	Duration between connection and charging	Numeric
deltaDisconnetDone	Duration between disconnection and charging	Numeric
t_arrivel	Hour and minute of connection time	Numeric
t_departure	Hour and minute of disconnection time	Numeric
DayOfTheMonth	Day of month for connection time	Categorical
DayOfTheWeek	Day of week for connection time	Categorical
Weekday	0 indicate weekend while 1 indicates weekday	Categorical
daylight	0 indicate night while 1 indicates daytime	Categorical
Month	Month of the year for connection time	Categorical
Year	Year of connection time	Categorical
kWh delivered	Total energy delivered throughout charging	Numeric
siteID	Identification of charging site	Categorical
spaceID	Identification of EVSEs	Categorical

5.3 Electric Vehicle Charging Sessions Behavior Analysis

The first stage in differentiating malicious charging sessions from benign ones is to analyze the system's behavior. Behavior analysis involves identifying characteristics, habits, critical times, and any possible information about the entities using charts and figures. Figure 3.1 shows the internal components in EVs and EVSEs. However, in real charging scenarios, charging site owners and third-party applications may not have access to all the communication within EVSEs or EVs without compromising users' privacy. Therefore, behavior analysis in this step targets higher-level components in a typical charging scenario, including charging sites, EVSEs, energy transfers, user habits, and other information about the session, such as location, start time, and departure time. We must profile each charging site, EVSE, its usage, users, and vehicles to determine these characteristics. Although not all information from charging sessions may be available to a charging site, more data result in better detection. Figure 5.2 shows a simple overview of the relations between endpoints in a charging scenario. Access to in-vehicle data, such as CAN bus data while charging or the links between users and their cars, can provide valuable behavior information but may not be practical with current technologies. For instance, the status of the battery, automatic charging, vehicle or battery health, and users' habits are a few benefits of having more informative data.

this thesis analyzes ACN data and its endpoint characteristics without considering user data because many users are unknown, and a typical charging site may not store users' information. A simple analysis of the number of sessions, EVSEs, and sites is presented in Table 5.2. Also, due to the lack of data for two charging stations, the analysis is performed for all the sites and EVSEs together, even though each charging site or station requires behavior analysis separately and collectively. These

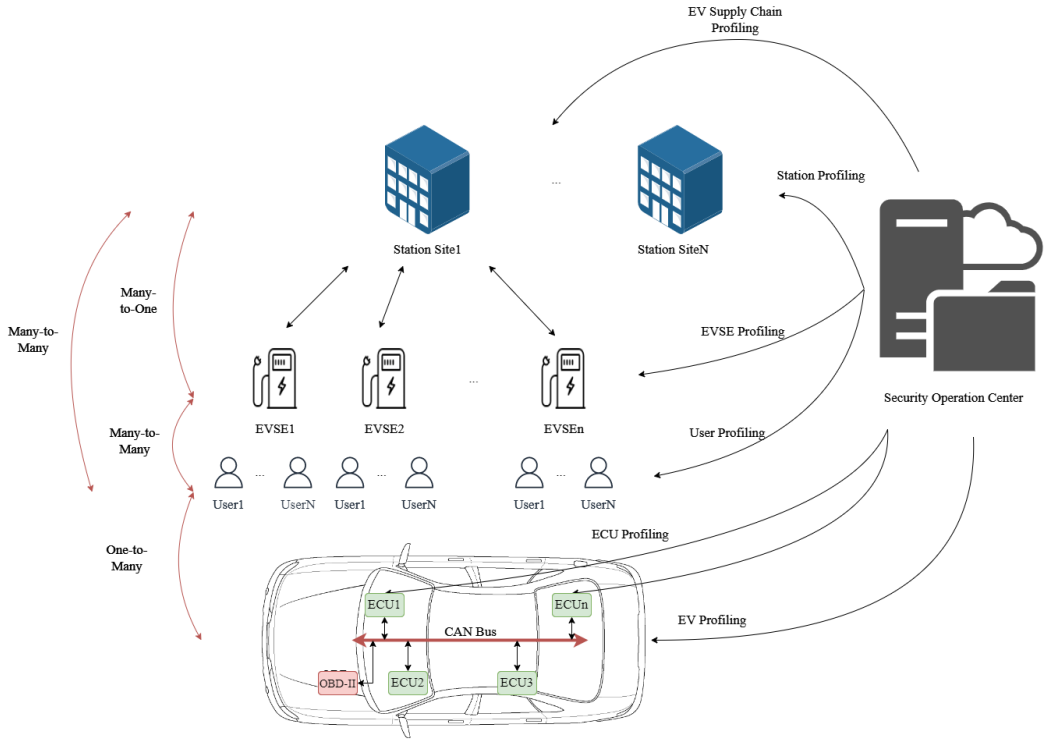

Figure 5.2: Overview of Relationships in Charging Scenario

behaviors can help us determine anomaly signatures in the next stage of the algorithm to detect unusual sessions. For behavior analysis, we categorize the behaviors into two: general behaviors and energy behaviors. The subsections below describe each category separately using charts and figures.

Table 5.2: ACN-Data Information for Available Charging Sites

Charging Site	# of EVSE	# of Sessions	# of Session after Drop
Caltech Site	55	8600	7096
JPL Site	52	17252	16491
Office Site	8	1284	1268
Total	114	27136	24855

5.3.1 General Behavior Analysis

The general behavior category includes the behavior in terms of habits and time for each day, month, and year of each charging site or station. This section consists of five figures, each providing valuable information that will be used in the next stage of the framework. The items below discuss the figures separately.

(a) **Charging Sites Monthly Session Counts**: Figure 5.3 bar chart shows the total number of sessions throughout the ACN dataset divided by months per charging site. The pie chart in the figure shows the percentage of total sessions in each charging site. We can observe that the JPL site has the most sessions, followed by the Caltech site and Office site, respectively, and the share of their sessions in total. It is critical to monitor the total number of sessions in each charging site, as an unusual number of sessions may indicate an attack, for example, someone trying to fill up the charging spaces by continuously charging and disconnecting a vehicle.

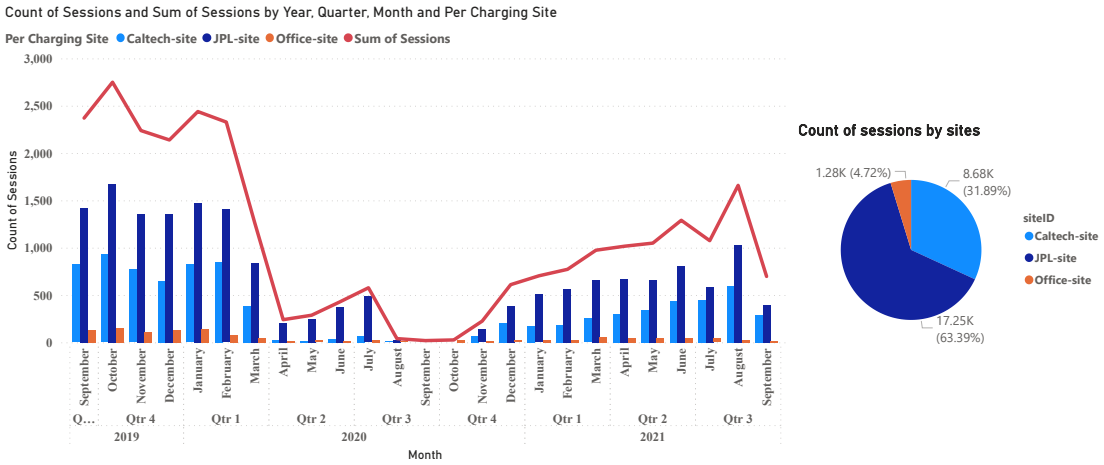

Figure 5.3: General Behavior Analysis: Number of Sessions per Charging Site

(b) **EVSE Monthly Session Counts**: Figure 5.4 demonstrates the same thing as figure 1 but per EVSE per charging site. Here we should monitor the number of sessions locally for each EVSE. An unusual number of sessions occurring on only

a few EVSEs while other EVSEs are empty may be a sign of anomaly behavior. For instance, in the Caltech bar chart, one EVSE in 2021 had the most sessions running while other EVSEs were not occupied. The same happened with the Office site in the second, third, and fourth quarters of 2020 and can signify anomalous activity. To speak more accurately, more specific information about the site, such as maintenance time or closed EVSEs, can help to find anomalies. The pie chart in the same figure shows the number of EVSEs in each charging site and the total percentage of EVSEs in that site.

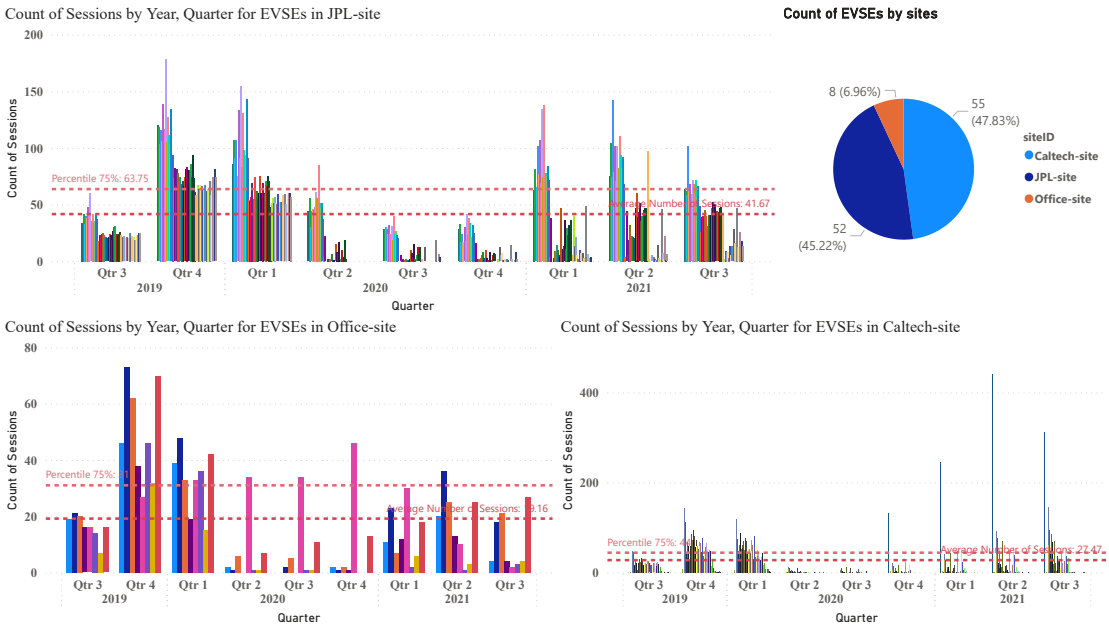

Figure 5.4: General Behavior Analysis: Number of Sessions per EVSE per Charging Site

(c) **Sessions Connection Time Category**: Figure 5.5 shows the number of sessions divided into four categories based on their connection time: weekday daylight, weekday night, weekend daylight, and weekend night. Also, the pie chart in the same figure shows the percentage of sessions that occurred in each category. Here we can observe that nearly 85% of all sessions started during weekday daylight, while a tiny portion of only 2% occurred during the weekend

night. Since all three charging sites are public, the result from this figure was predictable. Nevertheless, it is crucial to monitor the sites in off-peak times, primarily since most anomalies occur during this period, and this figure can point to such times.

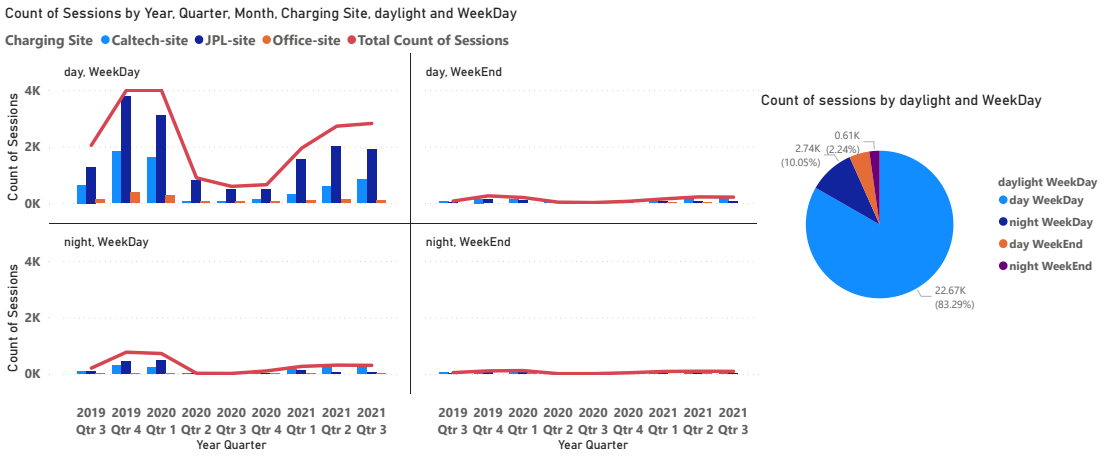

Figure 5.5: General Behavior Analysis: Number of Sessions per Charging Site at Weekdays/Weekends and Daylights/Nights

(d) **Sessions Connection and Disconnection Time Comparison**: Figure 5.6 demonstrates two distribution area charts for session connection and disconnection hours. According to this figure, 5 am to 10 am is the off-peak time for all three charging sites. Charging sites in ACN data behave nearly the same since they share some common characteristics, such as being public, located in Los Angeles, and near Caltech University. The peak of starting a session is near 3 pm (1 pm - 4 pm), while hours near 8 pm (7 pm - 10 pm) is the disconnection peak hour. Accordingly, users of these sites tend to charge their vehicles around noon and take off at night. However, vehicles starting their session in off-peak hours introduce more danger, as fewer people are at the site, and the attacker will have plenty of time to execute an attack. The off-peak duration should be continuously monitored for security.

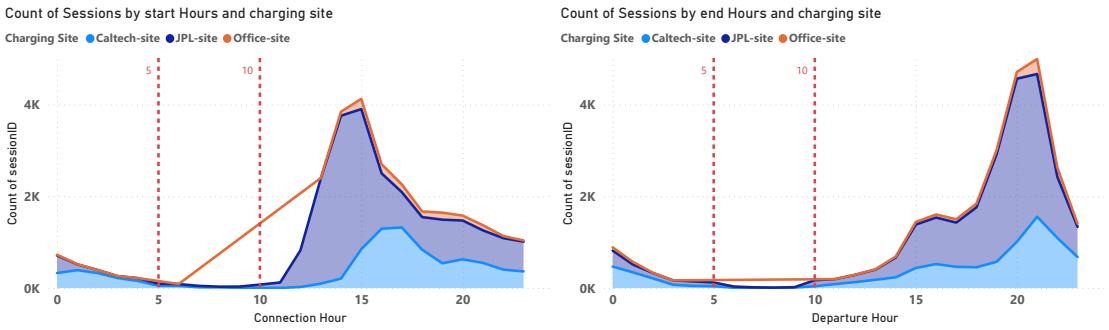

Figure 5.6: General Behavior Analysis: Distribution of Sessions Arrival and Departure Hours in a Day

(e) **Sessions Duration Types Comparison**: Figure 5.7 describes three critical durations in a charging session. DeltaConnectionDone for each session describes the duration between connections until the vehicle finishes charging. DeltaConnectionDisconnect shows the session's total duration, and deltaDisconnectDone is the duration after the vehicle is fully charged but still connected to the station. DeltaDisconnectDone is unsuitable for charging sites, as a vehicle may occupy an EVSE while not charging. The pie chart shows the average time of these three durations. Furthermore, constant x lines in each chart show a threshold for these sites that can be dangerous, considered waste, or need attention.

5.3.2 Energy Behavior Analysis

The energy behavior category consists of all energy transfers in a charging site, EVSE, and a session. This section consists of three figures and the items below discuss the figures separately.

(a) **Charging Sites and EVSEs Monthly Energy Deliver**: Figure 5.8 shows the total kWh energy delivered per month per charging site and EVSE. According to the first chart, the JPL site delivered the most kWh, followed by the Caltech site and Office site. Except for the third and fourth quarters of

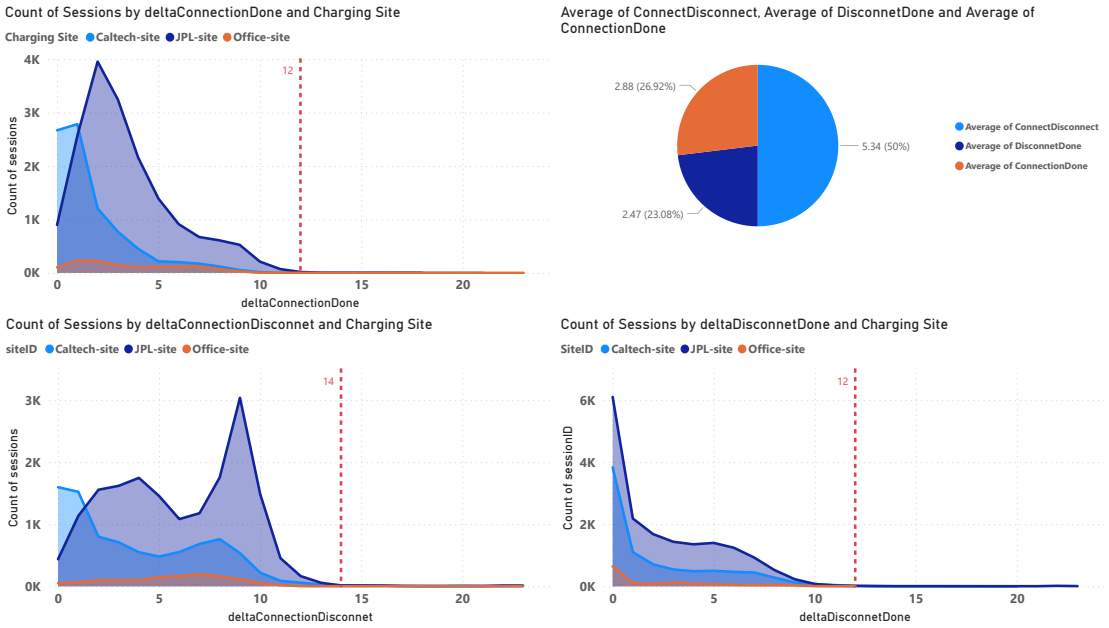

Figure 5.7: General Behavior Analysis: Distribution of Sessions Critical Times per Charging Site

the year 2020, which was also mentioned in the general behavior category, all other months seem normal. Even though there is no malicious data in this chart, energy delivered in charging sites is crucial for the smart grid and demand response [126]. The second chart shows the kWh delivered for EVSEs. Likewise, except for the fourth quarter of 2020, in which one EVSE delivered kWh unusually, the rest seems normal.

(b) **Charging Sites Energy Deliver Distribution**: Figure 5.9 shows total energy delivered distributions divided by daylight and weekday. As expected from general behavior analysis, energy transfers in all categories are below average, except for weekday daylight. As discussed in the previous part, only a few sessions occurred on weekends compared to weekdays due to charging sites being used as public charging sites. Monitoring this behavior allows efficient load balancing and charging scheduling for charging sites and smart grids [186].

(c) **Sessions Energy Deliver Distribution**: Figure 5.10 indicates the distri-

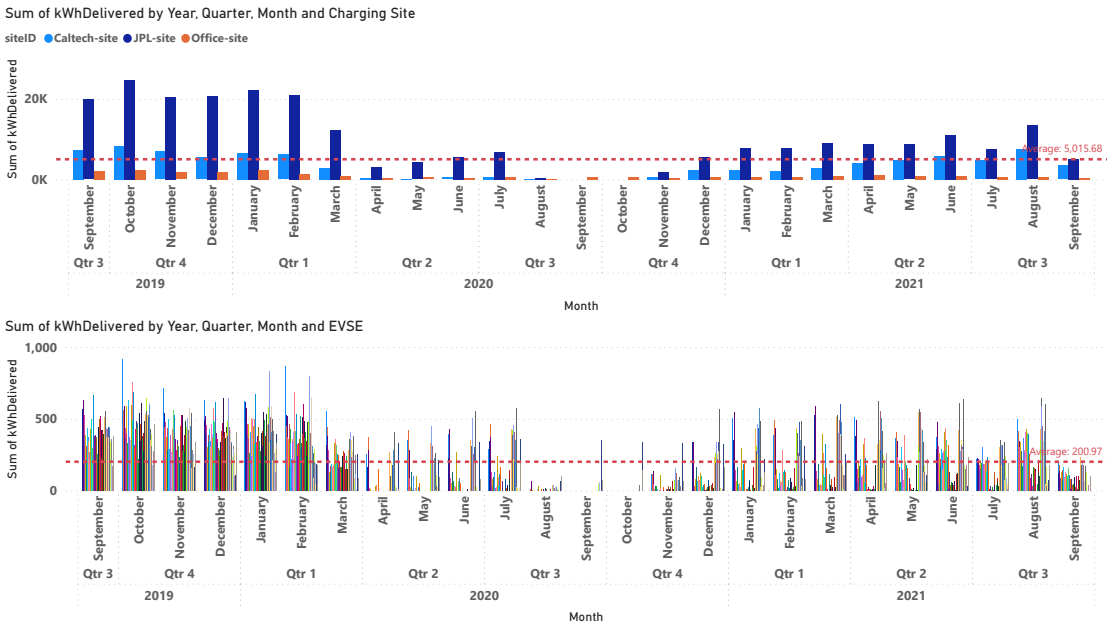

Figure 5.8: Energy Behavior Analysis: Total Daily Energy Delivered per Charging Site and per EVSE

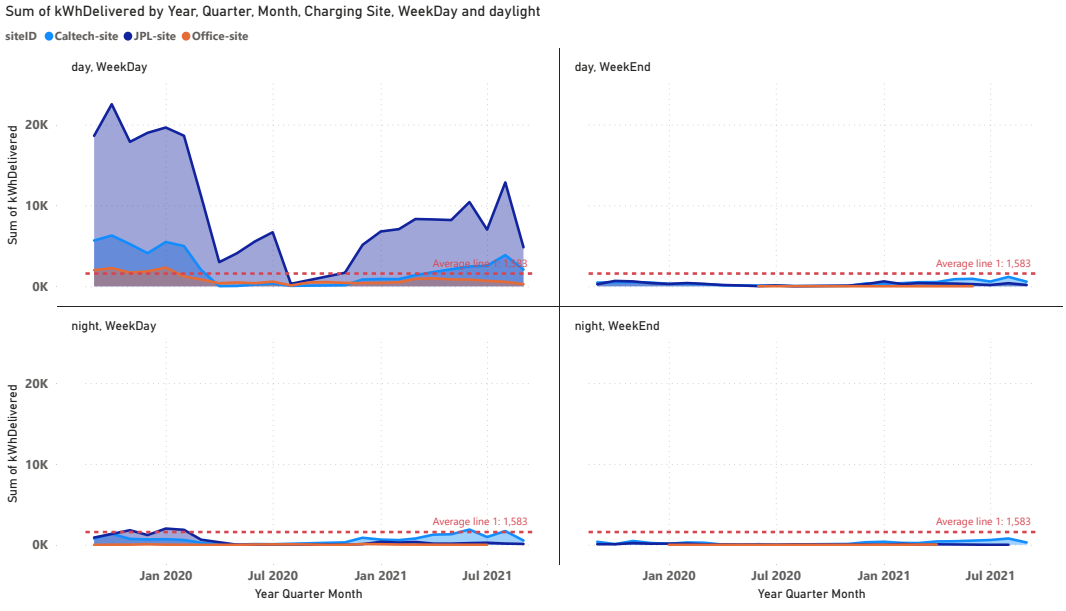

Figure 5.9: Energy Behavior Analysis: Energy Delivered Distribution per Charging Site at Weekdays/Weekends and Daylights/Nights

bution of energy delivered instead of the total energy delivered as was in the previous figure. It is critical to monitor energy delivered for scheduling and smart grid usage. ACN papers [179, 180] discussed the scheduling related to the energy delivered. The charts show that the energy delivered is mostly less than 60 kWh, and most sessions delivered around 0-20 kWh. Also, it would be valuable to profile users' energy delivered individually so that an anomaly can occur if a user exceeds their habit. However, user profiling is not part of this thesis due to the lack of user data.

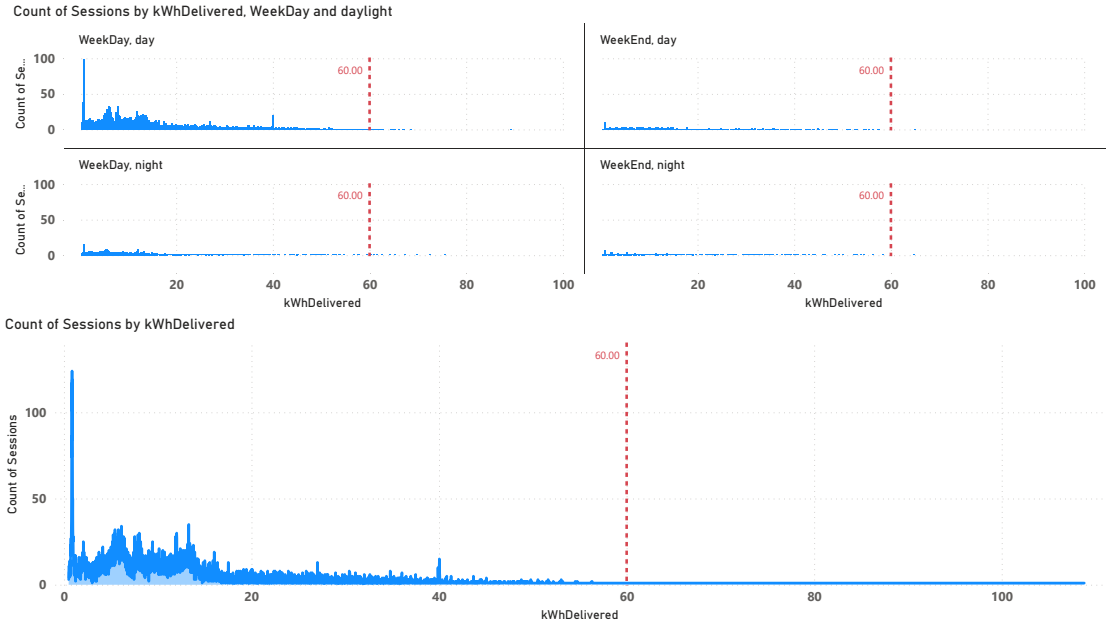

Figure 5.10: Energy Behavior Analysis: Distribution of Sessions Energy Delivered at Weekdays/Weekends and Daylights/Nights

5.4 Rule Based Detection

This step aims to identify as many signatures or rules as possible that apply correctly to the dataset and potentially detect anomalies. Rules should be established based on the behavior analysis in the previous step. Although rules are data-dependent and, in this thesis, are only based on the ACN data and available information, the

framework's steps of identifying rules are data-independent, which means the exact behavior analysis figures can help determine new rules and improve analysis for any charging site.

In this thesis, we identified five signatures for ACN data, detecting sessions as unusual, misused, or malicious. Rules are defined as follows:

1. **Waste Rule:** Any session with its deltaDisconnectDone (duration after charging until the vehicle is disconnected) exceeding 12 hours is considered an anomaly. We called this rule a waste of time as vehicles occupy a charging space while staying idle.

$$deltaDisconnetDone >= 12$$

2. **Duration Rule:** The second rule is to identify any session with a charging duration over 12 hours. Meaning any session with deltaConnectionDisconnect longer than 12 hours is detected as unusual. This rule targets vehicles that may block the charging done signal which can also result in excessive energy delivery.

$$deltaConnectionDisconnet >= 12$$

3. **Arrival Rule:** This rule intends to detect any session that occurs at unusual hours in a charging site. For ACN data, identified in the previous section, the unusual hours for all three charging sites are 5 am to 10 am. Therefore, this rule detects any session from 5 am-10 am. Likewise, this rule is for ACN data and may vary depending on charging sites.

$$5 <= t - arrival <= 10$$

4. **Behavior Rule:** This rule identifies any session during unusual working days/hours at a charging site. For ACN data and from the previous section, we identified

that sessions on weekend nights are rare and unusual. There are only a few sessions in comparison to other weekdays day or night and weekend days. Thus, this rule detects any session on weekend nights as an anomaly. Like other rules, this rule applies to ACN data and may vary for other charging sites.

$$WeekDay == 0 \cap DayLight == 0$$

5. **Energy Rule:** This rule aims to detect any session that delivers an unusual amount of energy/kWh. It is always better to profile users for energy transfer, EVSEs, and charging sites separately. However, ACN data does not provide enough information. Therefore, we only detect energy transfer based on the session. Like other rules, the threshold may vary based on the charging site's users, purpose, and location. The threshold for ACN data is 60 kWh.

$$kWhDelivered >= 60$$

It is important to know that rules are not unique to sessions, meaning multiple rules can be triggered by a session. Therefore, we label each session by all the rules that detect that session. With the rules established, we can identify anomalies in ACN data. In total, there are 1191 anomalies found out of 24855 sessions (after dropping sessions with no done charging time), around 0.06% anomalies. Table 5.3 shows the summary of the detected sessions and their corresponding rules.

5.5 Supervised Machine Learning Based Detection

So far, we have detected anomalous sessions based on several signatures derived from behavior analysis. The next step of the framework aims to develop a supervised machine-learning technique to detect anomalies based on rule-based detection (pre-

Table 5.3: Different classes in rule-based detection and number of sessions detected by those rules

Waste Duration	Waste Duration Arrival	Waste Duration Arrival Behaviour
78	2	1
Waste Duration Behaviour	Waste Duration Energy	Duration
14	2	312
Duration Arrival	Duration Arrival Behaviour	Duration Behaviour
14	5	22
Duration Energy	Arrival	Arrival Behaviour
11	238	25
Behaviour	Energy	Total
445	22	1191

vious step). The main intention of adding supervised machine learning on top of rule-based detection is to detect similar anomalies that have a low distance to rules' anomalies but are not triggered by them. This model also helps in real-time detection, which is crucial in real-world scenarios. Here, since rules are simple and computationally cheap, the machine learning model is expected to achieve high accuracy with some level of recall. The model needs to be robust, detect anomalies already detected by rules, and possibly give us some extra anomalies. In measurement, the ML model needs to have a good F2 score, as we value recall more than precision (detecting some sessions as anomalies that are not triggered by rules). To this end, we developed several machine-learning models after data preprocessing. Since our work is the first to detect anomalies in charging sessions, there are no other baselines to compare our model. However, we tried to apply multiple models as a comparison.

5.5.1 Pre Processing

Before developing models, preprocessing is required. Here, the target column is a label that indicates whether the session is an anomaly or not. Categorical values are one hot encoded first (except for spaceID, which was labeled due to its high cardinality). Then z-score normalization and the Yeo-Johnson transformation are applied to all

columns. For the last step, collinear features with high correlation and low variance features are removed from the dataset to make the model more robust. PCA is also used for better robustness. 50% of the dataset is used for testing, and we evaluate the final model in a 10-fold cross-validation technique for the best model. In this thesis, the authors decided on values and techniques such as grid search for hyper parameters in each model and by performing the same experiment multiple times, and choosing the best results. Table 5.4 shows a summary of the best preprocessing steps and properties.

Table 5.4: Preprocessing Summary for Supervised Machine Learning Table

	Description	**Value**
1	Target	label
2	Target Type	Binary
3	Label Encoded	SpaceID
4	Original Data	(24855, 16)
5	Missing Values	False
6	Numeric Features	7
7	Categorical Features	7
8	Transformed Train Set	(12427, 35)
9	Transformed Test Set	(12428, 35)
10	Shuffle Train-Test	True
11	Stratify Train-Test	True
12	Fold Generator	StratifiedKFold
13	Fold Number	10
14	Normalize	True
15	Normalize Method	Z-score
16	Transformation	True
17	Transformation Method	yeo-johnson
18	PCA	True
19	PCA Method	Linear
20	PCA Components	0.99
21	Ignore Low Variance	True
22	Remove Multicollinearity	True
23	Multicollinearity Threshold	0.9

5.5.2 Supervised Models

After preprocessing data based on Table 5.4, we developed supervised ML models to detect signature-based anomalies. Since no other studies with the same goals are available, different models are compared to each other to find the best model. Measurement metrics to find the most valid model are Accuracy, AUC, Recall, Precision, F1, Cohen's Kappa (Kappa) [147], Matthew's correlation coefficient (MCC) [287], F2, and TrainTime (Sec). However, models are ordered based on their F2 score, as discussed in the first paragraph of this section. Table 5.5 summarizes the results after applying models.

Table 5.5: Results of comparing different classifiers with rule-based detected sessions

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	F2	TT (Sec)
Gradient Boosting Classifier	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	2.560
Decision Tree Classifier	**0.9999**	**1.0000**	**1.0000**	**0.9984**	**0.9992**	**0.9992**	**0.9992**	**0.9997**	**0.059**
Ada Boost Classifier	0.9998	0.9999	1.0000	0.9969	0.9984	0.9983	0.9983	0.9994	0.573
Random Forest Classifier	0.9991	1.0000	0.9824	1.0000	0.9910	0.9906	0.9906	0.9858	1.165
Light Gradient Boosting Machine	0.9964	0.9998	0.9583	0.9700	0.9638	0.9619	0.9621	0.9604	0.237
Extra Trees Classifier	0.9864	0.9986	0.7354	0.9920	0.8430	0.8361	0.8472	0.7747	0.944
SVM - Linear Kernel	0.9724	0.0000	0.5274	0.8784	0.6549	0.6416	0.6664	0.5715	0.073
Linear Discriminant Analysis	0.9535	0.8993	0.5338	0.5389	0.5343	0.5099	0.5110	0.5335	0.091
K Neighbors Classifier	0.9722	0.9099	0.4694	0.9584	0.6257	0.6132	0.6577	0.5212	0.964
Logistic Regression	0.9695	0.9165	0.4761	0.8543	0.6076	0.5932	0.6226	0.5208	0.148
Naive Bayes	0.9328	0.8523	0.5033	0.3739	0.4279	0.3931	0.3986	0.4697	0.039
Ridge Classifier	0.9648	0.0000	0.3015	0.9962	0.4592	0.4466	0.5351	0.3493	0.036
Quadratic Discriminant Analysis	0.4779	0.5527	0.6357	0.0644	0.1154	0.0270	0.0512	0.2218	0.053

By observing the results in Table 5.5, Gradient Boosting Classifier (GBC) has the highest evaluation parameters. However, since Decision Tree Classifier (DT) also has a noticeably high F2 score and its training time is almost 100 times less than GBC, DT is selected as the most efficient algorithm for this thesis. To further improve the robustness of the model, an ensemble stacking classifier of the best model is also compared to the previous ones. This ensemble model stacks the three best classifiers (GBC, DT, Ada Boost), and then a single DT classifier decides on the final output. Stacking allows the use of each estimator's strength and thus makes the algorithm more robust. However, the ensemble model has a lower train/test time than a single

DT classifier and uses more resources. Table 5.6 shows the results of the stacked classifier with three estimators and DT as the final classifier.

Table 5.6: 10 fold cross validation results of stacked classifier with DT as final classifier

Fold	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	F2
0	1.0000	1.0000	1.0	1.0000	1.0000	1.0000	1.0000	1.0000
1	1.0000	1.0000	1.0	1.0000	1.0000	1.0000	1.0000	1.0000
2	1.0000	1.0000	1.0	1.0000	1.0000	1.0000	1.0000	1.0000
3	1.0000	1.0000	1.0	1.0000	1.0000	1.0000	1.0000	1.0000
4	1.0000	1.0000	1.0	1.0000	1.0000	1.0000	1.0000	1.0000
5	1.0000	1.0000	1.0	1.0000	1.0000	1.0000	1.0000	1.0000
6	1.0000	1.0000	1.0	1.0000	1.0000	1.0000	1.0000	1.0000
7	0.9992	0.9996	1.0	0.9841	0.9920	0.9916	0.9916	0.9968
8	1.0000	1.0000	1.0	1.0000	1.0000	1.0000	1.0000	1.0000
9	1.0000	1.0000	1.0	1.0000	1.0000	1.0000	1.0000	1.0000
Mean	0.9999	1.0000	1.0	0.9984	0.9992	0.9992	0.9992	0.9997
Std	0.0002	0.0001	0.0	0.0048	0.0024	0.0025	0.0025	0.0010

The confusion matrix of the final stacking classifier for testing and total (train and test), respectively, are: $\left(\begin{smallmatrix}11860 & 1\\ 0 & 567\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}23663 & 1\\ 0 & 1191\end{smallmatrix}\right)$. As seen in these two, only one session was found near signatures but not detected by them. Also, the accuracy is almost 100%. These results are reasonable as signatures in this thesis are simple and computationally cheap. However, in real-world charging sites, more complex signatures should be determined; thus, the supervised machine-learning technique will detect more sessions. So far, we have only detected signature-based anomalies using rules and machine learning models. However, many malicious or anomaly sessions may not be detected using rules. To this end, in the next section, unsupervised machine learning or anomaly detection techniques are developed and discussed.

5.6 Unsupervised Anomaly Based Detection

In real-world scenarios and charging sites, adversaries are challenging to detect with only rules. Thus, an unsupervised anomaly detector is required. To this end, in this section, we will study and apply anomaly detectors and find the best model for our current framework with ACN data. Like supervised learning, unsupervised learning also depends on the dataset and behaviors of the charging site. Hence, the best model for ACN data may be less accurate for other datasets, but the steps remain the same.

5.6.1 Pre Processing

Preprocessing for anomaly detection is similar to preprocessing for supervised detection, except for two new tricks. Here first, we omitted the column label and rule (targets of supervised learning), so our model learns the feature space without the actual output. Second, we have grouped three duration columns, including deltaConnectionDisconnet, deltaConnectionDone, and deltaDisconnetDone, and two columns of t-arrival and t-departure. Grouping means that in addition to the columns, we have added a few columns by calculating the statistical relations of the group, such as group minimum, maximum, mean, mode, and standard deviation. Grouping duration features can help the model learn more about these critical features because they have the most impact on finding an anomaly. Other preprocessing steps are the same as Table 5.4.

5.6.2 Unsupervised Models or Anomaly Detectors

The main difference between supervised and unsupervised techniques is that in supervised, we had the label column to evaluate the models' performance. In anomaly detectors, we cannot use the label column. Thus, it is more challenging to evaluate models and compare them. However, we can use the labels we had to tune our

anomaly detectors for better predictions.

Each model learns to detect anomalies in ACN data. The training starts with Random Grid Search to find the most efficient model's parameters. Then, using the best parameters, the model detects all the anomalies. So, each model detects some anomalies, but a measurement of which model did the best needs to be made more explicit. Since we already know some anomalies using rule-based and supervised models, we will use them as a measurement unit. The model that detects most of the already detected sessions is probably the best. This trick can narrow the model choice to only a few good models. However, there are better solutions than this measurement because anomaly detectors' main goal is to detect unknown sessions, not ones already malicious. Therefore, we use this trick for the first improvement to find the best model. Table 5.7 shows various models and their detection performance when results are compared to rule-based malicious sessions.

Table 5.7: Results of comparing anomaly detectors with rule-based detected sessions results

Name	precision	recall	f1-score	f2-score	accuracy	Kappa	MCC
Angle-base Outlier Detection	0.52	0.59	0.26	0.269	0.29	0.022	0.086
Clustering-Based Local Outlier	**0.59**	**0.77**	**0.61**	**0.670**	**0.86**	**0.252**	**0.310**
Connectivity-Based Local Outlier	0.57	0.59	0.58	0.585	0.91	0.156	0.158
Isolation Forest	**0.54**	**0.71**	**0.43**	**0.449**	**0.55**	**0.076**	**0.175**
Histogram-based Outlier Detection	**0.58**	**0.85**	**0.57**	**0.642**	**0.77**	**0.217**	**0.336**
K-Nearest Neighbors Detector	0.52	0.56	0.20	0.215	0.21	0.014	0.072
Local Outlier Factor	0.52	0.52	0.11	0.146	0.11	0.004	0.040
One-class SVM detector	**0.55**	**0.74**	**0.51**	**0.553**	**0.70**	**0.130**	**0.223**

The second step of fine-tuning is to decrease the distance of anomalies found in anomaly detectors to those detected in rule-based detection to find the best anomaly detector. In this step, models learn to detect malicious sessions that are more similar to the rule-based detection ones. So far, we have found a couple of good models, but tuning them in an extra step can determine the best one. We developed two leading solutions for this extra step as follows:

- The first method is to use a supervised model such as the Decision Tree Classifier

on top of the anomaly detector to tune the anomaly score of the anomalies so that the anomaly detector optimizes a certain parameter such as Kappa. Cohen's kappa evaluation metric is used here for optimization as it assesses the agreement of two values, and it is a perfect metric for unbalanced data such as anomaly detection [147]. Hence, a higher Kappa value means a higher number of correct anomalies, while the number of correct non-anomaly sessions is also high. This optimization can lead the model to detect only those previously detected anomalies in rule-based detection. Even though this optimization can be helpful, it may increase the total number of anomalies not detected in the rule-based, and the model will have bad precision, thus a bad F2 score. This solution may not be helpful in real-world charging sites as it detects rule-based anomalies rather than unknown ones.

- The second method is to tune the anomaly score factor of the models so that models detect most of the true anomalies while preserving other critical unknown anomalies. In other mathematical words, we want to optimize our model to have a good number of true positives (correct anomalies) while preserving a value for false positives. In this method, our models detect rule-based anomalies and some unknown anomalies that could not be detected using thresholds. Plotting the number of detected anomaly sessions based on an anomaly score threshold can provide valuable information for this approach.

Figure 5.11 shows the results of applying both techniques to tune the four anomaly detectors selected from Table 5.7. To better demonstrate the difference, below is the confusion matrix of the same anomaly detector for both solutions:

- Isolation Forest: Confusion matrix of method 1: $\left(\begin{smallmatrix} 6150 & 17514 \\ 56 & 1135 \end{smallmatrix}\right)$ and Confusion matrix of method 2: $\left(\begin{smallmatrix} 22361 & 1303 \\ 555 & 636 \end{smallmatrix}\right)$

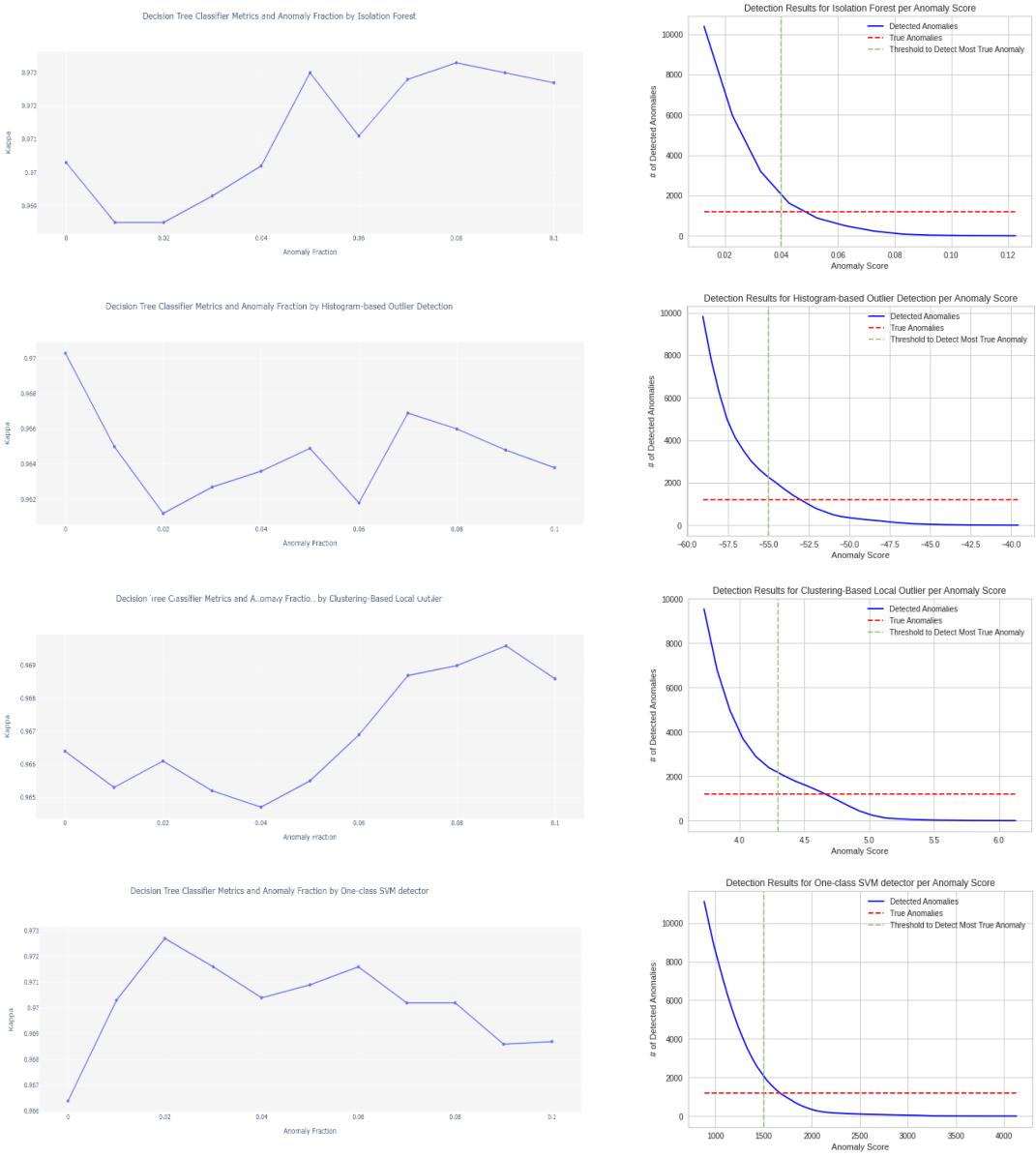

Figure 5.11: Column one shows the tuning results of method 1, and column two shows the tuning results of method 2 for four models Isolation Forest, Histogram-based Outlier Detection, Clustering-Based Local Outlier Detection, and One-class SVM Detector

- Histogram-based Outlier Detection: Confusion matrix of method 1: $\begin{pmatrix} 18002 & 5662 \\ 69 & 1122 \end{pmatrix}$ and Confusion matrix of method 2: $\begin{pmatrix} 22258 & 1406 \\ 327 & 864 \end{pmatrix}$

- Clustering-Based Local Outlier Detection: Confusion matrix of method 1: $\begin{pmatrix} 10162 & 13502 \\ 76 & 1115 \end{pmatrix}$ and Confusion matrix of method 2: $\begin{pmatrix} 22079 & 1585 \\ 611 & 580 \end{pmatrix}$

- One-class SVM Detector: Confusion matrix of method 1: $\begin{pmatrix} 20573 & 3091 \\ 537 & 654 \end{pmatrix}$ and Confusion matrix of method 2: $\begin{pmatrix} 22057 & 1607 \\ 712 & 479 \end{pmatrix}$

By looking at the confusion matrices, the second method has better anomalies. Even though the first method detects more known anomalies from the rule-based step, the number of false positives is so high that it may not be as practical and efficient in real-world charging sites. Also, detecting known anomalies is not a concern here, but detecting good unknown anomalies is essential. With method 2 set as the leading solution and comparing all four models' results, Histogram-based Outlier Detection outperforms other models. It was expected as the rules for this dataset are simple and threshold-based, so histograms can detect more of those rules and, therefore, better anomalies.

Using this information, we took Histogram-based Outlier Detection as our best-unsupervised model and Decision Tree as our best-supervised model. So far, we have detected threshold anomalies and unknown anomalies using machine learning. However, detecting a session as an anomaly may not be as valuable as detecting the type of anomaly. Thus, we have to detect the anomaly or malicious feature of the anomalous session. Finding the cause of anomalies is the primary goal of the final step.

5.7 Anomaly Sessions Root Cause Analysis

This section aims to detect the types of anomalies for each detected unknown (anomaly) session. Although several factors may cause a session anomaly, the rule-based detection section established some general rules and factors. Here, we classify each anomaly session based on the five rules we had before, as in Table 5.3. Each malicious session can correspond to more than one rule. We consider all possible classes based on Table 5.3 to find the cause of the detected session.

The benefit of this section is extracting the main factors that make a session anomalous. However, we only know the rules for sessions detected in rule-based/supervised machine learning sections. Therefore, we present two new solutions to detect the causes of unknown anomalies: semi-supervised learning and clustering. Each method requires tuning and testing, and like other sections, we compare various models to find the best one after discussing the preprocessing steps.

5.7.1 Pre Processing

Before developing the approaches, first, we have to combine the results from the anomaly detector and the supervised detector. All sessions, whether detected by rules, by the stacking supervised classifier, or by the Histogram-Based Outlier Detector, are combined. Some anomalies detected by the anomaly detector were already present in malicious sessions detected by rule-based methods. After combining the data (hereafter, we call it malicious sessions), there are 2733 anomaly sessions, 1192 sessions detected by rule-based methods, and 2270 sessions detected by the anomaly detector. Then, all preprocessing methods, the same as in the anomaly detection section, are applied to the combined data 5.6.1.

5.7.2 Anomaly Cause Detection

This section aims to develop two approaches, clustering and semi-supervised to detect a cause for each malicious session. We want to find the causes of unknown sessions while the causes of rule-based detections are known. The two approaches are as follows:

(a) **Clustering Approach:** This method aims to cluster all malicious sessions into groups. Each group clusters the known causes and labels the cluster with the same cause that appears most frequently. Three metrics are used to tune

the clustering and compare different methods, including Silhouette, Calinski-Harabasz (CH) [288], and Davies-Bouldin (DB) [28]. The silhouette shows how coherent the clusters are, the CH index shows cluster cohesion and separation, and the DB index shows the ratio of within-cluster and between-cluster distances. Also, the "least mistake" approach helps to fine-tune the best parameter in a model. While the CH and DB indexes help to find the optimum number of clusters, the number of false predictions helps to have more accurate labels for clusters. According to Table 5.3, there are classes with rare data that make clustering inaccurate and difficult to find a cluster containing only a single cause. In real-world charging sites, however, there will be more data and more classes as new rules apply, thus indicating better and more robust results through clustering. We compare four different clustering algorithms with different numbers of clusters for ACN data using the mentioned metrics. The results of the algorithms are shown in Table 5.8. According to this table, K-means with six clusters outperformed other methods. Also, by increasing the number of clusters, our metrics drop significantly. Therefore, six clusters would be an optimum value for our current anomalies. It is important to note that even though K-means with five clusters have better metrics than six clusters, mapping each cluster to a single cause was impossible, meaning many of the clusters grouped many known anomalies and the group could not be assigned only to one cause. Then, the unknown anomalies are clustered using the fine-tuned K-means, and Table 5.9 shows the number of anomalies in each cluster and the cause that occurred most frequently in the cluster.

(b) **Semisupervised Approach:** This approach uses a semi-supervised technique to predict the causes of anomalies using the known ones. First, we split the data into sessions with known causes (rule-based detection anomalies) and sessions with unknown causes (anomaly detection). Second, we divide the unknown

Table 5.8: Results of comparing clustering algorithms in clustering approach

Model	# False Predict	# Correct Predict	Silhouette	Calinski-Harabasz	Davies-Bouldin
Kmeans 4 Cluster	655	536	0.2249	267.9087	1.6063
Kmeans 5 Cluster	293	898	0.212	245.2776	1.7284
Kmeans 6 Cluster	**282**	**909**	**0.2198**	**230.6596**	**1.7141**
KModes 4 Cluster	240	951	0.104	115.7549	2.8671
KModes 5 Cluster	258	933	0.067	83.3724	3.6326
KModes 6 Cluster	252	939	0.0331	72.189	4.0891
Affinity Propagation 4 Cluster	1131	60	0.1045	48.1669	2.0096
Affinity Propagation 5 Cluster	1111	80	0.1045	48.1669	2.0096
Affinity Propagation 6 Cluster	1088	103	0.1045	48.1669	2.0096
Birch Clustering 4 Cluster	281	910	0.2068	251.5421	1.5611
Birch Clustering 5 Cluster	269	922	0.1975	223.4931	1.9244
Birch Clustering 6 Cluster	269	922	0.2026	214.8367	1.7804

Table 5.9: Final root causes results for anomaly-based detection sessions step in clustering approach

Cluster Number	Cluster 0	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5
Related Class (Most Occurring)	behaviour	Arrival Duration	behaviour Energy	duration	arrival	waste duration
# of Anomalies in Predicted in Cluster	234	220	319	125	532	112

sessions into three equal-sized folds and the known sessions into a 50%-50% split as train and validation data. The goal is to use the train data to train a classifier and predict one fold at a time of unknown sessions. Then, by combining the results of the predicted fold with train data, new train data emerges. The model predicts each fold and adds it to the last train data until the last fold. Models are then evaluated using the test data, which was 50% of the known sessions, with the same metrics as the supervised machine learning step. After training the final best model, it predicts all unknown sessions to determine the cause of individual anomaly sessions. This approach is more robust than clustering because our rules and sessions are limited. To improve the model's performance, and before predicting the folds using the initial train and test dataset, each model is trained using a random grid search method to find the best set of parameters. Likewise, the model is trained using the same grid search algorithm with five cross-validation folds before predicting each fold. Table 5.10 shows the comparison of models according to the above techniques. The table

shows that the decision tree classifier is the most efficient model for determining causes. Using a decision tree trained by a random grid search algorithm, the final causes for each unknown session are determined, as shown in Table 5.11.

Table 5.10: Results of comparing models in semisupervised approach

Model	Accuracy	Recall	Prec.	F1	Kappa	MCC	F2	TT (Sec)
Decision Tree Classsifier	**0.969748**	**0.810662**	**0.823005**	**0.812048**	**0.959400**	**0.959452**	**0.810034**	**0.113578**
K Nearest Neighbors	0.850420	0.386704	0.500873	0.416947	0.793998	0.796120	0.396002	0.773318
Random Forest Classifier	0.927731	0.548422	0.730960	0.587103	0.902268	0.903061	0.559140	1.578444
Gradient Boosting Classifier	0.939496	0.644615	0.659692	0.644404	0.918532	0.918795	0.643345	34.074160
Ada Boosting Classifier	0.662185	0.474389	0.430948	0.438101	0.548035	0.606733	0.455346	1.147373
Ridge Classifier	0.818487	0.245015	0.265390	0.242386	0.742810	0.750839	0.242487	0.135272
Logistic Regression	0.894118	0.465787	0.497115	0.473801	0.856324	0.857021	0.467611	0.754193
Support Vector Classifier	0.867227	0.327590	0.412537	0.341078	0.814921	0.822255	0.330540	0.445055
Gaussian Naive Bayes	0.393277	0.320400	0.298596	0.250337	0.295463	0.324865	0.268514	0.062385

Table 5.11: Final root causes results for anomaly-based detection sessions step in semisupervised approach

Class Name	arrival	arrival behaviour	behaviour	duration	duration arrival
Anomalies in Class	832	22	472	164	51

Although both methods can be effective, the semi-supervised approach is more robust in real-time cases where new rules and, thus, new anomalies are detected every day. Additionally, even though there are more rule-based detection classes, the models predicted fewer classes due to limited data. However, more data can result in more accurate causes in real-world scenarios. This SIEM-like framework which provides anomalous sessions with a possible cause of the anomaly can be critical for charging site owners to provide trustworthy EVSEs and will help the mass adoption of EVs by maintaining secure charging for users. However, this framework only considers features related to sessions and ignores individual users, habits, charging site loads, etc.

5.8 Concluding Remarks

The mass adoption of EVs requires secure EVSEs in various locations and safe EVs. Due to the rapid growth of EV usage and the cyber-physical nature of EVs and EVSEs, security and privacy issues have emerged. Previous research has identified gaps and vulnerabilities in EVs and EVSEs, highlighting the need for a more secure ecosystem. this thesis utilized the generic structure for EVs and EVSEs, as well as an EV-EVSE ecosystem architecture proposed in previous chapters, to address an ongoing security challenge: charging session monitoring. The ecosystem provided insights into the security gaps in the system, and in this chapter, we focus on filling one of these gaps.

Therefore, an intelligent monitoring framework is proposed to demonstrate the usage and importance of the proposed ecosystem architecture and risk assessment. The framework includes charging site and session behavior profiling, rule-based detection, supervised model development, anomaly detection, and anomaly root cause detection to enhance the security of charging sessions. The framework is evaluated using ACN charging session data, highlighting its significance in providing a more secure charging environment. The proposed ecosystem architecture can be utilized to develop more specific solutions for each component or be adopted for other use cases. Meanwhile, the monitoring framework, as a security solution for charging, can assist charge site owners in providing a secure environment for their users. Researchers can adopt the proposed framework to secure charging sites or explore the idea of combining the previous architecture and risk assessment to address other security gaps in this system. In the next chapter and future work, we will discuss additional possibilities for studies that can be conducted using this combination.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

EVs and EVSEs are two crucial components in the revolutionary shift toward a more sustainable future in transportation. EVs, powered by rechargeable batteries instead of conventional fuels, provide a significant solution to reduce carbon emissions, noise pollution, and dependence on non-renewable resources. On the other hand, EVSEs, the charging infrastructure, act as the critical enablers of this sustainable transition by providing the necessary power supply. They range from home charging units to public charging stations and fast charging networks, ensuring the smooth operation of EVs and offering flexibility and convenience to users. As the use of EVs increases daily and the economic benefits become more apparent, countries are investing heavily in this technology to make it widely available, safe, and secure. Some nations are even banning the manufacturing of conventional vehicles to address the scarcity and rising costs of fossil fuels.

Among the various challenges facing the mass adoption of EVs, one of the most critical is the issue of cybersecurity, an area receiving increasingly more attention. As we continue to witness the advancement of hacking techniques and the proliferation

of cybercriminals, the cybersecurity vulnerabilities inherent in EVs and EVSEs pose substantial risks. The potential compromise of these cyber-physical systems could endanger not only the passengers within the EVs but also pedestrians and other road users, with possible consequences extending to disrupting traffic systems or causing wide-ranging power outages. Recognizing these significant threats, researchers and industry professionals have started to delve deeper into the vulnerabilities of EVs and EVSEs, launching investigations into possible solutions to secure them.

Moreover, the advancement in the IoT has given birth to the IoV. EVs are now equipped to communicate with a multitude of entities on the road, including other vehicles, pedestrians, road sensors, and networks. This comprehensive network of interactions has spurred the rise of V2X-enabled ICVs. While the emergence of IoVs can address many previous vehicle challenges, it simultaneously introduces new ones, particularly an increase in potential cybersecurity threats. Further complicating the landscape is the rapid rise of AI and ML models, which are paving the way for autonomous vehicles. These vehicles are designed to operate without human drivers and are capable of sophisticated perception, planning, and control. The introduction of newly manufactured connected autonomous vehicles introduces a host of technical and security challenges to nations. These range from threats to smart grid infrastructure and breaches of privacy to a plethora of other security concerns. Moreover, as software becomes increasingly integrated into EVs and EVSEs to enhance customer service and improve operational efficiency, new vulnerabilities emerge. These include potential software vulnerabilities that could be exploited through hacking.

As a result, the need for comprehensive security analysis and robust cybersecurity measures for EVs and EVSEs has grown increasingly urgent. This thesis undertakes an extensive survey of the existing literature to extract the threats, challenges, and vulnerabilities inherent in the EV-EVSE ecosystem. Our objective is to address the gaps in the comprehensive security analysis present in earlier works by introducing

a new architecture, a risk framework, and an implementation use case—intelligent charging session monitoring. In the subsequent sections, we summarize our findings from each chapter and provide insights for future reference. Our overarching aim is to enrich the understanding of cybersecurity in the context of the EV infrastructure, thereby contributing to the development of a safer and more secure system for what promises to be the future of transportation. In future works of this thesis, we identify some security gaps and challenges that can be analyzed using the ideas and frameworks in this thesis.

In Chapter 2, we extensively explored prior research to uncover the key challenges, vulnerabilities, and components of EVs and EVSEs. We identified five primary security aspects: charging station security, information privacy, software security, connected vehicle security, and autonomous vehicle security. Our deep dive into the literature revealed a critical gap—the absence of comprehensive risk assessments that fully catalog and rank vulnerabilities based on their likelihood and impact. Using previous works, we identified generic EVs and EVSEs designs, and we discovered a significant security issue—the need for effective monitoring of charging sessions. Our proposed risk framework and architecture for EVs and EVSEs helped to identify this and various other overlooked security issues. This literature review forms the foundational bedrock upon which we developed our security solutions in subsequent chapters of this thesis.

Chapter 3 introduces a Data Flow Diagram of the EV-EVSE ecosystem. In this chapter, we analyze the major entities in this system, including the EV, EV service provider, EVSE, EVSE service provider, cloud, and smart grid. We meticulously detail all data flows, protocols, and data types that can be communicated within this system, and identify power flows and internal communications of EVs and EVSEs, building on NIST studies and our literature review. This architecture allows us to identify numerous security gaps that have often been overlooked in other studies. Pre-

vious research typically focuses on a single component or player within this ecosystem. However, our proposed architecture facilitates the identification of security requirements and gaps for future reference. One such gap is the need for intelligent charging session monitoring, which is a focal point of this thesis. We also discuss several of these gaps as potential areas for future study.

Upon proposing an architecture for the ecosystem, we recognized the necessity for a comprehensive security assessment of this system, with the goal of identifying all possible attacks and challenges. Chapter 4 discusses our proposed risk assessment framework for EVs and EVSEs. We developed criteria for evaluating the impact and likelihood of attacks and categorized EVs into five security aspects: charging station security, information privacy, software security, connected vehicle security, and autonomous vehicle security. Within each aspect, we pinpointed several attack surfaces where intruders could target. For each of these, we identified specific attack subsurfaces that attackers could exploit, vulnerabilities they could leverage, potential challenges and attacks posed to the system, and countermeasures for each of these attacks. We also identified STRIDE threats in each subsurface, alongside our criteria for evaluating impact, likelihood, and risk. We demonstrated the efficacy of our framework by applying it to eight different real-world attack scenarios where EVs were targeted and compromised by researchers or adversaries. This framework underscores the importance of exploring all possible attacks and challenges in this system for future studies.

Chapter 5 serves as a practical use case of the interplay between Chapters 3 and 4. Leveraging our proposed ecosystem architecture, we identified a security gap, monitoring charging sessions, and used our risk framework to extract possible challenges and attacks targeting EVSEs and charging sites. As a result, we proposed an intelligent charging session monitoring framework that employs machine learning techniques and a well-known security mechanism, SIEM. In this chapter, we introduced a five-

step framework comprising behavior analysis, rule-based detection, supervised-based detection, anomaly-based detection, and root cause analysis. This monitoring scheme enables the identification of fraudulent or malicious charging sessions at any charging site and potentially elucidates the reason for their malicious classification. Charging site owners and EVSE service providers can adopt this technique to significantly enhance the security of their charging stations.

6.2 Future Works

In this section, we discuss two main future directions of this work and how other researchers can continue studying the security of EV-EVSE systems using the proposed architecture and risk framework. We also address a critical aspect of the system that was not discussed earlier and will be a future point for this thesis.

6.2.1 EV-EVSE Universal Monitoring Framework:

In this thesis, we proposed an EV-EVSE ecosystem architecture showing all the data flows and protocols based on surveying other papers. Based on that, we proposed a charging session monitoring framework that monitors only one of the data flows, number 32 in Figure 3.1. However, it is not the only data flow that requires monitoring. For instance, monitoring any of the EV CAN bus data (number 8), EV communication data (numbers 21 and 22), EV assistant driver (number 10), EVSE telematics, and EVSE-EV charging and battery part can provide much valuable security information and prevent or mitigate attacks such as EV malfunction, charging malfunction, and EV or EVSE remote and network attacks. The authors aim to adopt the monitoring framework for other parts of the ecosystem to achieve a comprehensive universal monitoring framework for the EV-EVSE system. Although some of these parts are covered in other studies, such as intrusion detection systems for CAN bus

or security mechanisms [58, 265, 297], a universal monitoring framework can cover all the sections and can be the future of EV-EVSE security. Researchers can adopt and use the proposed EV-EVSE architecture to fill the security gaps in this ecosystem.

6.2.2 Public Key Infrastructure:

The system's privacy is one part of the EV-EVSE architecture we did not discuss enough. EVs establish handshakes with EVSEs when charging, and almost all current protocols use TLS for secure communication, which means it requires mutual key exchange and authentication. However, privacy is not limited to charging. EVs communicate with the cloud, EV vendor, other vehicles, drivers, and EVSEs communicate with the smart grid, EVSE vendor, other EVSEs, and management buildings. These extensive data exchanges require privacy analysis to maintain and separate personal and sensitive information from insensitive ones. Therefore, both EVs and EVSEs require authentication, encryption, and private message-sharing mechanisms. Even the charging session monitoring framework proposed in this thesis can use users' data and habits, which indicates that protecting users' privacy should also be part of the framework. All these points highlight the need for a standard and comprehensive PKI. Although some studies are working on privacy mechanisms and information-sharing solutions for EVs and EVSEs, such as [22, 190, 237], and some others have started to work on a general PKI, such as [132, 316], a standard general PKI solution that supports all communications, such as V2X, V2G, EV charging, and EVSE communications, is still missing. A crucial future work of this thesis is to determine the parts where privacy is required and add privacy solutions to the proposed framework. This extended monitoring framework can then be adopted to use users' data or applied to other EV-EVSE ecosystem sections.

Bibliography

[1] 3GPP TS 36.300, *Evolved universal terrestrial radio access (e-utra) and evolved universal terrestrial radio access network (e-utran); overall description; stage 2*, (2011).

[2] Khadige Abboud, Hassan Aboubakr Omar, and Weihua Zhuang, *Interworking of dsrc and cellular network technologies for v2x communications: A survey*, IEEE transactions on vehicular technology **65** (2016), no. 12, 9457–9470.

[3] Eslam G AbdAllah, Mohammad Zulkernine, Yuan Xiang Gu, and Clifford Liem, *Towards defending connected vehicles against attacks*, Proceedings of the Fifth European Conference on the Engineering of Computer-Based Systems, 2017, pp. 1–9.

[4] Samrat Acharya, Yury Dvorkin, Hrvoje Pandžić, and Ramesh Karri, *Cybersecurity of smart electric vehicle charging: A power grid perspective*, IEEE Access **8** (2020), 214434–214453.

[5] Samrat Acharya, Robert Mieth, Ramesh Karri, and Yury Dvorkin, *False data injection attacks on data markets for electric vehicle charging stations*, Advances in Applied Energy **7** (2022), 100098.

[6] Feyijimi Adegbohun, Annette Von Jouanne, and Kwang Y Lee, *Autonomous battery swapping system and methodologies of electric vehicles*, Energies **12** (2019), no. 4, 667.

[7] Simon Adhanom and David Coffin, *Electric vehicle supply equipment (evse) in the united states*, Office of Industries, US International Trade Commission, 2022.

[8] Raziye Aghapour, Mehdi Zeraati, Farkhondeh Jabari, Mohammadreza Sheibani, and Hamidreza Arasteh, *Cybersecurity and data privacy issues of electric vehicles smart charging in smart microgrids*, Electric Vehicle Integration via Smart Charging: Technology, Standards, Implementation, and Applications, Springer, 2022, pp. 85–110.

[9] Anchal Ahalawat, Sridhar Adepu, and Joseph Gardiner, *Security threats in electric vehicle charging*, 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), IEEE, 2022, pp. 399–404.

[10] M Nadeem Ahangar, Qasim Z Ahmed, Fahd A Khan, and Maryam Hafeez, *A survey of autonomous vehicles: Enabling communication technologies and challenges*, Sensors **21** (2021), no. 3, 706.

[11] Aiman Al-Sabaawi, Khamael Al-Dulaimi, Ernest Foo, and Mamoun Alazab, *Addressing malware attacks on connected and autonomous vehicles: recent techniques and challenges*, Malware Analysis Using Artificial Intelligence and Deep Learning (2021), 97–119.

[12] Manar Alanazi, Abdun Mahmood, and Mohammad Jabed Morshed Chowdhury, *Scada vulnerabilities and attacks: A review of the state-of-the-art and open issues*, Computers & Security (2022), 103028.

[13] Ahmed Abdu Alattab, Reyazur Rashid Irshad, Anwar Ali Yahya, and Amin A Al-Awady, *Privacy protected preservation of electric vehicles' data in cloud computing using secure data access control*, Energies **15** (2022), no. 21, 8085.

[14] Cristina Alcaraz, Javier Lopez, and Stephen Wolthusen, *Ocpp protocol: Security threats and challenges*, IEEE Transactions on Smart Grid **8** (2017), no. 5, 2452–2459.

[15] Bako Ali and Ali Ismail Awad, *Cyber and physical security vulnerability assessment for iot-based smart homes*, sensors **18** (2018), no. 3, 817.

[16] Mazhar Ali, Samee U Khan, and Athanasios V Vasilakos, *Security in cloud computing: Opportunities and challenges*, Information sciences **305** (2015), 357–383.

[17] Nadiah M Almutairy, Khalil HA Al-Shqeerat, and Husam Ahmed Al Hamad, *A taxonomy of virtualization security issues in cloud computing environments*, Indian Journal of Science and Technology **12** (2019), no. 3, 1–19.

[18] Aljawharah Alnasser, Hongjian Sun, and Jing Jiang, *Cyber security challenges and solutions for v2x communications: A survey*, Computer Networks **151** (2019), 52–67.

[19] Arwa Alromih, John A Clark, and Prosanta Gope, *A privacy-preserving energy theft detection model for effective demand-response management in smart grids*, arXiv preprint arXiv:2303.13204 (2023).

[20] Marica Amadeo, Claudia Campolo, and Antonella Molinaro, *Information-centric networking for connected vehicles: a survey and future perspectives*, IEEE Communications Magazine **54** (2016), no. 2, 98–104.

[21] Mani Amoozadeh, Arun Raghuramu, Chen-Nee Chuah, Dipak Ghosal, H Michael Zhang, Jeff Rowe, and Karl Levitt, *Security vulnerabilities of connected vehicle streams and their impact on cooperative driving*, IEEE Communications Magazine **53** (2015), no. 6, 126–132.

[22] Joseph Antoun, Mohammad Ekramul Kabir, Bassam Moussa, Ribal Atallah, and Chadi Assi, *A detailed security assessment of the ev charging ecosystem*, IEEE Network **34** (2020), no. 3, 200–207.

[23] Souhila Aoufi, Abdelouahid Derhab, and Mohamed Guerroumi, *Survey of false data injection in smart power grid: Attacks, countermeasures and challenges*, Journal of Information Security and Applications **54** (2020), 102518.

[24] Hala Assal and Sonia Chiasson, *Security in the software development lifecycle*, Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018), 2018, pp. 281–296.

[25] Man Ho Au, Joseph K Liu, Junbin Fang, Zoe L Jiang, Willy Susilo, and Jianying Zhou, *A new payment system for enhancing location privacy of electric vehicles*, IEEE transactions on vehicular technology **63** (2013), no. 1, 3–18.

[26] Omid Avatefipour and Hafiz Malik, *State-of-the-art survey on in-vehicle network communication (can-bus) security and vulnerabilities*, arXiv preprint arXiv:1802.01725 (2018).

[27] Ponnuru Raveendra Babu, Ruhul Amin, Alavalapati Goutham Reddy, Ashok Kumar Das, Willy Susilo, and YoungHo Park, *Robust authentication protocol for dynamic charging system of electric vehicles*, IEEE Transactions on Vehicular Technology **70** (2021), no. 11, 11338–11351.

[28] Chayan Bala, Tripti Basu, and Abhijit Dasgupta, *Automatic detection of k with suitable seed values for classic k-means algorithm using de*, 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, 2015, pp. 759–765.

[29] Gianmarco Baldini, *Detection of cybersecurity spoofing attacks in vehicular networks with recurrence quantification analysis*, Computer Communications **191** (2022), 486–499.

[30] Kaibin Bao, Hristo Valev, Manuela Wagner, and Hartmut Schmeck, *A threat analysis of the vehicle-to-grid charging protocol iso 15118*, Computer Science-Research and Development **33** (2018), no. 1, 3–12.

[31] Manoj Basnet, Subash Poudyal, Mohd Hasan Ali, and Dipankar Dasgupta, *Ransomware detection using deep learning in the scada system of electric vehicle charging station*, 2021 IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America), IEEE, 2021, pp. 1–5.

[32] Mohan Bharathidasan, V Indragandhi, Vishnu Suresh, Michał Jasiński, and Zbigniew Leonowicz, *A review on electric vehicle: Technologies, energy trading, and cyber security*, Energy Reports **8** (2022), 9662–9685.

[33] Narayan Bhusal, Mukesh Gautam, and Mohammed Benidris, *Cybersecurity of electric vehicle smart charging management systems*, 2020 52nd North American Power Symposium (NAPS), IEEE, 2021, pp. 1–6.

[34] Zoleikha Abdollahi Biron, Satadru Dey, and Pierluigi Pisu, *Real-time detection and estimation of denial of service attack in connected vehicle systems*, IEEE Transactions on Intelligent Transportation Systems **19** (2018), no. 12, 3893–3902.

[35] Rebecca M Blank, *Nist special publication (sp) 800-30 revision 1, guide for conducting risk assessments*, (2011).

[36] Rohit Bohara, Mirko Ross, Sven Rahlfs, and Sara Ghatta, *Cyber security and software update management system for connected vehicles in compliance*

with unece wp. 29, r155 and r156, Software Engineering 2023 Workshops, Gesellschaft für Informatik eV, 2023.

[37] Stuart A Boyer, *Scada: supervisory control and data acquisition*, International Society of Automation, 2009.

[38] Mehmet Bozdal, Maulana Randa, Mohammad Samie, and Ian Jennions, *Hardware trojan enabled denial of service attack on can bus*, Procedia Manufacturing **16** (2018), 47–52.

[39] Mehmet Bozdal, Mohammad Samie, Sohaib Aslam, and Ian Jennions, *Evaluation of can bus security challenges*, Sensors **20** (2020), no. 8, 2364.

[40] Benedikt Brecht and Thorsten Hehn, *A security credential management system for v2x communications*, Connected Vehicles, Springer, 2019, pp. 83–115.

[41] Alessandro Brighente, Mauro Conti, Denis Donadel, and Federico Turrin, *Evscout2. 0: electric vehicle profiling through charging profile*, ACM Transactions on Cyber-Physical Systems (2021).

[42] Richard Brown, Alex Marti, Chris Jenkins, and Susmit Shannigrahi, *Dynamic address validation array (dava) a moving target defense protocol for can bus*, Proceedings of the 7th ACM Workshop on Moving Target Defense, 2020, pp. 11–19.

[43] Christian Buckl, Alexander Camek, Gerd Kainz, Carsten Simon, Ljubo Mercep, Hauke Stähle, and Alois Knoll, *The software car: Building ict architectures for future electric vehicles*, 2012 IEEE International Electric Vehicle Conference, IEEE, 2012, pp. 1–8.

[44] Till Bunsen, Pierpaolo Cazzola, Marine Gorner, Leonardo Paoli, Sacha Scheffer, Renske Schuitmaker, Jacopo Tattini, and Jacob Teter, *Global ev outlook 2018: Towards cross-modal electrification*, (2018).

[45] Lisa Calearo, Mattia Marinelli, and Charalampos Ziras, *A review of data sources for electric vehicle integration studies*, Renewable and Sustainable Energy Reviews **151** (2021), 111518.

[46] Sean Campbell, Niall O'Mahony, Lenka Krpalcova, Daniel Riordan, Joseph Walsh, Aidan Murphy, and Conor Ryan, *Sensor technology in autonomous vehicles: A review*, 2018 29th Irish Signals and Systems Conference (ISSC), IEEE, 2018, pp. 1–4.

[47] Yue Cao, Houbing Song, Omprakash Kaiwartya, Bingpeng Zhou, Yuan Zhuang, Yang Cao, and Xu Zhang, *Mobile edge computing for big-data-enabled electric vehicle charging*, IEEE Communications Magazine **56** (2018), no. 3, 150–156.

[48] Yulong Cao, Ningfei Wang, Chaowei Xiao, Dawei Yang, Jin Fang, Ruigang Yang, Qi Alfred Chen, Mingyan Liu, and Bo Li, *Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks*, 2021 IEEE Symposium on Security and Privacy (SP), IEEE, 2021, pp. 176–194.

[49] Tomislav Capuder, Danijela Miloš Sprčić, Davor Zoričić, and Hrvoje Pandžić, *Review of challenges and assessment of electric vehicles integration policy goals: Integrated risk analysis approach*, International journal of electrical power & energy systems **119** (2020), 105894.

[50] Paul Carsten, Todd R Andel, Mark Yampolskiy, and Jeffrey T McDonald, *In-vehicle networks: Attacks, vulnerabilities, and proposed solutions*, Proceedings

of the 10th Annual Cyber and Information Security Research Conference, 2015, pp. 1–8.

[51] Samarjit Chakraborty, Martin Lukasiewycz, Christian Buckl, Suhaib Fahmy, Naehyuck Chang, Sangyoung Park, Younghyun Kim, Patrick Leteinturier, and Hans Adlkofer, *Embedded systems and software challenges in electric vehicles*, 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE, 2012, pp. 424–429.

[52] Keith Chamberlain and Salah Al-Majeed, *Standardisation of uk electric vehicle charging protocol, payment and charge point connection*, World Electric Vehicle Journal **12** (2021), no. 2, 63.

[53] Raghu Changalvala and Hafiz Malik, *Lidar data integrity verification for autonomous vehicle*, IEEE Access **7** (2019), 138018–138031.

[54] Anupam Chattopadhyay, Kwok-Yan Lam, and Yaswanth Tavva, *Autonomous vehicle: Security by design*, IEEE Transactions on Intelligent Transportation Systems **22** (2020), no. 11, 7015–7029.

[55] Hina Chaudhry and Theodore Bohn, *Security concerns of a plug-in vehicle*, 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), IEEE, 2012, pp. 1–6.

[56] Shang-Tse Chen, Cory Cornelius, Jason Martin, and Duen Horng Polo Chau, *Shapeshifter: Robust physical adversarial attack on faster r-cnn object detector*, Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Springer, 2018, pp. 52–68.

[57] Shanzhi Chen, Jinling Hu, Yan Shi, Ying Peng, Jiayi Fang, Rui Zhao, and Li Zhao, *Vehicle-to-everything (v2x) services supported by lte-based systems and 5g*, IEEE Communications Standards Magazine **1** (2017), no. 2, 70–76.

[58] Kun Cheng, Yuebin Bai, Yuan Zhou, Yun Tang, David Sanan, and Yang Liu, *Caneleon: Protecting can bus with frame id chameleon*, IEEE Transactions on Vehicular technology **69** (2020), no. 7, 7116–7130.

[59] Abraham A Clements, Naif Saleh Almakhdhub, Khaled S Saab, Prashast Srivastava, Jinkyu Koo, Saurabh Bagchi, and Mathias Payer, *Protecting bare-metal embedded systems with privilege overlays*, 2017 IEEE Symposium on Security and Privacy (SP), IEEE, 2017, pp. 289–303.

[60] Lisa Collingwood, *Privacy implications and liability issues of autonomous vehicles*, Information & Communications Technology Law **26** (2017), no. 1, 32–45.

[61] Mauro Conti, Denis Donadel, Radha Poovendran, and Federico Turrin, *Evexchange: A relay attack on electric vehicle charging system*, Computer Security–ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part I, Springer, 2022, pp. 488–508.

[62] MOST Cooperation, *Most specification*, Rev. 3.0, URL: www. mostcooperation. com, Jun (2008).

[63] JD Cross and R Hartshorn, *My electric avenue: Integrating electric vehicles into the electrical networks*, (2016).

[64] Ang Cui, Michael Costello, and Salvatore Stolfo, *When firmware modifications attack: A case study of embedded exploitation*, (2013).

[65] Gaoying Cui, Kun Shi, Yuchen Qin, Lin Liu, Bing Qi, and Bin Li, *Application of block chain in multi-level demand response reliable mechanism*, 2017 3rd International Conference on Information Management (ICIM), IEEE, 2017, pp. 337–341.

[66] Jin Cui, Lin Shen Liew, Giedre Sabaliauskaite, and Fengjun Zhou, *A review on safety failures, security attacks, and available countermeasures for autonomous vehicles*, Ad Hoc Networks **90** (2019), 101823.

[67] Lei Cui, Youyang Qu, Longxiang Gao, Gang Xie, and Shui Yu, *Detecting false data attacks using machine learning techniques in smart grid: A survey*, Journal of Network and Computer Applications **170** (2020), 102808.

[68] Jesus Cumplido, Cristina Alcaraz, and Javier Lopez, *Collaborative anomaly detection system for charging stations*, Computer Security–ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part II, Springer, 2022, pp. 716–736.

[69] Gianni Cuozzo, *Critical infrastructure cyber-attack through firmware exploitation.*, 2016.

[70] Soodeh Dadras, Sara Dadras, and Chris Winstead, *Collaborative attacks on autonomous vehicle platooning*, 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), IEEE, 2018, pp. 464–467.

[71] Swaroop Darbha, Shyamprasad Konduri, and Prabhakar R Pagilla, *Benefits of v2v communication for autonomous and connected vehicles*, IEEE Transactions on Intelligent Transportation Systems **20** (2018), no. 5, 1954–1963.

[72] Sagar Dasgupta, Mizanur Rahman, Mhafuzul Islam, and Mashrur Chowdhury, *A sensor fusion-based gnss spoofing attack detection framework for autonomous vehicles*, IEEE Transactions on Intelligent Transportation Systems **23** (2022), no. 12, 23559–23572.

[73] Soumya Kanti Datta, Rui Pedro Ferreira Da Costa, Jérôme Härri, and Christian Bonnet, *Integrating connected vehicles in internet of things ecosystems: Chal-*

lenges and solutions, 2016 IEEE 17th international symposium on a world of wireless, mobile and multimedia networks (WoWMoM), IEEE, 2016, pp. 1–6.

[74] Gonzalo De La Torre, Paul Rad, and Kim-Kwang Raymond Choo, *Driverless vehicle security: Challenges and future research opportunities*, Future Generation Computer Systems **108** (2020), 1092–1111.

[75] Sanchari Deb, Karuna Kalita, and Pinakeshwar Mahanta, *Review of impact of electric vehicle charging station on the power grid*, 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), IEEE, 2017, pp. 1–6.

[76] Sanchari Deb, Kari Tammi, Karuna Kalita, and Pinakeshwar Mahanta, *Impact of electric vehicle charging station load on distribution network*, Energies **11** (2018), no. 1, 178.

[77] Ranjit R Desai, Roger B Chen, and William Armington, *A pattern analysis of daily electric vehicle charging profiles: operational efficiency and environmental impacts*, Journal of Advanced Transportation **2018** (2018).

[78] Mahdi Dibaei, Xi Zheng, Kun Jiang, Robert Abbas, Shigang Liu, Yuexin Zhang, Yang Xiang, and Shui Yu, *Attacks and defences on intelligent connected vehicles: A survey*, Digital Communications and Networks **6** (2020), no. 4, 399–421.

[79] Poria Hasanpor Divshali and Corentin Evens, *Behaviour analysis of electrical vehicle flexibility based on large-scale charging data*, 2019 IEEE Milan PowerTech, IEEE, 2019, pp. 1–6.

[80] Shlomi Dolev and Nisha Panwar, *Peripheral authentication for autonomous vehicles*, 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), IEEE, 2016, pp. 282–285.

[81] Zheng Dong, Cong Liu, Yanhua Li, Jie Bao, Yu Gu, and Tian He, *Rec: Predictable charging scheduling for electric taxi fleets*, 2017 IEEE Real-Time Systems Symposium (RTSS), IEEE, 2017, pp. 287–296.

[82] Matthias Eisel, Johannes Schmidt, and Lutz M Kolbe, *Finding suitable locations for charging stations*, 2014 IEEE International Electric Vehicle Conference (IEVC), IEEE, 2014, pp. 1–8.

[83] Mahmoud Hashem Eiza and Qiang Ni, *Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity*, IEEE Vehicular Technology Magazine **12** (2017), no. 2, 45–51.

[84] Mahmoud Hashem Eiza, Qi Shi, Angelos Marnerides, and Thomas Owens, *Secure and privacy-aware proxy mobile ipv6 protocol for vehicle-to-grid networks*, 2016 IEEE International Conference on Communications (ICC), IEEE, 2016, pp. 1–6.

[85] Orhan Ekren, Celal Hakan Canbaz, and Çetin Berk Güvel, *Sizing of a solar-wind hybrid electric vehicle charging station by using homer software*, Journal of Cleaner Production **279** (2021), 123615.

[86] Julia A Ekstrom and Samantha Heitsch, *Adaptation finance challenges: Characteristic patterns facing*, (2018).

[87] Zakaria El Mrabet, Naima Kaabouch, Hassan El Ghazi, and Hamid El Ghazi, *Cyber-security in smart grid: Survey and challenges*, Computers & Electrical Engineering **67** (2018), 469–482.

[88] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan, *Cybersecurity challenges in vehicular communications*, Vehicular Communications **23** (2020), 100214.

[89] Karim Eldefrawy, Gene Tsudik, Aurélien Francillon, and Daniele Perito, *Smart: Secure and minimal architecture for (establishing dynamic) root of trust.*, Ndss, vol. 12, 2012, pp. 1–15.

[90] Eiman ElGhanam, Mohamed Hassan, Ahmed Osman, and Ibtihal Ahmed, *Review of communication technologies for electric vehicle charging management and coordination*, World Electric Vehicle Journal **12** (2021), no. 3, 92.

[91] Hossam ElHussini, Chadi Assi, Bassam Moussa, Ribal Atallah, and Ali Ghrayeb, *A tale of two entities: Contextualizing the security of electric vehicle charging stations on the power grid*, ACM Transactions on Internet of Things **2** (2021), no. 2, 1–21.

[92] Mohamed ElKashlan, Heba Aslan, Mahmoud Said Elsayed, Anca D Jurcut, and Marianne A Azer, *Intrusion detection for electric vehicle charging systems (evcs)*, Algorithms **16** (2023), no. 2, 75.

[93] Mica R Endsley, *Autonomous driving systems: A preliminary naturalistic study of the tesla model s*, Journal of Cognitive Engineering and Decision Making **11** (2017), no. 3, 225–238.

[94] Joseph M Ernst and Alan J Michaels, *Lin bus security analysis*, IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2018, pp. 2085–2090.

[95] Daniel J Fagnant and Kara Kockelman, *Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations*, Transportation Research Part A: Policy and Practice **77** (2015), 167–181.

[96] Rainer Falk and Steffen Fries, *Electric vehicle charging infrastructure security considerations and approaches*, Proc. of INTERNET (2012), 58–64.

[97] Rainer Falk and Steffen and Fries, *Securely connecting electric vehicles to the smart grid*, Int. Journal on Advances in Internet Technology **6** (2013), no. 1.

[98] Maria Carmen Falvo, Danilo Sbordone, I Safak Bayram, and Michael Devetsikiotis, *Ev charging stations and modes: International standards*, 2014 International Symposium on Power Electronics, Electrical Drives, Automation and Motion, IEEE, 2014, pp. 1134–1139.

[99] Dharmesh Faquir, Nestoras Chouliaras, Vlachou Sofia, Kalopoulou Olga, and Leandros Maglaras, *Cybersecurity in smart grids, challenges and solutions*, AIMS Electronics and Electrical Engineering **5** (2021), no. 1, 24–37.

[100] Khotimatul Fauziah, Yuli Astriani, Dionysius A Renata, Afrias Sarotama, Agus Suhendra, Eka R Priandana, et al., *Design of ac electric vehicle supply equipment based on safety standard*, 2021 3rd International Conference on High Voltage Engineering and Power Systems (ICHVEPS), IEEE, 2021, pp. 425–430.

[101] Ian Foster, Andrew Prudhomme, Karl Koscher, and Stefan Savage, *Fast and vulnerable: A story of telematic failures*, 9th USENIX Workshop on Offensive Technologies (WOOT 15), 2015.

[102] Yosra Fraiji, Lamia Ben Azzouz, Wassim Trojet, and Leila Azouz Saidane, *Cyber security issues of internet of electric vehicles*, 2018 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2018, pp. 1–6.

[103] GA Francia, *Connected vehicle security*, 15th International Conference on Cyber Warfare and Security (ICCWS 2020), 2020, pp. 173–181.

[104] Ankit Gangwal, Aakash Jain, and Mauro Conti, *On the feasibility of profiling electric vehicles through charging data*, arXiv preprint arXiv:2210.05433 (2022).

[105] Cong Gao, Geng Wang, Weisong Shi, Zhongmin Wang, and Yanping Chen, *Autonomous driving security: State of the art and challenges*, IEEE Internet of Things Journal (2021).

[106] Mario H Castaqeda Garcia, Alejandro Molina-Galan, Mate Boban, Javier Gozalvez, Baldomero Coll-Perales, Taylan Şahin, and Apostolos Kousaridas, *A tutorial on 5g nr v2x communications*, IEEE Communications Surveys & Tutorials (2021).

[107] Simson L Garfinkel, Ari Juels, and Ravikanth Pappu, *Rfid privacy: An overview of problems and proposed solutions*, IEEE Security & Privacy **3** (2005), no. 3, 34–43.

[108] Amit Garg and Nima Karimian, *Leveraging deep cnn and transfer learning for side-channel attack*, 2021 22nd International Symposium on Quality Electronic Design (ISQED), IEEE, 2021, pp. 91–96.

[109] Zacharenia Garofalaki, Dimitrios Kosmanos, Sotiris Moschoyiannis, Dimitrios Kallergis, and Christos Douligeris, *Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp)*, IEEE Communications Surveys & Tutorials (2022).

[110] Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J Alex Halderman, *Green lights forever: Analyzing the security of traffic infrastructure*, 8th USENIX Workshop on Offensive Technologies (WOOT 14), 2014.

[111] Amrita Ghosal and Mauro Conti, *Security issues and challenges in v2x: A survey*, Computer Networks **169** (2020), 107093.

[112] Mansi Girdhar, Junho Hong, Hyojong Lee, and Tai-Jin Song, *Hidden markov models-based anomaly correlations for the cyber-physical security of ev charging stations*, IEEE Transactions on Smart Grid **13** (2021), no. 5, 3903–3914.

[113] Antonios Gkortzis, Daniel Feitosa, and Diomidis Spinellis, *A double-edged sword? software reuse and potential security vulnerabilities*, Reuse in the Big Data Era: 18th International Conference on Software and Systems Reuse, ICSR 2019, Cincinnati, OH, USA, June 26–28, 2019, Proceedings 18, Springer, 2019, pp. 187–203.

[114] Dorothy J Glancy, *Privacy in autonomous vehicles*, Santa Clara L. Rev. **52** (2012), 1171.

[115] Gustavo González-Granadillo, Susana González-Zarzosa, and Rodrigo Diaz, *Security information and event management (siem): analysis, trends, and usage in critical infrastructures*, Sensors **21** (2021), no. 14, 4759.

[116] Raju Gottumukkala, Rizwan Merchant, Adam Tauzin, Kaleb Leon, Andrew Roche, and Paul Darby, *Cyber-physical system security of vehicle charging stations*, 2019 IEEE Green Technologies Conference (GreenTech), IEEE, 2019, pp. 1–5.

[117] UK gov, *Government vision for the rapid chargepoint network in england*, https://www.gov.uk/government/publications/government-vision-for-the-rapid-chargepoint-network-in-england/government-vision-for-the-rapid-chargepoint-network-in-england, May 2020.

[118] Andy Greenberg, *Hackers remotely kill a jeep on the highway—with me in it*, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway, 2015, pp. 21–22.

[119] Nils Gruschka and Norbert Luttenberger, *Protecting web services from dos attacks by soap message validation*, IFIP International Information Security Conference, Springer, 2006, pp. 171–182.

[120] Charu Guleria and Harsh Kumar Verma, *Improved detection and mitigation of ddos attack in vehicular ad hoc network*, 2018 4th International Conference on Computing Communication and Automation (ICCCA), IEEE, 2018, pp. 1–4.

[121] Erdem Gumrukcu, Ali Arsalan, Grace Muriithi, Charukeshi Joglekar, Ahmed Aboulebdeh, Mustafa Alparslan Zehir, Behnaz Papari, and Antonello Monti, *Impact of cyber-attacks on ev charging coordination: The case of single point of failure*, 2022 4th Global Power, Energy and Communication Conference (GPECOM), IEEE, 2022, pp. 506–511.

[122] M Zekeriya Gunduz and Resul Das, *Analysis of cyber-attacks on smart grid applications*, 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), IEEE, 2018, pp. 1–5.

[123] Muhammed Zekeriya Gunduz and Resul Das, *Cyber-security on smart grid: Threats and potential solutions*, Computer networks **169** (2020), 107094.

[124] Lulu Guo, Bowen Yang, Jin Ye, Hong Chen, Fangyu Li, Wenzhan Song, Liang Du, and Le Guan, *Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles*, IEEE Transactions on Industrial Informatics **17** (2020), no. 5, 3335–3347.

[125] Pinyao Guo, Hunmin Kim, Le Guan, Minghui Zhu, and Peng Liu, *Vcids: Collaborative intrusion detection of sensor and actuator attacks on connected vehicles*, Security and Privacy in Communication Networks: 13th International Conference, SecureComm 2017, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13, Springer, 2018, pp. 377–396.

[126] Omar Hafez and Kankar Bhattacharya, *Integrating ev charging stations as smart loads for demand response provisions in distribution systems*, IEEE Transactions on Smart Grid **9** (2016), no. 2, 1096–1106.

[127] Subir Halder, Amrita Ghosal, and Mauro Conti, *Secure over-the-air software updates in connected vehicles: A survey*, Computer Networks **178** (2020), 107343.

[128] Piroska Haller, Béla Genge, Fabrizio Forloni, Gianmarco Baldini, Massimo Carriero, and Georgios Fontaras, *Vetadetect: Vehicle tampering detection with closed-loop model ensemble*, International Journal of Critical Infrastructure Protection **37** (2022), 100525.

[129] Wenlin Han and Yang Xiao, *Privacy preservation for v2g networks in smart grid: A survey*, Computer Communications **91** (2016), 17–28.

[130] Kevin Harnett, Brendan Harris, Daniel Chin, Graham Watson, et al., *Doe/dhs/-dot volpe technical meeting on electric vehicle and charging station cybersecurity report*, Tech. report, John A. Volpe National Transportation Systems Center (US), 2018.

[131] Monowar Hasan, Sibin Mohan, Takayuki Shimizu, and Hongsheng Lu, *Securing vehicle-to-everything (v2x) communication platforms*, IEEE Transactions on Intelligent Vehicles **5** (2020), no. 4, 693–713.

[132] Thomas Hepp, Fabian Spaeh, Alexander Schoenhals, Philip Ehret, and Bela Gipp, *Exploring potentials and challenges of blockchain-based public key infrastructures*, IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2019, pp. 847–852.

[133] Ulrich Herberg, Daisuke Mashima, Jorjeta G Jetcheva, and Sanam Mirzazad-Barijough, *Openadr 2.0 deployment architectures: Options and implications*, 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2014, pp. 782–787.

[134] Cabell Hodge, Konrad Hauck, Shivam Gupta, and Jesse C Bennett, *Vehicle cybersecurity threats and mitigation approaches*, Tech. report, National Renewable Energy Lab.(NREL), Golden, CO (United States), 2019.

[135] David Ke Hong, John Kloosterman, Yuqi Jin, Yulong Cao, Qi Alfred Chen, Scott Mahlke, and Z Morley Mao, *Avguardian: Detecting and mitigating publish-subscribe overprivilege for autonomous vehicle systems*, 2020 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2020, pp. 445–459.

[136] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann, *Security threats to automotive can networks–practical examples and selected short-term countermeasures*, International Conference on Computer Safety, Reliability, and Security, Springer, 2008, pp. 235–248.

[137] Mohammad Aminul Hoque and Ragib Hasan, *Avguard: A forensic investigation framework for autonomous vehicles*, ICC 2021-IEEE International Conference on Communications, IEEE, 2021, pp. 1–6.

[138] Xiaoxuan Hu, Kun Wang, Xiulong Liu, Yanfei Sun, Peng Li, and Song Guo, *Energy management for ev charging in software-defined green vehicle-to-grid network*, IEEE Communications Magazine **56** (2018), no. 5, 156–163.

[139] Song Hua, Ence Zhou, Bingfeng Pi, Jun Sun, Yoshihide Nomura, and Hidetoshi Kurihara, *Apply blockchain technology to electric vehicle battery refueling*, (2018).

[140] Xiaohong Huang, Cheng Xu, Pengfei Wang, and Hongzhe Liu, *Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem*, IEEE access **6** (2018), 13565–13574.

[141] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo, *The security and privacy of smart vehicles*, IEEE Security & Privacy **2** (2004), no. 3, 49–55.

[142] R Hull, *Nissan disables leaf electric car app after revelation that hackers can switch on the heater to drain the battery*, https://www.thisismoney.co.uk/money/cars/article-3465459/Nissan-disables-Leaf-electric-car-app-hacker-revelation.html, 2016.

[143] Ahmed Hussein, Fernando Garcia, Jose Maria Armingol, and Cristina Olaverri-Monreal, *P2v and v2p communication for pedestrian warning on the basis of autonomous vehicles*, 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2016, pp. 2034–2039.

[144] Kazuki Iehira, Hiroyuki Inoue, and Kenji Ishida, *Spoofing attack using bus-off attacks against a specific ecu of the can bus*, 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2018, pp. 1–4.

[145] Inaam Ilahi, Muhammad Usama, Junaid Qadir, Muhammad Umar Janjua, Ala Al-Fuqaha, Dinh Thai Hoang, and Dusit Niyato, *Challenges and countermeasures for adversarial attacks on deep reinforcement learning*, IEEE Transactions on Artificial Intelligence **3** (2021), no. 2, 90–109.

[146] Shahrear Iqbal, Anwar Haque, and Mohammad Zulkernine, *Towards a security architecture for protecting connected vehicles from malware*, 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), IEEE, 2019, pp. 1–5.

[147] Md Shariful Islam, Wael Khreich, and Abdelwahab Hamou-Lhadj, *Anomaly detection techniques based on kappa-pruned ensembles*, IEEE Transactions on Reliability **67** (2018), no. 1, 212–229.

[148] Sasan Jafarnejad, Lara Codeca, Walter Bronzi, Raphael Frank, and Thomas Engel, *A car hacking experiment: When connectivity meets vulnerability*, 2015 IEEE globecom workshops (GC Wkshps), IEEE, 2015, pp. 1–6.

[149] Matthew Jagielski, Nicholas Jones, Chung-Wei Lin, Cristina Nita-Rotaru, and Shinichi Shiraishi, *Threat detection for collaborative adaptive cruise control in connected cars*, Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2018, pp. 184–189.

[150] Bojan Jelacic, Daniela Rosic, Imre Lendak, Marina Stanojevic, and Sebastijan Stoja, *Stride to a secure smart grid in a hybrid cloud*, Computer Security, Springer, 2017, pp. 77–90.

[151] Saurabh Jha, Shengkun Cui, Subho Banerjee, James Cyriac, Timothy Tsai, Zbigniew Kalbarczyk, and Ravishankar K Iyer, *Ml-driven malware that targets av safety*, 2020 50th annual IEEE/IFIP international conference on dependable systems and networks (DSN), IEEE, 2020, pp. 113–124.

[152] Baofeng Ji, Xueru Zhang, Shahid Mumtaz, Congzheng Han, Chunguo Li, Hong Wen, and Dan Wang, *Survey on the internet of vehicles: Network architectures and applications*, IEEE Communications Standards Magazine **4** (2020), no. 1, 34–41.

[153] Jay Johnson, Benjamin Anderson, Brian Wright, Jimmy Quiroz, Timothy Berg, Russell Graves, Josh Daley, Kandy Phan, Micheal Kunz, Rick Pratt, et al., *Cybersecurity for electric vehicle charging infrastructure.*, Tech. report, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2022.

[154] Jay Johnson, Timothy Berg, Benjamin Anderson, and Brian Wright, *Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses*, Energies **15** (2022), no. 11, 3931.

[155] Sebastian Käbisch, Anton Schmitt, Martin Winter, and Jörg Heuer, *Interconnections and communications of electric vehicles and smart grids*, 2010 First IEEE International Conference on Smart Grid Communications, IEEE, 2010, pp. 161–166.

[156] Balachandra Reddy Kandukuri, Atanu Rakshit, et al., *Cloud security issues*, 2009 IEEE International Conference on Services Computing, IEEE, 2009, pp. 517–520.

[157] Tae Un Kang, Hyun Min Song, Seonghoon Jeong, and Huy Kang Kim, *Automated reverse engineering and attack for can using obd-ii*, 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), IEEE, 2018, pp. 1–7.

[158] Adi Karahasanovic, Pierre Kleberger, and Magnus Almgren, *Adapting threat modeling methods for the automotive industry*, Proceedings of the 15th ESCAR Conference, 2017, pp. 1–10.

[159] Christina Katsini, George E Raptis, Kristina Livitckaia, Konstantinos Votis, and Christos Alexakos, *Digital forensic readiness in internet of vehicles: The denial-of-service on can bus case study*, (2022).

[160] John B Kenney, *Dedicated short-range communications (dsrc) standards in the united states*, Proceedings of the IEEE **99** (2011), no. 7, 1162–1182.

[161] Marwa Keshk, Nour Moustafa, Elena Sitnikova, and Gideon Creech, *Privacy preservation intrusion detection technique for scada systems*, 2017 Military Communications and Information Systems Conference (MilCIS), IEEE, 2017, pp. 1–6.

[162] Ajoy Kumar Khan and Hridoy Jyoti Mahanta, *Side channel attacks and their mitigation techniques*, 2014 First International Conference on Automation, Control, Energy and Systems (ACES), IEEE, 2014, pp. 1–4.

[163] Firoz Khan, R Lakshmana Kumar, Seifedine Kadry, Yunyoung Nam, and Maytham N Meqdad, *Autonomous vehicles: A study of implementation and security.*, International Journal of Electrical & Computer Engineering (2088-8708) **11** (2021), no. 4.

[164] Prince Waqas Khan and Yung-Cheol Byun, *Blockchain-based peer-to-peer energy trading and charging payment system for electric vehicles*, Sustainability **13** (2021), no. 14, 7962.

[165] Kavian Khorsravinia, Mohd Khair Hassan, Ribhan Zafira Abdul Rahman, and Syed Abdul Rahman Al-Haddad, *Integrated obd-ii and mobile application for electric vehicle (ev) monitoring system*, 2017 IEEE 2nd International Conference on Automatic Control and Intelligent Systems (I2CACIS), IEEE, 2017, pp. 202–206.

[166] Young-Jin Kim, Vladimir Kolesnikov, and Marina Thottan, *Tsaf: Tamper-resistant and scalable mutual authentication framework for plug-in ev charging*, 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2013, pp. 444–449.

[167] Taehyoung Ko, Cheongmin Ji, and Manpyo Hong, *Avod: Advanced verify-on-demand for efficient authentication against dos attacks in v2x communication*, Security and Communication Networks **2021** (2021), 1–9.

[168] Jelena Kocić, Nenad Jovičić, and Vujo Drndarević, *Sensors and sensor fusion in autonomous vehicles*, 2018 26th Telecommunications Forum (TELFOR), IEEE, 2018, pp. 420–425.

[169] Linghe Kong, Muhammad Khurram Khan, Fan Wu, Guihai Chen, and Peng Zeng, *Millimeter-wave wireless communications for iot-cloud supported au-*

tonomous vehicles: Overview, design, and challenges, IEEE Communications Magazine **55** (2017), no. 1, 62–68.

[170] Philip Koopman and Michael Wagner, *Challenges in autonomous vehicle testing and validation*, SAE International Journal of Transportation Safety **4** (2016), no. 1, 15–24.

[171] Matus Korman, Margus Välja, Gunnar Björkman, Mathias Ekstedt, Alexandre Vernotte, and Robert Lagerström, *Analyzing the effectiveness of attack countermeasures in a scada system*, Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, 2017, pp. 73–78.

[172] Martin Kosinka, Zdenek Slanina, Michal Petruzela, and Vojtech Blazek, *V2h control system software analysis and design*, 2020 20th International Conference on Control, Automation and Systems (ICCAS), IEEE, 2020, pp. 972–977.

[173] A Mohan Krishna, Amit Kumar Tyagi, and SVAV Prasad, *Preserving privacy in future vehicles of tomorrow*, JCR **7** (2020), no. 19, 6675–6684.

[174] Vipin Kumar Kukkala, Sooryaa Vignesh Thiruloga, and Sudeep Pasricha, *Roadmap for cybersecurity in autonomous vehicles*, IEEE Consumer Electronics Magazine **11** (2022), no. 6, 13–23.

[175] KEEN Security Lab, *New vehicle security research by keenlab: Experimental security assessment of bmw cars*, https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/, 2018.

[176] Fred Lambert, *The big tesla hack: A hacker gained control over the entire fleet, but fortunately he's a good guy*, https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/, 2017.

[177] Junghoon Lee, Gyung-Leen Park, Yeonju Han, and Seunghee Yoo, *Big data analysis for an electric vehicle charging infrastructure using open data and software*, Proceedings of the Eighth International Conference on Future Energy Systems, 2017, pp. 252–253.

[178] Michael Lee and Travis Atkison, *Vanet applications: Past, present, and future*, Vehicular Communications **28** (2021), 100310.

[179] Zachary Lee, Daniel Johansson, and Steven H Low, *Acn-sim: An open-source simulator for data-driven electric vehicle charging research*, Proceedings of the Tenth ACM International Conference on Future Energy Systems, 2019, pp. 411–412.

[180] Zachary J Lee, Tongxin Li, and Steven H Low, *Acn-data: Analysis and applications of an open ev charging dataset*, Proceedings of the Tenth ACM International Conference on Future Energy Systems, 2019, pp. 139–149.

[181] Lee Wilmoth Lerner, *Trustworthy embedded computing for cyber-physical control*, Ph.D. thesis, Virginia Polytechnic Institute and State University, 2015.

[182] Jesse Levinson, Jake Askeland, Jan Becker, Jennifer Dolson, David Held, Soeren Kammel, J Zico Kolter, Dirk Langer, Oliver Pink, Vaughan Pratt, et al., *Towards fully autonomous driving: Systems and algorithms*, 2011 IEEE intelligent vehicles symposium (IV), IEEE, 2011, pp. 163–168.

[183] Da Li, Zhaosheng Zhang, Peng Liu, Zhenpo Wang, and Lei Zhang, *Battery fault diagnosis for electric vehicles based on voltage abnormality by combining the long short-term memory neural network and the equivalent circuit model*, IEEE Transactions on Power Electronics **36** (2020), no. 2, 1303–1315.

[184] Hongyang Li, György Dán, and Klara Nahrstedt, *Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging*, IEEE Transactions on Smart Grid **8** (2016), no. 5, 2305–2313.

[185] Huaxin Li, Di Ma, Brahim Medjahed, Yu Seung Kim, and Pramita Mitra, *Analyzing and preventing data privacy leakage in connected vehicle services*, SAE International Journal of Advances and Current Practices in Mobility **1** (2019), no. 2019-01-0478, 1035–1045.

[186] Mushu Li and Lian Zhao, *A decentralized load balancing approach for neighbouring charging stations via ev fleets*, 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), IEEE, 2017, pp. 1–5.

[187] Yang Li, Meng Han, Zhen Yang, and Guoqing Li, *Coordinating flexible demand response and renewable uncertainties for scheduling of community integrated energy systems with an electric vehicle charging station: A bi-level approach*, IEEE Transactions on Sustainable Energy **12** (2021), no. 4, 2321–2331.

[188] Yongfu Li, Kezhi Li, Taixiong Zheng, Xiangdong Hu, Huizong Feng, and Yinguo Li, *Evaluating the performance of vehicular platoon control under different network topologies of initial states*, Physica A: Statistical Mechanics and its Applications **450** (2016), 359–368.

[189] Fanchao Liao, Eric Molin, and Bert van Wee, *Consumer preferences for electric vehicles: a literature review*, Transport Reviews **37** (2017), no. 3, 252–275.

[190] Suzanne Lightman, Suzanne Lightman, and Tanya Brewer, *Symposium on federally funded research on cybersecurity of electric vehicle supply equipment (evse)*, US Department of Commerce, National Institute of Standards and Technology, 2020.

[191] Kai Li Lim, Stuart Speidel, and Thomas Bräunl, *A unified telemetry platform for electric vehicles and charging infrastructure*, Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV (2020), 167–219.

[192] Kiho Lim, Tariqul Islam, Hyunbum Kim, and Jingon Joung, *A sybil attack detection scheme based on adas sensors for vehicular networks*, 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2020, pp. 1–5.

[193] Youseo Lim, Seungduc Yu, Gunbae Park, Kyungyoon Lee, and Kijun Park, *The implementation and demonstration of secured evci backend systems based on the public key infrastructure*, (2022).

[194] Hong Liu, Yan Zhang, and Tao Yang, *Blockchain-enabled security in electric vehicles cloud and edge computing*, IEEE Network **32** (2018), no. 3, 78–83.

[195] Joseph K Liu, Man Ho Au, Willy Susilo, and Jianying Zhou, *Enhancing location privacy for electric vehicles (at the right time)*, European Symposium on Research in Computer Security, Springer, 2012, pp. 397–414.

[196] Lanchao Liu, Mohammad Esmalifalak, Qifeng Ding, Valentine A Emesih, and Zhu Han, *Detecting false data injection attacks on power grid by sparse optimization*, IEEE Transactions on Smart Grid **5** (2014), no. 2, 612–621.

[197] David Lodge, *Hacking the mitsubishi outlander phev hybrid*, https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv, 2016.

[198] Jiajun Lu, Hussein Sibai, Evan Fabry, and David Forsyth, *No need to worry about adversarial examples in object detection in autonomous vehicles*, arXiv preprint arXiv:1707.03501 (2017).

[199] Ning Lu, Nan Cheng, Ning Zhang, Xuemin Shen, and Jon W Mark, *Connected vehicles: Solutions and challenges*, IEEE internet of things journal **1** (2014), no. 4, 289–299.

[200] Rongxing Lu, Lan Zhang, Jianbing Ni, and Yuguang Fang, *5g vehicle-to-everything services: Gearing up for security and privacy*, Proceedings of the IEEE **108** (2019), no. 2, 373–389.

[201] Feng Luo and Shuo Hou, *Cyberattacks and countermeasures for intelligent and connected vehicles*, SAE International Journal of Passenger Cars-Electronic and Electrical Systems **12** (2019), no. 1, 55–67.

[202] Qian Luo, Yurui Cao, Jiajia Liu, and Abderrahim Benslimane, *Localization and navigation in autonomous driving: Threats and countermeasures*, IEEE Wireless Communications **26** (2019), no. 4, 38–45.

[203] Xuewen Luo, Yiliang Liu, Hsiao-Hwa Chen, and Qing Guo, *Physical layer security in intelligently connected vehicle networks*, IEEE Network **34** (2020), no. 5, 232–239.

[204] Zachary MacHardy, Ashiq Khan, Kazuaki Obana, and Shigeru Iwashina, *V2x access technologies: Regulation, research, and remaining challenges*, IEEE Communications Surveys & Tutorials **20** (2018), no. 3, 1858–1877.

[205] Valerian Mannoni, Vincent Berg, Stefania Sesia, and Eric Perraud, *A comparison of the v2x communication systems: Its-g5 and c-v2x*, 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), IEEE, 2019, pp. 1–5.

[206] Manuel Mar, Julien Noel, and J Eric Dietz, *Cyber-physical review of a battery electric vehicle power train: Vulnerabilities and challenges*, 2021 IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America), IEEE, 2021, pp. 1–5.

[207] Clara Marina Martinez, Mira Heucke, Fei-Yue Wang, Bo Gao, and Dongpu Cao, *Driving style recognition for intelligent vehicle control and advanced driver assistance: A survey*, IEEE Transactions on Intelligent Transportation Systems **19** (2017), no. 3, 666–676.

[208] Mohammad Masdari and Marzie Jalali, *A survey and taxonomy of dos attacks in cloud computing*, Security and Communication Networks **9** (2016), no. 16, 3724–3751.

[209] Kunal Maurya, Mandeep Singh, and Neelu Jain, *Real time vehicle tracking system using gsm and gps technology-an anti-theft tracking system*, International Journal of Electronics and Computer Science Engineering **1** (2012), no. 3, 1103–1107.

[210] Roberto Merco, Zoleikha Abdollahi Biron, and Pierluigi Pisu, *Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control*, 2018 Annual American Control Conference (ACC), IEEE, 2018, pp. 5582–5587.

[211] Andrea Mercurio, Alessandro Di Giorgio, and Fabio Purificato, *Optimal fully electric vehicle load balancing with an admm algorithm in smartgrids*, 21st Mediterranean Conference on Control and Automation, IEEE, 2013, pp. 119–124.

[212] Roberto Metere, Zoya Pourmirza, Sara Walker, and Myriam Neaimeh, *An overview of cyber security and privacy on the electric vehicle charging infrastructure*, arXiv preprint arXiv:2209.07842 (2022).

[213] Charlie Miller and Chris Valasek, *A survey of remote automotive attack surfaces*, black hat USA **2014** (2014), 94.

[214] ———, *Remote exploitation of an unaltered passenger vehicle*, vol. 2015, 2015.

[215] Charlie Miller and Chris and Valasek, *Adventures in automotive networks and control units*, vol. 21, 2013, pp. 15–31.

[216] Sananda Mitra, Sumanta Bose, Sourav Sen Gupta, and Anupam Chattopadhyay, *Secure and tamper-resilient distributed ledger for data aggregation in autonomous vehicles*, 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), IEEE, 2018, pp. 548–551.

[217] Jean-Philippe Monteuuis, Jonathan Petit, Jun Zhang, Houda Labiod, Stefano Mafrica, and Alain Servel, *Attacker model for connected and automated vehicles*, ACM Computer Science in Car Symposium, 2018.

[218] Glenn Sean Morrison, *Threats and mitigation of ddos cyberattacks against the us power grid via ev charging*, Ph.D. thesis, Wright State University, 2018.

[219] Jamal Hayat Mosakheil, *Security threats classification in blockchains*, (2018).

[220] Subhojeet Mukherjee, Hossein Shirazi, Indrakshi Ray, Jeremy Daily, and Rose Gamble, *Practical dos attacks on embedded networks in commercial vehicles*, Information Systems Security: 12th International Conference, ICISS 2016, Jaipur, India, December 16-20, 2016, Proceedings 12, Springer, 2016, pp. 23–42.

[221] Pal-Stefan Murvay and Bogdan Groza, *Practical security exploits of the flexray in-vehicle communication protocol*, International Conference on Risks and Security of Internet and Systems, Springer, 2018, pp. 172–187.

[222] Mahmoud Nabil, Muhammad Bima, Ahmad Alsharif, Willaim Johnson, Surya Gunukula, Mohamed Mahmoud, and Mohamed Abdallah, *Priority-based and privacy-preserving electric vehicle dynamic charging system with divisible e-payment*, Smart Cities Cybersecurity and Privacy, Elsevier, 2019, pp. 165–186.

[223] Maryam M Najafabadi, Taghi M Khoshgoftaar, Clifford Kemp, Naeem Seliya, and Richard Zuech, *Machine learning for detecting brute force attacks at the network level*, 2014 IEEE International Conference on Bioinformatics and Bioengineering, IEEE, 2014, pp. 379–385.

[224] Ashish Nanda, Deepak Puthal, Joel JPC Rodrigues, and Sergei A Kozlov, *Internet of autonomous vehicles communications security: overview, issues, and directions*, IEEE Wireless Communications **26** (2019), no. 4, 60–65.

[225] Tony Nasr, Sadegh Torabi, Elias Bou-Harb, Claude Fachkha, and Chadi Assi, *Power jacking your station: In-depth security analysis of electric vehicle charging station management systems*, Computers & Security **112** (2022), 102511.

[226] Naman Singh Negi, Ons Jelassi, Stéphan Clémençon, and Sebastian Fischmeister, *A lstm approach to detection of autonomous vehicle hijacking.*, VEHITS, 2019, pp. 475–482.

[227] Hasen Nicanfar, Seyedali Hosseininezhad, Peyman TalebiFard, and Victor CM Leung, *Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations*, 2013 Proceedings IEEE INFOCOM, IEEE, 2013, pp. 3429–3434.

[228] Hasen Nicanfar, Peyman TalebiFard, Seyedali Hosseininezhad, Victor CM Leung, and Mark Damm, *Security and privacy of electric vehicles in the smart grid context: problem and solution*, Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications, 2013, pp. 45–54.

[229] Sen Nie, Ling Liu, and Yuefeng Du, *Free-fall: Hacking tesla from wireless to can bus*, Briefing, Black Hat USA **25** (2017), 1–16.

[230] Dennis K Nilsson, Ulf E Larson, Francesco Picasso, and Erland Jonsson, *A first simulation of attacks in the automotive network communications protocol flexray*, Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08, Springer, 2009, pp. 84–91.

[231] Dennis K Nilsson, Phu H Phung, and Ulf E Larson, *Vehicle ecu classification based on safety-security characteristics*, IET Road Transport Information and Control-RTIC 2008 and ITS United Kingdom Members' Conference, IET, 2008, pp. 1–7.

[232] Jason RC Nurse, Sadie Creese, and David De Roure, *Security risk assessment in internet of things systems*, IT professional **19** (2017), no. 5, 20–26.

[233] Chuka Oham, Salil S Kanhere, Raja Jurdak, and Sanjay Jha, *A blockchain based liability attribution framework for autonomous vehicles*, arXiv preprint arXiv:1802.05050 (2018).

[234] Arash Olia, Hossam Abdelgawad, Baher Abdulhai, and Saiedeh N Razavi, *Assessing the potential impacts of connected vehicles: mobility, environmental, and safety perspectives*, Journal of Intelligent Transportation Systems **20** (2016), no. 3, 229–243.

[235] The Netherlands Open Charge Alliance, Duiven, *Open charge point protocol*, https://www.openchargealliance.org/protocols/ocpp-16/, May 2015.

[236] Simon Parkinson, Paul Ward, Kyle Wilson, and Jonathan Miller, *Cyber threats facing autonomous and connected vehicles: Future challenges*, IEEE transactions on intelligent transportation systems **18** (2017), no. 11, 2898–2915.

[237] Marbin Pazos-Revilla, Ahmad Alsharif, Surya Gunukula, Terry N Guo, Mohamed Mahmoud, and Xuemin Shen, *Secure and privacy-preserving physical-*

layer-assisted scheme for ev dynamic charging system, IEEE Transactions on Vehicular Technology **67** (2017), no. 4, 3304–3318.

[238] Jonathan Petit and Steven E Shladover, *Potential cyberattacks on automated vehicles*, IEEE Transactions on Intelligent transportation systems **16** (2014), no. 2, 546–556.

[239] Minh Pham and Kaiqi Xiong, *A survey on security attacks and defense techniques for connected and autonomous vehicles*, Computers & Security **109** (2021), 102269.

[240] Victoria Y Pillitteri and Tanya L Brewer, *Guidelines for smart grid cybersecurity*, (2014).

[241] Zoya Pourmirza and Sara Walker, *Electric vehicle charging station: Cyber security challenges and perspective*, 2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE), IEEE, 2021, pp. 111–116.

[242] BK Powell, KE Bailey, and SR Cikanek, *Dynamic modeling and control of hybrid electric vehicle powertrain systems*, IEEE Control Systems Magazine **18** (1998), no. 5, 17–33.

[243] Richard M Pratt and Thomas E Carroll, *Vehicle charging infrastructure security*, 2019 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2019, pp. 1–5.

[244] Dominik Püllen, Nikolaos Athanasios Anagnostopoulos, Tolga Arul, and Stefan Katzenbeisser, *Security and safety co-engineering of the flexray bus in vehicular networks*, Proceedings of the International Conference on Omni-Layer Intelligent Systems, 2019, pp. 31–37.

[245] Adnan Qayyum, Muhammad Usama, Junaid Qadir, and Ala Al-Fuqaha, *Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward*, IEEE Communications Surveys & Tutorials **22** (2020), no. 2, 998–1026.

[246] Junjian Qi, Youngjin Kim, Chen Chen, Xiaonan Lu, and Jianhui Wang, *Demand response and smart buildings: A survey of control, communication, and cyber-physical security*, ACM Transactions on Cyber-Physical Systems **1** (2017), no. 4, 1–25.

[247] Jairo Quirós-Tortós, Luis F Ochoa, and Becky Lees, *A statistical analysis of ev charging behavior in the uk*, 2015 IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LATAM), IEEE, 2015, pp. 445–449.

[248] Maria Simona Răboacă, Nicu Bizon, and Phatiphat Thounthong, *Intelligent charging station in 5g environments: challenges and perspectives*, International Journal of Energy Research **45** (2021), no. 11, 16418–16435.

[249] Petar Radanliev, David Charles De Roure, Razvan Nicolescu, Michael Huth, Rafael Mantilla Montalvo, Stacy Cannady, and Peter Burnap, *Future developments in cyber risk assessment for the internet of things*, Computers in industry **102** (2018), 14–22.

[250] Eman Mohammed Radi, Noureddine Lasla, Spiridon Bakiras, and Mohamed Mahmoud, *Privacy-preserving electric vehicle charging for peer-to-peer energy trading ecosystems*, ICC 2019-2019 IEEE International Conference on Communications (ICC), IEEE, 2019, pp. 1–6.

[251] Panagiotis Radoglou-Grammatikis, Panagiotis Sarigiannidis, Eider Iturbe, Erkuden Rios, Saturnino Martinez, Antonios Sarigiannidis, Georgios Eftathopoulos, Yannis Spyridis, Achilleas Sesis, Nikolaos Vakakis, et al., *Spear*

siem: A security information and event management system for the smart grid, Computer Networks **193** (2021), 108008.

[252] Sampath Rajapaksha, Harsha Kalutarage, M Omar Al-Kadri, Garikayi Madzudzo, and Andrei V Petrovski, *Keep the moving vehicle secure: Context-aware intrusion detection system for in-vehicle can bus security*, 2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon), vol. 700, IEEE, 2022, pp. 309–330.

[253] Arun Sekar Rajasekaran, Maria Azees, and Fadi Al-Turjman, *A comprehensive survey on security issues in vehicle-to-grid networks*, Journal of Control and Decision (2022), 1–10.

[254] Gowthamraj Rajendran, Chockalingam Aravind Vaithilingam, Norhisam Misron, Kanendra Naidu, and Md Rishad Ahmed, *A comprehensive review on system architecture and international standards for electric vehicle charging stations*, Journal of Energy Storage **42** (2021), 103099.

[255] Li Ran, Wu Junfeng, Wang Haiying, and Li Gechen, *Design method of can bus network communication structure for electric vehicle*, International Forum on Strategic Technology 2010, IEEE, 2010, pp. 326–329.

[256] Sapna Ravindran, S Amal, YV Bhavya, and V Chandrasekar, *Ocpp based electric vehicle supply equipment and its user interface for ac charging in indian scenario*, 2020 IEEE 17th India Council International Conference (INDICON), IEEE, 2020, pp. 1–6.

[257] Pouyan Razmjouei, Abdollah Kavousi-Fard, Morteza Dabbaghjamanesh, Tao Jin, and Wencong Su, *Ultra-lightweight mutual authentication in the vehicle based on smart contract blockchain: Case of mitm attack*, IEEE Sensors Journal **21** (2020), no. 14, 15839–15848.

[258] Pouyan Razmjoui, Abdollah Kavousi-Fard, Tao Jin, Morteza Dabbaghjamanesh, Mazaher Karimi, and Alireza Jolfaei, *A blockchain-based mutual authentication method to secure the electric vehicles' tpms*, IEEE Transactions on Industrial Informatics (2023).

[259] Devin Reeh, Francisco Cruz Tapia, Yu-Wei Chung, Behnam Khaki, Chicheng Chu, and Rajit Gadh, *Vulnerability analysis and risk assessment of ev charging system under cyber-physical threats*, 2019 IEEE Transportation Electrification Conference and Expo (ITEC), IEEE, 2019, pp. 1–6.

[260] Abdul Rehman Javed, Zunera Jalil, Syed Atif Moqurrab, Sidra Abbas, and Xuan Liu, *Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles*, Transactions on Emerging Telecommunications Technologies **33** (2022), no. 10, e4088.

[261] John Reimers, Lea Dorn-Gomba, Christopher Mak, and Ali Emadi, *Automotive traction inverters: Current status and future trends*, IEEE Transactions on Vehicular Technology **68** (2019), no. 4, 3337–3350.

[262] David Rempel, Carleen Cullen, Mary Matteson Bryan, and Gustavo Vianna Cezar, *Reliability of open public electric vehicle direct current fast chargers*, Available at SSRN 4077554 (2022).

[263] Kui Ren, Qian Wang, Cong Wang, Zhan Qin, and Xiaodong Lin, *The security of autonomous driving: Threats, defenses, and future directions*, Proceedings of the IEEE **108** (2019), no. 2, 357–372.

[264] Braden Roberts, Kemal Akkaya, Eyuphan Bulut, and Mithat Kisacikoglu, *An authentication framework for electric vehicle-to-electric vehicle charging applications*, 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), IEEE, 2017, pp. 565–569.

[265] Marc Roeschlin, Giovanni Camurati, Pascal Brunner, Singh Mridula, and Capkun Srdjan, *Edgetdc: On the security of time difference of arrival measurements in can bus systems*, NDSS, 2023.

[266] Ronald S Ross, *Guide for conducting risk assessments*, (2012).

[267] ———, *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy*, (2018).

[268] Koosha Sadeghi, Ayan Banerjee, Javad Sohankar, and Sandeep KS Gupta, *Safedrive: An autonomous driver safety application in aware cities*, 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), IEEE, 2016, pp. 1–6.

[269] Nasrin Sadeghianpourhamami, Nazir Refa, Matthias Strobbe, and Chris Develder, *Quantitive analysis of electric vehicle flexibility: A data-driven approach*, International Journal of Electrical Power & Energy Systems **95** (2018), 451–462.

[270] Yalin E Sagduyu, Yi Shi, and Tugba Erpek, *Adversarial deep learning for over-the-air spectrum poisoning attacks*, IEEE Transactions on Mobile Computing **20** (2019), no. 2, 306–319.

[271] Florian Sagstetter, Martin Lukasiewycz, Sebastian Steinhorst, Marko Wolf, Alexandre Bouard, William R Harris, Somesh Jha, Thomas Peyrin, Axel Poschmann, and Samarjit Chakraborty, *Security challenges in automotive hardware/software architecture design*, 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE, 2013, pp. 458–463.

[272] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, and Kaoru Sezaki, *Caravan: Providing location privacy for vanet*, Tech. report, Washington Univ Seattle Dept of Electrical Engineering, 2005.

[273] Takami Sato and Qi Alfred Chen, *On robustness of lane detection models to physical-world adversarial attacks in autonomous driving*, arXiv preprint arXiv:2107.02488 (2021).

[274] Takami Sato, Junjie Shen, Ningfei Wang, Yunhan Jia, Xue Lin, and Qi Alfred Chen, *Dirty road can attack: Security of deep learning based automated lane centering under {Physical-World} attack*, 30th USENIX Security Symposium (USENIX Security 21), 2021, pp. 3309–3326.

[275] Neetesh Saxena and Bong Jun Choi, *Authentication scheme for flexible charging and discharging of mobile vehicles in the v2g networks*, IEEE Transactions on Information Forensics and Security **11** (2016), no. 7, 1438–1452.

[276] Neetesh Saxena, Santiago Grijalva, Victor Chukwuka, and Athanasios V Vasilakos, *Network security and privacy challenges in smart vehicle-to-grid*, IEEE Wireless Communications **24** (2017), no. 4, 88–98.

[277] Mohammad Ali Sayed, Ribal Atallah, Chadi Assi, and Mourad Debbabi, *Electric vehicle attack impact on power grid operation*, International Journal of Electrical Power & Energy Systems **137** (2022), 107784.

[278] Jens Schmutzler, Claus Amtrup Andersen, and Christian Wietfeld, *Evaluation of ocpp and iec 61850 for smart charging electric vehicles*, World Electric Vehicle Journal **6** (2013), no. 4, 863–874.

[279] Aymene Selamnia, Bouziane Brik, Sidi Mohammed Senouci, Abdelwahab Boualouache, and Shajjad Hossain, *Edge computing-enabled intrusion detection for c-v2x networks using federated learning*, GLOBECOM 2022-2022 IEEE Global Communications Conference, IEEE, 2022, pp. 2080–2085.

[280] Sergey Sergeevich Shadrin, Oleg Olegovich Varlamov, and Andrey Mikhailovich Ivanov, *Experimental autonomous road vehicle with logical artificial intelligence*, Journal of advanced transportation **2017** (2017).

[281] Shital Shah, Debadeepta Dey, Chris Lovett, and Ashish Kapoor, *Airsim: High-fidelity visual and physical simulation for autonomous vehicles*, Field and service robotics, Springer, 2018, pp. 621–635.

[282] Prinkle Sharma, David Austin, and Hong Liu, *Attacks on machine learning: Adversarial examples in connected and autonomous vehicles*, 2019 IEEE International Symposium on Technologies for Homeland Security (HST), IEEE, 2019, pp. 1–7.

[283] Vishal Sharma, Ilsun You, and Nadra Guizani, *Security of 5g-v2x: Technologies, standardization, and research directions*, IEEE Network **34** (2020), no. 5, 306–314.

[284] A Sheela, M Suresh, V Gowri Shankar, Hitesh Panchal, V Priya, M Atshaya, Kishor Kumar Sadasivuni, and Swapnil Dharaskar, *Fea based analysis and design of pmsm for electric vehicle applications using magnet software*, International Journal of Ambient Energy (2020), 1–6.

[285] A Sheikh, V Kamuni, Asfia Urooj, S Wagh, N Singh, and Dhiren Patel, *Secured energy trading using byzantine-based blockchain consensus*, IEEE Access **8** (2019), 8554–8571.

[286] Nataliya Shevchenko, Timothy A Chick, Paige O'Riordan, Thomas P Scanlon, and Carol Woody, *Threat modeling: a summary of available methods*, Tech. report, Carnegie Mellon University Software Engineering Institute Pittsburgh United ..., 2018.

[287] Peng Shi, Zhen Zhao, Huaqiang Zhong, Hangyu Shen, and Lianhong Ding, *An improved agglomerative hierarchical clustering anomaly detection method for scientific data*, Concurrency and Computation: Practice and Experience **33** (2021), no. 6, e6077.

[288] Vardhan Shorewala, *Anomaly detection and improvement of clusters using enhanced k-means algorithm*, 2021 5th International Conference on Computer, Communication and Signal Processing (ICCCSP), IEEE, 2021, pp. 115–121.

[289] Adam Shostack, *Threat modeling: Designing for security*, John Wiley & Sons, 2014.

[290] Farhan Siddiqui, Sherali Zeadally, Cristina Alcaraz, and Samara Galvao, *Smart grid privacy: Issues and solutions*, 2012 21st International Conference on Computer Communications and Networks (ICCCN), IEEE, 2012, pp. 1–5.

[291] Siemens, *Siemens charging stations*, `https://new.siemens.com/global/en/products/energy/medium-voltage/solutions/emobility/sicharge-d.html`, May 2020.

[292] Komal Singh and Sachin Sharma, *Advanced security attacks on vehicular ad hoc network (vanet)*, Int. J. Innov. Technol. Exploring Eng **9** (2019), no. 2, 3057–3064.

[293] Pranav Kumar Singh, Shivam Gupta, Ritveeka Vashistha, Sunit Kumar Nandi, and Sukumar Nandi, *Machine learning based approach to detect position falsification attack in vanets*, International Conference on Security & Privacy, Springer, 2019, pp. 166–178.

[294] Laurens Sion, Koen Yskout, Dimitri Van Landuyt, and Wouter Joosen, *Solution-aware data flow diagrams for security threat modeling*, Proceedings

of the 33rd Annual ACM Symposium on Applied Computing, 2018, pp. 1425–1432.

[295] Prabath Siriwardena, *Advanced api security*, Apress: New York, NY, USA (2014).

[296] Inna Skarga-Bandurova, Igor Kotsiuba, and Tetiana Biloborodova, *Cyber security of electric vehicle charging infrastructure: Open issues and recommendations*, 2022 IEEE International Conference on Big Data (Big Data), IEEE, 2022, pp. 3099–3106.

[297] Hyun Min Song, Ha Rang Kim, and Huy Kang Kim, *Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network*, 2016 international conference on information networking (ICOIN), IEEE, 2016, pp. 63–68.

[298] Srdjan Srdic and Srdjan Lukic, *Toward extreme fast charging: Challenges and opportunities in directly connecting to medium-voltage line*, IEEE Electrification Magazine **7** (2019), no. 1, 22–31.

[299] Sergio Luiz Stevan Jr and Felipe Adalberto Farinelli, *Can-bus remote monitoring: standalone can sensor reading and automotive diagnostics*, SAE International Journal of Connected and Automated Vehicles **2** (2019), no. 12-02-01-0003, 27–46.

[300] N Sulaiman, MA Hannan, Azah Mohamed, Pin Jern Ker, EH Majlan, and WR Wan Daud, *Optimization of energy management system for fuel-cell hybrid electric vehicles: Issues and recommendations*, Applied energy **228** (2018), 2061–2079.

[301] Hong-Tao Sun, Chen Peng, and Fei Ding, *Self-discipline predictive control of autonomous vehicles against denial of service attacks*, Asian Journal of Control **24** (2022), no. 6, 3538–3551.

[302] Xiaoqiang Sun, F Richard Yu, and Peng Zhang, *A survey on cyber-security of connected and autonomous vehicles (cavs)*, IEEE Transactions on Intelligent Transportation Systems **23** (2021), no. 7, 6240–6259.

[303] Mojtaba Tajmohammadi, Sayyed Majid Mazinani, Morteza Nikooghadam, and Zahraa Al-Hamdawee, *Lspp: Lightweight and secure payment protocol for dynamic wireless charging of electric vehicles in vehicular cloud*, IEEE Access **7** (2019), 148424–148438.

[304] Junko Takahashi, Yosuke Aragane, Toshiyuki Miyazawa, Hitoshi Fuji, Hirofumi Yamashita, Keita Hayakawa, Shintarou Ukai, and Hiroshi Hayakawa, *Automotive attacks and countermeasures on lin-bus*, Journal of Information Processing **25** (2017), 220–228.

[305] Yoshiyasu Takefuji, *Connected vehicle security vulnerabilities [commentary]*, IEEE Technology and Society Magazine **37** (2018), no. 1, 15–18.

[306] Shahab Tayeb, Matin Pirouz, Gabriel Esguerra, Kimiya Ghobadi, Jimson Huang, Robin Hill, Derwin Lawson, Stone Li, Tiffany Zhan, Justin Zhan, et al., *Securing the positioning signals of autonomous vehicles*, 2017 IEEE International Conference on Big Data (Big Data), IEEE, 2017, pp. 4522–4528.

[307] Ankit Thakkar and Ritika Lohiya, *A review on machine learning and deep learning perspectives of ids for iot: recent updates, security issues, and challenges*, Archives of Computational Methods in Engineering **28** (2021), 3211–3243.

[308] Vrizlynn LL Thing and Jiaxi Wu, *Autonomous vehicle security: A taxonomy of attacks and defences*, 2016 ieee international conference on internet of things

(ithings) and ieee green computing and communications (greencom) and ieee cyber, physical and social computing (cpscom) and ieee smart data (smartdata), IEEE, 2016, pp. 164–170.

[309] Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta, *On cellular botnets: measuring the impact of malicious devices on a cellular network core*, Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 223–234.

[310] David Trilla, Carles Hernandez, Jaume Abella, and Francisco J Cazorla, *Cache side-channel attacks and time-predictability in high-performance critical real-time systems*, Proceedings of the 55th Annual Design Automation Conference, 2018, pp. 1–6.

[311] Danny Trujillo and Edwin Marcelo García Torres, *Demand response due to the penetration of electric vehicles in a microgrid through stochastic optimization*, IEEE Latin America Transactions **20** (2022), no. 4, 651–658.

[312] Elisabeth Uhlemann, *Time for autonomous vehicles to connect [connected vehicles]*, IEEE vehicular technology magazine **13** (2018), no. 3, 10–13.

[313] Fuad Un-Noor, Sanjeevikumar Padmanaban, Lucian Mihet-Popa, Mohammad Nurunnabi Mollah, and Eklas Hossain, *A comprehensive study of key electric vehicle (ev) components, technologies, challenges, impacts, and future direction of development*, Energies **10** (2017), no. 8, 1217.

[314] Lewis E Unnewehr and SA Naser, *Electric vehicle technology*, (1982).

[315] Darshana Upadhyay and Srinivas Sampalli, *Scada (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations*, Computers & Security **89** (2020), 101666.

[316] Binod Vaidya, Dimitrios Makrakis, and Hussein T Mouftah, *Multi-domain public key infrastructure for vehicle-to-grid network*, MILCOM 2015-2015 IEEE Military Communications Conference, IEEE, 2015, pp. 1572–1577.

[317] Anitha Varghese and Arijit Kumar Bose, *Threat modelling of industrial controllers: A firmware security perspective*, 2014 International Conference on Anti-Counterfeiting, Security and Identification (ASID), IEEE, 2014, pp. 1–4.

[318] Roland Varriale, Ryan Crawford, and Michael Jaynes, *Risks of electric vehicle supply equipment integration within building energy management system environments: A look at remote attack surface and implications*, National Cyber Summit (NCS) Research Track 2021, Springer, 2022, pp. 163–173.

[319] Alexandr Vasenev, Florian Stahl, Hayk Hamazaryan, Zhendong Ma, Lijun Shan, Joerg Kemmerich, and Claire Loiseaux, *Practical security and privacy threat analysis in the automotive domain: Long term support scenario for over-the-air updates.*, VEHITS, 2019, pp. 550–555.

[320] Hrvoje Vdovic, Jurica Babic, and Vedran Podobnik, *Automotive software in connected and autonomous electric vehicles: A review*, IEEE Access **7** (2019), 166365–166379.

[321] Bin Wang, Yubo Wang, Hamidreza Nazaripouya, Charlie Qiu, Chi-Cheng Chu, and Rajit Gadh, *Predictive scheduling framework for electric vehicles with uncertainties of user behaviors*, IEEE Internet of Things Journal **4** (2016), no. 1, 52–63.

[322] Chwei-Sen Wang, Oskar H Stielau, and Grant A Covic, *Design considerations for a contactless electric vehicle battery charger*, IEEE Transactions on industrial electronics **52** (2005), no. 5, 1308–1314.

[323] Guang Wang, Zhihan Fang, Xiaoyang Xie, Shuai Wang, Huijun Sun, Fan Zhang, Yunhuai Liu, and Desheng Zhang, *Pricing-aware real-time charging scheduling and charging station expansion for large-scale electric buses*, ACM Transactions on Intelligent Systems and Technology (TIST) **12** (2020), no. 1, 1–26.

[324] Han Wang, Soheil Salehi, Hossein Sayadi, Avesta Sasan, Tinoosh Mohsenin, PD Sai Manoj, Setareh Rafatirad, and Houman Homayoun, *Evaluation of machine learning-based detection against side-channel attacks on autonomous vehicle*, 2021 IEEE 3rd International Conference on Artificial Intelligence Circuits and Systems (AICAS), IEEE, 2021, pp. 1–4.

[325] Jiadai Wang, Jiajia Liu, and Nei Kato, *Networking and communications in autonomous driving: A survey*, IEEE Communications Surveys & Tutorials **21** (2018), no. 2, 1243–1274.

[326] Ning Wang, Linhao Tang, and Huizhong Pan, *A global comparison and assessment of incentive policy on electric vehicle promotion*, Sustainable Cities and Society **44** (2019), 597–603.

[327] Xiaolei Wang, Wendao Yao, and Guangwen Shi, *A control system of electric vehicle based on can bus*, The 2011 International Conference on Advanced Mechatronic Systems, IEEE, 2011, pp. 580–582.

[328] David Weissman and Anura Jayasumana, *Integrating iot monitoring for security operation center*, 2020 Global Internet of Things Summit (GIoTS), IEEE, 2020, pp. 1–6.

[329] D Wellisch, J Lenz, A Faschingbauer, R Pöschl, and S Kunze, *Vehicle-to-grid ac charging station: an approach for smart charging development*, IFAC-PapersOnLine **48** (2015), no. 4, 55–60.

[330] Marko Wolf, André Weimerskirch, and Christof Paar, *Security in automotive bus systems*, Workshop on Embedded Security in Cars, Citeseer, 2004, pp. 1–13.

[331] Wenyuan Xu, Chen Yan, Weibin Jia, Xiaoyu Ji, and Jianhao Liu, *Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles*, IEEE Internet of Things Journal **5** (2018), no. 6, 5015–5029.

[332] Erotokritos Xydas, Charalampos Marmaras, Liana M Cipcigan, Nick Jenkins, Steve Carroll, and Myles Barker, *A data-driven approach for characterising the charging demand of electric vehicles: A uk case study*, Applied energy **162** (2016), 763–771.

[333] Aastha Yadav, Gaurav Bose, Radhika Bhange, Karan Kapoor, NCSN Iyengar, and Ronnie D Caytiles, *Security, vulnerability and protection of vehicular on-board diagnostics*, International Journal of Security and Its Applications **10** (2016), no. 4, 405–422.

[334] Eray Yağdereli, Cemal Gemci, and A Ziya Aktaş, *A study on cyber-security of autonomous and unmanned vehicles*, The Journal of Defense Modeling and Simulation **12** (2015), no. 4, 369–381.

[335] Chen Yan, Wenyuan Xu, and Jianhao Liu, *Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle*, Def Con **24** (2016), no. 8, 109.

[336] DianGe Yang, Kun Jiang, Ding Zhao, ChunLei Yu, Zhong Cao, ShiChao Xie, ZhongYang Xiao, XinYu Jiao, SiJia Wang, and Kai Zhang, *Intelligent and connected vehicles: Current status and future perspectives*, Science China Technological Sciences **61** (2018), no. 10, 1446–1471.

[337] Yun Yang, Zongtao Duan, and Mark Tehranipoor, *Identify a spoofing attack on an in-vehicle can bus based on the deep features of an ecu fingerprint signal*, Smart Cities **3** (2020), no. 1, 17–30.

[338] Donghuan Yao, Mi Wen, Xiaohui Liang, Zipeng Fu, Kai Zhang, and Baojia Yang, *Energy theft detection with energy privacy preservation in the smart grid*, IEEE Internet of Things Journal **6** (2019), no. 5, 7659–7669.

[339] Yuan Yao, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang, and Xingshe Zhou, *Voiceprint: A novel sybil attack detection method based on rssi for vanets*, 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, 2017, pp. 591–602.

[340] Dongdong Ye, Rong Yu, Miao Pan, and Zhu Han, *Federated learning in vehicular edge computing: A selective model aggregation approach*, IEEE Access **8** (2020), 23920–23935.

[341] Jin Ye, Lulu Guo, Bowen Yang, Fangyu Li, Liang Du, Le Guan, and Wenzhan Song, *Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions*, IEEE Journal of Emerging and Selected Topics in Power Electronics **9** (2020), no. 4, 4639–4657.

[342] Qiangsheng Ye, *Research and application of can and lin bus in automobile network system*, 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 6, IEEE, 2010, pp. V6–150.

[343] Ziwei Ye, Yuanbo Guo, Ankang Ju, Fushan Wei, Ruijie Zhang, and Jun Ma, *A risk analysis framework for social engineering attack based on user profiling*, Journal of Organizational and End User Computing (JOEUC) **32** (2020), no. 3, 37–49.

[344] Zhiyan Yi, Xiaoyue Cathy Liu, Ran Wei, Xi Chen, and Jiangpeng Dai, *Electric vehicle charging demand forecasting using deep learning model*, Journal of Intelligent Transportation Systems (2021), 1–14.

[345] Lu Yu, Juan Deng, Richard R Brooks, and Seok Bae Yun, *Automobile ecu design to avoid data tampering*, Proceedings of the 10th annual cyber and information security research conference, 2015, pp. 1–4.

[346] Yassine Zein, Mohamad Darwiche, and Ossama Mokhiamar, *Gps tracking system for autonomous vehicles*, Alexandria engineering journal **57** (2018), no. 4, 3127–3137.

[347] Changhua Zhang, Qi Huang, Jiashen Tian, Lei Chen, Yongxing Cao, and Ran Zhang, *Smart grid facing the new challenge: The management of electric vehicle charging loads*, Energy Procedia **12** (2011), 98–103.

[348] Guanchen Zhang, Shaoqing Tim Tan, and G Gary Wang, *Real-time smart charging of electric vehicles for demand charge reduction at non-residential sites*, IEEE Transactions on Smart Grid **9** (2017), no. 5, 4027–4037.

[349] Hongcai Zhang, Zechun Hu, Zhiwei Xu, and Yonghua Song, *An integrated planning framework for different types of pev charging facilities in urban area*, IEEE Transactions on Smart Grid **7** (2015), no. 5, 2273–2284.

[350] Li Zhang, Tim Brown, and Scott Samuelsen, *Evaluation of charging infrastructure requirements and operating costs for plug-in electric vehicles*, Journal of Power Sources **240** (2013), 515–524.

[351] Qingzhao Zhang, Shengtuo Hu, Jiachen Sun, Qi Alfred Chen, and Z Morley Mao, *On adversarial robustness of trajectory prediction for autonomous vehicles*, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022, pp. 15159–15168.

[352] Tao Zhang, Helder Antunes, and Siddhartha Aggarwal, *Defending connected vehicles against malware: Challenges and a solution framework*, IEEE Internet of Things journal **1** (2014), no. 1, 10–21.

[353] Tao Zhang and Quanyan Zhu, *Distributed privacy-preserving collaborative intrusion detection systems for vanets*, IEEE Transactions on Signal and Information Processing over Networks **4** (2018), no. 1, 148–161.

[354] Yan Zhang, Stein Gjessing, Hong Liu, Huansheng Ning, Laurence T Yang, and Mohsen Guizani, *Securing vehicle-to-grid communications in the smart grid*, IEEE Wireless Communications **20** (2013), no. 6, 66–73.

[355] Yongmin Zhang, Pengcheng You, and Lin Cai, *Optimal charging scheduling by pricing for ev charging station with dual charging modes*, IEEE Transactions on Intelligent Transportation Systems **20** (2018), no. 9, 3386–3396.

[356] Tianyu Zhao, Chi Zhang, Lingbo Wei, and Yanchao Zhang, *A secure and privacy-preserving payment system for electric vehicles*, 2015 IEEE International Conference on Communications (ICC), IEEE, 2015, pp. 7280–7285.

[357] Bowen Zheng, Muhammed O Sayin, Chung-Wei Lin, Shinichi Shiraishi, and Qi Zhu, *Timing and security analysis of vanet-based intelligent transportation systems*, 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), IEEE, 2017, pp. 984–991.

[358] Haibo Zhou, Wenchao Xu, Jiacheng Chen, and Wei Wang, *Evolutionary v2x technologies toward the internet of vehicles: Challenges and opportunities*, Proceedings of the IEEE **108** (2020), no. 2, 308–323.

[359] Juncheng Zhu, Zhile Yang, Monjur Mourshed, Yuanjun Guo, Yimin Zhou, Yan Chang, Yanjie Wei, and Shengzhong Feng, *Electric vehicle charging load fore-*

casting: A comparative study of deep learning approaches, Energies **12** (2019), no. 14, 2692.

[360] Ioannis Zografopoulos, Charalambos Konstantinou, and Nikos D Hatziargyriou, *Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations*, arXiv preprint arXiv:2205.11171 (2022).

[361] Ioannis Zografopoulos, Juan Ospina, Xiaorui Liu, and Charalambos Konstantinou, *Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies*, IEEE Access **9** (2021), 29775–29818.

Appendix A

Electric Vehicle and Charging Station Attacks and Challenges Descriptions

Here we demonstrate each of the attack definitions in Chapter 4's taxonomy. These definitions helped us determine the correct levels of impact, likelihood, and risks of each of the attacks.

Table A.1: Electric Vehicle Supply Equipment Attacks Vectors Threaten Different Aspects of Security

Aspects	Threat	Vulnerability	Description
Charging Station Security	Spoofing	EVSE Spoofing or Impersonation	Masquerading as an EVSE in order to gain unauthorized access to sensitive data, introduce malicious software, or manipulate the charging process
		Management Building Spoofing	Spoofing message transmissions to EVSE and the management building to gain unauthorized access
		Brute Force Attack	Bypassing EVSE authentication by repeatedly trying different authentication credentials
		Packet Sniffing/Spoofing	Intercepting and analyzing data packets exchanged between the EV and the EVSE to extract sensitive information
	Tampering	EVSE Charging Sessions Tampering	Manipulating charging session data, which results in incorrect billing, damage to the battery, or even a fire hazard
		Vandalizing EVSE	Physical tampering or damage to the EVSE, resulting in malfunctioning or unusability
		Measurement Tampering	Manipulating measurements of electricity consumed during charging, which leads to inaccurate billing or battery damage
		Injecting Malware	Inserting malicious code or malware to compromise an EVSE
	Repudiation	EVSE Communication and Session Eavesdropping	Intercepting and listening to the communication in order to modify messages, potentially leading to false accusations and disputes
		Side-channel Attacks, including Power-analysis	Monitoring or manipulating power consumption, electromagnetic radiation, or timing, leading to false accusations or repudiation
	Information Disclosure	Software Exploitation and Data Breach	Exploiting EVSE software to gain unauthorized access to sensitive data, including personal information
		Grid and SCADA Information Theft	Unauthorized access to the SCADA system or the smart grid that EVSE is connected to, and stealing sensitive information
		Charging Session Information Theft	Stealing sensitive information related to the charging session, such as the locations and payments
		Side-channel Attacks including Timing, Electromagnetic, and Fault Injection	Stealing sensitive information by analyzing electromagnetic signals, utilizing the time it takes to operate, and introducing faults into a system
	DoS	EVSE and Cloud Communication DDoS	Overwhelming the communication channel between the EVSEs and the cloud servers
		Botnet Attack	Taking over a large number of EVSE and uses them to generate massive amounts of traffic to overwhelm the server
		Demand Response DoS	Overloading DR feature of the system and prevent users from charging their EVs
		Power Replay Interference	Capturing and replaying power signals transmitted between EV and EVSE, which results in unauthorized charging or DoS
	Elevation of Privilege	Unauthorized Access to EVSE	Unauthorized physical or remote access to EVSE, which leads to manipulation or control of EVSE
		EVSE Hijacking	Taking control of EVSE and preventing users from accessing it by changing the authentication credentials
		SCADA Privilege Escalation	Gaining high levels of access or control over the EVSE and SCADA, leading to a compromised smart grid

Table A.2: Electric Vehicle Information Privacy Attacks Vectors Threaten Different Aspects of Security

Aspects	Threat	Vulnerability	Description
Information Privacy	Spoofing	User Data Spoofing	Altering or forging information about EV or EVSE users to deceive the system or other users for fraudulent activities
		EV Sensors Spoofing	Modifying the sensors data to provide false information to the EVSE, EVSE, and users
		User or Vehicle Identity Theft	Impersonating the identity of a user or a vehicle to gain access or conduct malicious activities such as fraud or theft
	Tampering	EV Sensors Data Tampering	Altering sensors data that the EV or EVSE rely on which results in incorrect decisions
		EV Embedded Systems Tampering	Compromising control systems within an EV, which results in unauthorized access, modification or deletion of data
		EV Blackbox Tampering	Modifying or manipulating data recorded by an EV's black box which affects accident investigation, insurance claims
		Demand Response Data Tampering	Altering data exchanged between EV and charging infrastructure to manipulate demand response signals or change billing information
	Repudiation	EV Communication Eavesdropping	Intercepting EV communication to capture sensitive data, including location, driving behaviour, or charging activity
		EV OBD Port Eavesdropping Attack	Intercepting sensitive data transmitted through the CAN bus and OBD port, such as ECU communications
	Information Disclosure	Relay and Tracking Attacks	Intercepting EV signals and relaying them to a different endpoint or tracking the vehicle's movements
		EV or User Information Theft	Stealing sensitive information about EVs or their users, such as sensor data, Vehicle Identification (VID), and other personally identifiable information (PII)
		Side-channel Attacks, including Cache Attacks	Stealing sensitive user data by exploiting vulnerabilities in the hardware or software of the EV's cache memory
		User Profiling Attack	Using data collected from various sources to create a detailed profile of the user for malicious purposes such as identity theft, targeted advertising
		EV Telemetry Data Theft	Stealing data transmitted in telemetry services such as GPS, Bluetooth, and Wi-Fi to get EV usage, driving behaviour, or personal data
	DoS	EV or EVSE Energy Trading Inference Attack	Inferring sensitive information related to the energy trading by analyzing the energy consumption patterns, revealing location or driving behaviour
		EV Communication Replay or Flooding Attack	Repeatedly sending messages to EV, overwhelming it with data and denying legitimate requests
	Elevation of Privilege	EV or EVSE Unauthorized Data Access	Gaining unauthorized entry into an EV or EVSE to steal or manipulate sensitive data, which may include personal information, location data, and energy management information

Table A.3: Electric Vehicle Software Security Attacks Vectors Threaten Different Aspects of Security

Aspects	Threat	Vulnerability	Description
Software Security	Spoofing	Brute Force Attack	Bypassing software authentication, leading to unauthorized access to EV software and system
		Firmware Spoofing	Gaining unauthorized access to the EV's firmware, replacing it with malicious firmware, and taking control of the vehicle
		EV Server or Software Impersonation	Impersonating EV server or software to gain access to sensitive data or perform malicious actions
		Spoofing Identity Authentication	Tricking EV or EVSE, bypassing authentication and gaining access to protected resources and performing actions on behalf of users
	Tampering	EV or EVSE Software Tampering	Maliciously altering the EV or EVSE software to exploit vulnerabilities and gain unauthorized access to sensitive data or systems
		Injecting Command, Malware or Insecure Code	Injecting malicious code, malware, or commands into the EV software leading to unauthorized access, data exfiltration, or denial of service
		Embedded System Tampering	Physical tampering of the embedded systems causing a malfunction or stealing data
		Firmware/OS Kernel Exploitation	Manipulating ECU firmware or kernel of EV, leading to unauthorized access and executing arbitrary code
		Over The Air Updates Tampering	Altering the firmware or software update process, resulting in unauthorized access or injection of malicious code
	Repudiation	Charging fraud and Transaction Manipulation	Manipulating charging sessions, payment transactions, or the EVSEs leading to financial losses for users and businesses
		EV or EVSE Software MitM Eavesdropping	Intercepting and listening in on the communication between the EVSE software and EV during the charging process, potentially gaining access to sensitive information such as user credentials or other private data
	Information Disclosure	Software Data Theft	Gaining access to EV software and stealing information such as location, driving patterns, and other personal data
		Side-channel Attacks, including Timing Attacks	Sensitive information stealing by exploiting vulnerabilities in the EV software or by analyzing execution times and reverse engineering the application
		Cloud Information Theft	Gaining access to the cloud services and stealing sensitive information such as user data, EV location, and billing information
	DoS	Updates and Over The Air Update DoS	Disrupting or overwhelming the update or over-the-air update process of EV
		EV and EVSE Software DDoS	Overwhelming or disrupting the normal functioning of the software, causing unavailability and resource depletion.
		Software Cloud Service DDoS	Overwhelming the cloud service infrastructure with a large number of requests, causing the service to become unavailable
		Software-initiated Fault Attacks for Embedded Systems	Exploiting vulnerabilities in the software running on an embedded to generate incorrect results or take incorrect actions
	Elevation of Privilege	Configuration and Relay Attacks	Manipulating the configuration or communication of software to gain unauthorized access or control
		Shrink Wrap Code Attacks	Exploiting known vulnerabilities in third-party code libraries or modules to elevate their privileges
		Firmware Exploitation	Exploiting vulnerabilities in the firmware of an EV to gain higher privileges and access to sensitive information

Table A.4: Connected Electric Vehicle Attacks Vectors Threaten Different Aspects of Security

Aspects	Threat	Vulnerability	Description
Connected Vehicles Security	Spoofing	Connected Vehicle Impersonation Attack	Posing as a legitimate vehicle to manipulate data or send false messages with the intention of compromising the platoon
		Replay Interference Attack	Intercepting and replaying legitimate messages in an attempt to manipulate the behavior of connected EVs
		Cooperative Interference Attack	Malicious entity's cooperation with a legitimate entity to send forged messages or disrupt communication
		Brute Force Attack	Gaining access to a vehicle's systems or data by systematically trying a large number of possible combinations
		Connected Entity Spoofing	Impersonating a connected entity, such as a vehicle or a roadside unit, to gain access or execute malicious actions
	Tampering	Botnet Attack	Using a network of compromised devices to launch a coordinated attack on the vehicles' systems
		Wi-fi Wardriving	Using tools to scan for wireless networks, identify vulnerabilities, or intercept data traffic for data tampering
		Physical (ECU or TCU) Tampering Attacks	Physically accessing ECUs or TCU and modifying their firmware, sensors, or hardware to gain unauthorized access or steal data
		Injecting Malware	Injecting malicious software into the system of the connected vehicle to gain access or steal data
		Injecting Insecure Code	Injecting malicious code into the connected vehicle to take control of the vehicle or steal sensitive information
	Repudiation	Message Repudiation, including Reply Attack and Data-Driven Attack	Manipulating data being transmitted to and from a vehicle to conceal or misrepresent their actions
		Event Logging Repudiation and Forensic Attack	Altering time stamps, deleting or adding entries, or modifying the logs to conceal or modify the evidence
	Information Disclosure	Packet Sniffing	Intercepting and analyzing network traffic to extract sensitive information
		Network Discovery Attacks	Discovering and probing network that connected vehicles use to communicate
		Vehicle Energy Management System and Electrical Drive System Data Theft	Intercepting and Stealing sensitive data related to the vehicle's energy management system and electrical drive system
		Connected Vehicle Profiling Attack	Monitoring communication of the network to gather information about vehicles and their drivers
	DoS	Radio Frequency Interference Attack	Transmitting a powerful radio frequency signal in the same frequency range as the EVs, causing interference
		Connected Entity DDoS	Flooding communication channel of connected entities with traffic or requests to overload and disrupt the communication
		Software Cloud Service DDoS	Overwhelming cloud-based service with a flood of traffic or requests, which makes it unavailable to users and EVs
		DSRC/V2X DDoS	Flooding the communication channel between vehicles and other entities in DSRC/V2X ecosystem.
	Elevation of Privilege	Rootkit attack	Gaining access to a higher level of privilege in the system through the use of a malicious rootkit software
		Connected Vehicles Hijacking	Taking control of a vehicle, allowing the attacker to manipulate the vehicle, such as steering, acceleration, and braking

Table A.5: Autonomous Electric Vehicle Attacks Vectors Threaten Different Aspects of Security

Aspects	Threat	Vulnerability	Description
Autonomous Vehicles Security	Spoofing	Spoofing Vehicle Bus Messages or OBD Port	Impersonating control messages to send fake commands and compromise ECUs functionality
		Spoofing Sensor Data	Manipulating or sending false data to the sensors to deceive the autonomous vehicle's perception
		Spoofing Traffic or Map Information	Manipulating or providing false traffic or map information, leading the vehicle to make incorrect decisions or routes
	Tampering	Injecting Malware	Unauthorized access to the vehicle's system and installs malicious software, compromising the vehicle or autonomous driver
		Vehicle Sensors Sybil Attack	Forging multiple fake identities (i.e., spoofing) to manipulate the sensor data of the vehicle, leading to tampering
		Tampering Vehicle Bus Messages	Manipulating the messages transmitted on the CAN bus to disrupt or modify the normal behaviour
		Vehicle Configuration Settings Tampering	Modifying vehicle parameters such as autonomous system, braking performance, and steering sensitivity
		Vehicle Navigation / Diagnostic Systems Tampering	Altering or falsifying important information or data, leading to incorrect decisions made by the vehicle
		Vehicle Sensor Tampering	Manipulation of the data collected by sensors on the vehicle, misleading the autonomous driving making incorrect decisions
		Adversarial Machine Learning Attacks	Manipulating or adding adversarial inputs to the machine learning algorithm to cause misclassification or malfunction in the autonomous vehicle's decision-making process
		Poisoning Attack in Machine Learning	Modifying the training data or input of a machine learning algorithm to degrade the accuracy of the model
	Repudiation	Message and Event Log Repudiation	Manipulating the message and event logs, which makes it difficult to verify the authenticity and accuracy of the logs
		Monitoring OBD or CAN Bus Message	Modifying CAN messages by attackers to cover their tracks and making them harder to investigate/detect their activities
	Information Disclosure	Data Privacy and Data Sharing Attack	Exploiting vulnerabilities in the data privacy and sharing mechanisms of vehicles to steal sensitive information
		Autonomous Driving System, Data Theft	Stealing data, transmitted between assistant system and components, such as driver behaviour or sensor data
		Autonomous Driving System Reverse Engineering	Reverse engineering the assistant system to learn its operations and potentially uncover sensitive information
	DoS	Sensor and Network Jamming Attack	Flooding the sensors and network communication with noise or interference causing them to malfunction
		Autonomous System DoS	Flooding the autonomous system requests, exploits vulnerabilities, or overloads with excessive computation
		In-Vehicle Bus Communication DoS	Sending a high volume of traffic or manipulates bus communication signals to disrupt ECUs communication
	Elevation of Privilege	Autonomous System Hijacking	Exerting control over a system to induce unintended actions, such as altering the route, accelerating or decelerating the vehicle, or abruptly bringing it to a stop

Vita

Candidate's full name: Soheil Shirvani

University attended:
Master of Computer Science University of New Brunswick, 2021-2023
Bachelor of Science in Electrical Engineering University of Tehran, 2016-2021

Publications:
Soheil Shirvani, Yaser Baseri, and Ali A. Ghorbani. "Evaluation Framework for Electric Vehicle Security Risk Assessment". Under the second review, submitted in June 2022, IEEE Transactions on Intelligent Transportation Systems. IEEE, 2022.

Soheil Shirvani and Ali A. Ghorbani. "A Comprehensive Study of EV-EVSE Ecosystem Architecture: Intelligent Monitoring Framework for Enhancing Charging Sessions Security". Under review, submitted in May 2023, IEEE Transactions on Intelligent Transportation Systems. IEEE, 2023.