energies

MDPI

Article

Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability

Zia Muhammad [1], Zahid Anwar [1,*], Bilal Saleem [2] and Jahanzeb Shahid [3]

[1] Department of Computer Science, Sheila and Robert Challey Institute for Global Innovation and Growth, North Dakota State University (NDSU), Fargo, ND 58108, USA
[2] Department of Cybersecurity, Air University, Islamabad 44000, Pakistan
[3] Department of Information Security, National University of Sciences and Technology, Islamabad 44000, Pakistan
[*] Correspondence: zahid.anwar@ndsu.edu

Abstract: With the global energy crisis, increasing demand, and a national-level emphasis on electric vehicles (EVs), numerous innovations are being witnessed throughout the EV industry. EVs are equipped with sensors that maintain a sustainable environment for the betterment of society and enhance human sustainability. However, at the same time, as is the case for any new digital technology, they are susceptible to threats to security and privacy. Recent incidents demonstrate that these sensors have been misused for car and energy theft, financial fraud, data compromise, and have caused severe health and safety problems, amongst other things. To the best of our knowledge, this paper provides a first systematic analysis of EV sustainability, digital technologies that enhance sustainability, their potential cybersecurity threats, and corresponding defense. Firstly, three robust taxonomies have been presented to identify the dangers that can affect long-term sustainability domains, including (1) life and well-being, (2) safe environment, and (3) innovation and development. Second, this research measures the impact of cybersecurity threats on EVs and correspondingly to their sustainability goals. Third, it details the extent to which specific security controls can mitigate these threats, thereby allowing for a smooth transition toward secure and sustainable future smart cities.

Keywords: cybersecurity; sustainability; smart cities; EVs; automotive cybersecurity; demand response; optimization; cyber threats; EV security; vehicle safety

check for updates

Citation: Muhammad, Z.; Anwar, Z.; Saleem, B.; Shahid, J. Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability. *Energies* **2023**, *16*, 1113. https://doi.org/10.3390/en16031113

Academic Editor: Chunhua Liu

Received: 19 December 2022
Revised: 13 January 2023
Accepted: 15 January 2023
Published: 19 January 2023

1. Introduction

Current technology evolution is a gradual step toward intelligent transportation systems (ITS) and smart cities. With incremental technological improvements, human reliance on the internet of things (IoT) has increased enormously. The IoT market is projected to grow by 194 billion US dollars, and the number of connected devices is estimated to grow to 525 billion by the end of 2027 [1]. This gradual adoption of IoT is due to its compatibility, ease of integration into EVs, road safety equipment, traffic controls, and intelligent transportation [2]. Currently, the world is facing a fuel crisis, and the global community is looking for alternative ways to use renewable energy sources and green energy to meet energy consumption needs. This drastic shift is a leading case for the enormous growth of EVs. In recent years, there has been a tremendous increase in EV sales and global acceptance of EVs around the world [3–5]. One of the main drivers of this smooth transition is the acceptance of innovation and trust in technology. By improving the efficiency of EVs, the transportation industry can be more environmentally friendly, productive, and agile.

1.1. Motivation

EVs facilitate drivers, maintain roadside safety, and improve sustainability by preventing injuries and reducing accidents [6,7]. However, on the other hand, user data security and privacy concerns are increasing with the embedded sensors that collect information such as personal identifiable information (PII), financial, health, charging logs, driving habits, video, location coordinates, and car-related data [8]. There are also many potential cyber threats to vehicular technology, such as third-party application libraries, identity thefts, private data breaches, cryptojackings [9], and ransomware [10]. Due to these threats, the confidentiality and privacy of user data is at continued risk [11]. This means that the more we try to make EVs sustainable by introducing cameras, tracking devices, and sensors, the more vulnerable we become to cybersecurity threats that target these sensors.

1.2. Challanges

The challenges arise because cybersecurity and sustainability are two different domains. Sustainability is related to the ecological balance between the environment, economic growth, and social well-being [12–14], while cybersecurity is the practice of protecting networks, systems, and programs from cyber-attacks. The importance of both domains cannot be denied. Sustainability researchers work on structural and economic components, such as reducing the time to market for EVs, minimizing costs, and introducing new sensors for environmental suitability. Therefore, new technology is introduced at a rapid pace, but their security controls are limited and may not be defined with the required pace that competes with the production rate [15]. This is because cybersecurity experts conduct limited studies in domains of sustainability; therefore, there is a research gap in the industry [16]. EV manufacturing is a big industry with a huge cash flow. Still, there is limited research available, and very few efforts are made to define guidelines and standards that highlight how to achieve sustainability without compromising cybersecurity. Hence, it is necessary to define the suitability aspects of EV sensors in comparison to their potential cyber threats and vulnerabilities. There is also a need to find a correlation between the sustainability of EVs and cyber threats targeting these EVs [17].

There are many types of sensors that, if properly used inside EVs, can help achieve certain sustainability goals; however, sensors have overlapping requirements and vulnerabilities, and it is not known which sensors affect or facilitate us to achieve what kind of sustainability goals. There exists no mapping between these sensors and the sustainability goals that they tend to achieve; therefore, there is a strong need to define a mapping between the cybersecurity challenges of sensors and their impact on sustainability. When we have these types of mapping, companies can direct their budget, efforts, and research toward developing security-hardened sensors that achieve a particular sustainability goal.

1.3. Methodology

To address these challenges, a survey of the current literature has been performed in the field of cybersecurity and three main domains of sustainability, including (1) life and well-being, (2) safe environment, and (3) innovation and development. Additionally, seventeen different types of EV sensors were surveyed, and their impacts were mapped to the appropriate sustainability domain. Twelve cybersecurity threats were indentified that can affect EV sensors and may lead to cyber attacks if exploited. Finally, the article proposes thirty-five security controls that can be used to secure EVs from cyber threats. To this effect, three taxonomies have been introduced: (1) sensor-to-sustainability, (2) threats-to-sensors, and (3) defenses-to-threats. These taxonomies classify multiple EV sensors into different domains of sustainability, visualize multiple cyber threats targeting sensors, and provide safeguards to defend against cyber threats.

1.4. Contribution

1. The article serves as a resource for cybersecurity and sustainability researchers, as well as EV manufacturers, by providing domain knowledge and insights into cybersecurity challenges and approaches for minimizing the impact of cyber threats on the sustainability benefits of EV technology.

2. The research proposes a novel sustainability–sensors–threats–controls taxonomy that firstly provides a benchmark for measuring the level of achievement in meeting sustainability goals by the types of sensors deployed in an EV. Second, it describes how much effort needs to be allocated for defending against cyber threats that a sensor presents.

1.5. Paper Organization

The paper is categorized into the following sections: Section 2 provides a survey and comparative analysis of recent studies on the chosen topic. Section 3 provides details on environmental sustainability and EV sensors. Section 4 highlights emerging cyber threats and past cyber attacks. Section 5 provides details of security controls that can be used to defend and make EVs secure. Section 6 contains current issues and open challenges. Section 7 concludes the paper and provides future directions.

2. Literature Review

The section provides current studies and highlights contemporary efforts that were reviewed during the research work. Recent research studies are comparatively analyzed based on their significant contributions, critical points, research focus, advantages, and limitations in Table 1. The table also compares this article with previous efforts.

Table 1. Comparative analysis of various dimensions of existing studies.

Author	Cyber Threats	Human Impact	Environmental Sustainability	Applications	Open Issues
Othman et al. [18]	×	✓	✓	✓	×
Silva et al. [19]	×	×	✓	×	✓
Hataba et al. [20]	✓	×	×	✓	×
Ahmed et al. [21]	×	×	✓	✓	✓
Alam et al. [22]	×	×	✓	✓	✓
Bathla et al. [23]	✓	✓	×	×	×
Bharat. et al. [24]	✓	×	✓	×	✓
Kim et al. [25]	✓	×	×	✓	×
Underlined article	✓	✓	✓	✓	✓

The growing use of sensors has been seen in both traditional internal combustion engine (ICE) vehicles as well as electric vehicles for increased monitoring, control, and optimization. However, the latter has comparatively more sensors than an ICE. According to research estimates [26], there are roughly around 1000 chips in a non-electric vehicle and twice as many in an electric one. In fact, the growing demand of electric vehicles in the year 2021–2022 saw a chip shortage in the USA [27]. Furthermore, sensors used in EVs tend to be more advanced in terms of circuitry, interfaces and resolution as compared to their ICE counterparts. While the ideas proposed in this research apply to both ICEs as well as EVs, the article specially targets EVs as its research target more so because unlike traditional ICEs, electric vehicles are being promoted by governments worldwide as a viable solution for environmental sustainability.

Given these considerations, we believe that electric vehicles are a particularly relevant and interesting research target, as they have the potential to significantly impact the sustainability of transportation systems and require careful attention to cybersecurity. Our research aims to explore the internal relationship between these issues in order to inform the development of more sustainable and secure electric vehicles.

Othman et al. [18] focus on implementing the safety characteristics of EVs, assessing their impact on public health and social well-being, and also highlighting the ways EVs evolve into autonomous vehicles that facilitate human life and future generations. Silva et al. [19] work on the environmental impact of EVs. The researchers explored the impact of EVs in terms of gas emissions, air quality index, traffic flow, soil impact, and noise pollution. Similarly, Hataba et al. [20] identified potential privacy problems, security issues, and cyber threats in autonomous vehicles. These researchers highlight data collection points, security challenges, cyber breaches and proposed a possible way to minimize and defend against these threats. Examples of attacks analyzed include traffic flow attacks, platooning, carpooling, and parking attack scenarios.

Ahmed et al. [21] surveyed EVs and their support for advanced driving assistance systems (ADAS) to highlight the advantages, limitations, and how this technology impacts the vehicle driver. The authors also highlighted practical applications of vehicles, laws of federal governance, legislation, and regulations. In another research, Alam and Georgakis [22] performed a comparative analysis of inter-connected EVs and covered multiple aspects of intelligent mobility management, such as traffic projection, message communication, and environmental impacts. The authors also highlighted the possible future impact of small-scale networks that the author constructed using simulations of traffic streams.

Bathla et al. [23] surveyed smart vehicles and highlighted their practical applications, current challenges, and future opportunities. The authors also discussed the effects of the smart automotive industry on public health and safety as well as current cybersecurity challenges and privacy issues. Bharathidasan et al. [24] conducted a systematic review of the drastic change in the transportation sector to highlight energy trends, technological requirements, and cybersecurity issues. The article focuses on integrating EVs with renewable energy sources, highlighting global scenarios of an energy crisis, and discusses open issues. Finally, Kim et al. [25] published an article covering the cybersecurity issues of autonomous vehicles by demonstrating possible attack scenarios. The authors highlighted potential security flaws and vulnerabilities that lead to exploitation and affect driver safety. The authors also provided a research pathway for defending against certain EV attacks using AI and machine learning techniques.

The research works compared in Table 1 are significant efforts that cover the wide domain of cybersecurity and sustainability. During the research, we were unable to find articles that build relationships, depict and taxonomize cybersecurity challenges with sustainability. To the best of our knowledge, this is the first systematic analysis that addresses the limitations of current works. This is achieved by extracting information about different EV sensors, cyber threats, and security defenses from the literature and then categorizing, mapping, and establishing a relationship between them to facilitate readers for an easier comprehension of how these domains relate.

3. Sustainability Impact of EVs

Sustainability is the ability to meet the needs of the present world without compromising the needs of future generations. In terms of EVs, sustainability refers to the ability of EVs to be a viable and environmentally friendly alternative to traditional gasoline-powered vehicles [28,29]. This means that EVs should be able to fully meet the transportation needs of people without negatively impacting the environment or depleting natural resources [30].

Various types of sensors in EVs play a vital role in making EVs more sustainable. Each sensor is designed to achieve a certain task, such as forward collision avoidance, emergency braking, vehicular communication, and street sign recognition. Figure 1 provides an illustration of multiple sensors that makes EVs more sustainable and helps improve vehicle safety. Sensors collect information about the vehicle's surroundings and assist the vehicle's driving system, which can in turn help reduce the risk of accidents.

EVs serve in multiple domains of sustainability, and on a broader level, sustainability can be divided into three major domains (also sometimes referred to as sustainability goals) such as (1) *life and well-being*, (2) *safe environment*, and (3) *innovation and development* [28,31].

1. **Life and well-being:** EVs reduce roadside accidents, minimum global deaths, ensure passenger safety, and provide ease for drivers [32]. Moreover, EVs reduce environmental health hazards as they help to improve the quality of life for people living in urban areas, where air pollution is often a major concern. The first sustainability goal, *life and well-being*, further divides into two subdomains as (1) *reduction of death rate* and (2) *ease and accessibility*.

2. **Safe environment:** EVs also have a positive impact on the environment because they do not produce any greenhouse gas emissions, which are a major contributor to climate change. In addition, EVs are often more energy efficient than gasoline-powered vehicles, which can help reduce reliance on fossil fuels and the associated environmental impacts. The second sustainability goal, *safe environment*, further divides into three subdomains as (1) *roadside safety*, (2) *intelligent transportation*, and (3) *eco-friendliness*.
3. **Innovation and development:** EV manufacturers are working to introduce innovation and cater to challenges through improved models that have longer battery life and are safer to drive. EVs have multiple sensors that help to improve fuel economy, minimize travel time, reduce congestion and drive innovation and development in the transportation sector. For example, the development of new technologies and infrastructure, such as charging stations, can help support the growth of the electric vehicle market and improve the overall sustainability of the transportation system. This third sustainability goal, *innovation and development*, is further divided into three subdomains as (1) *improved fuel economy*, (2) *minimize travel time*, and (3) *reduce congestion*.

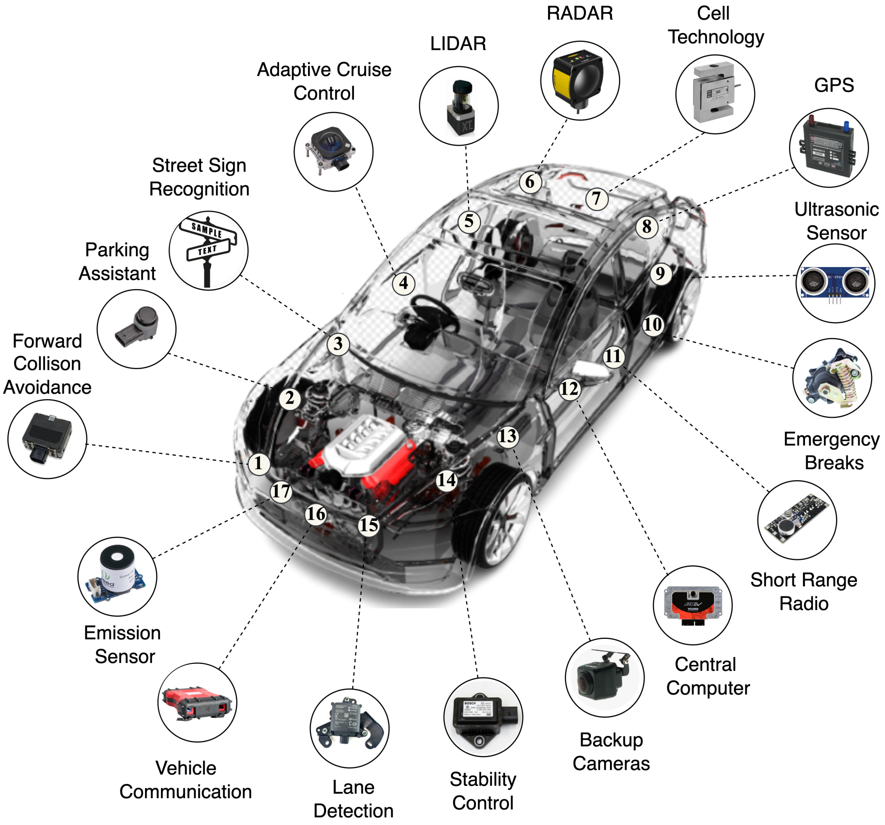

Figure 1. Illustration of numerous sensors and safety features of EVs.

The discussed domains and subdomains of sustainability are systematically visualized in the first taxonomy named *sensor-to-sustainability* in Figure 2. The taxonomy has two parts; part one classifies three main domains of sustainability as *life and well-being*, *safe environment*, and *innovation and development*, which are further broken up into subdomains. Part two then maps these domains to the various sensors designed by EV manufacturers that can help achieve these sustainability goals. For example, death rate due to accidents (a sustainability goal) can be achieved by installing forward collision avoidance sensors.

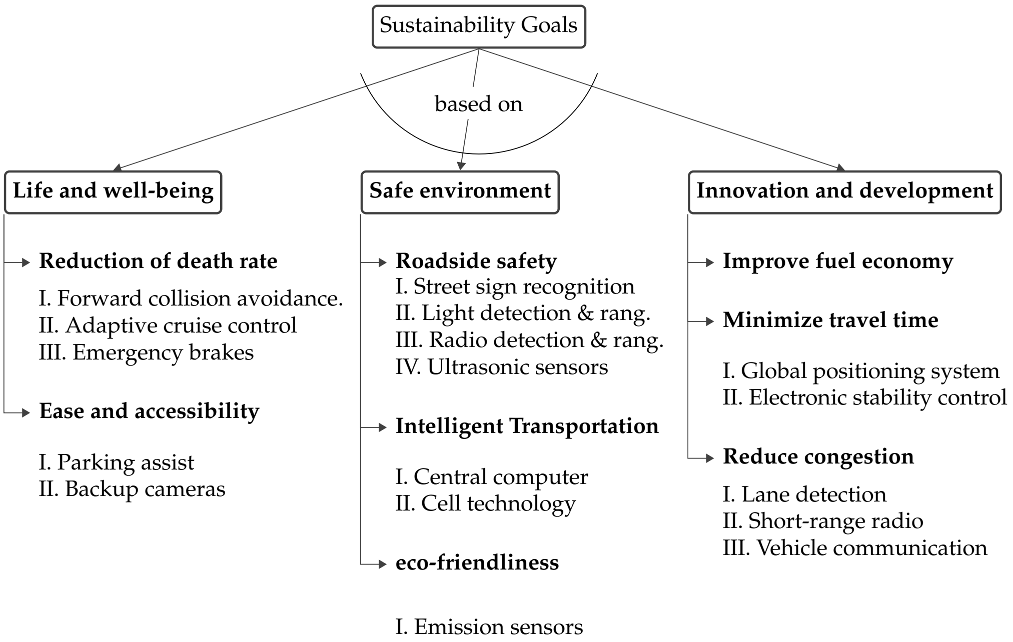

Figure 2. Sensor-to-Sustainability: first taxonomy that maps EV sensors with domains of sustainability.

The predicate logic representation of the taxonomy has been presented in Equation (1).

$$S \Rightarrow S' \tag{1}$$

$$S = \{sensor1, sensor2, sensor3, \dots\}$$
$$S' = \{domain1, domain2, domain3, \dots\}$$

In the given equation, (S) is used for the set of chosen sensors illustrated in Figure 1, and (S') is a set of sustainability domains. Thus, the given equation can be interpreted as the set of sensors (S) implies the domains of sustainability that they help achieve (S'). For the underlined scenario, we are considering three domains of sustainability and 17 EV sensors, but this set can be extended as per requirements. A detailed overview of the sustainability domain and EV sensors is added in the subsequent subsection.

3.1. Life and Well-Being (First Goal of Sustainability)

EVs detect the environment through multiple sensors and take certain actions that address different aspects of life and well-being, such as (1) *reduction of death rate* and (2) *ease and accessibility*.

3.1.1. Reduction of Death Rate

In 2021, 42,915 road accidents occurred in the USA alone [33]. These accidents cause severe injury to not only vehicle passengers and drivers but also pedestrians passing by [34]. EVs can help reduce deaths from transportation-related causes in several ways. First, because EVs produce zero emissions, they can help reduce air pollution, which is a major contributor to respiratory illnesses and other health problems [35]. Second, EVs are generally quieter than gasoline-powered vehicles, which can help reduce noise pollution, which has been linked to an increased risk of heart disease and other health problems [36]. Finally, EVs can help reduce traffic accidents because they are often equipped with advanced safety sensors that can help make roads safer for everyone [37,38]. The following provide an overview of the sensors that may reduce traffic deaths.

(i) *Forward collision avoidance:* Front-mounted sensors are designed to detect and avoid forward collisions with other vehicles and road objects. This is achieved by decreasing the speed and increasing the braking force [39]. Forward-facing sensors include radar, camera, or any other laser-based sensor.

(ii) *Adaptive cruise control (ACC):* ACC is a safety framework that automatically controls the acceleration and braking of a vehicle [40]. The framework automatically adjusts the speed of the vehicle with the car in front and maintains a safe distance. If the car ahead slows down, the ACC automatically slows down to match it.

(iii) *Automatic emergency braking (AEB):* AEB is a safety feature that detects and identifies possible collisions. It automatically activates the brakes to slow down and even stop moving vehicles before the crash [41].

3.1.2. Ease and Accessibility

EVs provide ease and accessibility in a number of ways. They are generally easier to drive, with smooth acceleration and a quiet, comfortable ride as compared to conventional vehicles. Additionally, EVs are often equipped with technology such as touchscreens and voice-activated assistants, which can make EVs easier and more convenient to use. Moreover, EVs provide ease to passengers with driving assistance and accessibility features for disabled and visually impaired people.

(i) *Parking assist:* The vehicle parking assistance system uses a variety of sensors and cameras around the vehicle to calculate the parking space and park appropriately within the space available [42]. Autonomous vehicles provide an easy interface for parking assistance; There is a button inside the vehicle to implement the framework. As soon as the button is pressed, the sensors will begin checking for space sufficient for the vehicle to be parked safely [43].

(ii) *Backup cameras:* Some EVs come with preinstalled rear-facing backup cameras that provide a precise view of the rear field and visualize the front view and blind spots. EVs have multiple backup cameras in different positions that are mounted to save lives, reduce vehicle-related crashes, and prevent injuries [44].

3.2. Safe Environment (Second Goal of Sustainability)

EVs are equipped with sensors that allow the vehicle to "see" its surroundings and identify objects such as other vehicles, pedestrians, and traffic signs. The vehicle's computer can then use this information to decide how to navigate the road safely. *Safe endowment* is further classified into three subgoals of sustainability such as (1) *roadside safety*, (2) *intelligent transportation*, and (3) *eco-friendliness* as follows:

3.2.1. Roadside Safety

(i) *Street sign recognition:* Street sign recognition is a framework that perceives street signs and reflects the intended action [45]. The instructions are normally shown on a dashboard screen. The framework traditionally utilizes a forward-looking camera placed behind the windshield to "look for" street signs. Most EVs use ADAS cameras that are front-mounted and efficient in detecting and capturing images of street signs, roads, pedestrians, vehicles, and other roadside objects [46].

(ii) *Automatic Emergency Braking System (AEBS):* AEBS is a security framework that takes automated action in applying brakes before a crash to slow or stop a vehicle to avoid serious impact. AEBS uses radars, cameras, or LIDAR technology to operate and tackle dangerous situations [47].

(iii) *Light detection and ranging (LIDAR):* LIDAR is used to determine how far something is from the vehicle. It is basically a distance-measuring unit that uses light signals for accurate positioning and for obtaining distance information [48]. This enables EVs to precisely detect still and moving objects even in low light conditions and challenging weather.

(iv) *Radio detection and ranging (RADAR):* A RADAR is an electromagnetic sensor used to recognize, find, track and distinguish different objects over impressive distances. It works by sending electromagnetic energy to targets [49]. RADAR is used to identify the location, velocity, and angle of an object.
LIDAR and RADAR are used to achieve the same goal of object detection [50]. They can be used together or individually, depending on the circumstances. They differ in that RADAR works on radio waves using either a fixed or rotating antenna having a large wavelength, while LIDAR uses laser light beams and is capable of building 3D models having a smaller wavelength [51].

(v) *Ultrasonic sensors:* An ultrasonic sensor is used to measure the distance from an objective by producing ultrasonic waves. It has two fundamental parts: a transmitter (which delivers sound) and a recipient (which experiences the sound after it travels to and bounces off the objective). These sensors and sonars are used in EVs for navigation and range assistance [52]. Moreover, the feature is helpful in vehicle parking and nearby object discovery.

3.2.2. Intelligent Transportation

(i) *Central computer:* A central computer is a powerful processing unit that controls the vital computation-related functions of EVs. These functions include deceleration, object detection, collision avoidance, lighting, window control, environmental control, speeding, and acceleration, among other things, and the central computer is involved in making some decisions involving the vehicle's drive [53].

(ii) *Cell technology:* Cell technology allows mobile communication based on a two-way radio system that transmits and receives data from a mobile unit to a wireless network. EVs use radio channels for minimal interference during communication [54].

3.2.3. Eco-Friendliness

(i) *Emission sensors:* EVs minimize hazardous and harmful emissions and are therefore considered eco-friendly vehicles. They tend to reduce noise pollution and allow for good fuel economy [55]. Importantly, fewer repairs are needed due to the lower number of vehicle parts. Just one electric car saves an average amount of 1.5 million grams of CO_2 per year. This is approximately equivalent to four return flights from Barcelona to London. An increasing percentage of EVs can cause a significant drop in harmful emissions [56]. More recent EVs models are revolutionary as they are close to zero-emissions producing virtually no exhaust from the onboard power source.

3.3. Innovation and Development (Third Goal of Sustainability)

With the growing popularity of EVs, many car manufacturers work hard to innovate and cater to the many challenges related to the drive. Multiple improved models and infrastructures have been produced that significantly benefit drivers and maintain a longer battery life. The research innovations also reduce pollutants that are harmful to the climate, such as hydrocarbons, carbon monoxide, ozone, lead, and different nitrogen oxide emissions [57] *Innovation and development* is further classified into three subgoals of sustainability as (1) *improved fuel economy*, (2) *minimize travel time*, and (3) *reduce congestion*.

3.3.1. Improved Fuel Economy

Fossil fuel is not a renewable resource, and its production is not consistent with the demand. Continuous economic growth, increasing dependence, uncontrolled gasoline appliances, and global conflict are creating crises for production [58]. This gradual movement toward EVs will reduce fuel dependency and create a better impact on the global economy.

3.3.2. Minimize Travel Time

EVs can minimize travel time by providing a more efficient means of transportation as compared to traditional vehicles. EVs are equipped with advanced navigation systems that can help drivers find the most efficient routes to their destinations. EVs are also capable of reaching higher speeds than traditional vehicles, allowing them to get from point A to point B faster. Owing to ongoing innovation, we may see regenerative braking systems that can convert the energy generated when braking back into electricity, helping to extend the range of the vehicle and minimize the stops needed for recharging. Presently, most traffic speeds depend on speed limits, traffic signs, roadside infrastructure, ramps, and junctions, which EVs will be able to incorporate as parameters for highly accurate trip time calculations to suggest alternative routes and further reduce travel time.

(i) *Global positioning system (GPS):* GPS is a satellite-based radio navigation framework that is used to identify the location. It is available in vehicles for accurate positioning, route finding, time estimation, and traffic information [59].

(ii) *Electronic stability control (ESC):* ESC is responsible for allowing for vehicle stability when making sharp turns and is especially effective under adverse conditions such as rain and snow, abrupt movements such as by animals on the road, and other similar circumstances. It ensures that the path is followed properly and activates the brakes to assist and control the vehicle while driving in slippery conditions [60]. ESC is one of the key dynamic security frameworks widely introduced around the world in all types of vehicles by manufacturers [61].

3.3.3. Reduce Congestion

As a critical component of traffic flow, vehicles play a vital role in the road traffic system. The transportation department finds the effect of autonomous vehicles on the capacity of highway sections and traffic signal intersections. With the electric vehicle autopilot mode and driving assistance, the quality of the journey will be better, fewer brakes will be applied, traffic rules will be followed, and alternative routes will be provided, so there is the possibility of enhancing the speed of traffic flow, and eventually reduce congestion and road blockages [62].

(i) *Lane detection:* Lane detection sensors are often used in EVs to help the vehicle stay within its lane on the road and avoid collisions. These sensors are typically part of the vehicle's advanced driver assistance system (ADAS), which is a suite of technologies designed to improve safety and driving performance [63]. If the vehicle begins to drift out of its lane, the sensors can alert the driver and/or take corrective action, such as applying the brakes or steering the vehicle back into the lane.

(ii) *Short-range radio (SRD):* SRD is a radio transmitter unit that performs short-range communication using low power. It is helpful for communicating with other vehicles, roadside components, and other objects [64].

(iii) *Vehicle communication:* The vehicular communication system is a radio network through which multiple vehicles and roadside units can communicate and exchange information. The information includes road signals, safety warnings, turn indicators, path priority, and traffic information. This kind of information is effective in avoiding road accidents, potential path findings, and mitigating traffic congestion. On a broader level, the communication is called vehicle-to-everything (V2X) communication [65]. The V2V communication happens using vehicular ad hoc networks (VANETs) or short-range radio. These are wireless networks through which vehicles can communicate and share information about the position, speed, stability, braking, direction, and urgency of the driving. Figure 3 provides an illustration of communication between vehicles and other components. V2X is divided into subcategories based on the sender and receiver, such as infrastructure, grid, vehicle, network, device, and pedestrians.

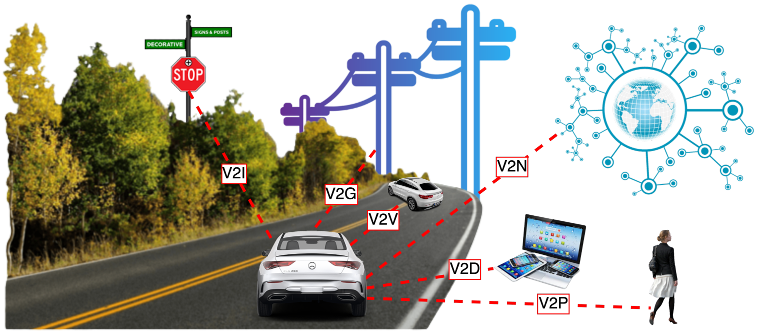

Figure 3. Concept diagram for Vehicle-to-Everything (V2X) Communication.

3.4. Implementation of Vehicle-to-Everything (V2X) Communication

Vehicle-to-Everything (V2X) communication is a set of technologies that allows vehicles to communicate. There are two main types of V2X communication: short range and long range [66].

Short-range V2X communication is typically based on technologies such as Zigbee or infrared. These have a limited range, usually less than 100 m, but are able to transmit data at high speeds and with low latency [67]. This is useful for applications such as cooperative collision avoidance, where vehicles need to quickly exchange information about their location and speed in order to avoid collisions.

Long-range V2X communication is typically based on cellular technologies such as 4G, 5G, and 6G. These technologies have a much larger range, usually several kilometers, but have higher latency and lower data rates [66]. This is useful for applications such as traffic management, where vehicles need to send and receive information about traffic conditions over a large area.

Moreover, some integrated circuits (ICs) are being introduced specifically to enable V2X communication [68]. These include dedicated communication modules that can be integrated into a vehicle's onboard systems, providing an off-the-shelf solution. These ICs will be able to handle various communication technologies and protocols and are expected to provide a more efficient and cost-effective way of implementing V2X communication.

1. Vehicle-to-Infrastructure (V2I) is a communication that allows vehicles to share data with roadside components, including but not limited to radio frequency identification (RFID) readers, traffic lights, cameras, lane markers, and signs.
2. Vehicle-to-Grid (V2G) communication is fundamental to smart charging but goes a step further. It also allows for the transfer of unused power stored in the batteries of cars. This power can be fed back into the grid to allow for efficient use of energy.
3. Vehicle-to-Vehicle (V2V) performs wireless transmission between different vehicles. Mostly, it utilizes an ad hoc mesh network or short-range radio to perform communication. Information-sharing includes but is not limited to car speed, braking, position, stability, and direction of travel.
4. Vehicle-to-Network (V2N) facilitates information exchange between multiple networks, including vehicles, lane markings, traffic lights, and other road infrastructure.
5. The Vehicle-to-Device (V2D) communication system is responsible for the exchange of data between a vehicle and any other electronic device that may be connected.
6. The Vehicle-to-Pedestrian (V2P) platform allows vehicle-to-pedestrian communication. This feature is fully applicable when smart road infrastructure is implemented. The key features proposed for V2P include information for children, individuals on bicycles, wheelchairs, and passengers.

4. Cyber Threats and Privacy Issues

The increasing use of sensors in EVs is creating cyber threats and privacy issues due to the sensitivity of the data collected and stored. Sensors collect various information, including driver and passenger identification, location data, and vehicle performance metrics, which can be used for malicious purposes [69]. Additionally, malicious actors can exploit software vulnerabilities to gain access to vehicle systems and take control of the car [70].

Threats and problems targeting sensors in EVs are not new. In the past, there have been several cases in which vehicle manufacturers have had to recall vehicles due to defects in electronic components. For example, in 2015, Tesla recalled 90,000 Model S sedans due to a faulty charging system that posed a fire risk [71]. Honda also had to recall over 1 million vehicles due to a defect in the airbag inflator system [72]. In April 2018, Tesla recalled over 123,000 vehicles due to a potential defect in the driver's side airbag inflator that could cause it to deploy unexpectedly [73]. Similarly, Fiat Chrysler automobiles recalled nearly 350,000 vehicles due to a software bug that could cause ignition problems [74]. In May 2019, Toyota recalled nearly 1.4 million vehicles due to a software defect that could cause the engine to stall or the airbags to deploy unexpectedly [75].

These recalls were made because EVs are equipped with sensors, and some of these sensors have larger attack surfaces due to their utilization of third-party software, faulty hardware, or limited software and hardware quality assurance testing. Some of these sensors are also vulnerable to cyber threats such as malware, remote access, zero-day exploits and intentional flaws introduced during manufacturing, and embedded system flaws [20,76]. Figure 4 provides an illustration of multiple cyber threats that, if vulnerable or exploited, can lead to cyber-attacks and cause severe damage to vehicle owners and manufacturers. The figure is labeled into twelve categories; the detailed impact of these threats on EV sensors has been discussed in subsequent subsections.

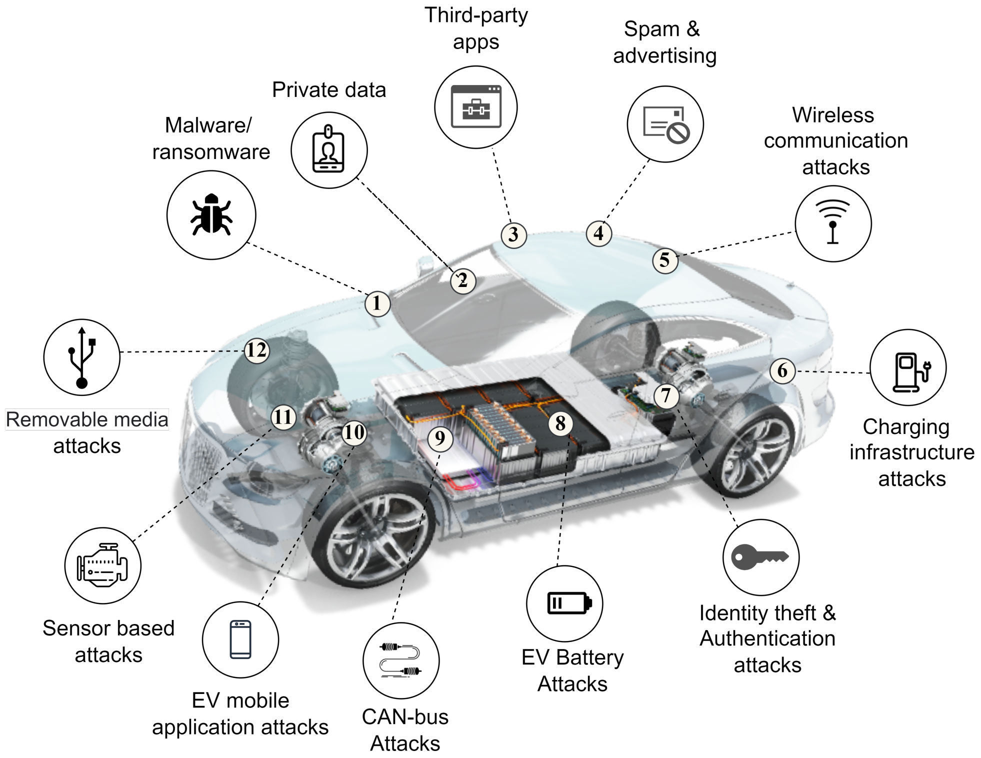

Figure 4. Illustration of security threats and cyber attacks targeting EVs.

Although all of these threats discussed are directed at EVs, what is less known is that they also affect long-term sustainability goals. Therefore, to understand how these cyber threats impact sustainability, we provide a detailed explanation. Previously, in Section 3, we introduced the first taxonomy (sensor-to-sustainability) in Figure 2 that mapped different EV sensor categories into the three sustainability goals that they help achieve. Next, in this section, a second taxonomy (threats-to-sensors) has been introduced in Figure 5 that visualizes different cyber threats that target EV sensors.

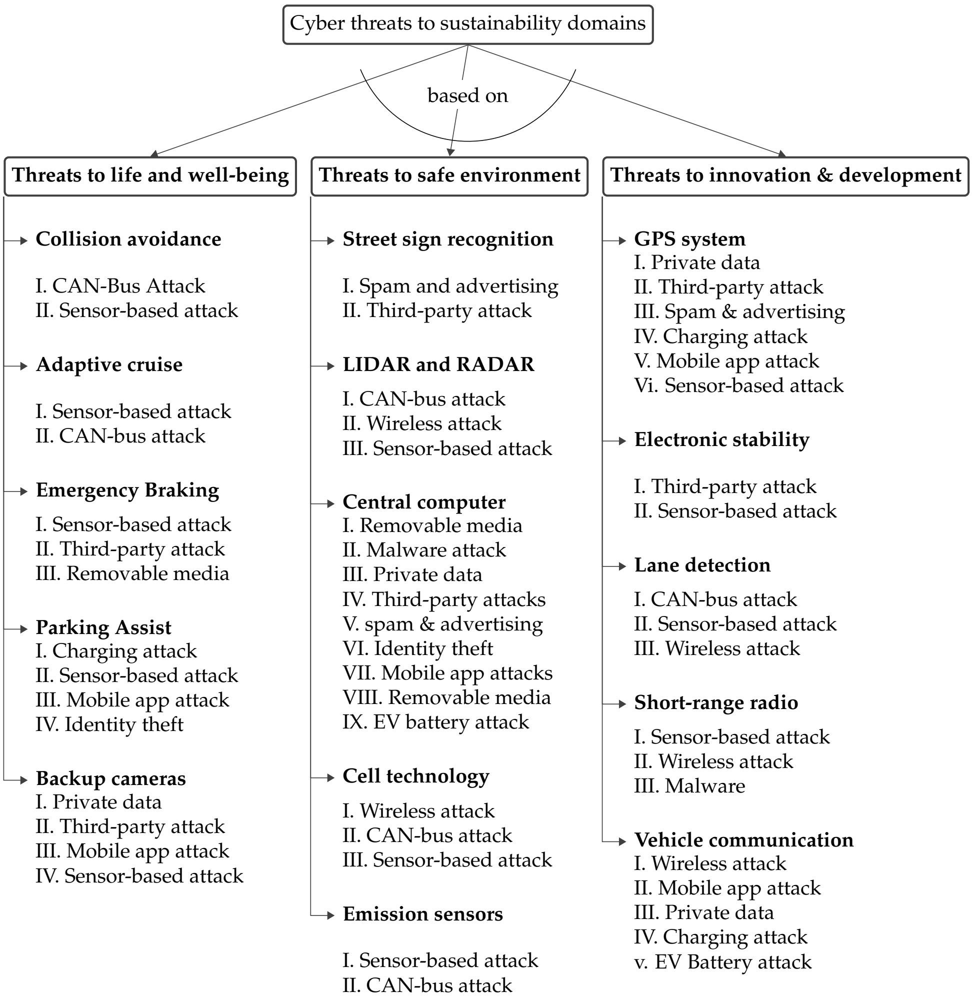

Figure 5. Threats-to-sensors: second taxonomy that maps security threats to EV sensors.

A logical relationship has been represented in Equation (2). The equation formally represents using predicate logic notation a relationship between important entities in an EV environment: namely, the sensors deployed and the threats they present.

In this equation, T represents a set of all threats targeting a set S of all sensors used in EVs deployed to maintain sustainability. A survey of the most common threats and their corresponding sensors was conducted, and a taxonomy diagram (threats-to-sensors) was created to visualize their mappings. This has been illustrated in Figure 5.

$$T \Rightarrow S \tag{2}$$

$$T = \{threat1, threat2, threat3, \dots\}$$
$$S = \{sensor1, sensor2, sensor3, \dots\}$$

The intention is that future researchers can utilize these two taxonomies together to identify those threats that, if materialized, would negatively impact the achievement of the sustainability domains of life, well-being, safe environment, innovation, and development.

To understand how cyber threats affect sustainability, a *transitive property* (also called *transitive Law* [77]) is applied to Equations (1) and (2), which states that if a threat $t \in T$ impacts a sensor $s \in S$ and s improves sustainability domain $s' \in S'$ then t also impacts s'. Logically, this can be written as $(T \Rightarrow S)$ and $(S \Rightarrow S')$, therefore $(T \Rightarrow S')$.

Applying the transitive property on Equations (1) and (2), we get Equation (3).

$$T \Rightarrow S' \tag{3}$$

This demonstrates that threats will not only impact EV sensors but will also affect long-term sustainability goals.

4.1. Malware

Malware refers to malicious software designed to harm a computer system. We are seeing an emergence of certain types of malware specifically targeting EVs. Malware that targets EVs can be categorized into four types, which are *spyware*, *trojan*, *ransomware*, and *cryptojackers*. The most common type of malware is ransomware [78]. In the past, hackers hit San Francisco transport systems and demanded 100 Bitcoins in ransom. All computers installed across the stations and the city transport network were hijacked and disabled, with all the screens displaying hackers' messages to the public [79]. Initially, these attacks targeted the government transportation sector such as metro stations, but they have since broadened in scope to include not just government institutions but automotive companies as well such as Tesla, Honda, Nisan, and Toyota. Ransomware bribes were around $6.9 million in 2019 and $20 billion in 2020. These are predicted to surpass $50 billion by the year 2023 [80].

4.2. Private Data

EVs are equipped with multiple sensors that generate data. Even when not driving, EVs generate data related to the drive from vehicular sensors. Data are not only limited to driving data but also includes personal information such as a person's voice calling, text messages, contact lists, email accounts, financial details, phone location, reminders, and even videos and photographs. EV manufacturers collect these data to design and train AI models to provide a better customer experience. These data are important for manufacturers as well as third parties to develop marketing strategies and for commercialization [81]. The data are worth millions and can be sold for revenue similar to how big-tech social media companies profit from personalized and location-based advertisements. In 2016, the worldwide consulting firm McKinsey estimated that global profits from vehicle-generated information could reach $75 billion by 2030 [82]. This financial benefit makes it an ideal target for hackers.

4.3. Third-Party Attacks

Third-party libraries are pre-existing software libraries or modules that are developed by external parties and made available for use by other developers. These libraries can be used to implement various features in EVs, such as navigation, communication, and sensory control. Companies may rely on these third-party libraries for a variety of reasons. Firstly, it may be more cost-effective and time-efficient to use a pre-existing library rather than developing the software from scratch. Secondly, third-party libraries may also offer specialized functionality or capabilities that a company may not have the resources or expertise to develop in-house. Many third-party libraries are freely available online, such as on open-source platforms such as GitHub.

However, there are potential risks associated with using third-party libraries. The library may contain vulnerabilities that can be exploited by hackers. For example, if a library has not been properly maintained or updated, it may contain known vulnerabilities that have not been patched [83]. In the past, a 19-year-old hacker, David Colombo from Germany, exploited a vulnerable application to break into Tesla cars. He could remotely unlock, track and access car features such as open windows, blink the flashlights, and even bypass keyless entry for starting the vehicle [84]. Another attack was performed on the Volkswagen (German vehicle manufacturer) infotainment system using third-party libraries to perform remote software updates. Researchers found the system vulnerable during a security assessment of the Volkswagen [85]. Researchers disclosed that vulnerabilities in the underlying software library had already been reported in the past, but surprisingly, the library was still integrated without proper verification and evaluation of the vehicle's infotainment system.

4.4. Spam and Advertising

Spam refers to misleading information, falsified service, and unsolicited messages. Attackers advertise spam messages or fake products to many internet users and network-connected devices to spread malware and make users click on phishing websites for credential harvesting. Some EVs are connected to the Internet and have a touch screen for display, navigation, music, voice dialing, and other accessibility features. In the past, security researchers found vulnerabilities in a vehicle control system that uses Qualcomm chipsets [86]. The vulnerability was exploitable through a remote code execution attack using a mobile device. After successful exploitation, researchers could view media and remotely listen to conversations. In 2020, a researcher was able to hack and display custom messages, dialogues, and symbols on the EV display screen using the Arduino circuit board [87]. These display screens and infotainment systems are vulnerable to spam, phishing, and advertisements. An attacker can advertise fake charging stations, lower rates, and other misleading information to trick drivers.

4.5. Wireless Communication Attacks

Electric cars use a variety of different communication protocols such as cell technology, bluetooth, zigbee, and radio frequency for wireless connectivity. These protocols aid in-vehicle messaging between connected sensors as well as facilitate V2X communications. In 2021, German security researchers performed a 'TBONE' attack on Tesla, in which drones were used to enter the EV's control system. The researchers gained access to the Tesla vehicle, which allowed them to unlock the car, open the charging port, and execute commands without touching the car [88]. This was achieved by taking advantage of the fact that all Tesla vehicles search and automatically connect to a WiFi network named *Tesla Service*, the credentials for which were openly leaked onto hacker forums. In the past, two laptops were stolen from an EV when thieves broke into the vehicle using a wireless signal-jamming device. Fortunately, no physical damage was incurred to the vehicle. In this scenario, these signal jammers were used to prevent the vehicle owner from engaging the locking mechanism [89].

4.6. Charging Infrastructure Attacks

Electric chargers are being installed everywhere, such as in parking spots, highways, shopping malls, and retail shopping centers in order to facilitate EV users. The charging infrastructure has become the most vulnerable place for hackers due to the lack of surveillance, ease of access, and a wide variety of exploitation options [90–92]. Multiple attack scenarios have been witnessed in the past. As of April 2022, a hacker hacked into UK Electric Vehicle Charging Points (EVCP), disabled onsite charging and started showing pornographic content on charging screens [93]. Similarly, Ukrainian charging stations were hacked, and the attacker published an inappropriate message against politicians [94]. The hack was carried out on Russia's M11 motorway, which extends from Moscow to Saint Petersburg. This attack was launched by exploiting a remote code execution back door in the charging station software deployed by an equipment manufacturer 'Rosseti Enterprise'.

4.7. Identity Theft and Authentications Attack

Identity theft in vehicles refers to unauthorized access to vehicles using the owner's stolen identity, such as the use of their keyless entry cards or the owner account associated with the EV that is used to control vehicular features. This attack is gaining popularity in EVs. Some EVs come with keyless entry and use an NFC-based card to unlock vehicle doors. Attackers can take advantage of this feature. A researcher demonstrated the "NFC Relay Attack" on an electric vehicle that allowed him to bypass keyless entry [95]. To demonstrate this attack, two thieves work simultaneously. One of the thieves acquires the relay device in close proximity to the owner's key card, while his accomplice positions the other part of the device to the vehicle to be stolen. There is also another variation of relay attacks that exploits a vulnerability in the bluetooth stack. A researcher was also successful in unlocking Tesla vehicles by exploiting this vulnerability in the bluetooth low energy (BLE) module available in Tesla [96]. In the past, an attacker retrofitted a gaming console and customized it in such a way that it was used as a signal transmission device: an alternative to a vehicle remote that unlocked a number of vehicles [97].

4.8. Battery and Energy Attacks

A vehicle's rechargeable battery is an important component because it is used for powering electric motors and other electronic components. In the past, attackers have hacked electric cars to siphon the energy in their batteries for cryptomining, whereby the computational resources and energy of the vehicle are used to mine cryptocurrency and earn money. In the past, one Tesla owner mined Ethereum and Bitcoin in the Tesla Model 3 and made $800 [98]. Similarly, in June 2021, researchers experimented with cryptocurrency mining in their EV [99]. They claimed that mining running for 12 h earned a total of 0.0117 Ether and $30.39 and concluded that non-stop mining for a year would earn 4.275 Ether or $11,092 at the time of the experiment. Recently, some EVs manufacturing companies are also integrating these features into specific models: for example, an EV manufacturer named Daymak introduced a vehicle named Spiritus that mines crypto in its free time and facilitates drivers with crypto rewards that can be redeemed in local currency [100].

Researchers have also demonstrated how an attacker may cryptojack someone else's EV resources to mine for cryptocurrency [9]. An attacker can even hijack an entire fleet of EVs simultaneously for cryptojacking. In 2018, an attacker hacked Tesla's cloud servers to mine cryptocurrencies by planting a malware known as Stratum in Tesla's web administration accounts [101]. In another scenario, researchers demonstrated the *power jacking attack*, which affects the connected power grid by exploiting software vulnerabilities in charging stations. This attack is also capable of disrupting the charging process, modifying firmware settings, changing billing, and even accessing PII [102].

4.9. CAN-Bus Attacks

The controller area network (CAN Bus) is a standard that allows microcontrollers and devices to communicate with each other without a host computer. The module is popular in in-vehicle networks and allows electronic control units (ECUs) to communicate with each other [103]. The CAN standard lacks provisions for encryption and authentication and is therefore vulnerable to security attacks. For instance, any unauthorized connected node is allowed to join and participate freely in the communication. The communication itself does not require specifying destination and source addresses, so every node can listen in to all messages as they are unencrypted [104]. An adversary can hijack and inject crafted instruction packets with high priority in CAN. Therefore, it is also vulnerable to eavesdropping, privacy invasion, data manipulation, and denial of service (DoS) attacks [105]. If the CAN or any of its connected components are compromised, various important vehicle functions that depend upon it can malfunction and even result in fatal accidents. In the past, a researcher demonstrated an attack using an Arduino device to inject CAN message to unlock doors, control navigation, and manipulate display messages [106].

4.10. Mobile Application Attacks

There are multiple EV applications available on mobile stores that assist EV drivers in finding available charging stations and make the charging process more convenient. Applications such as Charge-hub, Charge-point, Charge-way, EV-go, Charge Map, Open ChargeMap, Evmatch, ChargeFox, and Plug-Share provide information about nearby charging stations, allow the driver to reserve a spot and notify him in real time about the status of the charge. Some applications even allow for making payments for the charging fare. These applications contain users' personal information such as associated financial accounts, location coordinates, messages, call logs, and PII [107,108]. Some of these applications are provided by EV manufacturers and large companies, but many are third-party applications which are built and distributed by independent developers [109]. Poorly developed applications contain security flaws, backdoors, and privacy loopholes [110]. In 2016, the Nissan connect app was hacked to gain control of the EV functions including the vehicle sensors, air conditioning, and heating [111]. On 21 July 2015, two security researchers successfully hacked a Jeep Cherokee using an app called UConnect. The two were able to take control of the vehicle remotely, locking the driver out from the vehicle's controls and steering it toward a ditch [111].

4.11. Sensor-Based Attacks

Sensor-based attacks in EVs can be carried out by disrupting or manipulating the sensor data by physically tampering with the sensors or by exploiting their communication protocols [112]. A researcher demonstrated vulnerability exploitation for electromagnetic sensors and performed attacks on EV power converters to manipulate the vehicle voltage [113]. He proved that it is possible to control and manipulate the switching state for individual transistors in order to cause damage to the connected system. In the past, a researcher demonstrated a jamming device used to bypass a vehicle collision avoidance system and jam emergency braking to cause an accident. The attack was demonstrated on a Tesla model 3 [114]. Sensor-based attacks can cause unavailability of services, network disruption, message alteration, eavesdropping, and impersonation [112].

4.12. Removable Media Attacks

EVs are vulnerable to cyber attacks via removable media and USB devices, as these devices can be conveniently used to introduce malware (malicious code). Such EV malware can corrupt or delete the vehicle's system configuration files, execute malicious code on the vehicle's onboard computer, or gain access to the vehicle's internal network. In the past, there were many cases in which cybercriminals used different social engineering techniques such as the *USB key drop attack* to drop flash drives into parking spaces, place them in corporate offices, and even send infected malicious USB drives to a targeted victim as a gift [115]. The same technique of an infected USB can be used to cause potentially serious disruption to EVs. In the past, an attacker used an Arduino-based removable device to bypass the Mercedes infotainment system and thereby retrieve, decode, and modify CAN messages [106]. Similarly, some EVs allow updates using a flash drive or detachable media which provides hackers an opportunity for installing malicious software during a software update if the flash is compromised [116].

5. Safeguards

This section provides details of safeguards that can be used to secure EVs and make them resilient against cyber attacks. Earlier, in Section 3, the first taxonomy (sensor-to-sustainability) was introduced in Figure 2 that mapped different EV sensor categories into the three goals of sustainability that they help to attain. Next, in Section 4, a second taxonomy (threats-to-sensors) was introduced in Figure 5 that visualizes different cyber threats that target EV sensors. Now, in this section, the third and last taxonomy (defenses-to-threats) is introduced in Figure 6 that maps different security controls and safeguards to potential cybersecurity threats.

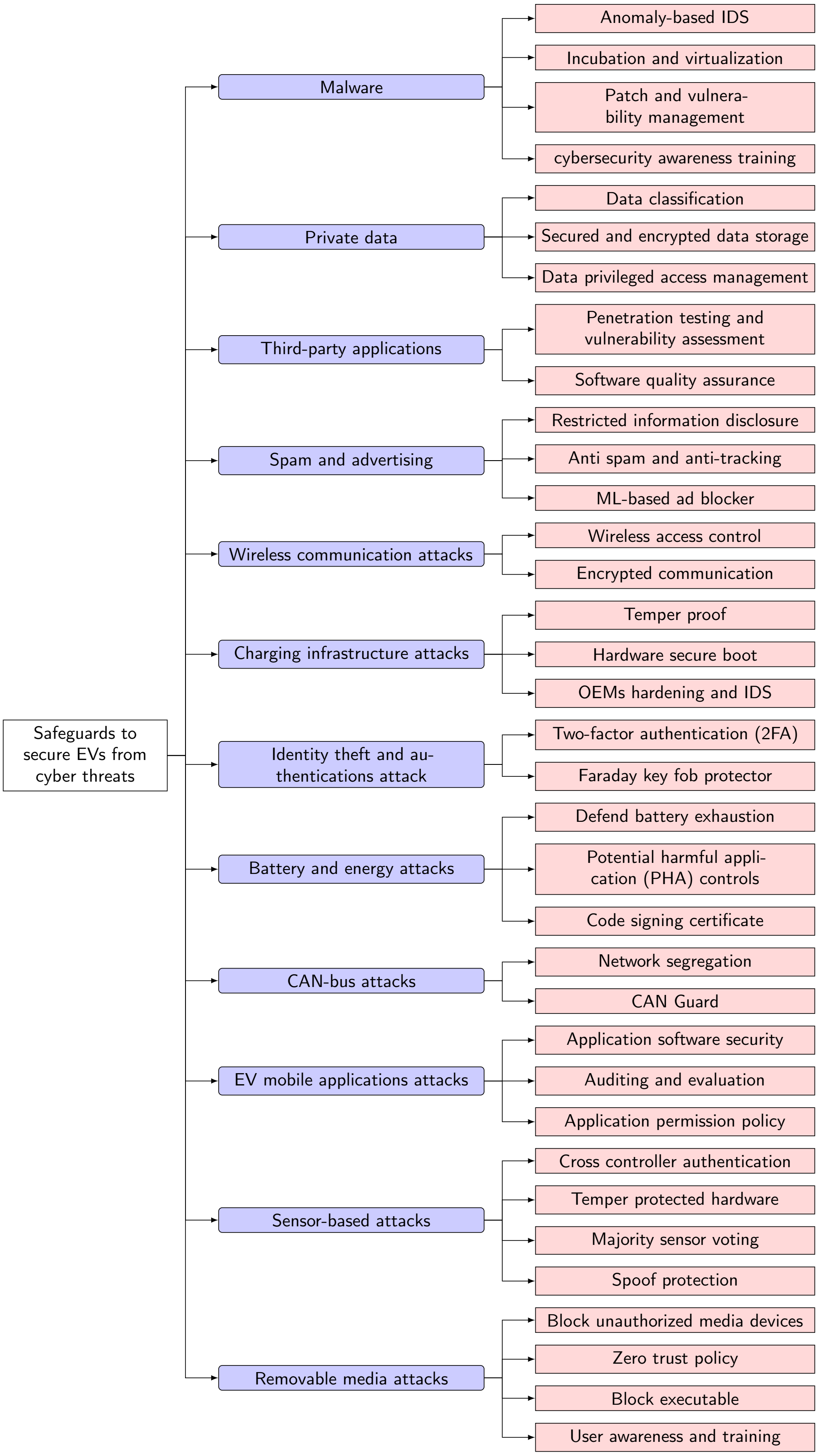
Safeguards to secure EVs from cyber threats
Malware
Anomaly-based IDS
Incubation and virtualization
Patch and vulnerability management
cybersecurity awareness training
Private data
Data classification
Secured and encrypted data storage
Data privileged access management
Third-party applications
Penetration testing and vulnerability assessment
Software quality assurance
Spam and advertising
Restricted information disclosure
Anti spam and anti-tracking
ML-based ad blocker
Wireless communication attacks
Wireless access control
Encrypted communication
Charging infrastructure attacks
Temper proof
Hardware secure boot
OEMs hardening and IDS
Identity theft and authentications attack
Two-factor authentication (2FA)
Faraday key fob protector
Battery and energy attacks
Defend battery exhaustion
Potential harmful application (PHA) controls
Code signing certificate
CAN-bus attacks
Network segregation
CAN Guard
EV mobile applications attacks
Application software security
Auditing and evaluation
Application permission policy
Sensor-based attacks
Cross controller authentication
Temper protected hardware
Majority sensor voting
Spoof protection
Removable media attacks
Block unauthorized media devices
Zero trust policy
Block executable
User awareness and training

Figure 6. Defenses-to-threats: third taxonomy that provides safeguards against cyber threats to EVs.

Equation (4) provides details of the third taxonomy (defenses-to-threats) illustrated in Figure 6 where T is used for the set of security threats illustrated in Figure 4 and D is the set of defenses proposed to protect EVs. The graphic visualization of these security controls is illustrated in Figure 6, and a detailed explanation has been added in subsequent subsections.

$$D \Rightarrow T \tag{4}$$

$$D = \{defense1, defense2, defense3, \dots\}$$
$$T = \{threat1, threat2, threat3, \dots\}$$

5.1. Malware

Malware attacks can be defended with the appropriate use of an anomaly-based intrusion detection system (IDS) [117]. These IDSes work by recording the baseline traffic behavior of a vehicular network and then comparing the live network with the recorded baseline patterns to detect anomalies or different behavior in the network [118]. Malware spread can also be controlled by limiting the direct installation of multiple applications on vehicular networks. EV manufacturers may introduce a mechanism to incubate applications in a virtual space such as a sandbox or virtual machine. This will minimize the chances of malware installation, propagation, and system failure because every new application will be thoroughly tested against malicious behavior before its actual deployment on EVs [119]. In addition, a patch and vulnerability management system can be introduced to protect the EV infrastructure against malicious updates and vulnerable programs [120]. Finally, cybersecurity awareness and the training of EV users will enable them to detect and report suspicious malware behavior in a timely manner.

5.2. Private Data

Data security pertains to securing vehicular data and user PII generated by an EV [121]. Not all EV data require an equal amount of protection. EV data sensitivity may be first determined using data classification techniques [122]. There can be many potential classes, but based on research, one sample data classification has been visualized in Figure 7. Four categories have been depicted: *secret*, *confidential*, *sensitive*, and *unclassified* [123,124]. Similarly, more or fewer categories can be made on the basis of the availability of chosen artifacts.

Once classified, appropriate data protection techniques can be employed to secure EVs data which include: (1) *data minimizing*, (2) *data masking, anonymization, and sanitization*, (3) *data tokenization*, and (4) *data encryption*. Data minimization involves collecting only the data that is necessary for a given purpose. Data masking obscures or changes data elements to prevent the data from being misused. Data anonymization is the process of removing identifying information from data. Sanitization is the process of removing or altering sensitive data from data, and data tokenization is the process of replacing sensitive data with a token or unique identifier. Finally, data encryption involves encoding data in unreadable ciphertext to ensure it is secure. EV manufacturers may choose to selectively apply one or more of the above to secure a particular class of data based on its sensitivity level. For instance, secret data require more confidentiality and integrity than unclassified data. Therefore, encrypted data storage can be maintained during transmission between communication channels, modules, and sensors. In addition to the above techniques, access control may be employed. For instance, data-privileged access management can be implemented for secret data based on rule-based access. Finally, EV manufacturers can explicitly design security policies that contain rules for data sharing of information, statistics, marketing and advertising with third parties.

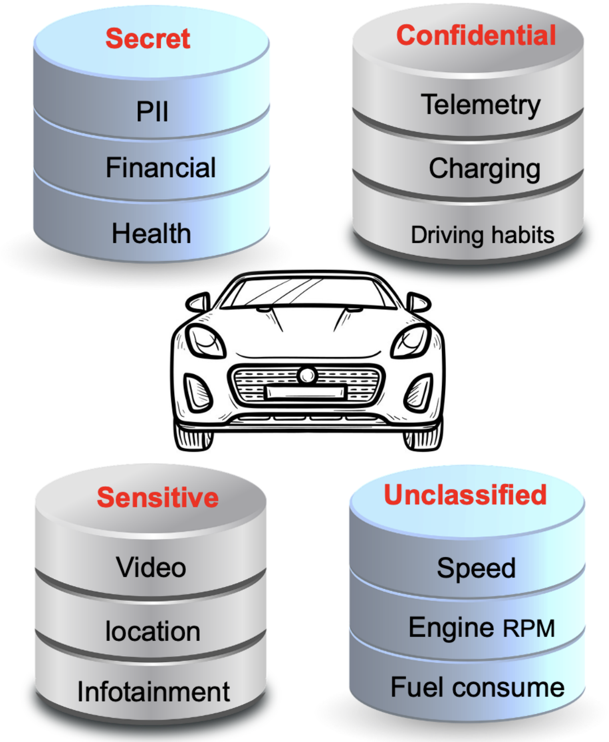

Figure 7. Visualization of data classification.

5.3. Third-Party Applications

Publicly available third-party applications and libraries may be tested and secured against existing vulnerabilities and security loopholes before integration. To securely integrate these third-party applications, pre-penetration testing and vulnerability assessment is recommended [125]. In addition, post-software quality assurance testing after successful integration can help to detect and remove compatibility issues or insecure communications before final production and use. Finally, software hardening may be performed against individual EV units and application modules to reduce the attack surface [126].

5.4. Spam and Advertising

Restricted and monitored third-party information disclosure helps in avoiding and defending against spam and targeted advertisements [127]. Most of the time, advertisements are customized based on user interests, age, gender, location coordinates, and search preferences. These data are collected and shared with third-party companies for profit or to analyze market trends [128]. Therefore, the installation of anti-spam and anti-tracking controls can prevent excessive exposure [129]. Similarly, machine-learning-based ad-blocking services can be pre-embedded by EV manufacturers to detect and block targeted advertisements in EVs and at charging stations [130].

5.5. Wireless Communication Attacks

To secure wireless communication against attacks, it is recommended to use strong wireless access controls that leverage advanced encryption standards for data transmission such as WAP2 and WAP3 [131]. In addition, EV manufacturers may abstain from the use of communication channels and protocols with hardcoded embedded credentials. Moreover, it is recommended to segregate EVs from connecting to untrusted devices and restricting auto-connect with open networks [132]. Moreover, encrypted communication may be used between inter-components and cross-vehicular components to avoid data intersection, message intrusion, and man-in-the-middle attack [133].

5.6. Charging Infrastructure Attacks

Electric vehicle charging stations are vulnerable to potential cyber threats and tempering [134]. Some EV chargers use a raspberry-Pi and insecure hardware that makes them vulnerable to potential cybersecurity threats [135]. Developing secure hardware standards that prevent access to the internal circuit board will aid in making EV chargers tamper-proof [136]. In addition, secure hardware boot can be used to authenticate system images and embed code to prevent unauthorized access or tampering [137]. Original equipment manufacturers are required to implement and use a combination of software-hardening techniques and temper-proof hardware [138]. Finally, EV charging stations may use AI-based intrusion detection systems (IDS) to detect and report malicious intents [139].

5.7. Identity Theft and Authentications Attack

In the past, the keyless entry has been compromised using a variety of attacks, such as jamming attacks in which a jamming device interrupts the communication between the key card and the vehicle to prevent it from locking. Similarly, NFC relay attacks have been used to steal vehicles [95]; hence, it is important to identify and defend against such attacks.

There can be several ways to identify unauthorized access to EVs using keyless entry cards, such as two-factor authentication using a smartphone or default vehicle application. The vehicle can be configured to send a notification to the registered owner's mobile every time the vehicle is unlocked or started using the key card. Similarly, the default vehicle application can create an alert. This way, the owner will be notified if someone else is using their key card to access the vehicle. Additionally, some vehicle applications allow remote locking and unlocking; thus, owners can disable the vehicle through the smartphone app if they suspect it is being stolen.

Similarly, the vehicle can be configured to require a unique access code to be entered before the vehicle can be started. Entering the wrong code multiple times will alert the owner about suspicious activity and lock the car. Another way to identify such attacks can be to build a driver profile based on facial features extracted through a dashboard-mounted camera and the driving habits analyzed over time. In such cases, if unauthorized access takes place, the driver will recognize it, and it can be trained to honk and send alerts to the owner.

Another important thing is to provide basic training to the users about how to safely store key cards, such as on the use of a faraday key fob protector that blocks radio frequency emissions and protects the keyless card entry of vehicles [140]. In addition, two-factor authentication (2FA) may be used to provide an additional layer of security [141]. 2FA will enable the proper usage of two or more factors to grant access to the vehicle, such as something you have (e.g., a key or keyless card), something you know (e.g., a security code/password), and something you are (e.g., face detection/fingerprint scanner) [142].

5.8. Battery and Energy Attacks

With the growing adoption of EVs, many people are misusing EV resources in order to generate passive income, such as the use of crypto mining by installing multiple GPUs with EV batteries. Similarly, there are numerous unnecessary applications and battery attacks that drain batteries and reduce EV performance [120,143]. To defend against these kinds of attacks, it is recommended to detect and remove potentially harmful applications (PHA) and monitor the impact of other system applications that—while they are meant to facilitate users—end up consuming too much battery [144]. In addition, a code signing certificate can be used to sign and verify access and apps that users may install [145]. Malicious software performs a battery exhaustion attack in which multiple malicious service requests are made to engage the maximum possible system resources and drain the battery. They may be monitored through drain detection or early warning systems [146].

5.9. CAN-Bus Attacks

Most sensors and controllers are connected directly to the CAN Bus so that they can communicate with any other EV device even though functionality-wise, they require connectivity to only a few selected devices. Some of these newly developed sensors are not thoroughly tested or quality ensured and have security vulnerabilities that lead to unauthorized access to the CAN network. Compromise of the CAN interconnection can lead to the misuse of multiple EV functionalities [147]. It is recommended to perform network segregation through the firewall to reduce CAN Bus attacks [103]. In addition, EV manufacturers can implement CAN Guard, which is a mechanism that detects anomalies, prevents malicious actors and blocks communication attacks. Similarly, CAN-IDS can detect and block malicious data, traffic, and message transmissions through the CAN network and identify compromised nodes existing in the network [148].

5.10. EV Mobile Applications Attacks

It is important to maintain EV application security standards by implementing secure coding practices and performing security assessments during the production phase [149]. A thorough auditing and evaluation can help identify security vulnerabilities, which can be patched before making applications available to mobile app stores. Similarly, publicly available third-party mobile applications have software bugs and should not be trusted to connect directly with EVs without proper research [150]. An application usage policy can be developed by EV manufacturers that outlines terms and conditions for directly connecting mobile application with EVs. Particularly for the infotainment system, the safest approach is for EV manufacturers to provide a hardened application themselves that provides also necessary functionality. The application may ensure minimal user data disclosure, encrypts all communication and addresses data leak prevention [151,152]. This will discourage the use of third-party untrusted applications that are freely available.

5.11. Sensor-Based Attacks

The EV sensors themselves may be secured against vulnerabilities, cyber-attacks, tempering, breakage, and damage in a number of ways. Firstly, it is recommended to make temper-protected hardware for sensors integrated inside and outside the vehicles [153]. Secondly, EV manufacturers may remove the possibility of integrating fake sensors, which auto repairers sometimes do in the market with the aim of data spoofing into embedded circuits associated with EVs or charging stations or to spoof sensory data. Implementing the cross-controller authentication of sensors and EV circuits [154] would protect against spoofing. In addition, there should be a majority sensor voting mechanism in case there exist redundant sensors to ensure data integrity [155].

5.12. Removable Media Attacks

Flash drives and USBs are the easiest way for malware propagation and device tempering [156]. Therefore, EV manufacturers may introduce a policy that provides users awareness discouraging the connection of unauthorized devices. A policy on the use of official USB drives obtained from the vehicle dealership with embedded patches would also help here. In addition, users should be aware about the dangers of inserting third-party, unknown, and infected USB drives to their vehicles [157]. Finally, there should be a zero-trust policy against detachable media. Every device should be scanned adequately against malicious software, and EVs may block auto-run executables as policy. [158,159].

6. Discussion and Open Issues

EVs offer numerous benefits and are considered a more sustainable and a viable alternative to traditional gasoline-powered vehicles. Aside from the security and privacy issues discussed above, there are still some other challenges associated with EVs that need to be addressed prior to widespread adoption. One of the main issues is the ready availability of charging infrastructure. Although the number of charging stations is increasing, there is still a lack of access in many places, particularly in rural and remote areas. Many a time, EV owners will have to travel long distances to find a charge point.

Another challenge for EVs is the cost. Although the upfront costs of EVs have decreased significantly in recent years, they still tend to be more expensive than traditional gasoline-powered vehicles. This cost barrier makes EVs less accessible to those with lower incomes.

Improving battery technology is another important challenge that needs to be addressed. Batteries are the most expensive part of EVs, and the current technology is limited in terms of range and longevity. Developing better batteries that are more efficient, have longer lifespans, and support long-range drives could drastically improve the consumer appeal of EVs.

In recent years, there have been numerous developments in the automotive industry, and new technological solutions are introduced to provide ease in driving and navigation. One such example is Comma.ai, which is a company that specializes in developing software and hardware that enables existing vehicles to become autonomous. Comma.ai uses specially designed sensors and hardware modules that are integrated into vehicles in order to obtain input about surroundings and take appropriate actions. The inputs are further classified using advanced AI and machine learning/deep learning models such as convolutional neural networks (CNN) and recurrent neural networks (RNN) for sensor data processing, image classification, object detection, semantic segmentation, and motion prediction [160]. In terms of sensor fusion, they use Kalman filters and extended Kalman filters (EKF) to combine and process data from various sensors such as cameras, radars, lidars, and microcontrollers. The specially designed hardware uses cameras such as the Sony IMX camera module, LIDARs such as Velodyne VLP-16, microcontrollers such as the Nvidia Jetson Xavier for processing power, and in terms of ICs, it uses processors such as Qualcomm Snapdragon, which is responsible for running the deep learning models and sensor fusion algorithms. The growing use of similar devices can make someone more vulnerable to cyber threats; therefore, it is important to audit and evaluate these kinds of devices.

The use of third-party mobile applications is increasing for electric vehicles as they provide a convenient way for users to access and control various features of their vehicles, such as charging status, battery level, and remote start. However, these applications also introduce new cybersecurity challenges and potential privacy leaks.

One such challenge is the vulnerabilities in the permission model in the Android operating system. Android apps often request access to various device features and data, such as location, camera, and microphone, contacts. Some of these permissions are categorized as highly sensitive and critical; however, some apps may request access to sensitive data or features that are not necessary for the app to function properly. This can lead to privacy leaks, as the app can collect and transmit personal information without the user's knowledge or consent.

Another cybersecurity challenge that arises from the use of third-party mobile apps for electric vehicles is the risk of malware. Malicious apps can be disguised as legitimate apps and can be used to gain unauthorized access to the vehicle's systems or steal personal information. For instance, EV-go is a charging application that utilizes multiple permissions including location, storage, and camera. On analyzing, we found that the application contains high-risk vulnerabilities that if exploited can lead to the disclosure of user's personal data.

In order to ensure that EVs can become a truly sustainable option, it is essential that governments, industry, and the public work together to address these challenges. Governments can provide incentives for purchasing EVs and installing charging stations, while the industry can focus on developing more efficient and affordable models. Finally, the public can help by advocating EV adoption, educating others on the benefits of EVs, and committing to more sustainable lifestyle choices.

7. Conclusions

EVs have the potential to reduce emissions and air pollution, reduce reliance on fossil fuels, and help secure a more sustainable future for the transportation industry. With continued research, development, and infrastructure investments, EVs could become the primary form of transportation. The most important research challenges in EVs are enhancing EVs' safety and privacy, developing secure charging infrastructure, improving the energy efficiency of batteries, increasing the range of vehicles, and reducing EVs' costs.

The article can be used as a baseline to understand and address future EV challenges. Multi-disciplinary researchers can use this research to develop a compatibility suite of security controls for EVs' sustainability features. We hope that the provided suggestions and future research direction facilitate industry professionals, academic institutions, cyber analysts, and automotive manufacturers to address these current challenges to make a smooth transition toward smart cities and a sustainable future.

Author Contributions: Methodology, Z.M. and B.S.; Supervision, Z.A.; Validation, Z.A. and J.S.; Visualization, Z.M. and B.S.; Writing—original draft, Z.M. and B.S.; Writing—review and editing, Z.A. and J.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by Sheila and Robert Challey Institute for Global Innovation and Growth, North Dakota State University (NDSU), USA.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Research and development of this study were conducted at the Sheila and Robert Challey Institute for Global Innovation and Growth at North Dakota State University, USA.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
ITS	Intelligent Transportation Systems
PII	Personal Identifiable Information
ESC	Electronic Stability Control
AEBS	Automatic Emergency Braking System
ACC	Adaptive Cruise Control
HMI	Human–Machine Interface
DHCP	Dynamic Host Configuration Protocol
EVSE	Electric Vehicle Supply Equipment
EVCP	Electric Vehicle Charging Points
BLE	Bluetooth Low Energy
CAN	Controller Area Network
ECUs	Electronic Control Units
DoS	Denial of Service
IDS	Intrusion Detection System
V2V	Vehicle-to-Vehicle communication
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2G	Vehicle-to-Grid
V2P	Vehicle-to-Pedestrian
V2D	Vehicle to Device
VANETs	Vehicles and hoc networks
RFID	Radio Frequency Identification
NHTSA	National Highway Traffic Safety Administration

LIDAR	Light Detection and Ranging
SRD	Short-Range Radio
CAS	Collision Avoidance System
GPS	Global Positioning System
RADAR	Radio Detection and Ranging
SRD	Short Radio Communication Device
ADAS	Advanced Driving Assistance system
2FA	Two-Factor Authentication
PHA	Potentially Harmful Applications
IDS	Intrusions Detection System
ICs	Integrated Circuits
ICE	Internal Combustion Engine
CNN	Convolutional Neural Networks
RNN	Recurrent Neural Networks
EKF	Extended Kalman Filters

References

1. Al-Sarawi, S.; Anbar, M.; Abdullah, R.; Al Hawari, A.B. Internet of things market analysis forecasts, 2020–2030. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 449–453.
2. Wiseman, Y. Autonomous vehicles. In *Research Anthology on Cross-Disciplinary Designs and Applications of Automation*; IGI Global: Hershey, PA, USA, 2022; pp. 878–889.
3. Iea. Electric Cars Fend off Supply Challenges to More Than Double Global Sales—Analysis. Available online: https://www.iea.org/commentaries/electric-cars-fend-off-supply-challenges-to-more-than-double-global-sales (accessed on 3 September 2022).
4. IEA Statistics. 2022. Available online: https://www.iea.org/data-and-statistics/charts/global-sales-and-sales-market-share-of-electric-cars-2010-2021 (accessed on 27 September 2022).
5. Chegini, H.; Naha, R.K.; Mahanti, A.; Thulasiraman, P. Process automation in an IoT–fog–cloud ecosystem: A survey and taxonomy. *IoT* **2021**, *2*, 92–118. [CrossRef]
6. Zhu, L. Analyzing the Advantages and Disadvantages of Different Sensors for Autonomous Vehicles. In Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022), Wuhan, China, 25–27 March 2022; Atlantis Press: Amsterdam, The Netherlands, 2022; pp. 1020–1024.
7. Ziajka-Poznańska, E.; Montewka, J. Costs and benefits of autonomous shipping—A literature review. *Appl. Sci.* **2021**, *11*, 4553. [CrossRef]
8. Cano, J.C.; Berrios, V.; Garcia, B.; Toh, C.K. Evolution of IoT: An industry perspective. *IEEE Internet Things Mag.* **2018**, *1*, 12–17. [CrossRef]
9. Malik, A.W.; Anwar, Z. Do Charging Stations Benefit from Cryptojacking? A Novel Framework for Its Financial Impact Analysis on Electric Vehicles. *Energies* **2022**, *15*, 5773. [CrossRef]
10. Malik, A.W.; Anwar, Z.; Rahman, A.U. A novel framework for studying the business impact of ransomware on connected vehicles. *IEEE Internet Things J.* **2022**. [CrossRef]
11. Saoudi, O.; Singh, I.; Mahyar, H. Autonomous Vehicles: Open-Source Technologies, Considerations, and Development. *arXiv* **2022**, arXiv:2202.03148.
12. Wilkinson, A.; Hill, M.; Gollan, P. The sustainability debate. *Int. J. Oper. Prod. Manag.* **2001**, *1*, 26 [CrossRef]
13. Goodland, R. The concept of environmental sustainability. *Annu. Rev. Ecol. Syst.* **1995**, *1*, 24. [CrossRef]
14. Lubin, D.A.; Esty, D.C. The sustainability imperative. *Harv. Bus. Rev.* **2010**, *88*, 42–50.
15. Mihet-Popa, L.; Saponara, S. Toward green vehicles digitalization for the next generation of connected and electrified transport systems. *Energies* **2018**, *11*, 3124. [CrossRef]
16. Salam, A. Internet of things for sustainable community development: Introduction and overview. In *Internet of Things for Sustainable Community Development*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1–31.
17. Kumar, A.D.; Chebrolu, K.N.R.; KP, S. A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities. *arXiv* **2018**, arXiv:1810.04144.
18. Othman, K. Exploring the implications of autonomous vehicles: A comprehensive review. *Innov. Infrastruct. Solut.* **2022**, *7*, 1–32. [CrossRef]
19. Silva, Ó.; Cordera, R.; González-González, E.; Nogués, S. Environmental impacts of autonomous vehicles: A review of the scientific literature. *Sci. Total. Environ.* **2022**, *1*, 154615. [CrossRef]
20. Hataba, M.; Sherif, A.; Mahmoud, M.; Abdallah, M.; Alasmary, W. Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey. *IEEE Open J. Commun. Soc.* **2022**, *3*, 811–829. [CrossRef]
21. Ahmed, H.U.; Huang, Y.; Lu, P.; Bridgelall, R. Technology Developments and Impacts of Connected and Autonomous Vehicles: An Overview. *Smart Cities* **2022**, *5*, 382–404. [CrossRef]

22. Alam, M.S.; Georgakis, P. The State of the Art of Cooperative and Connected Autonomous Vehicles from the Future Mobility Management Perspective: A Systematic Review. *Future Transp.* **2022**, *2*, 589–604. [CrossRef]
23. Bathla, G.; Bhadane, K.; Singh, R.K.; Kumar, R.; Aluvalu, R.; Krishnamurthi, R.; Kumar, A.; Thakur, R.; Basheer, S. Autonomous Vehicles and Intelligent Automation: Applications, Challenges, and Opportunities. *Mob. Inf. Syst.* **2022**, *2022*, 7632892. [CrossRef]
24. Bharathidasan, M.; Indragandhi, V.; Suresh, V.; Jasiński, M.; Leonowicz, Z. A review on electric vehicle: Technologies, energy trading, and cyber security. *Energy Rep.* **2022**, *8*, 9662–9685. [CrossRef]
25. Kim, K.; Kim, J.S.; Jeong, S.; Park, J.H.; Kim, H.K. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Comput. Secur.* **2021**, *103*, 102150. [CrossRef]
26. Electronics Sourcing How Many Chips Are in Our Cars? 2022. Available online: https://electronics-sourcing.com/2022/05/04/how-many-chips-are-in-our-cars/ (accessed on 10 January 2023).
27. Whalen, J. USA Will Miss Electric-Vehicle Targets without Big Investments in Semiconductor Manufacturing, Commerce Secretary Warns. 2021. Available online: https://www.washingtonpost.com/technology/2021/11/29/electric-vehicles-semiconductors-chips-act/ (accessed on 10 January 2023).
28. James, P.; Magee, L. Domains of sustainability. *Global Encyclopedia of Public Administration, Public Policy, and Governance*; Springer International Publishing: Cham, Switzerland, 2016; pp. 1–17.
29. Onat, N.C.; Kucukvar, M. A systematic review on sustainability assessment of electric vehicles: Knowledge gaps and future perspectives. *Environ. Impact Assess. Rev.* **2022**, *97*, 106867. [CrossRef]
30. Zeng, D.; Dong, Y.; Cao, H.; Li, Y.; Wang, J.; Li, Z.; Hauschild, M.Z. Are the electric vehicles more sustainable than the conventional ones? Influences of the assumptions and modeling approaches in the case of typical cars in China. *Resour. Conserv. Recycl.* **2021**, *167*, 105210. [CrossRef]
31. Basiago, A.D. Methods of defining 'sustainability'. *Sustain. Dev.* **1995**, *3*, 109–119. [CrossRef]
32. Tuncali, C.E.; Fainekos, G.; Prokhorov, D.; Ito, H.; Kapinski, J. Requirements-driven test generation for autonomous vehicles with machine learning components. *IEEE Trans. Intell. Veh.* **2019**, *5*, 265–280. [CrossRef]
33. Salman, R.E.; Alzaatreh, A. Market Basket Analysis of Chicago Road Accidents. In Proceedings of the 2022 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 21–24 February 2022; pp. 1–7.
34. Feng, S.; Magee, C.L. Technological development of key domains in electric vehicles: Improvement rates, technology trajectories and key assignees. *Appl. Energy* **2020**, *260*, 114264. [CrossRef]
35. Requia, W.J.; Mohamed, M.; Higgins, C.D.; Arain, A.; Ferguson, M. How clean are electric vehicles? Evidence-based review of the effects of electric mobility on air pollutants, greenhouse gas emissions and human health. *Atmos. Environ.* **2018**, *185*, 64–77. [CrossRef]
36. Hahad, O.; Kröller-Schön, S.; Daiber, A.; Münzel, T. The cardiovascular effects of noise. *Deutsch. Ärztebl. Int.* **2019**, *116*, 245. [CrossRef]
37. Gong, C.; Liu, J.; Han, Y.; Hu, Y.; Yu, H.; Zeng, R. Safety of Electric Vehicles in Crash Conditions: A Review of Hazards to Occupants, Regulatory Activities and Technical Support. *IEEE Trans. Transp. Electrif.* **2022**, *8*, 3870–3883. [CrossRef]
38. Fawzy, N.; Habib, H.F.; Mokhtari, S. Performance evaluation of electric vehicle model under skid control technique. *World Electr. Veh. J.* **2021**, *12*, 83. [CrossRef]
39. Narayanan, K.L.; Ram, C.R.S.; Subramanian, M.; Krishnan, R.S.; Robinson, Y.H. IoT based smart accident detection & insurance claiming system. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021; pp. 306–311.
40. Marsden, G.; McDonald, M.; Brackstone, M. Towards an understanding of adaptive cruise control. *Transp. Res. Part C Emerg. Technol.* **2001**, *9*, 33–51. [CrossRef]
41. Coelingh, E.; Eidehall, A.; Bengtsson, M. Collision warning with full auto brake and pedestrian detection-a practical example of automatic emergency braking. In Proceedings of the 13th International IEEE Conference on Intelligent Transportation Systems, Funchal, Portugal, 19–22 September 2010; pp. 155–160.
42. Liu, M.; Naoum-Sawaya, J.; Gu, Y.; Lecue, F.; Shorten, R. A distributed Markovian parking assist system. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 2230–2240. [CrossRef]
43. Ayyasamy, S. A Comprehensive Review on Advanced Driver Assistance System. *J. Soft Comput. Paradig.* **2022**, *4*, 69–81. [CrossRef]
44. Singh, S.; Saini, B.S. Autonomous cars: Recent developments, challenges, and possible solutions. In *Proceedings of the IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2021; Volume 1022, p. 012028.
45. Xie, K.; Zhang, Z.; Li, B.; Kang, J.; Niyato, D.; Xie, S.; Wu, Y. Efficient Federated Learning With Spike Neural Networks for Traffic Sign Recognition. *IEEE Trans. Veh. Technol.* **2022**, *71*, 9980–9992. [CrossRef]
46. Wang, J.; Chen, C.; Wang, C. Street Sign Recognition Algorithm Based on Deep Learning. In Proceedings of the 2020 3rd International Conference on Image and Graphics Processing, Singapore, 8–10 February 2020; pp. 31–35.
47. Ariyanto, M.; Haryadi, G.D.; Munadi, M.; Ismail, R.; Hendra, Z. Development of low-cost autonomous emergency braking system (AEBS) for an electric car. In Proceedings of the 2018 5th International Conference on Electric Vehicular Technology (ICEVT), Surakarta, Indonesia, 30–31 October 2018; pp. 167–171.
48. Reutebuch, S.E.; Andersen, H.E.; McGaughey, R.J. Light detection and ranging (LIDAR): An emerging tool for multiple resource inventory. *J. For.* **2005**, *103*, 286–292.

49. Sun, S.; Zhang, Y.D. 4D automotive radar sensing for autonomous vehicles: A sparsity-oriented approach. *IEEE J. Sel. Top. Signal Process.* **2021**, *15*, 879–891. [CrossRef]
50. Slepyan, G.; Vlasenko, S.; Mogilevtsev, D.; Boag, A. Quantum Radars and Lidars: Concepts, realizations, and perspectives. *IEEE Antennas Propag. Mag.* **2021**, *64*, 16–26. [CrossRef]
51. Yin, H.; Xu, X.; Wang, Y.; Xiong, R. Radar-to-lidar: Heterogeneous place recognition via joint learning. *Front. Robot. AI* **2021**, *8*, 661199. [CrossRef] [PubMed]
52. Divya, K.; Girisha, G. Autonomous Car Data Collection and Analysis. *Int. J. Sci. Res. Eng. Trends* **2021**, *7*.
53. Ondruš, J.; Kolla, E.; Vertal', P.; Šarić, Ž. How do autonomous cars work? *Transp. Res. Procedia* **2020**, *44*, 226–233. [CrossRef]
54. Saleh, S.; El-Wakeel, A.S.; Sorour, S.; Noureldin, A. Evaluation of 5G Cell Densification for Autonomous Vehicles Positioning in Urban Settings. In Proceedings of the 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, United Arab Emirates, 16–18 March 2021; pp. 1–6.
55. Dik, A.; Omer, S.; Boukhanouf, R. Electric Vehicles: V2G for Rapid, Safe, and Green EV Penetration. *Energies* **2022**, *15*, 803. [CrossRef]
56. Michaelides, E.E. Primary Energy Use and Environmental Effects of Electric Vehicles. *World Electr. Veh. J.* **2021**, *12*, 138. [CrossRef]
57. Rizza, V.; Torre, M.; Tratzi, P.; Fazzini, P.; Tomassetti, L.; Cozza, V.; Naso, F.; Marcozzi, D.; Petracchini, F. Effects of deployment of electric vehicles on air quality in the urban area of Turin (Italy). *J. Environ. Manag.* **2021**, *297*, 113416. [CrossRef]
58. Pipitone, E.; Caltabellotta, S.; Occhipinti, L. A Life Cycle Environmental Impact Comparison between Traditional, Hybrid, and Electric Vehicles in the European Context. *Sustainability* **2021**, *13*, 10992. [CrossRef]
59. Zein, Y.; Darwiche, M.; Mokhiamar, O. GPS tracking system for autonomous vehicles. *Alex. Eng. J.* **2018**, *57*, 3127–3137. [CrossRef]
60. Tumasov, A.; Vashurin, A.; Trusov, Y.P.; Toropov, E.; Moshkov, P.; Kryaskov, V.; Vasilyev, A. The application of hardware-in-the-loop (HIL) simulation for evaluation of active safety of vehicles equipped with electronic stability control (ESC) systems. *Procedia Comput. Sci.* **2019**, *150*, 309–315. [CrossRef]
61. Iombriller, S.F.; Bolognesi Prado, W.; Silva, M.A. *Comparative Analysis between American and European Requirements for Electronic Stability Control (ESC) Focusing on Commercial Vehicles*; Technical Report; SAE Internationa: Washington, DC, USA, 2019.
62. Rozas, H.; Muñoz-Carpintero, D.; Saéz, D.; Orchard, M.E. Solving in real-time the dynamic and stochastic shortest path problem for electric vehicles by a prognostic decision making strategy. *Expert Syst. Appl.* **2021**, *184*, 115489. [CrossRef]
63. Assidiq, A.; Khalifa, O.O.; Islam, M.R.; Khan, S. Real time lane detection for autonomous vehicles. In Proceedings of the 2008 International Conference on Computer and Communication Engineering, Kuala Lumpur, Malaysia, 13–15 May 2008; pp. 82–88.
64. Ahangar, M.N.; Ahmed, Q.Z.; Khan, F.A.; Hafeez, M. A survey of autonomous vehicles: Enabling communication technologies and challenges. *Sensors* **2021**, *21*, 706. [CrossRef] [PubMed]
65. Gschwendtner, C.; Sinsel, S.R.; Stephan, A. Vehicle-to-X (V2X) implementation: An overview of predominate trial configurations and technical, social and regulatory challenges. *Renew. Sustain. Energy Rev.* **2021**, *145*, 110977. [CrossRef]
66. Chen, S.; Hu, J.; Zhao, L.; Zhao, R.; Fang, J.; Shi, Y.; Xu, H. *Cellular Vehicle-to-Everything (C-V2X)*; Springer Nature: Berlin/Heidelberg, Germany, 2023.
67. Panigrahy, S.K.; Emany, H. A Survey and Tutorial on Network Optimization for Intelligent Transport System Using the Internet of Vehicles. *Sensors* **2023**, *23*, 555. [CrossRef]
68. Oh, I.; Batzorig, M.; Duulga, B.; Yim, K. Hardware-Software Interworking Real-Time V2X Dynamic Analysis Method. In *Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 215–223.
69. Aghapour, R.; Zeraati, M.; Jabari, F.; Sheibani, M.; Arasteh, H. Cybersecurity and Data Privacy Issues of Electric Vehicles Smart Charging in Smart Microgrids. In *Electric Vehicle Integration via Smart Charging*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 85–110.
70. Miller, C. Lessons learned from hacking a car. *IEEE Des. Test* **2019**, *36*, 7–9. [CrossRef]
71. Eisler, M.N. A Tesla in every garage? *IEEE Spectr.* **2016**, *53*, 34–55. [CrossRef]
72. Olsen, P. Honda Recalls 1.1 Million Vehicles for Faulty Replacement Airbags. Available online: https://www.consumerreports.org/car-recalls-defects/honda-recalls-vehicles-for-faulty-replacement-airbags/ (accessed on 30 November 2022).
73. Wang, C. Tesla Voluntarily Recalls 123,000 Model S Cars over Faulty Steering Component. 2018. Available online: https://www.cnbc.com/2018/03/29/tesla-recalls-123000-model-s-cars-over-potential-power-steering-failure-reports.html (accessed on 30 November 2022).
74. Mamiit, A. Chrysler Recalls 350K Cars, Suvs Due to Ignition Problem. 2014. Available online: https://www.techtimes.com/articles/16539/20140926/chrysler-recalls-350k-cars-suvs-due-to-ignition-problem.htm (accessed on 30 November 2022).
75. Atiyeh, C. Massive Takata Airbag Recall: Everything You Need to Know, including Full List of Affected Vehicles. 2021. Available online: https://www.caranddriver.com/news/a14499263/massive-takata-airbag-recall-everything-you-need-to-know-including-full-list-of-affected-vehicles/ (accessed on 30 November 2022).
76. Malik, S.; Sun, W. Analysis and simulation of cyber attacks against connected and autonomous vehicles. In Proceedings of the 2020 International Conference on Connected and Autonomous Driving (MetroCAD), Detroit, MI, USA, 27–28 February 2020; pp. 62–70.
77. Ovchinnikov, S. On the transitivity property. *Fuzzy Sets Syst.* **1986**, *20*, 241–243. [CrossRef]

78. Fatima, M.; Abbas, H.; Yaqoob, T.; Shafqat, N.; Ahmad, Z.; Zeeshan, R.; Muhammad, Z.; Rana, T.; Mussiraliyeva, S. A survey on common criteria (CC) evaluating schemes for security assessment of IT products. *PeerJ Comput. Sci.* **2021**, *7*, e701. [CrossRef] [PubMed]
79. BBC News. Hackers Hit San Francisco Transport Systems. 2016. Available online: https://www.bbc.com/news/technology-38127096 (accessed on 1 October 2022).
80. Otorio Automotive Industry. Ransomware: The Cyber Attacks on The Automotive Industry. 2021. Available online: https://www.otorio.com/blog/ransomware-the-cyber-attacks-on-the-automotive-industry/ (accessed on 1 October 2022).
81. Dibaei, M.; Zheng, X.; Jiang, K.; Abbas, R.; Liu, S.; Zhang, Y.; Xiang, Y.; Yu, S. Attacks and defences on intelligent connected vehicles: A survey. *Digit. Commun. Netw.* **2020**, *6*, 399–421. [CrossRef]
82. Mckinsey. Monetizing Car Data. 2016. Available online: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/monetizing-car-data (accessed on 4 October 2022).
83. Ntousakis, G.; Ioannidis, S.; Vasilakis, N. Detecting Third-Party Library Problems with Combined Program Analysis. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, 15–19 November 2021; pp. 2429–2431.
84. Vice Article. How a Hacker Controlled Dozens of Teslas Using a Flaw in Third-Party App. 2022. Available online: https://www.vice.com/en/article/akv7z5/how-a-hacker-controlled-dozens-of-teslas-using-a-flaw-in-third-party-app (accessed on 4 October 2022).
85. O'Donnell, L. Volkswagen Cars Open to Remote Hacking, Researchers Warn. 2018. Available online: https://threatpost.com/volkswagen-cars-open-to-remote-hacking-researchers-warn/131571/ (accessed on 18 January 2023).
86. Dimitrova, M. Vulnerable Audio Decoder Exposes Conversations of Millions of Android Users (CVE-2021-30351). 2022. Available online: https://sensorstechforum.com/qualcomm-cve-2021-30351/ (accessed on 18 January 2023).
87. Lab, U. Custom Text and Transmission Information Displayed on Dashboard. 2022. Available online: https://upstream.auto/research/automotive-cybersecurity/?id=5090 (accessed on 18 January 2023).
88. The Drive Tech. The Drive Tech. 2021. Available online: https://www.thedrive.com/tech/40438/researchers-used-a-drone-and-a-wifi-dongle-to-break-into-a-tesla (accessed on 4 October 2022).
89. Cimpanu, C. Thieves Using Radio Jammers to Prevent Drivers from Locking Their Cars. 2016. Available online: https://www.bleepingcomputer.com/news/security/thieves-using-radio-jammers-to-prevent-drivers-from-locking-their-cars/ (accessed on 18 January 2023).
90. Johnson, J.; Berg, T.; Anderson, B.; Wright, B. Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies* **2022**, *15*, 3931. [CrossRef]
91. Tushar, W.; Yuen, C.; Huang, S.; Smith, D.B.; Poor, H.V. Cost minimization of charging stations with photovoltaics: An approach with EV classification. *IEEE Trans. Intell. Transp. Syst.* **2015**, *17*, 156–169. [CrossRef]
92. Acharya, S.; Dvorkin, Y.; Pandžić, H.; Karri, R. Cybersecurity of smart electric vehicle charging: A power grid perspective. *IEEE Access* **2020**, *8*, 214434–214453. [CrossRef]
93. BBC News. Isle of Wight: Council's Electric Vehicle Chargers Hacked to Show Porn Site. 2022. Available online: https://www.bbc.com/news/uk-england-hampshire-61006816 (accessed on 18 January 2023).
94. Independent News. Russian EV Charging Stations Hacked. 2022. Available online: https://www.independent.co.uk/news/world/europe/putin-charging-station-hacked-ukraine-russia-b2026260.html (accessed on 18 January 2023).
95. Conti, M.; Donadel, D.; Poovendran, R.; Turrin, F. EVExchange: A Relay Attack on Electric Vehicle Charging System. *arXiv* **2022**, arXiv:2203.05266.
96. Lambert, F. Tesla Singled out in Bluetooth Hack That Can Unlock Cars. 2022. Available online: https://electrek.co/2022/05/17/tesla-singled-out-bluetooth-hack-unlock-cars/ (accessed on 18 January 2023).
97. Robinson, M. £20,000 Keyless Car Theft Device Disguised as a Game Boy Recovered by Police. 2021. Available online: https://www.carthrottle.com/post/20000-keyless-car-theft-device-disguised-as-a-game-boy-recovered-by-police/ (accessed on 18 January 2023).
98. Thehill Education. How Tesla Owners Can Mine Cryptocurrency with Their Cars. 2022. Available online: https://thehill.com/changing-america/enrichment/education/589045-how-tesla-owners-can-mine-cryptocurrency-with-their/ (accessed on 4 October 2022).
99. Jose Antonio, Electric Vehicle used for Coin Mine Experiment. 2021. Available online: https://thekoreancarblog.com/2021/06/24/hyundai-ioniq-5-used-for-bitcoin-mine-experiment/ (accessed on 18 January 2023).
100. Yahoo News, This Electric Vehicle Mines Crypto in Its Free Time. Available online: https://news.yahoo.com/this-electric-vehicle-mines-crypto-in-its-free-time-191748861.html (accessed on 18 January 2023).
101. investopedia News. Tesla's Cloud Was Hacked for Mining Cryptocurrency. 2019. Available online: https://www.investopedia.com/news/teslas-cloud-was-hacked-mining-cryptocurrency/ (accessed on 4 October 2022).
102. Nasr, T.; Torabi, S.; Bou-Harb, E.; Fachkha, C.; Assi, C. Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. *Comput. Secur.* **2022**, *112*, 102511. [CrossRef]
103. Bozdal, M.; Samie, M.; Jennions, I. A survey on can bus protocol: Attacks, challenges, and potential solutions. In Proceedings of the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 16–17 August 2018; pp. 201–205.

104. Bloom, G. WeepingCAN: A stealthy CAN bus-off attack. In Proceedings of the Workshop on Automotive and Autonomous Vehicle Security, Virtual, 25 February 2021. [CrossRef]
105. Jedh, M.; Othmane, L.B.; Ahmed, N.; Bhargava, B. Detection of message injection attacks onto the can bus using similarities of successive messages-sequence graphs. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 4133–4146. [CrossRef]
106. Upstream, Open-Source App Controls and Alters Vehicles through CAN Bus. Available online: https://upstream.auto/research/automotive-cybersecurity/?id=4710 (accessed on 18 January 2023).
107. Topman, N.; Adnane, A. Mobile applications for connected cars: Security analysis and risk assessment. In Proceedings of the NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 25–29 April 2022; pp. 1–6.
108. Mirza, S.; Abbas, H.; Shahid, W.B.; Shafqat. A Malware Evasion Technique for Auditing Android Anti-Malware Solutions. In Proceedings of the 2021 IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Bayonne, France, 27–29 October 2021; pp. 125–130.
109. Kavitha, D.; Ravikumar, S. Designing an IoT based autonomous vehicle meant for detecting speed bumps and lanes on roads. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 7417–7426. [CrossRef]
110. Chatzoglou, E.; Kambourakis, G.; Kouliaridis, V. A Multi-Tier Security Analysis of Official Car Management Apps for Android. *Future Internet* **2021**, *13*, 58. [CrossRef]
111. Zahid Anwar, Overlooked Security Challenges in Electric Vehicle. 2022. Available online: https://dda.ndus.edu/ddreview/overlooked-security-challenges-in-electric-vehicle-charging-infrastructure/ (accessed on 2 October 2022).
112. El-Rewini, Z.; Sadatsharan, K.; Sugunaraj, N.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity attacks in vehicular sensors. *IEEE Sens. J.* **2020**, *20*, 13752–13767. [CrossRef]
113. Dayanikli, G.Y.; Hatch, R.R.; Gerdes, R.M.; Wang, H.; Zane, R. Electromagnetic sensor and actuator attacks on power converters for electric vehicles. In Proceedings of the 2020 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 21 May 2020; pp. 98–103.
114. Insideevsforum, Collision Avoidance Almost Caused an Accident. Available online: https://www.insideevsforum.com/community/index.php?threads%2Fcollision-avoidance-almost-caused-an-accident.8307%2F (accessed on 18 January 2023).
115. Liam Tung, Ransomware Warning: Cyber Criminals Are Mailing out USB Drives That Install Malware. Available online: https://www.zdnet.com/article/fbi-cybercriminals-are-mailing-out-usb-drives-that-will-install-ransomware/ (accessed on 18 January 2023).
116. JohnrMod3. Can I Do a Software Update via Flash Drive? 2022. Available online: https://teslamotorsclub.com/tmc/threads/can-i-do-a-software-update-via-flash-drive.270264/ (accessed on 18 January 2023).
117. Kosmanos, D.; Pappas, A.; Maglaras, L.; Moschoyiannis, S.; Aparicio-Navarro, F.J.; Argyriou, A.; Janicke, H. A novel intrusion detection system against spoofing attacks in connected electric vehicles. *Array* **2020**, *5*, 100013. [CrossRef]
118. Kummerow, A.; Schäfer, K.; Gupta, P.; Nicolai, S.; Bretschneider, P. Combined Network Intrusion and Phasor Data Anomaly Detection for Secure Dynamic Control Centers. *Energies* **2022**, *15*, 3455. [CrossRef]
119. Mousavian, S.; Erol-Kantarci, M.; Ortmeyer, T. Cyber Attack Protection for a Resilient Electric Vehicle Infrastructure. In Proceedings of the 2015 IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, 6–10 December 2015.
120. Lee, S.; Park, Y.; Lim, H.; Shon, T. Study on analysis of security vulnerabilities and countermeasures in ISO/IEC 15118 based electric vehicle charging technology. In Proceedings of the 2014 International Conference on IT Convergence and Security (ICITCS), Beijing, China, 28–30 October 2014; pp. 1–4.
121. Patil, S.; Joshi, S. Demystifying user data privacy in the world of IOT. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 4412–4418. [CrossRef]
122. Guo, L.; Ye, J.; Yang, B. Cyberattack Detection for Electric Vehicles Using Physics-Guided Machine Learning. *IEEE Trans. Transp. Electrif.* **2021**, *7*, 2010–2022. [CrossRef]
123. Hossin, M.; Sulaiman, M.N. A review on evaluation metrics for data classification evaluations. *Int. J. Data Min. Knowl. Manag. Process.* **2015**, *5*, 1.
124. Aggarwal, C.C. Data classification. In *Proceedings of the Data Mining*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 285–344.
125. Noori, M.; Tatari, O. Development of an agent-based model for regional market penetration projections of electric vehicles in the USA. *Energy* **2016**, *96*, 215–230. [CrossRef]
126. Arkin, B.; Stender, S.; McGraw, G. Software penetration testing. *IEEE Secur. Priv.* **2005**, *3*, 84–87. [CrossRef]
127. Yim, H.J.; Kim, S.; Lim, B.M.; Park, S.I.; Hur, N. Application-based targeted advertisement system for ATSC 3.0 UHD service. *IEEE Trans. Broadcast.* **2020**, *67*, 56–67. [CrossRef]
128. Lee, J.; Kim, H.J.; Shin, I.H.; Cho, J.; Lee, S.J.; Kwak, H.Y. Design of an advertisement scenario for electric vehicles using digital multimedia broadcasting. In *Proceedings of the International Conference on Security-Enriched Urban Computing and Smart Grid*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 288–291.
129. Coshkun, A.; Amanzholova, A. Use of Naive Bayes Classifier for Spam Filtering. *A. Asaui atyndağy Halykaralyk Kazak-Tùrìk Univ. Habar.* **2019**, *111*, 117–122.
130. Garimella, K.; Kostakis, O.; Mathioudakis, M. Ad-blocking: A study on performance, privacy and counter-measures. In Proceedings of the 2017 ACM on Web Science Conference, Troy, NY, USA, 25–28 June 2017; pp. 259–262.

131. Pathan, A.S.K.; Lee, H.W.; Hong, C.S. Security in wireless sensor networks: Issues and challenges. In Proceedings of the 2006 8th International Conference Advanced Communication Technology, Phoenix Park, Republic of Korea, 20–22 February 2006; Volume 2, p. 6.
132. Healy, M.; Newe, T.; Lewis, E. Security for wireless sensor networks: A review. In Proceedings of the 2009 IEEE Sensors Applications Symposium, New Orleans, LA, USA, 19 February 2009; pp. 80–85.
133. Cheng, F.C. Automatic and secure Wi-Fi connection mechanisms for IoT end-devices and gateways. In *Proceedings of the International Conference for Emerging Technologies in Computing*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 98–106.
134. Harnett, K.; Harris, B.; Chin, D.; Watson, G. *DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report*; Technical Report; John A. Volpe National Transportation Systems Center (US): Washington, DC, USA, 2018.
135. Behl, M.; DuBro, J.; Flynt, T.; Hameed, I.; Lang, G.; Park, F. Autonomous electric vehicle charging system. In Proceedings of the 2019 Systems and Information Engineering DESIGN symposium (SIEDS), Charlottesville, VA, USA, 26 April 2019; pp. 1–6.
136. Shelke, M.; Pardhi, A.; Lanjewar, B.; Mokase, N. Zigbee Live Electricity Meter Monitoring with Tempering Proof. *Int. J. Res. Sci. Eng.* **2017**, *3*.
137. Gedeon, A.S.; Buttyán, L.; Papp, D.F. Secure Boot and Firmware Update on a Microcontroller-Based Embedded Board. Bachelor's Thesis, Faculty of Electrical Engineering And Informatics, Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary, 2020.
138. Mourad, A.; Laverdiere, M.A.; Debbabi, M. Security Hardening of Open Source Software. 2006. Available online: https://www.researchgate.net/profile/Azzam-Mourad/publication/220919944_Security_hardening_of_open_source_software/links/02bfe51463a5bb5d4f000000/Security-hardening-of-open-source-software.pdf (accessed on 18 January 2023).
139. Ding, R. Performant Software Hardening under Hardware Support. Ph.D. Thesis, Georgia Institute of Technology, Atlanta, GA, USA, 2021.
140. Filley, J. Mobile Device Isolation and Faraday Containers. 2018. Available online: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C35&q=Mobile+Device+Isolation+and+Faraday+Containers&btnG= (accessed on 18 January 2023).
141. Babu, P.R.; Amin, R.; Reddy, A.G.; Das, A.K.; Susilo, W.; Park, Y. Robust authentication protocol for dynamic charging system of electric vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 11338–11351. [CrossRef]
142. Schneier, B. Two-factor authentication: Too little, too late. *Commun. ACM* **2005**, *48*, 136. [CrossRef]
143. Alghassab, M. Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector. *Energies* **2021**, *15*, 218. [CrossRef]
144. Ioulianou, P.P.; Vassilakis, V.G.; Logothetis, M.D. Battery drain denial-of-service attacks and defenses in the Internet of Things. *J. Telecommun. Inf. Technol.* **2019**, *2*, 37–45. [CrossRef]
145. Schiavo, J. Code signing for end-user peace of mind. *Netw. Secur.* **2010**, *2010*, 11–13. [CrossRef]
146. Buennemeyer, T.K.; Gora, M.; Marchany, R.C.; Tront, J.G. Battery exhaustion attack detection with small handheld mobile computers. In Proceedings of the 2007 IEEE International Conference on Portable Information Devicesm, Orlando, FL, USA, 25–29 March 2007; pp. 1–5.
147. Woo, S.; Jo, H.J.; Lee, D.H. A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 993–1006. [CrossRef]
148. Casillo, M.; Coppola, S.; De Santo, M.; Pascale, F.; Santonicola, E. Embedded intrusion detection system for detecting attacks over CAN-BUS. In Proceedings of the 2019 4th International Conference on System Reliability and Safety (ICSRS), Rome, Italy, 20–22 November 2019; pp. 136–141.
149. La Polla, M.; Martinelli, F.; Sgandurra, D. A survey on security for mobile devices. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 446–471. [CrossRef]
150. Meng, X.; Qian, K.; Lo, D.; Shahriar, H.; Talukder, M.A.I.; Bhattacharya, P. Secure mobile IPC software development with vulnerability detectors in Android studio. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; Volume 1, pp. 829–830.
151. Kim, G.; Lim, J.; Kim, J. Mobile security solution for sensitive data leakage prevention. In Proceedings of the 5th International Conference on Communications and Broadband Networking, New York, NY, USA, 20–22 February 2017; pp. 59–64.
152. Muhammad, Z.; Amjad, M.F.; Abbas, H. A Systematic Evaluation of Android Anti-Malware Tools for Detection of Contemporary Malware. In Proceedings of the 2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing (EUC), Shenyang, China, 20–22 October 2021; pp. 117–124.
153. Ukil, A.; Sen, J.; Koilakonda, S. Embedded security for Internet of Things. In Proceedings of the 2011 2nd National Conference on Emerging Trends and Applications in Computer Science, Shillong, Meghalaya, 4–5 March 2011; pp. 1–6.
154. Meng, L.; Ren, S.; Tang, G.; Yang, C.; Yang, W. Uav sensor spoofing detection algorithm based on gps and optical flow fusion. In Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, Nanjing, China, 10–12 January 2020; pp. 146–151.
155. Fan, C.; Tan, J. A majority voting scheme in wireless sensor networks for detecting suspicious node. In Proceedings of the 2009 Second International Symposium on Electronic Commerce and Security, Washington, DC, USA, 22–24 May 2009; Volume 2, pp. 495–498.
156. Jafarnejad, S.; Codeca, L.; Bronzi, W.; Frank, R.; Engel, T. A car hacking experiment: When connectivity meets vulnerability. In Proceedings of the 2015 IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, 6–10 December 2015.

157. Fabian, M. Endpoint security: Managing USB-based removable devices with the advent of portable applications. In Proceedings of the 4th Annual Conference on INFORMATION Security Curriculum Development, Kennesaw, GA, USA, 28 September 2007; pp. 1–5.
158. Tian, D.; Bates, A.; Butler, K.R.; Rangaswami, R. Provusb: Block-level provenance-based data protection for usb storage devices. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 242–253.
159. Larimer, J. USB autorun attacks against linux. In Proceedings of the Hackito Ergo Sum 2011, Paris, France, 9 April 2011.
160. Alsubaei, F.S. Reliability and security analysis of artificial intelligence-based self-driving technologies in Saudi Arabia: A case study of Openpilot. *J. Adv. Transp.* **2022**, *2022*, 2085225. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.