Living on the Electric Vehicle and Cloud Era: A Study of Cyber Vulnerabilities, Potential Impacts, and Possible Strategies

Long Vu
Kennesaw State University
Marietta, Georgia, USA
lvu6@students.kennesaw.edu

Kun Suo
Kennesaw State University
Marietta, Georgia, USA
ksuo@kennesaw.edu

Md Romyull Islam, Nobel Dhar
Kennesaw State University
Marietta, Georgia, USA
{mislam22,ndhar}@students.kennesaw.edu

Tu N. Nguyen, Selena He, Yong Shi
Kennesaw State University
Marietta, Georgia, USA
{tu.nguyen,she4,yshi5}@kennesaw.edu

ABSTRACT

In recent years, electric vehicles (EVs) have emerged as a sustainable alternative to conventional automobiles. Distinguished by their environmental friendliness, superior performance, reduced noise, and low maintenance requirements, EVs offer numerous advantages over traditional vehicles. The integration of electric vehicles with cloud computing has heralded a transformative shift in the automotive industry. However, as EVs become increasingly interconnected with the internet, various devices, and infrastructure, they become susceptible to cyberattacks. These attacks pose a significant risk to the safety, privacy, and functionality of both the vehicles and the broader transportation infrastructure.

In this paper, we delve into the topic of electric vehicles and their connectivity to the cloud. We scrutinize the potential attack vectors that EVs are vulnerable to and the consequential impact on vehicle operations. Moreover, we outline both general and specific strategies aimed at thwarting these cyberattacks. Additionally, we anticipate future developments aimed at enhancing EV performance and reducing security risks.

CCS CONCEPTS

• **Security and privacy** → **Trusted computing**; **Mobile and wireless security**; • **Computer systems organization** → *Embedded systems.*

KEYWORDS

Electric Vehicle, Hardware, Software, Cyber Security, Connectivity

ACM Reference Format:
Long Vu, Kun Suo, Md Romyull Islam, Nobel Dhar, Tu N. Nguyen, Selena He, and Yong Shi. 2024. Living on the Electric Vehicle and Cloud Era: A Study of Cyber Vulnerabilities, Potential Impacts, and Possible Strategies. In *2024 ACM Southeast Conference (ACMSE 2024), April 18–20, 2024, Marietta, GA, USA.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3603287.3651209

ACMSE 2024, April 18–20, 2024, Marietta, GA, USA

ACM ISBN 979-8-4007-0237-2/24/04.
https://doi.org/10.1145/3603287.3651209

1 INTRODUCTION

In recent years, electric vehicles (EVs) offer a promising solution for developing a sustainable and environmentally friendly transportation industry in the future due to their numerous advantages, including low carbon emissions, enhanced operational flexibility, reduced noise, and higher efficiency than conventional internal combustion engine vehicles [38]. Although electric vehicles might seem like a new innovation, the technology has been there for more than a century. In the past decade, the global electric vehicle market has grown significantly, with continuous improvement in cruising range, richer model choices, and better performance. The adoption of electric vehicles is expanding due to technological advancements, government support, growing environmental awareness and changing consumer preferences, and evolving charging infrastructure. Global EV sales in 2012 were just 120,000. However, electric vehicle sales doubled in 2021 from the previous year to reach 6.6 million, which accounts for about 10% of global car sales. According to the IEA report [9], sales of electric vehicles reached 2 million units in the first quarter of 2022 alone, a 75% increase over the same period in 2021, and such the growth trend will continue in many countries for many years ahead.

Unlike traditional cars, EVs contain a vast array of software, applications, and connectivity; including in-vehicle, vehicle-to-vehicle, vehicle-to-cloud, vehicle-to-infrastructure communications, etc. This connectivity can be seamlessly integrated with smart systems to provide EV owners with advanced features and services. In addition, the integration of cloud computing technology into electric vehicles is crucial to establish an efficient and intelligent operation and management platform. Many companies currently use hybrid or private clouds to manage their systems, applications, or services [3]. Increased production of connected vehicles, new self-driving features and the proliferation of software that enables cars to park and drive themselves have led to a staggering surge in the number of cyberattacks targeting the auto industry. With widespread connected wireless networks, increased data collection, and EV platforms generating a growing number of attack vectors, ranging from OEM backend servers to vehicle electronic control units (ECUs), and even through the Bluetooth functionality of in-vehicle entertainment. A recent report [13] revealed that 82% of attacks against the automotive industry were conducted remotely. Additionally, keyless entry theft accounted for 94% of all cars recovered by tracker in 2021 [12].

This paper discusses the model of electric vehicles living connected to cloud platforms, network vulnerabilities, types of attacks, possible impacts, and strategies for prevention. Specifically, we analyze the interaction of modern electric vehicles and the cloud, introducing different levels of operation and specific case scenarios. We also examine possible cyber risks and how they affect the safety and performance of EV systems. The contribution of this paper is that we do not consider general vehicles, but focus on the connection and interaction of new electric vehicle platforms and cloud platforms, rethinking the threats of traditional network security under electric vehicle platforms and new unique challenges for electric vehicles. We analyze the cyber attack vectors, characteristics, and potential impact on current electric vehicle platforms. Aiming at these flaws, we summarize a series of effective security strategies and countermeasures to overcome or minimize the impact of cyber attacks on electric vehicles.

The remaining sections of the paper are outlined as follows. Section 2 emphasizes the crucial reasons for establishing seamless communication between electric vehicles and the cloud while also explaining the structure of EV-cloud communication. In Section 3, the common attack vectors of EVs and potential cyber-attacks likely to occur on EVs are discussed, along with an analysis of the impacts caused by these attacks. Section 4 examines both general and specific countermeasures that can be employed to defend against these attacks. Section 5 provides an overview of the related research in this field. The existing limitations and areas for prospective future research are examined in Section 6. Finally, the paper concludes with a summary in Section 7.

2 THE CONNECTION BETWEEN EVS AND OUTSIDE WORLD

Modern electric vehicles contain a large number of sensors, which can generate a large amount of data during EV operation. Although most of the data processing happens inside the vehicle itself, smart vehicles still need to interact with the outside world. To improve overall functionality, enhance the driving experience, identify potential hazards, and reduce collisions, electric vehicles need to interface with various systems and devices, including smartphones, base stations, charging stations, and even other vehicles. They exchange information using a variety of wireless communication technologies, such as Dedicated Short-Range Communications (DSRC), Wi-Fi, Bluetooth, GPS, and cellular networks. Contemporary vehicle-to-vehicle (V2X) communication can be categorized into four main types: vehicle-to-vehicle (V2V), vehicle-to-device (V2D), vehicle-to-infrastructure (V2I), and vehicle-to-cloud (V2C) [27]. Table 1 demonstrates a variety of network connection types, network technologies in use, and the kinds of information transmitted between them.

2.1 The Interaction of Modern Electric Vehicles and the Cloud

In recent years, the advent of electric vehicles and their integration with cloud computing has revolutionized the automotive industry. Electric vehicles need to communicate with the cloud for several reasons. 1) *Remote monitoring and diagnosis.* As EVs transmit information about the battery state of charge, charging process, vehicle location, and performance parameters, this data helps identify potential problems, diagnose them, and provide preventive care and support. 2) *Software update.* Software updates are frequently needed for electric vehicles to enhance performance, provide new features, and fix safety issues. Through the cloud connection, the car can undergo immediate over-the-air (OTA) software upgrades. 3) *Third-party applications.* Owners of electric vehicles can access various connected services and applications through cloud connectivity. These services may include navigation systems with real-time traffic updates, remote climate control, personalized recommendations for charging stations, etc [20]. 4) *Distance estimation.* By analyzing data such as the charging level and speed of electric vehicles in the cloud, manufacturers can improve range estimation algorithms and more accurately predict the range of electric vehicles. EV users can optimize their charging strategy and ease range anxiety with the real-time accessibility of charging station locations. All of the above-mentioned services for electric vehicles need to be realized through cloud connections. The development and sustainability of future electric transportation are supported by integrating EVs with cloud computing, which is of considerable relevance for increasing the usage of electric vehicles.

Table 1: Types of V2X Connectivity, Technology and Data

Connectivity	Network Technology	Information Exchange
Vehicle-to-Vehicle	DSRC	Speed, Road Congestion, Lane Changing
Vehicle-to-Device	Cellular Networks such as 4G, 5G, Wi-Fi, Bluetooth	Parking and Charging Station Availability, Navigation
Vehicle-to-Infrastructure	DSRC, Cellular Network, Wi-Fi	Traffic congestion, Weather Updates
Vehicle-to-Cloud	Cellular Network, Wi-Fi	Vehicle Data, Sensor Data, OTA Update

2.2 Case Studies of Cloud-based Services on EVs

Cloud-based Application. Under the trend of software-defined vehicles and vehicle-cloud integration, cloud computing has become an important foundation for the user experience of electric vehicles. An example of a cloud-based application for electric vehicles is the Everon [7]. This application is a management platform that uses Google Cloud to connect drivers with charging stations. It also provides services such as locating stations through an interface powered by Google Maps and obtaining accurate pricing information from charging stations. Everon allows users to track, manage and optimize their electric vehicle charging. Likewise, Volkswagen has partnered with Microsoft Azure [23] to power an onboard navigation system and allow Volkswagen EVs to locate charging stations and recommend charging points along the way. The cloud can avoid route conflicts between multiple vehicles from the planning level, and greatly improve the reliability and safety of driving an electric vehicle.

Cloud-based Maintenance. Electric vehicles employ multiple sensors to gather data on various driving behaviors, including driver acceleration, braking, energy regeneration, and other relevant

parameters. In addition, the data also includes battery information such as temperature, voltage, charge and discharge times, trip details such as start and end times, charger connection and disconnection times, and information from sensors such as radar, lidar, cameras, etc. [43]. The generated real-time data can be used for various purposes such as improving battery efficiency, enhancing vehicle safety, maintenance, and better user experience [22]. To increase battery performance and lifespan in electric vehicles, Bosch is creating a cloud-based solution. The system combines data from the fleet, cloud computing, and artificial intelligence (AI) to achieve the goal. The vehicle's remote control unit collects and filters the battery data before sending it to the Bosch cloud for analysis by sophisticated algorithms. The self-learning system evaluates battery conditions and chooses the best parameter settings for optimum performance. Bosch cloud then returns the results, including recommendations and condition reports, back to vehicles [2].

2.3 EV-Cloud Communication Structure

As shown in Figure 1, the communication structure between EVs and the cloud can generally be divided into three layers.

Vehicle Layer. The vehicle layer comprises a cluster of nearby vehicles that communicate wirelessly, facilitating better distribution of computing and storage resources among each other. This layer is responsible for collecting vehicle-related information through the sensors, including cameras, radar, lidar, and other devices within the vehicle. Besides, V2V communication also involves using DSRC frequencies and sharing data such as speed, position, direction, etc., which enables the system to have a 360-degree understanding of the surrounding environment. V2I enables vehicles in transit to be connected to road systems. Their components include traffic lights, cameras, lane markings, street lights, signage, and parking meters. Part of the collected information will be sent to the nearby edge layers for further processing.

Edge Layer. The edge layer is mainly used for the connection between the vehicle layer and the cloud layer. This layer consists of edge servers, base stations (BS), and roadside units (RSUs) for the initial processing of information and sending necessary data to the cloud for further analysis. Compared to the cloud, edge servers have less computing power but are still considered relatively high compared to user-level devices [28] (i.e., electric vehicles). It also provides instant services and stores data about local road infrastructure. The vehicle connects to the BS and RSU through wireless communication such as a cellular 4G/5G network or short-range communication like Bluetooth.

Cloud Layer. Cloud servers are generally located remotely from end users. The computing power of the cloud greatly exceeds that of edge nodes, and it can quickly calculate large amounts of data and process complex but non-latency-sensitive calculations. Data collected by individual edge nodes that requires additional processing is transmitted to the cloud layer. This data is usually permanently stored for future analysis.

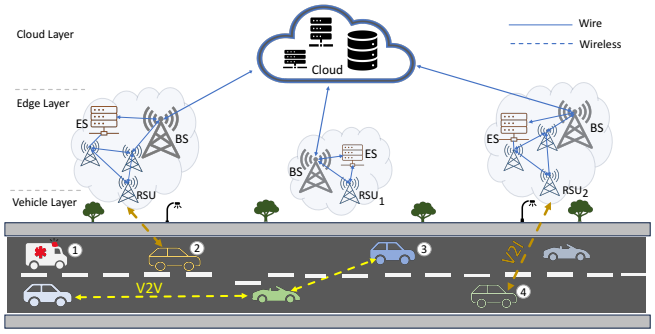

Figure 1: Three Layers of Communication Structure between the EVs and Cloud

2.4 Examples of Communication Scenarios

In this section, we introduce several concrete examples of EVs communicating within a certain layer or among different layers in the above communication structure.

Scenario 1: Yield for Ambulance. Vehicle ① sends an alarm to electric vehicle ② and nearby vehicles. As shown in Figure 1, vehicle ① is an ambulance. As it operates, it sends signals to nearby vehicles for clearing the road ahead. Once other vehicles receive the alert message about the emergency vehicle, they move out of the way. The communication in this scenario happens only within the vehicle layers. Because very little data needs to be processed, there is almost no need to interact with the edge and cloud layer.

Scenario 2: Traffic Jam Notification. RSU1 sends notifications about traffic congestion ahead to vehicles within its coverage area. RSU1 can detect current traffic jams by estimating the traffic state using occupancy rate and occupancy time [42]. When traffic congestion is detected, RSU1 sends alerts to all nearby vehicles in its immediate area. As Figure 1 depicts, the electric vehicle ③ is notified because it is located within the coverage of RSU1. In this scenario, communication only happens between the edge and vehicle layer.

Scenario 3: Over-the-Air Update. Electric vehicle ④ gets software update alerts via the cloud server. Initially, the manufacturer loads the software package into cloud storage over a secure connection and notifies the user of the update [50]. When the user accepts the request, it connects with the nearby edge server through RSU2 and the base station. Then, the edge server communicates with the cloud and verifies the security of the software. As seen in this example, all three levels must cooperate for over-the-air upgrades for EVs.

3 EV CYBER VULNERABILITIES AND IMPACTS

Electric vehicles communicate with other vehicles, infrastructure, and the cloud using different connection channels such as DSRC, cellular networks, WiFi, or Bluetooth. These channels support many functions, including data sharing, charging station availability, remote control, software updates, and cloud connectivity. Due to

these connectivities to the external world, electric vehicles have become more vulnerable to cyber threats. With the continuous development of intelligence and network interconnection, weak authentication mechanisms or insecure encryption protocols might make electric vehicles even more vulnerable to attacks. This raises the prominence of cyber security for electric vehicles.

According to a recent Deloitte report [4] on cybersecurity issues in the automotive industry, 84% of vehicle cyberattacks are processed remotely. The cybersecurity vulnerabilities in electric vehicles could lead to critical data leaks, or an attacker could gain access to safety systems and ultimately take control of the entire vehicle. For example, an attacker can forge the signals transmitted between a vehicle and the infrastructure to mislead other vehicles, potentially causing traffic jams or even accidents [39]. One NCC study also disclosed vulnerabilities in Tesla Model 3 and Model Y keyless systems [17]. In addition, cyberattacks can significantly reduce the efficiency of electric vehicles as well.

In this section, we delve into the diverse attack vectors and types of attacks that may arise during the communication between EVs and the infrastructure (e.g., cloud, edge, etc.). Additionally, we analyze the potential impacts of these attacks on the EV system.

3.1 Common EV Attack Vectors

Malware or virus software that aims to disrupt in-vehicle computer functions or obtain unauthorized access to data poses a significant danger to EVs. Multiple vulnerabilities, such as roadside network wireless communications, in-vehicle Wi-Fi hotspots, and Internet connectivity, could allow malware or hackers to infect smart vehicles. Malware-infected devices such as cell phones, iPods, and laptops can also be physically or wirelessly connected to vehicles and then used to share insecure files between vehicles. Typically, attackers gain access to the vehicle internal system using one of two attack vectors – remote access or physical access. To exploit an ECU, an attacker may use various interfaces on the smart vehicle system stack. For example, wireless attacks often enter internal communication buses through gateways. As electric vehicles become more connected to the external environment and their intelligence becomes more complex, the number of attacks and the risk of vulnerabilities also increases. Ultimately, whether it is a physical or wireless attack, the security and efficiency of smart vehicle systems will be significantly compromised.

Nowadays, hackers are using various advanced technologies to attack smart vehicles. As shown in Figure 2, there exist several entry points for smart vehicles that might be at risk [30]. By analyzing cases from 2010, a report [14] from Upstream found that the top three common attack vectors were keyless entry/start engine systems, servers, and mobile applications. The numbers in Figure 2 represent the percentage of the total number of incidents under each attack vector.

3.2 Types of EV Attacks

The information exchange between various units, including RSU, base station, EV, edge server, infrastructure, and cloud, is depicted by the communication model in Figure 1. However, wireless message transmission makes it vulnerable to various attacks that can be classified into different categories, such as attacks on infrastructure,

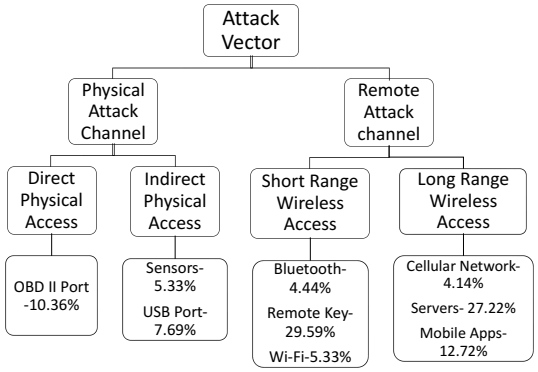

Figure 2: Common Attack Vectors on EV System

communication channels, network edges, core networks, and data networks [45]. For instance, Regulus Cyber researchers discovered that the GNSS (GPS) receiver of Tesla Model S and Tesla Model 3 models was vulnerable to wireless and remote spoofing attacks [18]. This revealed significant security flaws in critical functions like telematics, sensor fusion, and navigation capabilities. This section will discuss common attacks based on the aforementioned scenarios.

Eavesdropping. In this attack, information exchanged can be eavesdropped by the attacker and violates the confidentiality of the users [45]. For example, an attacker can listen to the messages with the help of receivers installed roadside and able to inject fake messages to manipulate other users. For instance, researchers from the University of Oxford have developed a wireless eavesdropping system at the EV physical layer for HomePlug charging system [29].

Jamming. Attackers purposefully create false signals or messages on the same frequency channel where proper transmission occurs in order to interfere with vehicles' ability to communicate and force them to make wrong decisions or actions [46].

Message Spoofing/Forgery. An adversary creates and broadcasts fake messages or misleading alerts or modifies the original message, which could lead nearby vehicles, infrastructure, and users to take wrong actions and result in accidents. For example, they can modify the location information and mislead users [45].

Replay Attack. To impede traffic and cause the receiving cars to respond inappropriately to fictional road conditions, an attacker resends previously created messages or signals by other vehicles, persons, and equipment [45]. Qasem et al. found that replay attacks were often used for remote keyless controlled EVs [25].

Man-in-the-Middle (MitM). The attacker positions themselves between the transmitting and the receiving vehicles, sniffs any data being passed between them, and then tries to impersonate one of them. The MiM attack breaches the vehicle networks' integrity, authenticity, and non-repudiation policies [36]. With a MitM attack, a hacker would take advantage of a signal that appears to be legitimate, such as a WiFi or USB port on a charging station, allowing them to completely rewire the charging request and gain root access to the charging station or electric vehicle.

Table 2: Types of Attacks and Possible Scenarios

Attacks	Scenario-1	Scenario-2	Scenario-3
Eavesdropping	✓		
Jamming		✓	
Message Spoofing		✓	
Replay Attack	✓		
Man-in-the-Middle			✓
Sybil Attack	✓		
Fake Attack		✓	
Denial-of-Service		✓	
Malware Injection			✓
Location Tracking	✓		
Impersonate Attack		✓	
Black Hole Attack	✓		

Sybil Attack. An attacker, by creating multiple false identities that appear to originate from different vehicles, generates various messages and broadcasts them to other vehicles, infrastructure, and users [46]. Fraiji et al. reported that a Sybil attack could easily make the server have a wrong view of the charging station queue, which can have a negative impact on the drivers' decision-making [34].

Fake Attack. An attacker may act as a base station, edge server, or RSU along the road, or a local server, to attract victims into connecting to it. If they do, their sensitive information, such as access credentials and passwords, can be exposed [45].

Denial-of-Service (DoS) Attack. DoS attacks are a class of attacks that try to prevent authorized users from accessing resources by interfering with the availability of network services. The availability of vehicle networks may be seriously jeopardized if this attack is undertaken in a distributed manner to create a distributed DoS attack [39]. The SaiFlow research team from Israel recently discovered that attackers can use Open Charging Station Protocol (OCPP) of the WebSocket communication to render electric vehicle charging stations unusable and cause service interruptions [8].

Malware Injection. Attackers try to attack the integrity and security of the system by introducing malicious software or code into the EV or Cloud infrastructure. This may allow for unauthorized entry, data theft, or system control. The harmful software is also capable of destroying the applications in vehicles and impairing their functionality [36].

Location Tracking. In this scenario, attackers monitor and analyze messages made by targets to keep track of the location of authorized vehicles [39], which could lead to an invasion of privacy or even harm to personal safety.

Impersonate Attack. Using a fake vehicle identity, an attacker tries to impersonate another authorized vehicle. The attacker can get the credentials of another legitimate vehicle to carry out this assault successfully. Attacks using false identities are frequently the starting point for more complex attacks [45].

Black Hole Attack. Black hole attack gets its name from its characteristics. Instead of sending packets ahead, attackers drop them all like a black hole. Therefore, critical information cannot be delivered to legitimate users. This assault may cause massive data loss since it is difficult to detect [39]. Both black hole attacks and DoS attacks will cause service interruption or even data damage and loss in EVs.

It's important to note that all the attacks mentioned above can occur in the scenarios listed in Table 2. This is because all communication is carried out wirelessly through various communication protocols that are susceptible to attacks. Here we just marked the corresponding box in the table to identify the most likely scenario under certain types of attack.

3.3 Impacts of Attack on EVs

Due to the various attack surfaces that exist across cloud-EV communication, it is generally possible for an electric vehicle to be attacked. For instance, based on Section 3.1, the key fob appears to be the most commonly used attack vector. Recent reports indicate that a security researcher from Belgium has discovered a method to gain control of the firmware of Tesla Model X key fobs, allowing them to potentially steal cars that haven't received the latest software update [19]. Cyber-attacks on electric vehicles can introduce serious negative impacts on users, vehicles, enterprises, and society in multiple ways, ranging from minor inconveniences to major security risks. Here we list some potential outcomes.

Loss of Mobility. Disabling an electric vehicle battery management system could result in a loss of power to the vehicle, rendering it immobile and leaving drivers stranded, potentially creating traffic jams. As more transportation sector becomes electrified, a cyber attack on charging stations could overwhelm the infrastructure, causing a denial of charging service, incapacitating vehicles, damaging systems, and disrupting grid functionality.

Data Leakage. Intelligent navigation, voice control, and onboard cameras in EVs have brought us great convenience and safety but also generated large amounts of data. Attackers can access the onboard computer system of EVs, which may steal personal privacy security information [15] such as vehicle tracking, audio, video, images, biometric information, driving habits, etc. At the same time, in-vehicle data may also include information related to national security and public interests, such as military management areas, vehicle flow, logistics, and charging network operation.

Remote Control and Safety Risks. If there are loopholes or insecure configurations in the electric vehicle system, hackers may invade the system through remote attacks, obtain sensitive data

Table 3: Security Strategies Against Attacks

Attacks	Counter Measures	References
Eavesdropping	• Both asymmetric and symmetric cryptography can effectively prevent attack. • Adding friendly jammers to network.	[36], [52]
Jamming	• Addressed through the implementation of direct sequence spread spectrum techniques and physical layer frequency hopping. • Multi-antenna-based approach is preferred due to its capability to mitigate interference from unwanted sources.	[35], [46]
Message Spoofing	• Security measures such as checksums, trapdoor hash functions, reedsolomon codes, message authentication codes, and digital signatures can be used to enhance data protection. • Use of vehicular public key infrastructure.	[44], [41]
Replay Attacks	• Timestamps can be applied to sensitive packets, or alternatively, all messages can be timestamped using broadcast time for added security and accuracy. • By digitally signing each message and including a sequence number, the integrity and order of the messages can be ensured.	[6], [51]
Man-in-the-Middle	• Employing authentication techniques alongside robust cryptographic methods ensures secure communication. • One viable option is to implement a multiway challenge-response protocol, such as the Needham-Schroeder protocol.	[32], [45]
Sybil Attack	• Use of temporary certificates to establish a centralized validation authority. • Employ public key infrastructure for key distribution and revocation.	[26], [47]
Fake Attack	• Implementing Public Key Infrastructure (PKI) and certificate-based authentication provides a robust security framework.	[45]
Denial-of-Service	• Digital signatures and the usage of specific authentication techniques. • Using small lifetime public and private key pairs along with a hash function.	[32], [48]
Malware Injection	• Strong privacy preservation mechanisms and secure communication protocols. • Machine learning algorithms have been developed in malware detection.	[36], [37]
Location Tracking	• Using temporary and anonymous keys. • Differential privacy is a promising approach to safeguarding location privacy.	[33], [36]
Impersonate Attack	• Using strong message authentication techniques. • Use of MAC and IP addresses, TAs (trust authorities), and user authentication with digital signatures.	[46]
Black Hole Attack	• Use of hybrid intrusion detection systems and secure routing architectures	[36], [31]

about the vehicle, tamper with the functions, abuse the system, or perform illegal operations. Attackers could also gain remote control of EV systems, allowing them to manipulate critical functions such as speed or steering, which could put drivers and other road users at risk of accidents or collisions [5].

Financial Losses and Reputation Damage. Cyber attacks on charging infrastructure or the grid could disrupt a vehicle's ability to charge or move, reduce its functionality and usefulness, and further cause financial loss to the vehicle owner or operator. Additionally, these actions may also damage the reputation of the manufacturer or operator, resulting in a loss of trust and customer loyalty [10].

4 SECURITY STRATEGIES

Protecting electric vehicles from cyberattacks is critical as it not only ensures passenger safety, but also protects user privacy, prevents vehicle fraud, maintains the integrity of vehicle software, fosters trust in the technology and ensures regulatory compliance. To effectively address these critical issues, this section focuses on general strategies that can be adopted to minimize the risk of cyber threats and specific countermeasures against different attacks. We also discussed that for the overall architecture design of electric smart vehicle network security, it is necessary to establish multiple security lines on the vehicle side and the cloud.

4.1 Strategies Against Attacks

The frequency of attacks targeting electric vehicles steadily increases, necessitating robust security measures to safeguard EVs from cyber threats. In Section 3.1, we examined various attack vectors in EVs and their ramifications. This section will outline common preventive measures that can be adopted to mitigate the potential consequences. Here we list safety measures that both electric vehicle users and manufacturers can implement to prevent cybersecurity attacks.

Software Update. Keeping software up to date strengthens its defenses against threats. However, users need to ensure the update is from a legitimate manufacturer. Hackers often send deceptive update notifications masquerading as real upgrades to inject malware. Installing unauthorized software and systems can seriously compromise physical and digital security [16, 21].

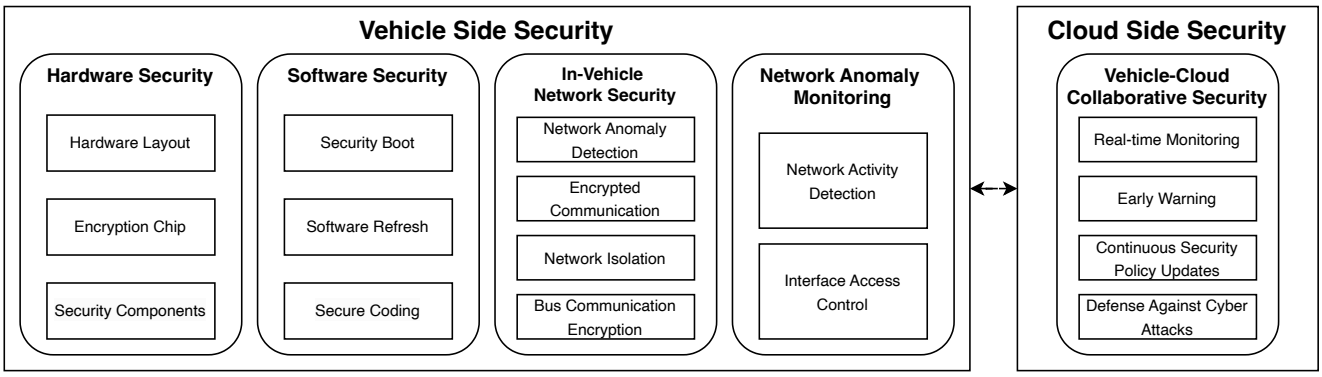

Figure 3: Security Architecture Design Components

Restrict In-vehicle Wireless Services. EV wireless systems such as in-vehicle Wi-Fi, satellite radio, telematics, and Bluetooth, can inadvertently offer hackers an entry point to vehicles. To minimize the risk, users can turn off some features when not in use [1].

Avoid Untrusted Apps and Services. Refrain from downloading apps or software from untrusted sources, as they may contain malware that can compromise the security of vehicles.

Other Measurements. Employ encryption and implement multiple authentication measures to safeguard sensitive information, such as vehicle data and user credentials, from unauthorized access and potential breaches. Enhance the security of your vehicle's systems and data by strictly controlling access and employing multi-authentication methods, granting access only to authorized personnel who require it [21]. Manufacturers and users should conduct regular security assessments to identify and address software and hardware vulnerabilities in the vehicle.

In addition to the above-mentioned general means of defending against cyber-attacks for electric vehicles, we also provide a comprehensive overview of specific defense mechanisms against different cyber-attacks in Table 3. This overview is designed to address the impacts of cyber-attacks discussed in Section 3.2, aiming to mitigate these effects. For different attack methods, the response defense strategies are also different. For example, for eavesdropping, asymmetric ciphers and symmetric ciphers can be used. For replay attacks, using timestamp-based data packets or network messages containing digital signatures is a more effective means of defense.

4.2 EV Cyber Security Architecture Design

For the overall architecture design of the network security in electric smart vehicles, it should include the establishment of multiple security defense lines on both the vehicle side and the cloud side, as shown in Figure 3. On the vehicle side, first, the security software and hardware architecture design is the key foundation. At the hardware security level, it includes the security design of hardware layout, encryption chip, security components, etc. For software security, the representative examples include security boot, refresh, and coding. Secondly, the in-vehicle network security architecture is also important, which mainly implements network bus anomaly detection and encrypted communication through means such as in-vehicle network security isolation and bus communication encryption. Finally, during vehicle operation, network anomaly monitoring is also necessary, mainly to realize network activity detection and interface access control. On the cloud side, it is critical to further establish vehicle-cloud collaborative security to realize real-time monitoring, early warning, and continuously updated security policies to defend against various types of cyber attacks.

5 RELATED WORK

EV Communication. The connection between electric vehicles (EVs) and their surroundings is crucial for safety, charging infrastructure optimization, over-the-air updates, autonomous driving, and more. In studies by Arena et al. [27], and Fraiji et al. [34], the focus was on communication between general vehicles and infrastructure, as well as devices. In this paper, we paid more attention to electric vehicle platforms and discussed communication between EVs and their surrounding environment, which includes mainly the cloud, infrastructure, other vehicles, and devices. We also examine the communication channels used and the type of information exchanged between them.

Attacks on EV. Understanding the potential security risks associated with electric vehicles is crucial, as they can be vulnerable to various attacks. While Bozdal et al. [30] have identified some attack vectors, our paper further highlights a few additional attack vectors specific to EVs. Additionally, we provide information on the percentage of attacks that occurred due to these attack vectors. Several papers, including [34, 36, 39, 40, 45, 46], have classified attacks on V2X communication channels, which result from wireless connections. For instance, Islam et al. [40] focused on attacks between vehicles and infrastructure, while authors of [49] mentioned attacks that only happen in LTE-enabled services. Moreover, [36, 45] grouped attacks according to trust, security, and privacy concerns. Our paper analyzes common attacks during cloud-EV communication using a few scenarios discussed in the above model.

Security Strategies. Various researchers, cited in sources [26, 31–33, 36, 37, 44–48, 51, 52] have put forth security strategies to address different types of attacks, as discussed earlier. For example, Zhang et al. [52] suggest using friendly jammers to minimize the effects of eavesdropping, while the author of [47] advocates for Public Key Infrastructure as a means of key distribution and revocation

against the Sybil attack. ElSalamouny et al. [33] recommend using differential privacy to safeguard location privacy. While the studies mentioned above propose specific strategies, this paper emphasizes general strategies that EV users and manufacturing industries should adopt to mitigate the impacts of cyber attacks.

6 CURRENT LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

Despite EVs' numerous benefits, certain limitations must be addressed to ensure an enhanced user experience. Embracing innovative techniques holds the key to overcoming these barriers and propelling the development of EVs. Below, we outline some of the current limitations and future directions for EV development, especially from the security perspective.

EV Charging Infrastructure. With EVs' increasing popularity, the charging infrastructure's significance cannot be overstated. However, locating and utilizing charging stations for EV owners can be challenging, especially during long journeys, as accessibility and convenience remain limited in certain regions [24]. As charging stations become more connected to the cloud, they become susceptible to potential attacks. It is crucial to implement secure communication protocols between EVs, charging stations, and backend systems and develop robust intrusion detection systems to detect and respond promptly to cybersecurity threats.

Safety and Privacy. As electric vehicles (EVs) become more connected and autonomous, they are more vulnerable to cyberattacks, which can jeopardize the safety and security of the vehicle and its passengers. To mitigate and minimize the risks of cyberattacks, research is essential to develop improved privacy-preserving techniques, cybersecurity protocols, and methods [11]. These measures ensure EVs' continued advancement and secure integration in our transportation systems.

Vehicle and Grid Interaction. Vehicle-to-Grid (V2G) and Grid-to-Vehicle (G2V) technologies are gradually evolving, enabling electric vehicles to interact with the power grid by consuming and supplying electricity. One key area of the research is the development of scalable and secure cloud-based platforms to effectively manage V2G and G2V interactions, encompassing data exchange, scheduling, and billing. Investigating and implementing robust security measures to safeguard V2G and G2V communications, as well as data stored in the cloud, while prioritizing user privacy during transactions, remains difficult and challenging.

7 CONCLUSIONS

Electric Vehicles (EVs) are often referred to as next-generation computing platforms and computers on wheels, showcasing their cutting-edge technological advancements. Over the years, the adoption of electric vehicles has surged. This growth is driven by numerous advantages such as reduced pollution, lower noise levels, enhanced efficiency, advanced technology, and superior driving comfort compared to traditional automobiles. This study delves into the crucial topic of electric vehicles and their integration with cloud connectivity. We examine the potential attack vectors that EVs might be susceptible to and the resulting impact on the vehicle. Furthermore, we propose specific and general strategies to mitigate these cyber threats and anticipate future developments to enhance performance and overcome challenges. The findings of this study can serve as a valuable resource for researchers interested in EV platforms and cybersecurity issues related to EVs, directing their focus and encouraging further investigations in this field. As research in electric vehicle technology advances, the future for EVs appears promising. With increased investment and ongoing innovation, electric vehicles have the potential to revolutionize transportation and lead the way toward a more sustainable and environmentally friendly future.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their suggestions and feedback. This work was supported in part by U.S. NSF grants CPS-2103459, SHF-2210744, 2244450, AMPS-2229073, and CNS-2103405.

REFERENCES

[1] [n. d.]. *5 Tips for Protecting Your Connected Vehicle against Cyberattacks.* https://tinyurl.com/srypvysc.
[2] [n. d.]. *Battery in the Cloud.* https://tinyurl.com/muyw2ffe.
[3] [n. d.]. *Cloud Technology for Electric Vehicles.* https://tinyurl.com/4jvc3fwk.
[4] [n. d.]. *Connecting Canada Securing the Vehicle of the Future.* https://www2.deloitte.com/ca/en/pages/risk/articles/securing-the-vehicles-of-the-future.html.
[5] [n. d.]. *Cyberattack on Cars Increased 225% in Last Three Years.* https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/.
[6] [n. d.]. *ETSI ITS Security, Threat, Vulnerability and Risk Analysis (TVRA).* https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.01.01_60/tr_102893v010101p.pdf.
[7] [n. d.]. *Everon: Moving Up a Gear with Microservices on Google Kubernetes Engine.* https://cloud.google.com/customers/everon.
[8] [n. d.]. *Hijacking EV Charge Points to Cause DoS.* https://www.saiflow.com/hijacking-chargers-identifier-to-cause-dos/.
[9] [n. d.]. *IEA (2022), Electric Vehicles.* https://www.iea.org/reports/electric-vehicles.
[10] [n. d.]. *Impact of Cyber Attack on Your Business.* https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business.
[11] [n. d.]. *The Increasing Need for Electric Vehicle Cyber Security.* shorturl.at/inprT.
[12] [n. d.]. *Keyless Cars Twice as Likely to be Stolen as Non-Keyless Models.* https://www.driving.co.uk/news/keyless-cars-twice-as-likely-to-be-stolen-as-non-keyless-models/.
[13] [n. d.]. *New Study Shows Just How Bad Vehicle Hacking Has Gotten.* https://www.cnet.com/roadshow/news/2019-automotive-cyber-hack-security-study-upstream/.
[14] [n. d.]. *Race to Secure Connected Cars.* https://approov.io/blog/the-race-to-secure-connected-cars.
[15] [n. d.]. *The Rise of Cyber-Attacks in the Automotive Industry.* https://www.uscybersecurity.net/automotive-industry/.
[16] [n. d.]. *Six Ways to Protect Against Autonomous Vehicle Cyber Attacks.* https://innovationatwork.ieee.org/six-ways-to-protect-against-autonomous-vehicle-cyber-attacks/.
[17] [n. d.]. *Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks.* https://tinyurl.com/2p93e3zm.
[18] [n. d.]. *Tesla Model S and Model 3 Prove Vulnerable to GPS Spoofing Attacks.* https://rb.gy/cr6um.
[19] [n. d.]. *Tesla Model-X Hacked and Stolen in Minutes Using New Key Fob Hack.* https://www.zdnet.com/article/tesla-model-x-hacked-and-stolen-in-minutes-using-new-key-fob-hack/.
[20] [n. d.]. *Top 4 Car Features That Rely on Vehicle-to-Cloud Connectivity.* https://autocrypt.io/4-car-features-rely-on-vehicle-to-cloud-connectivity/.
[21] [n. d.]. *Use These Car Hacking Safety Tips to Protect Your Vehicle from Cyber Threats.* https://northstar-ins.com/car-hacking-safety-tips/.
[22] [n. d.]. *V2X in the Connected Car of the Future.* https://www.qorvo.com/design-hub/blog/v2x-in-the-connected-car-of-the-future.
[23] [n. d.]. *Volkswagen Automotive Cloud.* https://www.volkswagen.co.uk/en/electric-and-hybrid/discover-electric/volkswagen-automotive-cloud.html.
[24] [n. d.]. *What are the Downsides to Electric Cars?* shorturl.at/iBZ59.
[25] Qasem Abu Al-Haija and Abdulaziz A Alsulami. 2022. Detection of Fake Replay Attack Signals on Remote Keyless Controlled Vehicles Using Pre-Trained Deep Neural Network. *Electronics* 11, 20 (2022), 3376.
[26] Mohammed Saeed Al-Kahtani. 2012. Survey on Security Attacks in Vehicular Ad Hoc Networks (VANETs). In *International Conference on Signal Processing and*

Communication Systems. IEEE, Gold Coast, QLD, Australia.

[27] Fabio Arena and Giovanni Pau. 2019. An Overview of Vehicular Communications. *Future Internet* 11 (01 2019), 27. https://doi.org/10.3390/fi11020027

[28] Peter Arthurs, Lee Gillam, Paul Krause, Ning Wang, Kaushik Halder, and Alexandros Mouzakitis. 2022. A Taxonomy and Survey of Edge Cloud Computing for Intelligent Transportation Systems and Connected Vehicles. *IEEE Transactions on Intelligent Transportation Systems* (2022).

[29] Richard Baker and Ivan Martinovic. 2019. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA, USA.

[30] Mehmet Bozdal, Mohammad Samie, Sohaib Aslam, and Ian Jennions. 2020. Evaluation of CAN Bus Security Challenges. *Sensors* 20, 8 (2020), 2364.

[31] Sonja Buchegger and Jean-Yves Le Boudec. 2004. A Robust Reputation System for P2P and Mobile Ad-Hoc Networks. *P2P and Mobile Ad-hoc Networks, Second Workshop on the Economics of Peer-to-peer Systems* (2004).

[32] Ming-Chin Chuang and Jeng-Farn Lee. 2013. TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks. *IEEE Systems Journal* (2013).

[33] Ehab ElSalamouny and Sébastien Gambs. 2016. Differential Privacy Models for Location-based Services. *Transactions on Data Privacy* 9, 1 (2016), 15–48.

[34] Yosra Fraiji, Lamia Ben Azzouz, Wassim Trojet, and Leila Azouz Saidane. 2018. Cyber Security Issues of Internet of Electric Vehicles. In *IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, Barcelona, Spain.

[35] Haji M Furqan, Muhammad Sohaib J Solaija, Jehad M Hamamreh, and Huseyin Arslan. 2019. Intelligent Physical Layer Security Approach for V2X Communication. *arXiv preprint arXiv:1905.05075* (2019).

[36] Amrita Ghosal and Mauro Conti. 2020. Security Issues and Challenges in V2X: A Survey. *Computer Networks* 169 (2020), 107093.

[37] William Hardy, Lingwei Chen, Shifu Hou, Yanfang Ye, and Xin Li. 2016. DL4MD: A Deep Learning Framework for Intelligent Malware Detection. In *Proceedings of the International Conference on Data Science (ICDATA)*. Las Vegas, NV, USA.

[38] Chris Harto. 2020. Electric Vehicle Ownership Costs: Chapter 2–Maintenance. *Consumer Reports, September* (2020), 20–1.

[39] Jiaqi Huang, Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. 2020. Recent Advances and Challenges in Security and Privacy for V2X Communications. *IEEE Open Journal of Vehicular Technology* (2020).

[40] Mhafuzul Islam, Mashrur Chowdhury, Hongda Li, and Hongxin Hu. 2018. Cybersecurity Attacks in Vehicle-to-Infrastructure Applications and Their Prevention. *Transportation Research Record Journal of the Transportation Research Board* (2018).

[41] N. S. Jayalakshmi, Rachel Rajadurai, and K. Indumathi. 2013. Vehicular Network: Properties, Structure, Challenges, Attacks, Solutions for Improving Scalability and Security. *International Journal of Scientific & Engineering Research* 4. Issue 6.

[42] Zahid Khan, Anis Koubaa, and Haleem Farman. 2020. Smart Route: Internet-of-Vehicles (IoV)-Based Congestion Detection and Avoidance (IoV-Based CDA) Using Rerouting Planning. *Journal of Applied Sciences* (2020).

[43] Boyang Li, Mithat C. Kisacikoglu, Chen Liu, Navjot Singh, and Melike Erol-Kantarci. 2017. Big Data Analytics for Electric Vehicle Integration in Green Smart Cities. *IEEE Communications Magazine* (2017).

[44] Chang Liu, Chi Yang, Xuyun Zhang, and Jinjun Chen. 2015. External Integrity Verification for Outsourced Big Data in Cloud and IoT: A Big Picture. *Future Generation Computer Systems* (2015).

[45] Rongxing Lu, Lan Zhang, Jianbing Ni, and Yuguang Fang. 2019. 5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy. *Proc. IEEE* (2019).

[46] Mujahid Muhammad and Ghazanfar Ali Safdar. 2018. Survey on Existing Authentication Issues for Cellular-Assisted V2X Communication. *Vehicular Communications* 12 (2018), 50–65.

[47] Ashwin Rao, Ashish Sangwan, Arzad A. Kherani, Anitha Varghese, Bhargav Bellur, and Rajeev Shorey. 2007. Secure V2V Communication With Certificate Revocations. In *2007 Mobile Networking for Vehicular Environments*.

[48] Maxim Raya and Jean-Pierre Hubaux. 2005. The Security of Vehicular Ad Hoc Networks. In *Proceedings of the 3rd ACM workshop on Security of Ad Hoc and Sensor Networks*. 11–21.

[49] Salman Raza, Shangguang Wang, Manzoor Ahmed, Muhammad Rizwan Anwar, et al. 2019. A Survey on Vehicular Edge Computing: Architecture, Applications, Technical Issues, and Future Directions. *Wireless Communications and Mobile Computing* (2019).

[50] Eberhard Scheuble. 2020. Secure Over-the-air Updates for Connected Vehicles. *ATZelectronics Worldwide* 15, 5 (2020), 48–53.

[51] Gongjun Yan Yan, Gyanesh Choudhary, Michele C Weigle, and Stephan Olariu. 2007. Providing VANET Security Through Active Position Detection. In *Proceedings of the fourth ACM International Workshop on Vehicular Ad Hoc Networks*. Montréal, Québec, Canada.

[52] Ning Zhang, Nan Cheng, Ning Lu, Xiang Zhang, Jon W Mark, and Xuemin Shen. 2015. Partner Selection and Incentive Mechanism for Physical Layer Security. *IEEE Transactions on Wireless Communications* 14, 8 (2015), 4265–4276.