NEURALSLATE OPEN ACCESS JOURNALS

# Risks of Cyber Threats and Developing Robust Security Protocols within Electric Vehicle Charging Infrastructure

**Li Xuefeng**
Department of Mechanical Engineering, Yunnan Rural Technical College

**Zhang Wei,**
School of Computer Sciences, Inner Mongolia Agricultural University

## Abstract

The electric vehicle (EV) charging infrastructure is undergoing rapid expansion, concurrent with the increasing adoption of EVs. This interconnected infrastructure entails communication between vehicles, charging stations, and back-end servers, giving rise to various cyber risks. The risks include unauthorized access, data manipulation, Denial of Service (DoS) attacks, firmware and software attacks, physical tampering, and risks associated with EV ecosystem integration. Unauthorized access may lead to theft of personal information or unauthorized control over charging, while data manipulation could cause incorrect billing or even physical harm. DoS attacks and physical tampering can disrupt charging services, and outdated software might be exploited. Integration with other systems like smart grids may also expose broader infrastructure to risks. To counter these risks, the development of robust security protocols is essential. This involves a comprehensive risk assessment and management; strong access control and authentication; data encryption and integrity checks; network security measures such as firewalls and intrusion detection; regular software and firmware updates; physical security controls; adherence to cybersecurity standards like ISO/IEC 27001, NIST, GDPR; security awareness and training; a clear incident response plan; collaboration with industry stakeholders such as automakers and utility providers; and regular third-party security audits. Together, these strategies form a complex defense against the multifaceted and significant risks associated with the cyber threats to EV charging infrastructure, necessitating ongoing adaptation as technology evolves and new threats emerge.

***Indexing terms**: Electric Vehicle (EV) Charging Infrastructure, Cyber Risks, Security Protocols, Risk Management, Unauthorized Access*

## Introduction

The rapid expansion of Electric Vehicle (EV) charging infrastructure is intricately intertwined with the surging adoption of electric vehicles, creating a complex ecosystem that interconnects charging stations, vehicles, and back-end servers [1]–[3]. This symbiotic growth is driven by technological advancements and a global push towards sustainable transportation solutions [4]–[6]. As the number of EVs on the roads continues to increase, the need for an accessible and reliable charging network becomes paramount. This has led to the development of various types of charging stations, ranging from residential chargers to high-power fast chargers strategically positioned along highways and urban centers [7].

The interconnected nature of EV charging infrastructure is facilitated by a blend of hardware and software systems. Charging stations are equipped with diverse charging connectors to accommodate different EV models and standards. Furthermore, the integration of Internet of Things (IoT) technology enables real-time communication between charging stations, vehicles, and central servers. This connectivity allows EV owners to conveniently locate available charging stations, check their status, and initiate charging sessions through dedicated mobile apps or online platforms [8]–[10]. Meanwhile, charging stations communicate with central servers to manage billing, monitor power consumption, and ensure optimal grid utilization [11].

The backbone of this expansive network lies within the back-end servers and software platforms that orchestrate the entire EV charging process. These servers manage user authentication, payment processing, and data exchange between charging stations and utility providers. Moreover, they play a pivotal role in load management and demand

response, dynamically distributing the available power among multiple charging stations to prevent grid overload. Smart algorithms and predictive analytics are employed to forecast charging patterns, allowing operators to optimize the deployment of charging infrastructure and plan for future expansion [12].

Charging Standards and Protocols form an integral part of Electric Vehicle (EV) charging infrastructure, facilitating the compatibility and uniformity between various EV manufacturers and charging equipment providers [13]–[15]. The CHAdeMO standard, primarily used by Japanese automakers, was one of the first DC fast-charging standards and operates at up to 62.5 kW. The Combined Charging System (CCS) is another DC fast-charging protocol that combines single-phase AC, three-phase AC, and DC charging into one connector. It has been endorsed by major European and American automakers and has the capacity to charge at levels up to 350 kW. Meanwhile, the Type 1 and Type 2 connectors are predominantly used for AC charging in the United States and Europe, respectively [16].

Interoperability is essential for the widespread adoption of electric vehicles, and charging standards play a crucial role in ensuring this. The Mennekes Type 2 connector is an example of an attempt to standardize the connection interface across Europe. It has been adopted as the official charging plug in the European Union and is also used in other regions [17]. Furthermore, in an effort to bridge the differences between various standards, there have been collaborative efforts among industry stakeholders [18]–[20]. Multi-standard charging stations, equipped with different connectors to accommodate various charging standards, are emerging as a practical solution to the fragmented charging landscape [21].

Charging protocols also encompass the communication between the vehicle, charging station, and potentially the broader electrical grid. OCPP (Open Charge Point Protocol) is a universal protocol that enables EV chargers to communicate with a central system, regardless of the manufacturer. This openness fosters a competitive market, as operators can choose equipment from various vendors without being locked into a single provider [22]–[24]. Other communication protocols, like ISO 15118, facilitate secure communication between the vehicle and charging station, including features like Plug and Charge, where charging preferences and payment are handled automatically upon plugging in the vehicle [25].

## Risks of Cyber Threats in EV Charging Infrastructure

Unauthorized Access in EV (Electric Vehicle) Charging Infrastructure is an emerging and critical concern as the world shifts toward sustainable transportation. Attackers may target various components within the EV charging ecosystem, such as the charging stations themselves or the backend servers that manage them. Charging stations are increasingly integrated with user-friendly interfaces, like mobile apps and touch screens, to provide real-time updates and manage billing. These interfaces are connected to a complex network that includes payment systems and user profiles, creating various entry points for attackers [26]–[28]. The unauthorized access can lead to theft of personal and payment information, creating a direct financial risk to the customers using the charging stations [29].

The problem of unauthorized access becomes even more complex considering the different communication protocols and standards that are used in EV charging infrastructure. These systems communicate through a variety of means, including cellular networks, Wi-Fi, and RFID technology. The diverse landscape of communication protocols can present a multitude of potential vulnerabilities. An attacker exploiting these weaknesses may gain unauthorized access to crucial components within the charging infrastructure. This not only threatens the security of personal and financial information but also can lead to unauthorized control over charging processes [30]–[32]. One of the immediate consequences of unauthorized access is the potential for the theft of sensitive personal and payment information. For many users, charging stations are linked to credit cards, bank accounts, or other payment

methods. An attacker gaining unauthorized access to this information could engage in fraudulent transactions or sell the information on the dark web. Additionally, personal information like home addresses, phone numbers, and vehicle details could also be at risk, leading to further security concerns for individuals [33].

Unauthorized control over charging processes is another significant aspect of this issue. Attackers with control over the charging systems could manipulate the charging process itself. They may alter charging schedules, change charging rates, or even stop the charging process altogether [34]–[36]. In extreme cases, they might cause physical damage to the vehicle or the charging equipment. The integrity of the charging process is vital not only for the vehicle's functionality but also for the broader electrical grid stability, particularly when dealing with large-scale charging facilities [37]. Data Manipulation within the context of Electric Vehicle (EV) charging infrastructure is a pressing issue that can have varied and severe consequences. The transfer of data between EVs and charging stations involves an intricate exchange of information that governs various aspects such as charging rates, billing, time of charging, and even the synchronization with grid demands [38]–[40]. Attackers who successfully manipulate this data exchange can introduce inaccuracies or malicious alterations, leading to incorrect billing, misinformation, or potential physical harm to both the vehicle and charging hardware [41].

The first and perhaps most immediate concern with data manipulation is the potential for incorrect billing. The charging process's financial aspects are governed by the precise tracking of how much energy is consumed, the time of consumption, and the agreed-upon rates. If an attacker manipulates this data, it could lead to customers being overcharged or undercharged. While undercharging may seem advantageous to the consumer, it could lead to financial losses for charging providers and instability in the pricing models that could indirectly affect all users [42].

Misinformation is another critical consequence of data manipulation in the EV charging infrastructure. By altering the data related to charging rates, times, or availability, attackers could create confusion and operational inefficiencies. Misleading information may result in customers being directed to occupied charging stations or being provided with incorrect details about charging duration. In a broader context, this could disrupt the overall management of energy distribution, leading to grid imbalances and operational inefficiencies in the electricity supply chain [43].

The manipulation of data could also lead to physical harm to both the vehicle and charging hardware. Charging an electric vehicle is a delicate process that requires a specific alignment of voltages, currents, and timing. An attacker altering this data could cause the charging process to operate outside of the safe parameters. This may result in overheating, improper charging, or even physical damage to the battery, charging equipment, or other connected systems. Such damage not only represents a significant financial risk but also poses safety concerns for individuals using or maintaining the charging facilities [44].

Further, the consequences of data manipulation may extend beyond the immediate stakeholders like the vehicle owner or charging station operator. The increasingly interconnected nature of energy systems means that disturbances in the charging processes could have ripple effects on the broader electrical grid. Inaccuracies in the data regarding energy consumption, demand, and supply might lead to imbalances in the grid, causing stability issues and inefficiencies in energy distribution across different parts of the network [45].

Lastly, data manipulation in EV charging infrastructure raises concerns about trust and reliability in this rapidly growing sector. As EVs become more prevalent, the reliance on accurate and secure data exchange between vehicles and charging stations becomes paramount. Manipulation of this data undermines confidence in the system, potentially slowing adoption rates and hindering collaboration between various stakeholders, including vehicle manufacturers, energy providers, and governmental bodies [46]–[48].

The issue of data manipulation, therefore, is not just a technical challenge but has far-reaching implications for the development and success of electric mobility as a whole [49].

Denial of Service (DoS) Attacks on EV charging stations represents a significant threat in the growing landscape of electric mobility, manifesting a distinct form of disruption. A DoS attack is typically characterized by an overwhelming flow of traffic directed at a targeted system, causing it to become inoperable [50]–[52]. In the context of EV charging infrastructure, this means that charging stations can be rendered non-functional, leading to charging delays and a complete disruption of service. The impact of such attacks can be extensive, affecting individual users, service providers, and even the broader transportation and energy systems [53].

For individual users of electric vehicles, a DoS attack on a charging station could lead to significant inconvenience and disruption. If a charging station is rendered inoperable, users may find themselves stranded or delayed, unable to charge their vehicles as needed. In areas where charging infrastructure is still limited, the effects could be even more pronounced, potentially leaving users with few or no alternatives. This could create a sense of unreliability around the use of electric vehicles and deter potential future adoption [54].

From the perspective of service providers operating the charging stations, DoS attacks can have serious financial and operational consequences [55]–[57]. Charging stations that are inoperable due to an attack represent a direct loss of revenue for operators. Moreover, the downtime associated with a DoS attack may require substantial effort to rectify, including potential hardware replacements, software updates, and increased monitoring. Repeated or widespread attacks could erode customer trust and satisfaction, affecting the long-term success of the charging service provider [58].

On a broader scale, DoS attacks on EV charging stations can also have implications for the overall transportation system and energy grid. As the adoption of electric vehicles continues to grow, the availability and reliability of charging infrastructure become integral to the functioning of the transportation network [59]–[61]. A targeted or widespread DoS attack on charging stations could create bottlenecks or disrupt the regular flow of traffic, affecting not only individual vehicle owners but also commercial fleets, public transportation, and emergency services [62]. Furthermore, modern EV charging infrastructure often integrates with the wider energy grid, allowing for intelligent energy management and grid stabilization. A DoS attack could disrupt these integrations, leading to imbalances in the energy grid [63]–[65]. In a scenario where large numbers of electric vehicles are being charged simultaneously during peak demand, a DoS attack on critical charging infrastructure could exacerbate grid instability, with potential consequences for overall energy supply and distribution [66].

Lastly, the threat of DoS attacks on EV charging stations highlights the evolving nature of security concerns in the transportation sector. As technology advances and charging infrastructure becomes increasingly interconnected, new vulnerabilities and attack vectors emerge [67]. DoS attacks symbolize a shift from merely physical threats to a convergence of physical and cyber risks, revealing the multifaceted nature of security in the age of electric mobility [68]–[70]. The impact of such attacks is not confined to the digital domain but permeates the real world, affecting individuals' daily lives, business operations, and the robustness of essential infrastructures [71].

Firmware and Software Attacks on EV charging infrastructure represent a sophisticated and insidious threat to the security and integrity of these systems. The prevalence of outdated or insecure firmware and software within the charging ecosystem can create vulnerabilities that attackers may exploit to gain unauthorized access or even create a persistent presence within the charging system. The implications of such attacks are multifaceted and far-reaching, affecting users, service providers, manufacturers, and the overall development of the electric vehicle sector [72].

Firstly, the exploitation of outdated or insecure firmware and software can lead to unauthorized control over the charging process itself. Attackers may manipulate charging rates, schedules, or even cause physical damage to the vehicle or charging equipment [73]–[75]. The very core functionality of the charging station could be undermined, leading to a loss of trust and confidence among users and posing potential safety hazards. Individual users may find their personal information at risk or experience financial losses through fraudulent billing, stemming from the unauthorized access [76].

Service providers and operators of charging infrastructure stand to face significant operational and financial challenges as a result of firmware and software attacks [77]–[79]. Once an attacker establishes a persistent presence within the system, they may have ongoing access to sensitive information or control over critical functionalities. Addressing this persistent threat could require substantial resources, including regular security audits, updates, and potentially even hardware replacements [80]–[82]. Failure to adequately address these vulnerabilities could result in legal liabilities, reputational damage, and loss of market share [83].

Manufacturers of charging stations and associated equipment are also affected by the threat of firmware and software attacks. They bear a certain responsibility for ensuring the security of their products, particularly in an environment where continuous updates and patches are often necessary to maintain robust defenses against evolving threats [84]. An exploited vulnerability could reflect poorly on a manufacturer's reputation for quality and security, leading to decreased sales and strained relationships with service providers and regulators [85].

In a broader context, the threat of firmware and software attacks on EV charging infrastructure reveals the inherent complexities of securing a rapidly evolving technological landscape. The integration of various hardware components, communication protocols, and software platforms creates a diverse and multifaceted ecosystem. Keeping all elements up-to-date and secure requires coordinated efforts across various stakeholders, including manufacturers, service providers, regulatory bodies, and even end-users [86]–[88]. The persistent nature of some firmware and software attacks also means that traditional security measures may not always be sufficient, demanding new approaches and continuous vigilance [89].

Finally, the issue of firmware and software attacks on EV charging infrastructure can have implications for the larger push toward sustainable transportation. The success of electric vehicles is partly dependent on the availability and reliability of charging infrastructure. Security threats, particularly those that can create a persistent and insidious presence within the system, may undermine public confidence and slow the adoption rate of electric vehicles. This, in turn, could hinder the global efforts to reduce emissions and transition towards cleaner, more sustainable transportation options [90].

Physical Tampering with charging stations represents a particularly tangible threat in the EV charging infrastructure. Unlike cyber threats that target software or digital interfaces, physical tampering involves the direct manipulation of the hardware or physical components of the charging station. Attackers may alter functionality, install malicious devices, or create hidden vulnerabilities that can be exploited later. The consequences of physical tampering are extensive, affecting individual users, service providers, safety, and the broader trust in electric vehicle technology. For individual users, tampering may lead to incorrect billing, damage to the vehicle, or exposure to personal information. Service providers face financial losses, legal liabilities, and a decline in user trust. Moreover, physical tampering may pose safety risks as unauthorized alterations to the hardware could lead to malfunctions, overheating, or other hazardous conditions [91]–[93]. Overall, the threat of physical tampering underscores the importance of securing not only the digital aspects of EV charging infrastructure but also the physical components, encompassing a comprehensive approach to security [94]–[96]. EV Ecosystem Integration Risks highlight another complex and multifaceted challenge within the field of electric mobility. As electric

vehicles and their charging infrastructure become more intertwined with other systems, such as energy management or smart grid technologies, new vulnerabilities emerge that can expose broader infrastructure to risks. Integration with energy management systems often involves real-time data exchange, coordination, and control to optimize energy consumption, align with grid demands, and even support renewable energy integration. While these connections offer significant benefits in terms of efficiency and sustainability, they also create potential points of entry for attackers. If not properly secured, these integrations can be exploited to gain unauthorized access to not just the charging station but also the connected energy management or smart grid systems. This can lead to cascading failures, disruption of energy supply, or manipulation of critical energy management functions [97].

The very interconnectedness that drives efficiency and innovation in the EV ecosystem also amplifies the potential impact of security breaches, necessitating a holistic and robust approach to risk management [93], [98], [99]. The integration risks further emphasize the importance of cross-sector collaboration, shared security standards, and vigilance in the continuous monitoring of potential threats. Together, both physical tampering and integration risks underscore the diverse and evolving nature of security challenges in the realm of electric vehicle charging infrastructure, revealing the need for comprehensive, multi-layered strategies to safeguard these essential components of modern transportation [100].

## Developing Robust Security Protocols

Risk Assessment and Comprehensive Security Measures form a crucial aspect of safeguarding EV charging infrastructure from various threats. These measures, comprising a blend of methodologies and technologies, serve as a structured approach to identify, assess, and mitigate risks to both the physical and digital components of the charging ecosystem [101].

The initial phase involves a thorough assessment of risks, where potential vulnerabilities, threats, and their possible impact are identified and evaluated. This encompasses understanding the hardware, software, integration points, user interactions, and even the geographical location of charging stations. Assessing the risks not only provides insight into what could go wrong but also helps prioritize where efforts and resources should be focused. This process needs to be dynamic and ongoing, reflecting the evolving nature of technology, regulations, and potential attack vectors [102].

Continuous monitoring stands as a pivotal part of the security measures, ensuring real-time or near-real-time awareness of the system's state. This includes monitoring the performance, user activities, network traffic, and any anomalies that might indicate an unauthorized access or potential threat [103]–[105]. It's an essential layer in early detection, helping to spot issues before they escalate into significant breaches or malfunctions [106].

Access control, strong authentication, and authorization mechanisms act as gatekeepers to the system. By controlling who has access to various parts of the charging infrastructure and under what conditions, these measures reduce the risk of unauthorized intrusion [107]–[109]. Implementing robust authentication methods, such as multi-factor authentication, ensures that only authorized personnel can make changes or access sensitive information. This is a critical defense line, particularly when managing a distributed network of charging stations that may be accessible to a wide array of users [110]. Implementation of firewalls, intrusion detection systems, and network segmentation adds further layers of protection. Firewalls act as barriers, controlling the traffic between different parts of the network and blocking potential malicious activities. Intrusion detection systems actively look for signs of attempts to breach the system, providing alerts and insights into potential threats. Network segmentation involves dividing the network into smaller, isolated segments, so that if one part is compromised, the breach doesn’t automatically spread to the entire system.

Collectively, these measures form a comprehensive security strategy, weaving together various tools, practices, and technologies into a cohesive defense against a wide array of potential threats. They illustrate the multifaceted nature of security in the context of EV charging infrastructure, reflecting a recognition that protecting these critical systems requires more than just isolated solutions or ad-hoc responses. Rather, it necessitates an integrated, proactive approach, where security is embedded into the design, operation, and ongoing management of the charging infrastructure [111].

Data Protection within the EV charging infrastructure is a vital aspect that encompasses various strategies, technologies, and compliances to secure sensitive information. As the charging infrastructure involves the handling of user identification, payment details, vehicle specifications, and even real-time communication with other systems, ensuring the confidentiality and integrity of this data becomes paramount [112].

End-to-end encryption plays a crucial role in safeguarding data, both in transit and at rest. When data is encrypted, it is transformed into a format that can only be read by those possessing the corresponding decryption key [113]–[115]. Ensuring encryption for data in transit means that information sent between the vehicle, charging station, and backend servers is protected from interception or eavesdropping. Likewise, encrypting data at rest ensures that information stored on servers, databases, or within the charging station itself is secure from unauthorized access [116]. This twofold approach ensures that data is shielded at all stages, from its creation and transmission to storage and eventual disposal [117].

Mechanisms to validate data integrity are equally essential, ensuring that the information has not been altered or tampered with during its lifecycle. This could involve cryptographic methods to verify the authenticity of data or employing integrity checks that alert to any unexpected changes. Protecting the integrity of data not only safeguards against malicious alterations but also ensures that the data remains accurate and reliable, supporting the correct functioning of the charging infrastructure and associated systems.

Compliance with relevant standards and regulations adds another dimension to data protection within the EV charging infrastructure. Standards like ISO/IEC 27001 provide a framework for managing and safeguarding information, guiding organizations in implementing robust information security management systems (ISMS). Adherence to the National Institute of Standards and Technology (NIST) guidelines offers further benchmarks and best practices in cybersecurity. Complying with regulations such as the General Data Protection Regulation (GDPR) ensures that the handling of personal data aligns with legal requirements, including consent, transparency, and the right to access or erase personal information [118].

Together, these aspects of data protection form a comprehensive approach that recognizes the multifaceted nature of information security within the EV charging infrastructure. By employing encryption, ensuring integrity, and aligning with international standards and regulations, the charging infrastructure demonstrates a commitment to safeguarding user privacy, financial transactions, operational data, and the broader trust in electric vehicle technology. These measures reflect an understanding that data is not just a collection of bits and bytes but a valuable asset that underpins the functionality, reliability, and success of the entire electric vehicle ecosystem. Ensuring robust data protection is therefore not just a technical challenge but a fundamental part of building confidence, adherence to the rule of law, and the ongoing growth and sustainability of electric mobility.

Regular Maintenance and Updates form a fundamental layer of defense in the security posture of EV charging infrastructure. This proactive approach focuses on continuously updating software and firmware to patch known vulnerabilities, and it's complemented by regular security assessments and audits conducted by independent third parties. These practices serve to ensure the integrity, availability, and robustness of the charging

systems, while also adapting to the constantly evolving landscape of threats and vulnerabilities.

The continuous updating of software and firmware represents an essential practice in minimizing the window of opportunity for attackers to exploit known vulnerabilities. As soon as a vulnerability is discovered, manufacturers and developers often release patches or updates to fix the issue. If these updates are not applied promptly, the vulnerability remains open, and attackers may exploit it to gain unauthorized access or control. Continuous updating ensures that the charging infrastructure is armed with the latest defenses, reflecting an agile response to new threats. This is particularly vital in the context of EV charging, where the combination of physical hardware, networking protocols, and user interactions creates a complex environment that can harbor multiple potential weak points [119].

Regular security assessments and audits by independent third parties add another critical dimension to the maintenance and updating process. Independent assessments offer an unbiased evaluation of the security measures, identifying potential weaknesses or oversights that may not be apparent to the internal team. These assessments can take various forms, including vulnerability scanning, penetration testing, or comprehensive security audits. By probing the system from an outsider's perspective, these assessments mimic potential attack methods, uncovering hidden vulnerabilities, and providing insights into how the system might withstand real-world threats. The independence of the third-party assessors ensures an objective view, free from potential conflicts of interest or internal biases [120].

The combination of continuous updates and independent assessments creates a dynamic and responsive security model. This approach recognizes that security is not a one-time task but an ongoing process, adapting and evolving in tandem with technological advancements, changes in user behavior, and the emergence of new threats. By keeping software and firmware up-to-date and subjecting the system to regular external scrutiny, the EV charging infrastructure maintains a proactive stance, anticipating potential risks rather than merely reacting to breaches once they occur [121]–[123]. Furthermore, these practices contribute to building trust and confidence among users, service providers, and regulators. Knowing that the charging infrastructure is actively maintained, regularly assessed, and aligned with current best practices offers assurance that the system is resilient and that the providers are committed to safeguarding user information, financial transactions, and the overall integrity of the charging process. Regular maintenance and updates, therefore, are not merely technical necessities but integral components of responsible stewardship, transparency, and accountability within the EV charging ecosystem.

Physical Security and Incident Response are two interconnected aspects that play a vital role in securing the EV charging infrastructure. Both elements recognize that security is not solely a digital or technological concern but extends to the physical environment and involves preparation for potential incidents.

Physical Security measures include the implementation of locks, surveillance, and alarms to protect the charging stations and associated hardware. Locks and barriers restrict unauthorized access to sensitive components, such as internal electronics or connectors, which might be tampered with or vandalized. Surveillance systems, such as cameras, provide monitoring and oversight, acting as both a deterrent to potential attackers and a means of collecting evidence if an incident occurs. Alarms add an additional layer, alerting authorities or security personnel to potential breaches or suspicious activities. These measures collectively offer a tangible defense, safeguarding not only the hardware but also the integrity of the data, user interactions, and overall functionality of the charging system. Physical security also supports the broader perception of safety and trust, reinforcing the user's confidence in the infrastructure and the associated services [124].

Developing a well-defined Incident Response Plan complements the physical security measures by ensuring that the organization is prepared to act swiftly if a security incident occurs. An incident response plan outlines the steps to be taken, the roles and responsibilities, communication protocols, and recovery measures to be implemented in the event of a breach, failure, or other security incidents. This plan is not just a reactive measure but involves proactive preparation, training, and regular drills to ensure that all stakeholders are aware of their roles and that the response can be executed efficiently. By having a well-defined and practiced plan, the time between detecting an incident and initiating a response can be minimized, reducing the potential impact, containing the breach, and accelerating recovery. This includes coordinating with law enforcement, regulatory bodies, or other third parties as needed, ensuring that the response aligns with legal and regulatory requirements.

The synergy between physical security and incident response reflects a comprehensive understanding of security in the EV charging context. It recognizes that protecting the charging infrastructure involves more than just digital firewalls or encryption but extends to the physical environment and includes a readiness to respond to incidents with agility and coordination. This approach underscores the multifaceted nature of security, encompassing technological measures, human factors, legal considerations, and the continuous adaptation to an ever-changing threat landscape [125]–[127]. By implementing robust physical security measures and crafting a well-defined incident response plan, the EV charging infrastructure demonstrates a commitment to resilience, accountability, and the ongoing effort to safeguard this critical aspect of modern transportation and energy management.

## Conclusion

The unauthorized access to charging stations or backend servers is one of the significant risks within the electric vehicle (EV) charging infrastructure. This unauthorized access can lead to multiple issues, including the theft of personal and payment information. Since many charging stations require user identification and payment details, unauthorized access can expose sensitive data to malicious actors. Additionally, gaining unauthorized control over charging processes can lead to unauthorized charging of vehicles, impacting not only the vehicle owner but also the integrity and trustworthiness of the charging infrastructure itself.

Data manipulation is another severe risk in the EV charging infrastructure. Attackers might alter or tamper with the data transferred between EVs and charging stations, leading to various problems. Incorrect billing, for instance, can result from manipulated data, leading to financial discrepancies. Misinformation about charging statuses can create confusion for both drivers and operators of charging stations. In extreme cases, manipulating data can lead to potential physical harm to the vehicle and charging hardware, as incorrect data might cause overcharging or other technical issues.

Denial of Service (DoS) attacks is a prominent threat in many interconnected systems, including the EV charging infrastructure. By overwhelming charging stations with traffic, attackers can render them inoperable. The impact of such an attack goes beyond mere inconvenience, as charging delays can disrupt daily schedules and transportation plans. In densely populated urban areas where charging stations are heavily used, a successful DoS attack can significantly disrupt the service and availability of EV charging, affecting many users simultaneously.

Firmware and software attacks present risks stemming from outdated or insecure firmware and software within the charging system. Attackers can exploit known vulnerabilities to create a persistent presence within the charging infrastructure. Once inside, they can carry out various malicious activities, such as altering charging processes or collecting sensitive information. This type of attack may be particularly insidious, as it can be challenging to detect and may remain active for an extended period, continually compromising the security and integrity of the EV charging network [128]–[130]. Physical tampering and EV ecosystem integration risks further complicate

the cybersecurity landscape for EV charging infrastructure. Attackers may physically alter charging stations or install malicious devices to gain unauthorized access or disrupt functionality. Physical tampering can be particularly challenging to prevent and detect, as it requires physical security measures in addition to cybersecurity protocols. The integration of EV charging with other systems, such as energy management or smart grids, also introduces broader infrastructure risks. If these integrations are not properly secured, vulnerabilities in the charging infrastructure can lead to more widespread impacts, potentially affecting the stability and security of the entire energy system.

Robust security protocols necessitate the thorough understanding and management of potential risks. This starts with a comprehensive risk assessment, where organizations identify, analyze, and evaluate the possible security threats. In developing risk management strategies, companies must prioritize threats and decide on the most suitable mitigation techniques. The process doesn't end at the implementation stage, though. Continuous monitoring of the risks is vital, coupled with periodic reviews that help adapt and modify the strategies as new risks emerge or existing ones evolve. This dynamism in risk management keeps the security measures aligned with the ever-changing threat landscape.

Access control and authentication form a core part of developing robust security protocols. Implementing strong authentication and authorization mechanisms ensures that only authorized users have access to different levels of the infrastructure, thus keeping sensitive information away from unauthorized hands. Alongside this, data encryption and integrity are paramount in safeguarding the data. End-to-end encryption must be in place for data both in transit and at rest, ensuring complete privacy and security of information. Additionally, mechanisms to validate data integrity confirm that the information has not been altered, guaranteeing its authenticity and reliability.

Network security is essential in limiting potential attack surfaces. This involves the implementation of firewalls, intrusion detection systems, and network segmentation, which together act as barriers against unauthorized access. Continuous updating of software and firmware is also integral, as it patches known vulnerabilities, keeping the systems secure against exploits. Physical security, though often overlooked, is a vital aspect. Implementing locks, surveillance, and alarms prevents physical tampering with the systems, adding an additional layer of security that complements the digital measures [131], [132]. Adhering to relevant standards and regulations, such as ISO/IEC 27001, NIST, GDPR, etc., ensures that the implemented security measures meet the globally recognized best practices. It also aids in maintaining data privacy and enhances the trust of stakeholders. Concurrently, educating all stakeholders about potential risks and best practices through security awareness and training creates a human firewall against threats. Developing a well-defined incident response plan ensures that, should a security incident occur, the appropriate steps are taken quickly and efficiently, minimizing potential damage.

Collaboration with industry stakeholders such as automakers, charging equipment manufacturers, utility providers, and others promotes shared knowledge and the development of collective defense strategies. Such cooperative efforts can lead to the creation of unified standards and more effective, industry-wide security measures. Regular third-party security assessments and audits provide an unbiased evaluation of the implemented security protocols. By having an independent third party review the measures, organizations can uncover overlooked vulnerabilities and gain insights into areas for improvement, leading to more robust and resilient security mechanisms.

## References

[1] J. Pisarov L. and G. Mester, “The use of autonomous vehicles in transportation,” *Tehnika*, vol. 76, no. 2, pp. 171–177, 2021.

[2] P. Czech, "Autonomous vehicles: basic issues," *Sci. J. Sil. Univ. Technol. Ser. Transp.*, vol. 100, pp. 15–22, Sep. 2018.
[3] Y. Ma, Z. Wang, H. Yang, and L. Yang, "Artificial intelligence applications in the development of autonomous vehicles: a survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 2, pp. 315–329, Mar. 2020.
[4] S. Kato *et al.*, "Autoware on Board: Enabling Autonomous Vehicles with Embedded Systems," in *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*, 2018, pp. 287–296.
[5] J. L. F. Pereira and R. J. F. Rossetti, "An integrated architecture for autonomous vehicles simulation," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, Trento, Italy, 2012, pp. 286–292.
[6] V. Ilkova and A. Ilka, "Legal aspects of autonomous vehicles — An overview," in *2017 21st International Conference on Process Control (PC)*, Strbske Pleso, Slovakia, 2017, pp. 428–433.
[7] V. S. R. Kosuru and A. K. Venkitaraman, "CONCEPTUAL DESIGN PHASE OF FMEA PROCESS FOR AUTOMOTIVE ELECTRONIC CONTROL UNITS," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 9, pp. 1474–1480, 2022.
[8] T. G. R. Reid *et al.*, "Localization Requirements for Autonomous Vehicles," *arXiv [cs.RO]*, 03-Jun-2019.
[9] F. M. Favarò, N. Nader, S. O. Eurich, M. Tripp, and N. Varadaraju, "Examining accident reports involving autonomous vehicles in California," *PLoS One*, vol. 12, no. 9, p. e0184952, Sep. 2017.
[10] Committee on Autonomous Vehicles in Support of Naval Operations, Naval Studies Board, Division on Engineering and Physical Sciences, National Research Council, and National Academy of Sciences, *Autonomous vehicles in support of naval operations*. Washington, D.C., DC: National Academies Press, 2005.
[11] M. Azeroual, Y. Boujoudar, A. Aljarbouh, H. El Moussaoui, and H. El Markhi, "A multi-agent-based for fault location in distribution networks with wind power generator," *Wind Engineering*, vol. 46, no. 3, pp. 700–711, 2022.
[12] V. S. R. Kosuru and A. K. Venkitaraman, "Evaluation of Safety Cases in The Domain of Automotive Engineering," *International Journal of Innovative Science and Research Technology*, vol. 7, no. 9, pp. 493–497, 2022.
[13] D. J. Yeong, G. Velasco-Hernandez, J. Barry, and J. Walsh, "Sensor and Sensor Fusion Technology in Autonomous Vehicles: A Review," *Sensors* , vol. 21, no. 6, Mar. 2021.
[14] S. Shah, D. Dey, C. Lovett, and A. Kapoor, "AirSim: High-Fidelity Visual and Physical Simulation for Autonomous Vehicles," in *Field and Service Robotics*, 2018, pp. 621–635.
[15] D. J. Glancy, "Privacy in autonomous vehicles," *Santa Clara Law Rev.*, 2012.
[16] A. Aljarbouh, "Accelerated simulation of hybrid systems: method combining static analysis and run-time execution analysis." Rennes 1, 2017.
[17] S. Jahandari and D. Materassi, "Analysis and compensation of asynchronous stock time series," 2017, pp. 1085–1090.
[18] G. E. Marchant and R. A. Lindor, "The coming collision between autonomous vehicles and the liability system," *Santa Clara Law Rev.*, 2012.
[19] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, and M. Hafeez, "A Survey of Autonomous Vehicles: Enabling Communication Technologies and Challenges," *Sensors* , vol. 21, no. 3, Jan. 2021.
[20] W. Wachenfeld and H. Winner, "The Release of Autonomous Vehicles," in *Autonomous Driving: Technical, Legal and Social Aspects*, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 425–449.
[21] I. Pozharkova, A. Aljarbouh, S. H. Azizam, A. P. Mohamed, F. Rabbi, and R. Tsarev, "A simulation modeling method for cooling building structures by fire robots," 2022, pp. 504–511.
[22] W. Schwarting, A. Pierson, J. Alonso-Mora, S. Karaman, and D. Rus, "Social behavior for autonomous vehicles," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 116, no. 50, pp. 24972–24978, Dec. 2019.
[23] L. Li, W.-L. Huang, Y. Liu, N.-N. Zheng, and F.-Y. Wang, "Intelligence Testing for Autonomous Vehicles: A New Approach," *IEEE Transactions on Intelligent Vehicles*, vol. 1, no. 2, pp. 158–166, Jun. 2016.

[24] Y. Wiseman, "Autonomous Vehicles," in *Research Anthology on Cross-Disciplinary Designs and Applications of Automation*, IGI Global, 2022, pp. 878–889.
[25] A. K. Venkitaraman and V. S. R. Kosuru, "A review on autonomous electric vehicle communication networks-progress, methods and challenges," *World Journal of Advanced Research and Reviews*, vol. 16, no. 3, pp. 013–024, 2022.
[26] J. C. Gerdes and S. M. Thornton, "Implementable Ethics for Autonomous Vehicles," in *Autonomes Fahren: Technische, rechtliche und gesellschaftliche Aspekte*, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 87–102.
[27] M. V. Rajasekhar and A. K. Jaswal, "Autonomous vehicles: The future of automobiles," in *2015 IEEE International Transportation Electrification Conference (ITEC)*, 2015, pp. 1–6.
[28] S. A. Bagloee, M. Tavana, M. Asadi, and T. Oliver, "Autonomous vehicles: challenges, opportunities, and future implications for transportation policies," *Journal of Modern Transportation*, vol. 24, no. 4, pp. 284–303, Dec. 2016.
[29] A. Aljarbouh, "Accelerated Simulation of Hybrid Systems: Method combining static analysis and run-time execution analysis.(Simulation Accélérée des Systèmes Hybrides: méthode combinant analyse statique et analyse à l'exécution)." University of Rennes 1, France, 2017.
[30] J. Meyer, H. Becker, P. M. Bösch, and K. W. Axhausen, "Autonomous vehicles: The next jump in accessibilities?," *Research in Transportation Economics*, vol. 62, pp. 80–91, Jun. 2017.
[31] P. A. Hancock, I. Nourbakhsh, and J. Stewart, "On the future of transportation in an era of automated and autonomous vehicles," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 116, no. 16, pp. 7684–7691, Apr. 2019.
[32] S. Campbell *et al.*, "Sensor Technology in Autonomous Vehicles : A review," in *2018 29th Irish Signals and Systems Conference (ISSC)*, 2018, pp. 1–4.
[33] V. S. R. Kosuru, A. K. Venkitaraman, V. D. Chaudhari, N. Garg, A. Rao, and A. Deepak, "Automatic Identification of Vehicles in Traffic using Smart Cameras," 2022, pp. 1009–1014.
[34] S. D. Pendleton *et al.*, "Perception, Planning, Control, and Coordination for Autonomous Vehicles," *Machines*, vol. 5, no. 1, p. 6, Feb. 2017.
[35] J.-F. Bonnefon, A. Shariff, and I. Rahwan, "The social dilemma of autonomous vehicles," *Science*, vol. 352, no. 6293, pp. 1573–1576, Jun. 2016.
[36] W. Huang, K. Wang, Y. Lv, and F. Zhu, "Autonomous vehicles testing methods review," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, 2016, pp. 163–168.
[37] R. Jabeur, Y. Boujoudar, M. Azeroual, A. Aljarbouh, and N. Ouaaline, "Microgrid energy management system for smart home using multi-agent system," *Int. J. Elect. Computer Syst. Eng.*, vol. 12, no. 2, pp. 1153–1160, 2022.
[38] J. Wang, L. Zhang, Y. Huang, and J. Zhao, "Safety of Autonomous Vehicles," *Journal of Advanced Transportation*, vol. 2020, Oct. 2020.
[39] S. Kato, E. Takeuchi, Y. Ishiguro, Y. Ninomiya, K. Takeda, and T. Hamada, "An Open Approach to Autonomous Vehicles," *IEEE Micro*, vol. 35, no. 6, pp. 60–68, Nov. 2015.
[40] W. Schwarting and J. Alonso-Mora, "Planning and decision-making for autonomous vehicles," *, and Autonomous …*, 2018.
[41] I. Haq *et al.*, "Machine Vision Approach for Diagnosing Tuberculosis (TB) Based on Computerized Tomography (CT) Scan Images," *Symmetry* , vol. 14, no. 10, p. 1997, 2022.
[42] A. Aljarbouh, "Selection of the optimal set of versions of N-version software using the ant colony optimization," 2021, vol. 2094, p. 032026.
[43] V. S. R. Kosuru and A. K. Venkitaraman, "Preventing the False Negatives of Vehicle Object Detection in Autonomous Driving Control Using Clear Object Filter Technique," 2022, pp. 1–6.
[44] A. Aljarbouh, Y. Zeng, A. Duracz, B. Caillaud, and W. Taha, "Chattering-free simulation for hybrid dynamical systems semantics and prototype implementation," 2016, pp. 412–422.
[45] A. Aljarbouh, "Non-standard zeno-free simulation semantics for hybrid dynamical systems," 2019, pp. 16–31.

[46] M. Martínez-Díaz and F. Soriguera, "Autonomous vehicles: theoretical and practical challenges," *Transportation Research Procedia*, vol. 33, pp. 275–282, Jan. 2018.
[47] F. Duarte and C. Ratti, "The Impact of Autonomous Vehicles on Cities: A Review," *Journal of Urban Technology*, vol. 25, no. 4, pp. 3–18, Oct. 2018.
[48] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations," *Transp. Res. Part A: Policy Pract.*, vol. 77, pp. 167–181, Jul. 2015.
[49] A. Aljarbouh and B. Caillaud, "Chattering-free simulation of hybrid dynamical systems with the functional mock-up interface 2.0," 2016, vol. 124, pp. 95–105.
[50] B. Friedrich, "The Effect of Autonomous Vehicles on Traffic," in *Autonomous Driving: Technical, Legal and Social Aspects*, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 317–334.
[51] D. Rojas Rueda and M. J. Nieuwenhuijsen, "Autonomous vehicles and public health," *Annu. Rev. Public Health*, 2020.
[52] J. Janai, F. Güney, A. Behl, and A. Geiger, "Computer Vision for Autonomous Vehicles: Problems, Datasets and State of the Art," *Foundations and Trends® in Computer Graphics and Vision*, vol. 12, no. 1–3, pp. 1–308, 2020.
[53] A. K. Venkitaraman and V. S. R. Kosuru, "Electric Vehicle Charging Network Optimization using Multi-Variable Linear Programming and Bayesian Principles," 2022, pp. 1–5.
[54] I. Trifonov, A. Aljarbouh, and A. Beketaeva, "Evaluating the effectiveness of turbulence models in the simulation of two-phases combustion," *International Review on Modelling and Simulations*, vol. 14, no. 4, pp. 291–300, 2021.
[55] C. Wu, A. M. Bayen, and A. Mehta, "Stabilizing Traffic with Autonomous Vehicles," in *2018 IEEE International Conference on Robotics and Automation (ICRA)*, 2018, pp. 6012–6018.
[56] C. Zhao, L. Li, X. Pei, Z. Li, F.-Y. Wang, and X. Wu, "A comparative study of state-of-the-art driving strategies for autonomous vehicles," *Accid. Anal. Prev.*, vol. 150, p. 105937, Feb. 2021.
[57] A. Broggi, P. Medici, P. Zani, and A. Coati, "Autonomous vehicles control in the VisLab intercontinental autonomous challenge," *Annu. Rev. Control*, 2012.
[58] A. Aljarbouh, M. Fayaz, and M. S. Qureshi, "Non-Standard Analysis for Regularization of Geometric-Zeno Behaviour in Hybrid Systems," *Systems*, vol. 8, no. 2, p. 15, 2020.
[59] A. Martinho, N. Herber, M. Kroesen, and C. Chorus, "Ethical issues in focus by the autonomous vehicles industry," *Transp. Rev.*, 2021.
[60] W. Nelson, "Continuous-curvature paths for autonomous vehicles," in *Proceedings, 1989 International Conference on Robotics and Automation*, 1989, pp. 1260–1264 vol.3.
[61] H.-P. Schöner, "Simulation in development and testing of autonomous vehicles," in *18. Internationales Stuttgarter Symposium*, 2018, pp. 1083–1095.
[62] A. Aljarbouh, A. Duracz, Y. Zeng, B. Caillaud, and W. Taha, "Chattering-free simulation for hybrid dynamical systems," *HAL*, vol. 2016, 2016.
[63] P. Davidson and A. Spinoulas, "Autonomous vehicles: what could this mean for the future of transport," *Australian Institute of Traffic*, 2015.
[64] V. V. Dixit, S. Chand, and D. J. Nair, "Autonomous Vehicles: Disengagements, Accidents and Reaction Times," *PLoS One*, vol. 11, no. 12, p. e0168054, Dec. 2016.
[65] A. Reschka, "Safety Concept for Autonomous Vehicles," in *Autonomous Driving: Technical, Legal and Social Aspects*, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 473–496.
[66] V. S. R. Kosuru and A. K. Venkitaraman, "Developing a deep Q-learning and neural network framework for trajectory planning," *European Journal of Engineering and Technology Research*, vol. 7, no. 6, pp. 148–157, 2022.
[67] S. Jahandari, A. Kalhor, and B. N. Araabi, "Order determination and transfer function estimation of linear mimo systems: application to environmental modeling," *Environmental Modeling and Software*, 2016.
[68] M. Kuderer, S. Gulati, and W. Burgard, "Learning driving styles for autonomous vehicles from demonstration," in *2015 IEEE International Conference on Robotics and Automation (ICRA)*, 2015, pp. 2641–2646.

[69] F. Favarò, S. Eurich, and N. Nader, "Autonomous vehicles' disengagements: Trends, triggers, and regulatory limitations," *Accid. Anal. Prev.*, vol. 110, pp. 136–148, Jan. 2018.
[70] R. Krueger, T. H. Rashidi, and J. M. Rose, "Preferences for shared autonomous vehicles," *Transp. Res. Part C: Emerg. Technol.*, 2016.
[71] J. A. Albarakati *et al.*, "Multi-Agent-Based Fault Location and Cyber-Attack Detection in Distribution System," *Energies*, vol. 16, no. 1, p. 224, 2022.
[72] V. S. Rahul, "Kosuru; Venkitaraman, AK Integrated framework to identify fault in human-machine interaction systems," *Int. Res. J. Mod. Eng. Technol. Sci*, 2022.
[73] A. Rasouli and J. K. Tsotsos, "Autonomous Vehicles That Interact With Pedestrians: A Survey of Theory and Practice," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 900–918, Mar. 2020.
[74] P. Kopelias, E. Demiridi, and K. Vogiatzis, "Connected & autonomous vehicles–Environmental impacts–A review," *Sci. Total Environ.*, 2020.
[75] P. A. Hancock, "Some pitfalls in the promises of automated and autonomous vehicles," *Ergonomics*, vol. 62, no. 4, pp. 479–495, Apr. 2019.
[76] A. Aljarbouh and B. Caillaud, "Robust simulation for hybrid systems: chattering path avoidance," *arXiv preprint arXiv:1512.07818*, 2015.
[77] W. Enang and C. Bannister, "Modelling and control of hybrid electric vehicles (A comprehensive review)," *Renewable Sustainable Energy Rev.*, vol. 74, pp. 1210–1239, Jul. 2017.
[78] J. Y. Yong, V. K. Ramachandaramurthy, K. M. Tan, and N. Mithulananthan, "A review on the state-of-the-art technologies of electric vehicle, its impacts and prospects," *Renewable Sustainable Energy Rev.*, vol. 49, pp. 365–385, Sep. 2015.
[79] A. König, L. Nicoletti, D. Schröder, and S. Wolff, "An overview of parameter and cost for battery electric vehicles," *World Electric Vehicle*, 2021.
[80] F. Douma and S. A. Palodichuk, "Criminal liability issues created by autonomous vehicles," *Santa Clara Law Rev.*, 2012.
[81] H. A. Ignatious and M. Khan, "An overview of sensors in Autonomous Vehicles," *Procedia Comput. Sci.*, 2022.
[82] S. Royo and M. Ballesta-Garcia, "An overview of lidar imaging systems for autonomous vehicles," *NATO Adv. Sci. Inst. Ser. E Appl. Sci.*, 2019.
[83] A. Aljarbouh, M. S. Ahmed, M. Vaquera, and B. D. Dirting, "Intellectualization of information processing systems for monitoring complex objects and systems," *Современные инновации, системы и технологии*, vol. 2, no. 1, pp. 9–17, 2022.
[84] S. Jahandari, "Graph-theoretic Identification of Dynamic Networks." University of Minnesota, 2022.
[85] A. Aljarbouh and B. Caillaud, "On the regularization of chattering executions in real time simulation of hybrid systems," 2015, p. 49.
[86] S. Pettigrew, C. Worrall, Z. Talati, and L. Fritschi, "Dimensions of attitudes to autonomous vehicles," *Urban, Planning and*, 2019.
[87] M. Clamann, M. Aubert, and M. L. Cummings, "Evaluation of vehicle-to-pedestrian communication displays for autonomous vehicles," trid.trb.org, 17–02119, 2017.
[88] A. Nunes, B. Reimer, and J. F. Coughlin, "People must retain control of autonomous vehicles," pp. 169–171, Apr. 2018.
[89] Y. Liang, "Structural Vibration Signal Denoising Using Stacking Ensemble of Hybrid CNN-RNN. Advances in Artificial Intelligence and Machine Learning. 2022; 3 (2): 65." 2006.
[90] A. Aljarbouh *et al.*, "Application of the K-medians Clustering Algorithm for Test Analysis in E-learning," in *Proceedings of the Computational Methods in Systems and Software*, Springer, 2022, pp. 249–256.
[91] A. Talebpour and H. S. Mahmassani, "Influence of connected and autonomous vehicles on traffic flow stability and throughput," *Transp. Res. Part C: Emerg. Technol.*, vol. 71, pp. 143–163, Oct. 2016.
[92] M. Likhachev and D. Ferguson, "Planning Long Dynamically Feasible Maneuvers for Autonomous Vehicles," *Int. J. Rob. Res.*, vol. 28, no. 8, pp. 933–945, Aug. 2009.
[93] J. Lee, D. Lee, Y. Park, S. Lee, and T. Ha, "Autonomous vehicles can be shared, but a feeling of ownership is important: Examination of the influential factors for intention to use autonomous vehicles," *Transp. Res. Part C: Emerg. Technol.*, vol. 107, pp. 411–422, Oct. 2019.

[94] J. Lu, Z. Chen, Z. Ma, F. Pan, L. A. Curtiss, and K. Amine, "Corrigendum: The role of nanotechnology in the development of battery materials for electric vehicles," *Nat. Nanotechnol.*, vol. 12, no. 1, p. 90, Jan. 2017.
[95] E. J. Cairns and P. Albertus, "Batteries for electric and hybrid-electric vehicles," *Annu. Rev. Chem. Biomol. Eng.*, vol. 1, pp. 299–320, 2010.
[96] D. B. Richardson, "Electric vehicles and the electric grid: A review of modeling approaches, Impacts, and renewable energy integration," *Renewable Sustainable Energy Rev.*, 2013.
[97] A. Chavez, D. Koutentakis, Y. Liang, S. Tripathy, and J. Yun, "Identify statistical similarities and differences between the deadliest cancer types through gene expression," *arXiv preprint arXiv:1903.07847*, 2019.
[98] L. M. Hulse, H. Xie, and E. R. Galea, "Perceptions of autonomous vehicles: Relationships with road users, risk, gender and age," *Saf. Sci.*, vol. 102, pp. 1–13, Feb. 2018.
[99] Y. Wiseman and I. Grinberg, "Autonomous vehicles should not collide carelessly," *Advanced Science and Technology Letters*. u.cs.biu.ac.il, 2016.
[100] A. J. Albarakati *et al.*, "Microgrid energy management and monitoring systems: A comprehensive review," *Frontiers in Energy Research*, vol. 10, p. 1097858, 2022.
[101] R. Sell, A. Rassõlkin, R. Wang, and T. Otto, "Integration of autonomous vehicles and Industry 4.0," *Proc. Eston. Acad. Sci.*, vol. 68, no. 4, p. 389, 2019.
[102] A. J. Albarakati *et al.*, "Real-time energy management for DC microgrids using artificial intelligence," *Energies*, vol. 14, no. 17, p. 5307, 2021.
[103] H. S. Das, M. M. Rahman, S. Li, and C. W. Tan, "Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review," *Renewable Sustainable Energy Rev.*, vol. 120, p. 109618, Mar. 2020.
[104] H. Tu, H. Feng, S. Srdic, and S. Lukic, "Extreme Fast Charging of Electric Vehicles: A Technology Overview," *IEEE Transactions on Transportation Electrification*, vol. 5, no. 4, pp. 861–878, Dec. 2019.
[105] J. Kim, J. Oh, and H. Lee, "Review on battery thermal management system for electric vehicles," *Appl. Therm. Eng.*, 2019.
[106] V. Rutskiy *et al.*, "Prospects for the Use of Artificial Intelligence to Combat Fraud in Bank Payments," in *Proceedings of the Computational Methods in Systems and Software*, Springer, 2022, pp. 959–971.
[107] V. Timmers and P. A. J. Achten, "Non-exhaust PM emissions from electric vehicles," *Atmos. Environ.*, 2016.
[108] J. De Santiago, H. Bernhoff, and B. Ekergård, "Electrical motor drivelines in commercial all-electric vehicles: A review," *IEEE Transactions*, 2011.
[109] S. Pelletier, O. Jabali, and G. Laporte, "50th anniversary invited article—goods distribution with electric vehicles: review and research perspectives," *Transportation science*, 2016.
[110] S. Jahandari and D. Materassi, "Sufficient and necessary graphical conditions for miso identification in networks with observational data," *IEEE Trans. Automat. Contr.*, vol. 67, no. 11, pp. 5932–5947, 2021.
[111] X. Wu, Z. Bai, J. Jia, and Y. Liang, "A Multi-Variate Triple-Regression Forecasting Algorithm for Long-Term Customized Allergy Season Prediction," *arXiv preprint arXiv:2005.04557*, 2020.
[112] A. A. A. Ahmed, A. Aljabouh, P. K. Donepudi, and M. S. Choi, "Detecting fake news using machine learning: A systematic literature review," *arXiv preprint arXiv:2102.04458*, 2021.
[113] H. Rahimi-Eichi, U. Ojha, F. Baronti, and M.-Y. Chow, "Battery Management System: An Overview of Its Application in the Smart Grid and Electric Vehicles," *IEEE Ind. Electron. Mag.*, vol. 7, no. 2, pp. 4–16, Jun. 2013.
[114] E. Silvas, T. Hofman, and N. Murgovski, "Review of optimization strategies for system-level design in hybrid electric vehicles," *IEEE Transactions*, 2016.
[115] C. C. Chan, "An overview of electric vehicle technology," *Proc. IEEE*, vol. 81, no. 9, pp. 1202–1213, Sep. 1993.
[116] S. Jahandari and A. Srivastava, "Detection of Delays and Feedthroughs in Dynamic Networked Systems," *IEEE Control Systems Letters*, vol. 7, pp. 1201–1206, 2022.

[117] D. Nelson-Gruel, Y. Chamaillard, and A. Aljarbouh, “Modeling and estimation of the pollutants emissions in the Compression Ignition diesel engine,” 2016, pp. 317–322.
[118] A. Duracz *et al.*, “Advanced hazard analysis and risk assessment in the ISO 26262 functional safety standard using rigorous simulation,” 2020, pp. 108–126.
[119] Z. Bai, R. Yang, and Y. Liang, “Mental task classification using electroencephalogram signal,” *arXiv preprint arXiv:1910.03023*, 2019.
[120] S. Jahandari, F. F. Beyglou, A. Kalhor, and M. T. Masouleh, “A robust adaptive linear control for a ball handling mechanism,” 2014, pp. 376–381.
[121] H. H. Wu, A. Gilchrist, K. Sealy, P. Israelsen, and J. Muhs, “A review on inductive charging for electric vehicles,” in *2011 IEEE International Electric Machines & Drives Conference (IEMDC)*, 2011, pp. 143–147.
[122] P. Sun, R. Bisschop, H. Niu, and X. Huang, “A Review of Battery Fires in Electric Vehicles,” *Fire Technol.*, vol. 56, no. 4, pp. 1361–1410, Jul. 2020.
[123] K. Liu, K. Li, Q. Peng, and C. Zhang, “A brief review on key technologies in the battery management system of electric vehicles,” *Front. Mech. Eng. Chin.*, vol. 14, no. 1, pp. 47–64, Mar. 2019.
[124] S. Jahandari and D. Materassi, “Optimal selection of observations for identification of multiple modules in dynamic networks,” *IEEE Trans. Automat. Contr.*, vol. 67, no. 9, pp. 4703–4716, 2022.
[125] S. F. Tie and C. W. Tan, “A review of energy sources and energy management system in electric vehicles,” *Renewable Sustainable Energy Rev.*, vol. 20, pp. 82–102, Apr. 2013.
[126] K. V. Singh, H. O. Bansal, and D. Singh, “A comprehensive review on hybrid electric vehicles: architectures and components,” *Journal of Modern Transportation*, vol. 27, no. 2, pp. 77–107, Jun. 2019.
[127] C. Zhang, K. Li, and S. Mcloone, “Battery modelling methods for electric vehicles-A review,” *2014 European Control*, 2014.
[128] R. J. Bessa and M. A. Matos, “Economic and technical management of an aggregation agent for electric vehicles: a literature survey,” *Eur. Trans. Electr. Power*, 2012.
[129] A. Ahmad, M. S. Alam, and R. Chabaan, “A Comprehensive Review of Wireless Charging Technologies for Electric Vehicles,” *IEEE Transactions on Transportation Electrification*, vol. 4, no. 1, pp. 38–63, Mar. 2018.
[130] M. F. M. Sabri, K. A. Danapalasingam, and M. F. Rahmat, “A review on hybrid electric vehicles architecture and energy management strategies,” *Renewable Sustainable Energy Rev.*, vol. 53, pp. 1433–1442, Jan. 2016.
[131] X. Zeng, M. Li, D. Abd El-Hady, and W. Alshitari, “Commercialization of lithium battery technologies for electric vehicles,” *Advanced Energy*, 2019.
[132] M. U. Cuma and T. Koroglu, “A comprehensive review on estimation strategies used in hybrid and battery electric vehicles,” *Renewable Sustainable Energy Rev.*, vol. 42, pp. 517–531, Feb. 2015.