Network Security Vulnerabilities in Smart Vehicle-to-Grid Systems Identifying Threats and Proposing Robust Countermeasures

Andrej Novak
Affiliation: University of Maribor,
Faculty of Electrical Engineering and Computer Science, Slovenia
Alexei Ivanov
Affiliation: Tallinn University of Technology, School of Information Technologies, Estonia

Keywords: Smart Vehicle-to-Grid (V2G),
Electric Vehicles (EVs),
Network Security Vulnerabilities,
Countermeasures,
Authentication Protocols,
Intrusion Detection Systems (IDS),
Cyber-attacks

Abstract

Background: With the rise of electric vehicles (EVs), Smart Vehicle-to-Grid (V2G) Systems have emerged as a promising technology, enabling EVs to interact with the power grid for energy transactions. While this technology offers advantages in grid management and renewable energy integration, it also presents potential security vulnerabilities.
Objective: This research aims to identify and analyze potential threats to V2G systems and propose robust countermeasures to address these vulnerabilities.
Methods: A comprehensive review of V2G system architecture was conducted to identify potential security threats. These threats include Eavesdropping, Man-in-the-Middle Attacks, Denial of Service attacks, Physical Tampering, Malware and Firmware Attacks, Replay Attacks, False Data Injection, and Identity Spoofing.
Results: To mitigate these threats, several countermeasures were identified. These include End-to-End Encryption to protect data during transmission, Authentication Protocols for transaction verification, Intrusion Detection Systems for monitoring suspicious activities, Regular Firmware Updates, Rate Limiting, Physical Security Measures, Time-Stamping and Sequence Numbers to prevent replay attacks, Data Integrity Checks, Role-Based Access Control, and Security Awareness and Training.
Conclusion: As Smart V2G Systems become more prevalent, their security is of utmost importance. By recognizing potential threats and implementing the proposed countermeasures, V2G systems can remain secure, ensuring the benefits of this technology are realized without compromising the safety of the grid or EV owners.

Introduction

The automotive industry's shift towards electric vehicles (EVs) has been marked by significant advancements in battery technology, particularly in the development of lithium-ion batteries. These batteries have become the standard for EVs due to their high energy density and power-

to-weight ratio, which allows for longer driving ranges and more efficient energy utilization [1]–[3]. The chemistry of lithium-ion batteries involves the movement of lithium ions between the anode and cathode through an electrolyte, providing a continuous flow of electric current. Innovations in the materials used for the electrodes and electrolytes have led to improvements in the battery's overall performance, including increased lifespan and energy storage capacity [4]. One of the most promising advancements in battery technology is the development of solid-state batteries. Unlike traditional lithium-ion batteries that use a liquid or gel-like electrolyte, solid-state batteries employ a solid electrolyte. This solid electrolyte can be made from various materials such as ceramics or polymers, and it allows for a more compact and lightweight design [5]–[7]. The solid-state design eliminates the risk of leakage and reduces the chances of thermal runaway, a dangerous condition where the battery's temperature can rapidly increase, leading to potential failure or even explosion. This makes solid-state batteries inherently safer and more stable [8].

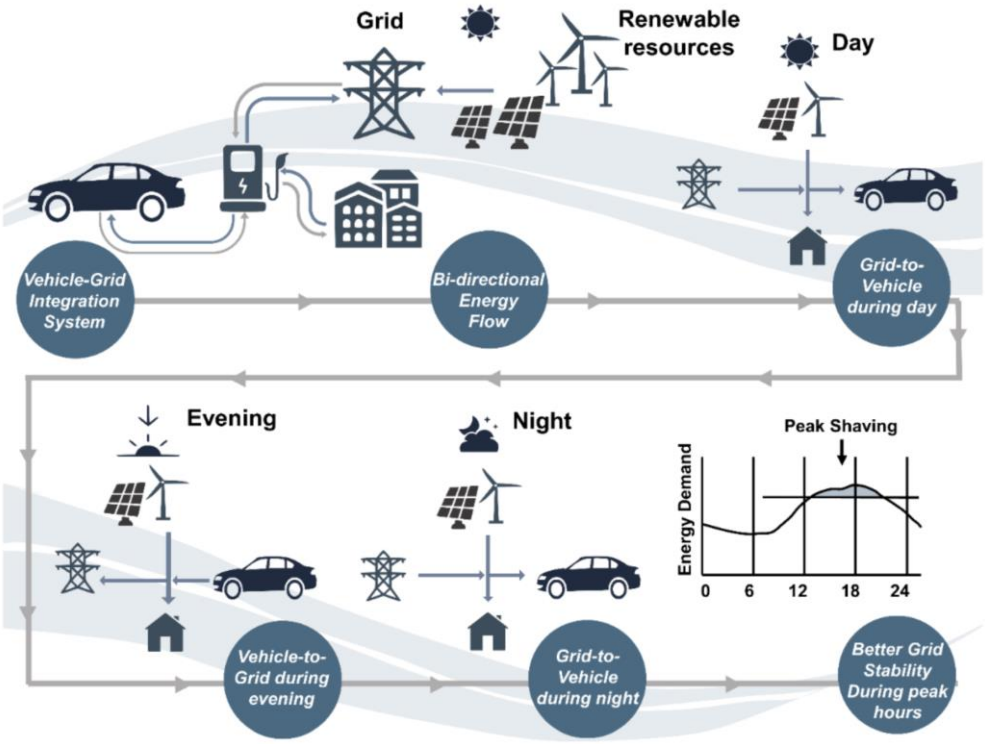

Fig 1. V2G concept in different times. Source [9]

The transition to solid-state batteries also offers the potential for faster charging times. Traditional lithium-ion batteries are limited in their charging speed by the rate at which the liquid electrolyte can transport lithium ions between the electrodes. In solid-state batteries, the solid electrolyte can facilitate a more direct and efficient ion transfer, allowing for quicker charging [10]. This is a critical advancement for the automotive industry, as reducing charging times is essential for making EVs more convenient and appealing to a broader consumer base. Faster charging not only enhances the user experience but also alleviates concerns about range anxiety, where drivers fear running out of battery power before reaching their destination [11]–[13].

In addition to the improvements in safety and charging times, solid-state batteries also promise greater energy storage capabilities. The solid electrolyte's structure allows for the use of different materials in the electrodes, such as lithium metal, which can significantly increase the battery's energy density. A higher energy density means that the battery can store more energy in the same amount of space, allowing for longer driving ranges and potentially reducing the overall size and weight of the battery pack. This can lead to more efficient vehicle designs and further contribute to the reduction of greenhouse gas emissions, aligning with global efforts to combat climate change [14]. The rapid adoption of electric vehicles and the corresponding advancements in battery technology represent a profound transformation in the automotive industry. While lithium-ion batteries have paved the way for this shift, the emergence of solid-state batteries offers even more promising prospects for the future of transportation. The combination of improved safety, faster charging times, and greater energy storage capabilities positions solid-state batteries as a key technology that could accelerate the transition to a more sustainable and efficient transportation system [15], [16]. The ongoing research and development in this field are likely to yield further innovations, shaping the automotive landscape in the years to come [17]–[19].

A critical aspect of the widespread adoption of electric vehicles (EVs) is the development of a robust charging infrastructure. This infrastructure must be comprehensive and versatile, encompassing home chargers, workplace chargers, and public fast-charging stations. The challenge lies in creating a network that is not only extensive but also accessible and efficient. Home chargers provide the convenience of overnight charging, but they often require significant electrical upgrades. Workplace chargers extend this convenience to the office, but they necessitate cooperation from employers and commercial property owners. Public fast-charging stations are essential for long-distance travel, but their installation involves substantial costs, technical considerations, and coordination with local utilities and governments [20].

Fast charging is a vital component of the charging infrastructure, allowing EV drivers to recharge their vehicles in a matter of minutes rather than hours. The technical details of fast charging involve higher voltage and current levels, which facilitate the rapid transfer of energy into the battery. This is achieved through specialized charging equipment and connectors that can handle the increased power flow. However, this rapid charging process generates more heat and can strain the battery, potentially impacting its overall lifespan and performance. Cooling systems and intelligent charging algorithms are often employed to mitigate these effects, balancing the need for speed with the preservation of battery health [21].

The impact of fast charging on battery life is a complex issue that involves multiple factors, including the battery's chemistry, design, and the frequency of fast charging. While fast charging can reduce the time needed to recharge, it may also lead to increased wear and tear on the battery [22]–[24]. This wear can result in a gradual decrease in the battery's capacity and efficiency over time. Manufacturers and researchers are continually working on optimizing the charging process to minimize these effects, employing advanced battery management systems that monitor and control the charging parameters to ensure optimal performance and longevity.

Evolving standards for high-power charging are essential to the development of a cohesive and interoperable charging network. Various charging standards exist around the world, reflecting different voltage levels, connector types, and communication protocols. The harmonization of these standards is crucial to ensure that EV drivers can access charging stations regardless of the vehicle make or location. Collaborative efforts among automakers, governments, and industry organizations are underway to develop and promote universal charging standards.

These efforts aim to simplify the charging experience for consumers and facilitate the integration of charging infrastructure across different regions and markets. The establishment of a widespread network of charging stations, encompassing home, workplace, and public fast-charging options, is a multifaceted challenge that requires careful planning, investment, and collaboration. The technical complexities of fast charging, its impact on battery life, and the need for standardized high-power charging protocols add layers of complexity to this endeavor [25].

Electric propulsion systems are at the core of the performance and efficiency of electric vehicles (EVs), providing the advantage of instant torque delivery that contributes to swift acceleration. The technical workings of electric motors can be categorized into different types, each with unique characteristics and applications. Induction motors, for example, operate on the principle of electromagnetic induction and are known for their robustness and simplicity. Permanent magnet motors, on the other hand, utilize magnets to generate a magnetic field, offering higher efficiency and power density but often at a higher cost [26]–[28]. Motor controllers play a vital role in the operation of electric motors, regulating the voltage and current supplied to the motor to control its speed, torque, and direction. These controllers use sophisticated algorithms to translate the driver's inputs into precise electrical commands, ensuring smooth and responsive performance. The development of advanced control algorithms has further enhanced the efficiency and adaptability of electric propulsion systems. Techniques such as field-oriented control (FOC) and direct torque control (DTC) allow for more precise control over the motor's magnetic fields, optimizing energy consumption and improving the overall driving experience [29].

Efficiency optimization in electric propulsion systems is a complex task that involves balancing performance, reliability, and energy consumption. Various strategies are employed to achieve this balance, including the design of the motor itself, the selection of materials, and the implementation of advanced control algorithms. Energy losses can occur in the form of heat due to resistance in the windings, friction in the bearings, and eddy currents in the core. By minimizing these losses through careful design and control, the overall efficiency of the electric motor can be significantly enhanced. This not only improves the vehicle's range but also reduces its environmental impact [30]–[32].

Regenerative braking systems add another layer of complexity and innovation to electric propulsion systems. Unlike conventional braking, where kinetic energy is dissipated as heat, regenerative braking captures and stores this energy during deceleration. When the driver applies the brakes, the electric motor operates in reverse, acting as a generator and converting the kinetic energy back into electrical energy. This energy is then stored in the battery for later use, effectively increasing the vehicle's overall efficiency and range. The integration of regenerative braking requires careful coordination between the braking system, motor controller, and battery management system, ensuring that the energy recovery process is smooth and effective [33].

Vehicle-to-Grid (V2G) technology

Vehicle-to-Grid (V2G) technology represents a significant advancement in the integration of electric vehicles (EVs) with the power grid [34], [35]. This innovative system allows for a two-way exchange of electricity between electric vehicles and the grid, enabling not only the charging of EVs but also the ability to feed energy back into the grid when needed. V2G technology leverages the energy stored in EV batteries, transforming them into temporary energy storage units that can be utilized to balance supply and demand within the grid. This is

achieved through intelligent charging systems that can control the flow of energy, taking into account factors such as grid requirements, energy prices, and the state of charge of the vehicle's battery [36]–[38]. By creating a more dynamic and responsive energy ecosystem, V2G technology fosters a more efficient and sustainable use of renewable energy sources, thereby contributing to the reduction of greenhouse gas emissions [39]. The integration of electric vehicles into the grid through V2G technology is of paramount importance for enhanced energy management. As the adoption of EVs continues to grow, the energy demand for charging these vehicles will also increase [40]–[42].

Without proper integration and management, this could lead to significant challenges in maintaining grid stability. V2G technology helps in mitigating these challenges by allowing EVs to act as a distributed energy resource. This means that during peak demand periods, energy stored in EV batteries can be fed back into the grid, reducing the strain on power plants and helping to maintain grid stability. Conversely, during periods of low demand, EVs can be charged using excess energy from the grid, thus optimizing energy utilization [43].

Furthermore, the integration of EVs into the grid through V2G technology plays a vital role in supporting the transition to renewable energy. Traditional energy sources are often unable to respond quickly to fluctuations in demand, leading to inefficiencies and increased emissions. By utilizing the energy stored in EV batteries, V2G technology provides a flexible and responsive energy resource that can be used to smooth out these fluctuations. This enhances the grid's ability to accommodate variable renewable energy sources such as wind and solar, making it easier to integrate them into the energy mix. In turn, this supports the broader goals of reducing reliance on fossil fuels, lowering emissions, and moving towards a more sustainable and resilient energy system. The synergy between electric vehicles and the grid through V2G technology represents a promising pathway towards a cleaner and more efficient energy future [44]–[46].

The Vehicle-to-Grid (V2G) concept represents a transformative approach to energy management, enabling bi-directional energy flow between electric vehicles (EVs) and the electrical grid. Unlike traditional charging systems where energy flows only from the grid to the vehicle, V2G allows energy to be transferred back to the grid from the vehicle's battery. This bi-directional flow creates opportunities for enhanced grid stability, renewable energy integration, and additional revenue streams for EV owners [47]. The components of V2G systems can be broadly categorized into three main areas: EVs, charging stations, and grid infrastructure. EVs in a V2G system must be equipped with compatible charging technology that allows for both charging and discharging of the battery. Charging stations, or Electric Vehicle Supply Equipment (EVSE), must be capable of handling bi-directional energy flow and communicating with both the vehicle and the grid. The grid infrastructure, including transmission lines, substations, and control centers, must be designed to accommodate the additional complexity of energy flow from potentially thousands of individual vehicles, requiring sophisticated energy management and control systems [48]–[50].

The technical requirements for V2G implementation are multifaceted and encompass various domains, from hardware design to communication protocols and regulatory compliance. On the hardware side, both the vehicle's onboard charger and the charging station must support bi-directional power conversion, allowing energy to flow in both directions efficiently. Communication between the vehicle, charging station, and grid operator is crucial for coordinating charging and discharging cycles, aligning with grid demands, and optimizing

energy pricing. This requires the implementation of standardized communication protocols that ensure interoperability and security across different devices and systems.

The integration of V2G into the existing grid also necessitates careful consideration of grid stability and power quality. The intermittent nature of renewable energy sources, such as wind and solar, can lead to fluctuations in the grid's voltage and frequency. V2G systems can help mitigate these fluctuations by absorbing excess energy during periods of high renewable generation and supplying energy back to the grid during periods of high demand. This requires advanced control algorithms that can respond to grid conditions in real-time, balancing the needs of the grid with the state of charge and availability of the connected vehicles.

Regulatory and economic factors also play a significant role in the feasibility and attractiveness of V2G implementation. Policies and incentives that support the development and deployment of V2G technology can accelerate its adoption, while clear regulations regarding energy transactions, grid participation, and consumer protection are essential for building trust and confidence in the system. The development of appropriate business models and pricing structures is equally important, ensuring that all stakeholders, including EV owners, utilities, and grid operators, benefit from the value created by V2G [51].

The V2G concept represents a paradigm shift in energy management, leveraging the distributed energy storage capacity of EVs to enhance grid flexibility and sustainability. The successful implementation of V2G requires a comprehensive and integrated approach, encompassing the technical design of EVs and charging stations, the development of intelligent control and communication systems, and the alignment of regulatory and economic frameworks. The ongoing collaboration between the automotive industry, energy sector, policymakers, and researchers is key to unlocking the full potential of V2G, contributing to a more resilient and efficient energy system that supports the continued growth of electric mobility [52].

Potential Threats and Vulnerabilities in V2G Systems

Eavesdropping

Eavesdropping in the context of communication between Electric Vehicles (EVs) and the grid refers to the unauthorized interception of data transmitted between these two entities [53]–[56]. This is a significant concern in the modern world where EVs are becoming increasingly popular, and the integration of these vehicles with the grid is essential for efficient energy management [57]–[59]. The communication between EVs and the grid often involves the exchange of sensitive information such as user profiles, charging schedules, billing details, and energy consumption patterns. Unauthorized access to this information can lead to various security and privacy risks, making the protection of these communications a priority for both manufacturers and energy providers [60].

The theft of sensitive data through eavesdropping can have serious consequences for both individuals and organizations. For individuals, it may lead to personal information being exposed, such as home addresses, travel patterns, and financial details. This information can be used for malicious purposes like identity theft or targeted attacks [61]–[63]. For organizations, the unauthorized interception of communication can lead to the exposure of proprietary information, such as pricing strategies and energy management algorithms. This can result in competitive disadvantages and potential legal liabilities, making the prevention of eavesdropping a critical aspect of business operations [64].

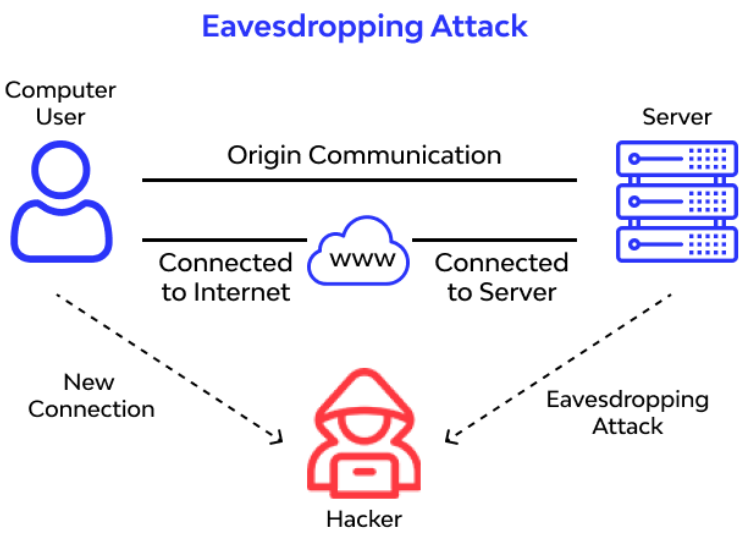

Fig 2. Eavesdropping attack. Source: [65]

The technology used in the communication between EVs and the grid is often based on wireless networks, making it susceptible to various eavesdropping techniques. Attackers can employ devices that capture the radio waves transmitted between the EV and the grid, decoding the information without the knowledge or consent of the parties involved. The complexity of these attacks can vary, ranging from simple passive listening to more sophisticated techniques that manipulate the communication to extract specific information. The use of encryption and secure communication protocols is essential in mitigating these risks, but they must be implemented with care to ensure that they are effective against evolving threats.

The regulatory landscape also plays a vital role in addressing the risks associated with eavesdropping on EV-grid communication. Governments and regulatory bodies must establish clear guidelines and standards to ensure that manufacturers and energy providers implement appropriate security measures [66]–[68]. This includes defining the minimum requirements for encryption, authentication, and data integrity, as well as conducting regular audits and assessments to ensure compliance. Collaboration between different stakeholders, including industry experts, academics, and policymakers, is essential to develop a comprehensive approach that balances the need for innovation and efficiency with the protection of privacy and security [69].

Man-in-the-Middle Attacks (MitM):

Man-in-the-Middle Attacks (MitM) in the context of communication between Electric Vehicles (EVs) and the grid represent a particularly insidious form of cyber threat [70]–[72]. In a MitM attack, the attacker positions themselves between the EV and the grid, intercepting and potentially altering the communication between the two. This can lead to unauthorized energy transactions, manipulation of charging schedules, and other malicious activities. The complexity of these attacks and the potential consequences make them a significant concern for both the automotive and energy industries [73]. The mechanics of a MitM attack involve the attacker impersonating both the EV and the grid, effectively taking control of the communication channel. This can be achieved through various techniques, such as ARP spoofing, DNS hijacking, or exploiting vulnerabilities in the communication protocols. Once

the attacker has established control, they can monitor the communication, alter messages, or even initiate unauthorized transactions. For example, they might manipulate the charging schedule to draw energy at peak times, leading to higher costs, or initiate unauthorized energy sales back to the grid, creating financial and legal liabilities [74]. The potential consequences of MitM attacks on EV-grid communication are far-reaching. Unauthorized energy transactions can lead to financial losses for both consumers and energy providers [75]–[77]. The manipulation of charging schedules can disrupt the stability of the grid, leading to inefficiencies and potential power outages. Furthermore, the exposure of sensitive information, such as user profiles and energy consumption patterns, can lead to privacy violations and other security risks. The multifaceted nature of these attacks requires a comprehensive approach to prevention, detection, and mitigation [78].

Preventing MitM attacks requires a combination of technological and procedural measures. On the technological front, the implementation of robust encryption and authentication protocols is essential. This ensures that the communication between the EV and the grid is secure, and any attempt to intercept or alter the communication can be detected. Public Key Infrastructure (PKI) and Transport Layer Security (TLS) are examples of technologies that can be used to secure the communication channel. Procedural measures include regular security assessments, employee training, and collaboration with industry experts to stay abreast of emerging threats and vulnerabilities [79]–[81].

The regulatory environment also plays a crucial role in addressing the risks associated with MitM attacks. Governments and regulatory bodies must establish clear guidelines and standards for securing EV-grid communication. This includes defining minimum requirements for encryption, authentication, and monitoring, as well as conducting regular audits to ensure compliance. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that balances the need for innovation and efficiency with the protection of privacy and security [82].

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are cyber threats that can have a profound impact on the Vehicle-to-Grid (V2G) system, where electric vehicles (EVs) interact with the power grid. These attacks involve overwhelming the V2G system with an excessive amount of traffic, rendering it unavailable to legitimate users. The consequences of these attacks can range from temporary disruptions to long-term damage to the infrastructure, making them a critical concern for both the automotive and energy sectors [83]–[85].

DoS and DDoS attacks are executed by sending a flood of requests to the targeted V2G system, overwhelming its capacity to respond. In a DoS attack, this flood originates from a single source, while in a DDoS attack, it comes from multiple sources, often coordinated through a network of compromised computers or devices. The sheer volume of traffic in these attacks can exhaust the system's resources, such as bandwidth, processing power, and memory, causing it to become slow or entirely unresponsive. This can disrupt the normal functioning of the V2G system, affecting charging schedules, energy transactions, and other essential operations [86].

The impact of DoS and DDoS attacks on the V2G system can be far-reaching. Temporary unavailability can lead to inconvenience and financial losses for both EV owners and energy providers [87]–[89]. In more severe cases, the disruption of the V2G system can affect the stability of the entire power grid, leading to inefficiencies, increased costs, and potential power outages. The potential for cascading failures and the interconnected nature of modern energy

systems make these attacks a significant threat to the overall energy infrastructure. Furthermore, the recovery from a successful attack can be time-consuming and costly, requiring extensive efforts to identify, mitigate, and prevent future incidents [90].

Preventing and mitigating DoS and DDoS attacks requires a combination of technological and procedural measures. Technologically, the implementation of intrusion detection systems, firewalls, and traffic filtering can help identify and block malicious traffic before it reaches the V2G system. Regular monitoring and analysis of network traffic can provide early warning signs of an impending attack, allowing for proactive measures to be taken [91]–[93]. Procedurally, organizations must develop and maintain comprehensive security policies, conduct regular security assessments, and provide training to employees to ensure that they are aware of the risks and best practices for prevention and response [94]. The regulatory environment also plays a vital role in addressing the risks associated with DoS and DDoS attacks on the V2G system. Governments and regulatory bodies must establish clear guidelines and standards for securing the V2G communication and infrastructure. This includes defining minimum requirements for network security, monitoring, and incident response, as well as conducting regular audits to ensure compliance. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that balances the need for innovation and efficiency with the protection of the critical energy infrastructure [95].

Physical Tampering

Physical tampering with Electric Vehicles (EVs) or grid infrastructure represents a unique and tangible threat that can lead to unauthorized modifications or data theft. Unlike cyber threats that exploit vulnerabilities in software or communication protocols, physical tampering involves direct access to the hardware components of the EV or the grid system. This form of attack can have serious consequences, affecting the functionality, safety, and security of both the individual vehicle and the broader energy infrastructure [96].

Physical tampering can take various forms, ranging from simple vandalism to sophisticated manipulation of hardware components. An attacker with direct access to an EV might install malicious devices to intercept or alter communication with the grid, leading to unauthorized energy transactions or exposure of sensitive information. Similarly, tampering with grid infrastructure, such as substations or charging stations, can disrupt the normal functioning of the energy system, leading to inefficiencies, increased costs, or even potential power outages. The physical nature of these attacks makes them challenging to detect and prevent, requiring a combination of security measures and vigilance.

The impact of physical tampering on the EV and grid system can be far-reaching. Unauthorized modifications to an EV can affect its performance, safety, and reliability, leading to potential accidents or breakdowns [9], [97], [98]. Data theft can expose personal information, such as travel patterns and financial details, leading to privacy violations and other security risks. Tampering with grid infrastructure can have broader consequences, affecting the stability and resilience of the entire energy system. The interconnected nature of modern energy infrastructure means that localized tampering can have cascading effects, creating vulnerabilities that can be exploited by other forms of attacks [99].

Preventing and mitigating physical tampering requires a combination of technological and procedural measures. Technologically, the implementation of tamper-evident seals, intrusion detection systems, and secure hardware design can help detect and deter unauthorized access. Regular inspections and monitoring of both EVs and grid infrastructure can provide early

warning signs of potential tampering, allowing for proactive measures to be taken. Procedurally, organizations must develop and maintain comprehensive security policies, conduct regular security assessments, and provide training to employees to ensure that they are aware of the risks and best practices for prevention and response [100]–[102]. Collaboration with law enforcement and other stakeholders is also essential to address the broader societal aspects of physical tampering [103]. The regulatory environment plays a vital role in addressing the risks associated with physical tampering. Governments and regulatory bodies must establish clear guidelines and standards for securing both EVs and grid infrastructure. This includes defining minimum requirements for physical security, monitoring, and incident response, as well as conducting regular audits to ensure compliance. Collaboration between different stakeholders, including manufacturers, energy providers, security experts, and policymakers, is essential to develop a cohesive approach that balances the need for innovation and efficiency with the protection of physical assets [104].

Malware and Firmware Attacks

The introduction of malicious software, or malware, to compromise the Vehicle-to-Grid (V2G) system's operation represents a significant cyber threat that can have profound implications for both the automotive and energy sectors [105]–[107]. Malware attacks target the software components of the V2G system, including the communication protocols, control algorithms, and user interfaces, with the intent to disrupt, manipulate, or gain unauthorized access to the system. The complexity and potential consequences of malware attacks require a comprehensive approach to prevention, detection, and mitigation [108]. Malware can be introduced into the V2G system through various means, including phishing emails, malicious websites, infected USB devices, or direct attacks on vulnerable software components [109]–[111]. Once introduced, the malware can execute a wide range of malicious activities, such as intercepting communication, altering charging schedules, initiating unauthorized transactions, or even causing physical damage to the EV or grid infrastructure [112]–[114]. The success of a malware attack depends on the attacker's ability to exploit vulnerabilities in the system without detection, requiring sophisticated techniques and often leveraging zero-day exploits or other advanced methods [115].

The impact of malware attacks on the V2G system can be substantial. Disruption of the normal operation can lead to inefficiencies, increased costs, or even potential power outages. Unauthorized transactions or manipulation of charging schedules can result in financial losses for both consumers and energy providers, as well as potential legal liabilities. Furthermore, the exposure of sensitive information, such as user profiles and energy consumption patterns, can lead to privacy violations and other security risks [116]–[118]. The interconnected nature of modern energy systems means that localized malware attacks can have cascading effects, creating vulnerabilities that can be exploited by other forms of attacks [119]. Preventing and mitigating malware attacks requires a combination of technological and procedural measures [120]. Technologically, the implementation of robust antivirus software, firewalls, intrusion detection systems, and secure software development practices can help detect and prevent the introduction of malware. Regular software updates, patch management, and vulnerability assessments are essential to ensure that the system is protected against emerging threats [121]–[124]. Procedurally, organizations must develop and maintain comprehensive security policies, conduct regular security training, and foster a culture of vigilance and awareness to ensure that employees and users are aware of the risks and best practices for prevention and response [125].

The regulatory environment also plays a vital role in addressing the risks associated with malware attacks on the V2G system. Governments and regulatory bodies must establish clear

guidelines and standards for securing the V2G communication and infrastructure. This includes defining minimum requirements for software security, monitoring, and incident response, as well as conducting regular audits to ensure compliance. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that balances the need for innovation and efficiency with the protection of the critical energy infrastructure [126].

Replay Attacks

Replay attacks, within the context of Electric Vehicles (EVs) and grid communication, involve attackers capturing valid data transmissions and replaying them at a later time to initiate unauthorized actions. This type of attack can be particularly insidious, as it leverages legitimate data, making detection and prevention more challenging [127]–[129]. The potential consequences of replay attacks can range from unauthorized energy transactions to manipulation of charging schedules, making them a significant concern for both the automotive and energy sectors [130]. In a replay attack, the attacker intercepts and records a valid communication between the EV and the grid, such as a command to start charging or a confirmation of an energy transaction. This captured data is then replayed at a later time, tricking the system into accepting it as a legitimate request. Since the data itself is valid, traditional security measures such as encryption and authentication may not be sufficient to detect or prevent the attack. The success of a replay attack depends on the attacker's ability to capture and replay the data without detection, requiring sophisticated techniques and careful timing [131].

The impact of replay attacks on the EV and grid system can be substantial. Unauthorized energy transactions can lead to financial losses for both consumers and energy providers, as well as potential legal liabilities. Manipulation of charging schedules can disrupt the stability of the grid, leading to inefficiencies and potential power outages. Furthermore, the exposure of sensitive information, such as user profiles and energy consumption patterns, can lead to privacy violations and other security risks. The complexity and potential consequences of replay attacks require a comprehensive approach to prevention, detection, and mitigation.

Preventing and mitigating replay attacks requires a combination of technological and procedural measures. Technologically, the implementation of time-sensitive authentication and unique transaction identifiers can help detect and prevent replay attempts. By ensuring that each communication is uniquely tied to a specific time or transaction, the system can recognize and reject replayed data. Regular monitoring and analysis of network traffic can provide early warning signs of potential replay attacks, allowing for proactive measures to be taken. Procedurally, organizations must develop and maintain comprehensive security policies, conduct regular security assessments, and provide training to employees to ensure that they are aware of the risks and best practices for prevention and response [132] [133].

The regulatory environment also plays a vital role in addressing the risks associated with replay attacks. Governments and regulatory bodies must establish clear guidelines and standards for securing EV-grid communication. This includes defining minimum requirements for time-sensitive authentication, monitoring, and incident response, as well as conducting regular audits to ensure compliance. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that balances the need for innovation and efficiency with the protection of privacy and security [134].

False Data Injection

False Data Injection (FDI) attacks in the context of Electric Vehicles (EVs) and grid communication involve attackers sending false or manipulated data to either the grid or the EV, leading to incorrect energy transactions or other unauthorized actions. This type of cyber threat is particularly concerning as it directly targets the integrity of the data being exchanged, potentially undermining the trust and reliability of the entire system. The consequences of FDI attacks can be far-reaching, affecting both individual consumers and the broader energy infrastructure [135].

In an FDI attack, the attacker alters or fabricates data that is then sent to the grid or the EV, causing the system to act on incorrect information. This could include manipulating energy consumption readings, altering charging schedules, or initiating unauthorized energy transactions. The success of an FDI attack depends on the attacker's ability to bypass security measures and inject the false data without detection. This may require exploiting vulnerabilities in the communication protocols or leveraging other forms of attacks, such as phishing or malware, to gain access to the system [136]. The impact of FDI attacks on the EV and grid system can be substantial. Incorrect energy transactions can lead to financial losses for both consumers and energy providers, as well as potential legal liabilities. Manipulation of charging schedules or energy consumption readings can disrupt the stability of the grid, leading to inefficiencies, increased costs, or even potential power outages. Furthermore, the erosion of trust in the integrity of the data being exchanged can have long-term consequences, affecting consumer confidence and hindering the adoption and success of EVs and smart grid technologies [137].

Preventing and mitigating FDI attacks requires a combination of technological and procedural measures. Technologically, the implementation of robust data integrity checks, encryption, and authentication protocols can help detect and prevent the injection of false data. Anomaly detection algorithms and regular monitoring of network traffic can provide early warning signs of potential FDI attacks, allowing for proactive measures to be taken. Procedurally, organizations must develop and maintain comprehensive security policies, conduct regular security assessments, and provide training to employees to ensure that they are aware of the risks and best practices for prevention and response [138]–[140].

The regulatory environment also plays a vital role in addressing the risks associated with FDI attacks. Governments and regulatory bodies must establish clear guidelines and standards for securing EV-grid communication. This includes defining minimum requirements for data integrity, encryption, authentication, and monitoring, as well as conducting regular audits to ensure compliance. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that balances the need for innovation and efficiency with the protection of data integrity and security [141].

Identity Spoofing

Identity Spoofing in the context of Electric Vehicles (EVs) and grid communication is a deceptive practice where attackers pretend to be a legitimate EV or grid entity to initiate unauthorized transactions or other malicious activities [142]. This type of attack directly targets the authentication mechanisms of the system, undermining the trust and security that are foundational to the successful integration of EVs with the grid. The consequences of identity spoofing can be far-reaching, affecting both individual consumers and the broader energy infrastructure [143].

In an identity spoofing attack, the attacker impersonates a legitimate entity within the EV-grid ecosystem, such as a specific EV, charging station, or energy provider. This can be achieved through various means, including stealing credentials, exploiting vulnerabilities in the authentication protocols, or leveraging other forms of attacks, such as phishing or malware. Once the attacker has successfully assumed the identity of a legitimate entity, they can initiate unauthorized transactions, manipulate charging schedules, or access sensitive information. The success of an identity spoofing attack depends on the attacker's ability to convincingly mimic the legitimate entity without detection, requiring sophisticated techniques and careful planning.

The impact of identity spoofing on the EV and grid system can be substantial. Unauthorized transactions can lead to financial losses for both consumers and energy providers, as well as potential legal liabilities. Manipulation of charging schedules or access to sensitive information can disrupt the stability of the grid, leading to inefficiencies, increased costs, or even potential power outages. Furthermore, the erosion of trust in the authentication mechanisms of the system can have long-term consequences, affecting consumer confidence and hindering the adoption and success of EVs and smart grid technologies [144].

Preventing and mitigating identity spoofing requires a combination of technological and procedural measures. Technologically, the implementation of robust authentication protocols, multi-factor authentication, and continuous monitoring can help detect and prevent impersonation attempts. Regular security assessments and penetration testing can provide insights into potential vulnerabilities and areas for improvement. Procedurally, organizations must develop and maintain comprehensive security policies, conduct regular security training, and foster a culture of vigilance and awareness to ensure that employees and users are aware of the risks and best practices for prevention and response [145]–[147].

The regulatory environment also plays a vital role in addressing the risks associated with identity spoofing. Governments and regulatory bodies must establish clear guidelines and standards for securing EV-grid communication. This includes defining minimum requirements for authentication, monitoring, and incident response, as well as conducting regular audits to ensure compliance. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that balances the need for innovation and efficiency with the protection of identity and security [148].

Robust Countermeasures

End-to-End Encryption

Encrypting data during transmission between Electric Vehicles (EVs) and the grid is a fundamental security measure that ensures that even if data is intercepted, it remains unreadable to unauthorized entities. This practice is vital in the context of the growing integration of EVs with the energy grid, where sensitive information such as charging schedules, energy consumption patterns, billing details, and user profiles are routinely exchanged. The implementation of encryption not only protects the confidentiality of this information but also contributes to the overall integrity and trustworthiness of the system.

Encryption involves the transformation of plain text data into a scrambled format using a specific algorithm and encryption key. Only entities with the corresponding decryption key can revert the scrambled data back to its original form. This ensures that even if an attacker intercepts the data during transmission, they cannot read or manipulate it without access to the decryption key. Various encryption algorithms and protocols are available, each with different

levels of security and performance characteristics. The choice of encryption method must be carefully considered based on the specific requirements of the EV-grid communication, such as data sensitivity, transmission speed, and regulatory compliance [149]. The implementation of encryption in the EV-grid ecosystem provides several benefits. First and foremost, it protects the privacy of individual users by ensuring that personal information and behavior patterns are not exposed to unauthorized entities. Second, it safeguards the integrity of energy transactions, preventing attackers from altering or fabricating data to initiate unauthorized actions. Third, it contributes to the overall resilience of the energy system by reducing the potential impact of cyberattacks, such as eavesdropping or man-in-the-middle attacks. Finally, it fosters consumer confidence and regulatory compliance by demonstrating a commitment to security and privacy [150].

However, the implementation of encryption also presents challenges that must be addressed. The management of encryption keys is a critical aspect that requires careful consideration to ensure that keys are securely generated, stored, and managed. Weak or compromised keys can undermine the effectiveness of encryption, leading to potential vulnerabilities. Additionally, the computational overhead associated with encryption can affect the performance of the communication, particularly in resource-constrained environments such as embedded systems in EVs. Balancing the need for robust security with the requirements for efficiency and usability is a complex task that requires expertise and ongoing vigilance [151].

The regulatory environment plays a vital role in guiding and overseeing the implementation of encryption in EV-grid communication. Governments and regulatory bodies must establish clear guidelines and standards that define the minimum requirements for encryption, key management, and compliance monitoring [152]–[154].Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that aligns with industry best practices and legal obligations [155].

Authentication Protocols

The mutual authentication between Electric Vehicles (EVs) and the grid before initiating any transaction is a critical security measure that ensures the integrity and confidentiality of the communication. This process involves both the EV and the grid verifying each other's identity, establishing trust, and ensuring that they are communicating with legitimate entities. Mutual authentication can be achieved using cryptographic keys or certificates, providing a robust defense against various cyber threats such as identity spoofing, man-in-the-middle attacks, and unauthorized access.

Cryptographic keys and certificates are essential tools in the mutual authentication process. Cryptographic keys are secret values used in conjunction with encryption algorithms to secure the communication. They can be symmetric, where both parties share the same key, or asymmetric, where each party has a pair of public and private keys. Certificates, on the other hand, are digital documents issued by a trusted Certificate Authority (CA) that vouch for the identity of the holder. They contain the public key and other identifying information, providing a secure means to verify the authenticity of the communicating parties [156]. The implementation of mutual authentication using cryptographic keys or certificates provides several benefits. First, it ensures that both the EV and the grid are communicating with legitimate entities, preventing attackers from impersonating either party. This protects against unauthorized transactions and other malicious activities that could result from false identities.

Second, it establishes a secure communication channel, allowing sensitive information such as charging schedules, energy consumption patterns, and billing details to be exchanged securely. Third, it fosters trust and confidence in the system, encouraging the adoption and success of EVs and smart grid technologies [157]. However, the implementation of mutual authentication also presents challenges that must be carefully addressed. The management of cryptographic keys and certificates is a complex task that requires robust policies, procedures, and technological measures. Keys must be securely generated, stored, and managed to prevent unauthorized access or compromise. Certificates must be obtained from reputable CAs and regularly updated to ensure their validity. The computational overhead associated with mutual authentication can also affect the performance of the communication, particularly in resource-constrained environments. Balancing the need for robust security with the requirements for efficiency and usability is a complex task that requires ongoing vigilance and expertise [158]–[160]. The regulatory environment plays a vital role in guiding and overseeing the implementation of mutual authentication in EV-grid communication. Governments and regulatory bodies must establish clear guidelines and standards that define the minimum requirements for authentication, key management, and compliance monitoring. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that aligns with industry best practices and legal obligations [161].

Deep Learning Based Intrusion Detection Systems (IDS)

Monitoring the Vehicle-to-Grid (V2G) network for any suspicious activities and alerting the system administrators is a crucial aspect of maintaining the security and integrity of the communication between Electric Vehicles (EVs) and the grid [162], [163]. This practice involves continuous observation, analysis, and evaluation of the network traffic and system behavior to detect anomalies, unauthorized access, or other signs of potential threats. The timely detection and response to suspicious activities are vital to prevent or mitigate potential cyberattacks, unauthorized transactions, or other malicious activities [164]. Monitoring the V2G network requires the implementation of various technological tools and methodologies. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are commonly used to analyze network traffic and identify patterns or behaviors that may indicate an attack. Security Information and Event Management (SIEM) systems can aggregate and correlate data from multiple sources, providing a comprehensive view of the network's security posture. Machine learning and artificial intelligence algorithms can be employed to detect subtle or complex anomalies that may not be recognizable through traditional methods [165]. The choice of monitoring tools and techniques must be carefully aligned with the specific requirements, risks, and characteristics of the V2G network [166].

The effectiveness of monitoring also depends on the establishment of clear policies, procedures, and responsibilities. System administrators must define what constitutes suspicious or unauthorized activities, set thresholds for alerts, and establish protocols for response and escalation [167], [168]. Regular training and awareness programs are essential to ensure that all stakeholders, including administrators, operators, and users, are aware of the risks, best practices, and their respective roles in maintaining security [169]–[171]. Collaboration with external experts, industry groups, and law enforcement agencies can provide additional insights, support, and resources to enhance the monitoring capabilities. The application of deep learning in Intrusion Detection Systems (IDS) for Vehicle-to-Grid (V2G) networks represents a significant advancement in the field of cybersecurity. Utilizing neural networks, these systems

are capable of processing vast amounts of data, far beyond what traditional methods could handle [172]–[174].

This ability to manage and analyze large datasets is essential in the context of V2G networks, where continuous streams of information flow between vehicles and the grid. The neural networks are trained to recognize the intricate patterns within this data, allowing them to differentiate between normal operations and potential threats [175]. This training phase is a critical aspect of the system's functionality, requiring careful selection and preparation of the data to ensure that the neural network can accurately identify the characteristics of both legitimate and malicious activities [176]. Training the neural networks on a dataset containing both normal and malicious activities is a complex process that requires meticulous attention to detail [177], [178]. The dataset must be representative of the real-world scenarios that the IDS will encounter, encompassing various types of legitimate interactions and potential attack vectors [179]. The training process involves feeding this data into the neural network, allowing it to learn the subtle differences between normal and suspicious behavior. This learning process often involves the use of supervised learning techniques, where labeled data is used to guide the network in understanding the underlying patterns [180], [181]. The quality of the training data and the methods used to train the network play a vital role in the system's ability to accurately detect intrusions in the V2G network [182].

The deep learning models used in IDS for V2G networks can include various architectures, each with its unique advantages. Convolutional Neural Networks (CNNs) are particularly well-suited for processing spatial data, such as images or structured grid data [183]. In the context of V2G networks, CNNs can be used to analyze the spatial relationships between different elements of the network, identifying patterns that may indicate an intrusion attempt. On the other hand, Recurrent Neural Networks (RNNs) are designed to handle temporal data, making them ideal for analyzing sequences of events over time [184], [185]. In a V2G network, RNNs can be used to monitor the flow of information between vehicles and the grid, detecting anomalies that may signify a breach in security [186]–[188]. The choice of architecture depends on the specific requirements of the V2G network and the nature of the data being analyzed [189].

Real-time processing and analysis of data are crucial for the timely detection of any suspicious activities in the V2G network. Deep learning models are capable of handling the continuous streams of data that characterize V2G interactions, analyzing them in real-time to identify potential threats [190]. This real-time analysis is essential for prompt response to any detected intrusions, allowing system administrators to take immediate action to mitigate the threat. The ability to process data in real-time requires not only powerful computational resources but also efficient algorithms that can analyze the data quickly without sacrificing accuracy. The development and optimization of these real-time analysis techniques are ongoing challenges in the field of deep learning-based IDS for V2G networks [191].

The application of deep learning in IDS for V2G networks represents a sophisticated approach to cybersecurity, leveraging the power of neural networks to process large amounts of data and identify complex patterns. The training of these networks on datasets containing both normal and malicious activities, the choice of appropriate architectures like CNNs or RNNs, and the ability to analyze data in real-time are all critical components of this approach [192]. Together, these elements enable the IDS to monitor the V2G network effectively [193]–[195], discerning the subtle differences between legitimate and potentially harmful behavior, and alerting system administrators to any suspicious activities in a timely manner [196]–[198]. The ongoing

research and development in this field continue to push the boundaries of what is possible [199], [200], enhancing the security and reliability of V2G networks [201].

Regular Firmware Updates

Ensuring that the Vehicle-to-Grid (V2G) system's software is regularly updated to patch any known vulnerabilities is a fundamental practice in maintaining the security and integrity of the communication between Electric Vehicles (EVs) and the grid. Software updates, including patches, fixes, and enhancements, address known weaknesses, bugs, or vulnerabilities that could be exploited by attackers to gain unauthorized access, initiate malicious activities, or disrupt the normal operation of the system. Regularly updating the software is vital to protect against evolving cyber threats and to ensure the continued reliability, performance, and compliance of the V2G system [202]. The process of updating the V2G system's software involves several key steps. First, continuous monitoring and assessment of the system are required to identify potential vulnerabilities, either through internal evaluations, vendor notifications, or public security advisories. Once a vulnerability is identified, the corresponding patch or update must be obtained from a reputable source, such as the software vendor or a trusted third party. The update must then be tested in a controlled environment to ensure compatibility, stability, and effectiveness. Finally, the update must be deployed across the system, following established protocols and schedules to minimize disruptions and risks [203].

The implementation of regular software updates provides several benefits. First, it ensures that the V2G system is protected against known vulnerabilities, reducing the potential attack surface and enhancing overall security. Second, it fosters compliance with regulatory requirements, industry standards, and best practices, demonstrating a commitment to responsible cybersecurity management. Third, it contributes to the overall performance, reliability, and usability of the system, ensuring that it continues to meet the evolving needs and expectations of users, operators, and regulators [204].

However, the process of updating the V2G system's software also presents challenges that must be carefully managed. The complexity of the V2G ecosystem, involving various interconnected components, devices, and protocols, can make the coordination and deployment of updates a complex task. Incompatibilities or conflicts between updates and existing configurations can lead to disruptions, malfunctions, or other unintended consequences. Balancing the need for timely updates with the requirements for stability, usability, and efficiency requires careful planning, expertise, and ongoing vigilance [205]. The regulatory environment plays a vital role in guiding and overseeing the process of updating the V2G system's software. Governments and regulatory bodies must establish clear guidelines and standards that define the minimum requirements for vulnerability management, patching, and compliance monitoring. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that aligns with industry best practices and legal obligations [206].

Rate Limiting

Implementing rate limiting as a measure to prevent Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks is a critical strategy in securing the Vehicle-to-Grid (V2G) system. DoS and DDoS attacks involve overwhelming the system with an excessive number of requests or traffic, rendering it slow or entirely unavailable to legitimate users. Rate limiting is a technique that controls the number of requests a user or system can make within a specified time frame, thereby mitigating the potential impact of these attacks on the V2G communication between Electric Vehicles (EVs) and the grid [207]. Rate limiting works by monitoring and

controlling the rate of incoming requests to the V2G system. If the number of requests from a particular source exceeds a predefined threshold, additional requests are delayed or rejected. This ensures that the system's resources are not monopolized by potentially malicious traffic, allowing legitimate users to continue accessing the system. Rate limiting can be implemented at various levels, including the network, application, or user level, and can be tailored to the specific requirements, risks, and characteristics of the V2G network [208].

The implementation of rate limiting provides several benefits in the context of V2G security. First, it offers a robust defense against DoS and DDoS attacks, ensuring that the system remains available and responsive even under attack. Second, it contributes to the overall stability and performance of the system, preventing resource exhaustion and potential cascading failures. Third, it fosters compliance with regulatory requirements and industry best practices, demonstrating a proactive approach to cybersecurity [209].

However, the implementation of rate limiting also presents challenges that must be carefully considered. Setting the appropriate thresholds for rate limiting requires a deep understanding of the normal behavior and usage patterns of the V2G system. Too strict limitations may hinder legitimate users, while too lenient limitations may fail to prevent attacks. Balancing the need for security with the requirements for usability and efficiency is a complex task that requires ongoing monitoring, tuning, and expertise [210]–[212]. Governments and regulatory bodies must establish clear guidelines and standards that define the minimum requirements for rate limiting, monitoring, and compliance. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that aligns with industry best practices and legal obligations [213].

Physical Security Measures

Securing the physical components of the Vehicle-to-Grid (V2G) system, such as charging stations, with locks, surveillance cameras, and alarms, is an essential aspect of a comprehensive security strategy. While much attention is often given to cybersecurity measures, the physical security of the V2G infrastructure is equally vital. Physical tampering, unauthorized access, or theft of equipment can lead to serious disruptions, data breaches, or other malicious activities. Implementing robust physical security measures ensures the integrity, availability, and resilience of the V2G communication between Electric Vehicles (EVs) and the grid.

Locks are fundamental in controlling access to critical components such as charging stations, control panels, and communication devices. By restricting access to authorized personnel only, locks prevent unauthorized individuals from tampering with or altering the equipment. Surveillance cameras provide continuous monitoring and recording of the physical environment, allowing for the detection of suspicious activities, vandalism, or other potential threats. Alarms can be configured to trigger alerts or notifications in response to specific events, such as unauthorized access, providing timely warnings and enabling rapid response [214]–[216].

The implementation of physical security measures provides several benefits in the context of V2G security. First, it offers robust protection against physical tampering, theft, or vandalism, ensuring that the system's hardware components remain secure and functional. Second, it complements cybersecurity measures, providing a layered defense that addresses both virtual and physical threats. Third, it fosters compliance with regulatory requirements, industry standards, and best practices, demonstrating a comprehensive approach to security [217].

However, the implementation of physical security measures also presents challenges that must be carefully considered. The design and deployment of locks, surveillance cameras, and alarms must be tailored to the specific requirements, risks, and characteristics of the V2G infrastructure. Balancing the need for robust security with considerations for usability, aesthetics, and cost requires careful planning, expertise, and ongoing management. Collaboration with law enforcement, security experts, and other stakeholders is essential to ensure that the physical security measures are effective, compliant, and aligned with broader community and societal considerations [218]. The regulatory environment plays a vital role in guiding and overseeing the physical security of the V2G system. Governments and regulatory bodies must establish clear guidelines and standards that define the minimum requirements for physical security, monitoring, and compliance. Collaboration between different stakeholders, including manufacturers, energy providers, security experts, and policymakers, is essential to develop a cohesive approach that aligns with industry best practices and legal obligations [219].

Time-Stamping and Sequence Numbers

Preventing replay attacks in the Vehicle-to-Grid (V2G) system is crucial to maintaining the integrity and security of the communication between Electric Vehicles (EVs) and the grid. Replay attacks involve capturing valid data transmissions and replaying them at a later time to initiate unauthorized actions. To counter this threat, each transaction can be time-stamped or assigned a unique sequence number, and cryptographic hashes can be used to ensure that the data being transmitted has not been altered in transit [220]. Time-stamping involves adding a time marker to each transaction, indicating when it was created or sent. If a replayed transaction is detected, the time-stamp can be checked against the current time, and if the difference exceeds a certain threshold, the transaction can be rejected. Unique sequence numbers work similarly by assigning a one-time number to each transaction. If a transaction with a previously used sequence number is detected, it can be flagged as a replay and rejected.

Cryptographic hashes provide an additional layer of security by ensuring the integrity of the data being transmitted. A cryptographic hash function takes the data and produces a fixed-size string of bytes, typically a hash value. If even a single bit of the original data is changed, the hash value will change dramatically. By comparing the hash value of the received data with the hash value of the original data, the system can verify that the data has not been altered in transit [221].

The combination of time-stamping, unique sequence numbers, and cryptographic hashes provides a robust defense against replay attacks. It ensures that each transaction is uniquely tied to a specific time or sequence, and that the integrity of the data is maintained throughout the transmission. This not only prevents unauthorized actions but also enhances the overall trust and reliability of the V2G system.

However, the implementation of these measures also presents challenges that must be carefully considered. The management of time-stamps and sequence numbers requires synchronization and coordination across the system, which can be complex in a distributed and dynamic environment like V2G. Cryptographic hashes require careful selection and management of hash functions and keys to ensure their effectiveness and security. Balancing the need for robust protection against replay attacks with considerations for performance, usability, and cost requires careful planning, expertise, and ongoing management [222].

The regulatory environment plays a vital role in guiding and overseeing these measures in the V2G system. Governments and regulatory bodies must establish clear guidelines and standards that define the minimum requirements for preventing replay attacks, including the use of time-

stamps, sequence numbers, and cryptographic hashes. Collaboration between different stakeholders, including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that aligns with industry best practices and legal obligations [223].

Role-Based Access Control (RBAC)

Ensuring that only authorized personnel can access and modify the Vehicle-to-Grid (V2G) system is a foundational aspect of securing the communication between Electric Vehicles (EVs) and the grid. Unauthorized access or modifications can lead to serious disruptions, data breaches, unauthorized transactions, or other malicious activities. Implementing robust access control measures is vital to protect the integrity, confidentiality, and availability of the V2G system [224].

Access control involves defining and enforcing who can access the V2G system, what they can do once they have access, and under what circumstances they can perform those actions. This can be achieved through a combination of authentication, authorization, and auditing mechanisms. Authentication verifies the identity of the user, typically through usernames, passwords, tokens, or biometric data. Authorization determines what actions the authenticated user is allowed to perform, based on predefined roles, permissions, and policies. Auditing continuously monitors and records access and modification activities, providing accountability and enabling detection and response to potential violations [225].

The implementation of access control provides several benefits in the context of V2G security. First, it ensures that only authorized personnel, such as system administrators, operators, or maintenance staff, can access and modify the system, preventing unauthorized individuals from tampering with or altering the system. Second, it provides granularity and flexibility in defining access rights, allowing different levels of access and control based on roles, responsibilities, and needs. Third, it fosters compliance with regulatory requirements, industry standards, and best practices, demonstrating a comprehensive approach to security [226].

However, the implementation of access control also presents challenges that must be carefully managed. The complexity of the V2G ecosystem, involving various interconnected components, devices, and protocols, can make the coordination and enforcement of access control a complex task. Balancing the need for robust security with considerations for usability, efficiency, and cost requires careful planning, expertise, and ongoing management. Regular training and awareness programs are essential to ensure that all authorized personnel are aware of the risks, best practices, and their respective roles in maintaining security.

The regulatory environment plays a vital role in guiding and overseeing access control in the V2G system. Governments and regulatory bodies must establish clear guidelines and standards that define the minimum requirements for authentication, authorization, and auditing. Collaboration between different stakeholders [227], [228], including manufacturers, energy providers, cybersecurity experts, and policymakers, is essential to develop a cohesive approach that aligns with industry best practices and legal obligations [229].

Conclusion

Eavesdropping is a significant threat to Vehicle-to-Grid (V2G) systems, where unauthorized interception of communication between the Electric Vehicle (EV) and the grid can lead to the theft of sensitive data such as personal information, energy consumption patterns, and financial details [230]. The lack of robust encryption and secure communication channels can make the system susceptible to eavesdropping, compromising the privacy of the user and potentially

leading to other malicious activities. Man-in-the-Middle (MitM) attacks are particularly insidious in V2G systems. Attackers can intercept and alter the communication between the EV and the grid, leading to unauthorized energy transactions. By positioning themselves between the communicating parties, attackers can manipulate the information being exchanged, such as altering energy pricing or rerouting energy transfers, resulting in financial losses and undermining the integrity and reliability of the entire V2G system. DoS and DDoS attacks pose a significant threat to V2G systems. Attackers can flood the V2G system with excessive traffic, causing it to become slow or entirely unavailable. In a DDoS attack, multiple compromised systems are used to launch a coordinated assault, magnifying the impact. These attacks can disrupt the normal functioning of the energy grid, leading to outages and instability, and prevent EV owners from charging or discharging their vehicles. Physical tampering with the EV or grid infrastructure is another serious concern. Direct physical access to the components can lead to unauthorized modifications, data theft, or even physical damage. Attackers can alter the hardware, install malicious devices, or manipulate the system's configuration, leading to a wide range of problems, from incorrect energy transactions to complete system failure. Malware and firmware attacks can compromise the V2G system's operation by introducing malicious software into the system. This can be done through infected USB drives, malicious downloads, or other means. Once inside the system, the malware can alter the functioning of the V2G system, steal data, or provide remote access to attackers. Firmware attacks can embed malicious code at a deeper system level, making detection and removal more challenging. Replay attacks are a specific type of threat where attackers capture valid data transmissions and replay them to initiate unauthorized actions. In the context of V2G systems, this could mean replaying a legitimate energy transaction to gain unauthorized access to energy or financial benefits. Since the data being replayed is valid, it can be challenging to detect these attacks, and the captured data can be reused maliciously. False data injection and identity spoofing are interconnected threats that can cause significant harm to V2G systems. Attackers can send false data to the grid or the EV, causing incorrect energy transactions, or pretend to be a legitimate EV or grid entity to initiate unauthorized transactions. False data can lead to imbalances in the energy grid and financial losses, while identity spoofing can allow attackers to impersonate legitimate users or devices, gaining unauthorized access and control, and undermining the integrity and reliability of the V2G system [231].

Robust countermeasures are essential to secure Vehicle-to-Grid (V2G) systems from various threats and vulnerabilities. Implementing end-to-end encryption ensures that even if data is intercepted during transmission, it remains unreadable, thereby protecting sensitive information from unauthorized access. Authentication protocols are vital, where both the Electric Vehicle (EV) and the grid should authenticate each other before initiating any transaction. This can be achieved using cryptographic keys or certificates, ensuring that only legitimate entities can engage in energy transactions. Intrusion Detection Systems (IDS) play a crucial role in monitoring the V2G network for any suspicious activities, alerting system administrators to potential threats. Regular firmware updates are necessary to ensure that the V2G system's software is up to date, patching any known vulnerabilities that could be exploited by attackers. Implementing rate limiting is an effective strategy to prevent DoS or DDoS attacks, controlling the flow of traffic and maintaining the system's availability [232], [233]. Physical security measures are equally important, securing the physical components of the V2G system, such as charging stations, with locks, surveillance cameras, and alarms to deter tampering or theft. Time-stamping and sequence numbers can be used to prevent replay attacks, where each transaction can be time-stamped or assigned a unique sequence number, ensuring that captured data cannot be reused maliciously. Data integrity checks, using cryptographic hashes, ensure

that the data being transmitted has not been altered in transit, maintaining the accuracy and reliability of the information. Finally, Role-Based Access Control (RBAC) is essential to ensure that only authorized personnel can access and modify the V2G system, limiting the potential for unauthorized changes and maintaining the overall security and integrity of the system.

References

[1] 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.
[2] 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.
[3] J. Kim, J. Oh, and H. Lee, "Review on battery thermal management system for electric vehicles," *Appl. Therm. Eng.*, 2019.
[4] G. Samata, P. Sudhakar, and G. Jyothsna, "In silico Analysis of Spike Protein Glycoprotein A of Omicron variant and identification of variant specific peptide based Vaccine," *Research Journal of Biotechnology Vol*, vol. 18, p. 7, 2023.
[5] 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.
[6] E. Silvas, T. Hofman, and N. Murgovski, "Review of optimization strategies for system-level design in hybrid electric vehicles," *IEEE Transactions*, 2016.
[7] C. C. Chan, "An overview of electric vehicle technology," *Proc. IEEE*, vol. 81, no. 9, pp. 1202–1213, Sep. 1993.
[8] H. M. Khalid, Q. Ahmed, and J. C.-H. Peng, "Health monitoring of li-ion battery systems: A median expectation diagnosis approach (MEDA)," *IEEE Transactions on Transportation Electrification*, vol. 1, no. 1, pp. 94–105, 2015.
[9] S. S. Ravi and M. Aziz, "Utilization of Electric Vehicles for Vehicle-to-Grid Services: Progress and Perspectives," *Energies*, vol. 15, no. 2, p. 589, Jan. 2022.
[10] A. Aljarbouh and B. Caillaud, "On the regularization of chattering executions in real time simulation of hybrid systems," 2015, p. 49.
[11] V. Delgado-Gomes, J. F. Martins, C. Lima, and P. N. Borza, "Smart grid security issues," in *2015 9th International Conference on Compatibility and Power Electronics (CPE)*, 2015, pp. 534–538.
[12] P. Jokar, N. Arianpoo, and V. C. M. Leung, "A survey on security issues in smart grids," *Secur. Commun. Netw.*, vol. 9, no. 3, pp. 262–273, Feb. 2016.
[13] L. T. Berger and K. Iniewski, *Smart Grid Applications, Communications, and Security*. Nashville, TN: John Wiley & Sons, 2012.
[14] H. M. Khalid *et al.*, "Dust accumulation and aggregation on PV panels: An integrated survey on impacts, mathematical models, cleaning mechanisms, and possible sustainable solution," *Solar Energy*, vol. 251, pp. 261–285, 2023.
[15] X. Zeng, M. Li, D. Abd El-Hady, and W. Alshitari, "Commercialization of lithium battery technologies for electric vehicles," *Advanced Energy*, 2019.
[16] 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.

[17] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, Mar. 2020.
[18] S.-K. Kim and J.-H. Huh, "A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective," *Energies*, vol. 11, no. 8, p. 1973, Jul. 2018.
[19] C. Peng, H. Sun, and M. Yang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Transactions on*, 2019.
[20] S. Umamaheswar, L. G. Kathawate, W. B. Shirsath, S. Gadde, and P. Saradha, "Recent turmeric plants agronomy analysis and methodology using Artificial intelligence," *International Journal of Botany Studies*, vol. 7, no. 2, pp. 233–236, 2022.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] H. M. Khalid and J. C.-H. Peng, "Improved recursive electromechanical oscillations monitoring scheme: A novel distributed approach," *IEEE Trans. Power Syst.*, vol. 30, no. 2, pp. 680–688, 2014.
[26] 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.
[27] 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.
[28] C. Zhang, K. Li, and S. Mcloone, "Battery modelling methods for electric vehicles-A review," *2014 European Control*, 2014.
[29] A. Padma, S. Gadde, B. S. P. Rao, and G. Ramachandran, "Effective Cleaning System management using JSP and Servlet Technology," 2021, pp. 1472–1478.
[30] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart grid security: Threats, vulnerabilities and solutions," *Int. J. Smart Grid Clean Energy*, pp. 1–6, 2012.
[31] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, Fourth 2012.
[32] T. Flick and J. Morehouse, *Securing the smart grid: Next generation power grid security*. Syngress Publishing, 2014.
[33] S. Jahandari and D. Materassi, "Identification of dynamical strictly causal networks," 2018, pp. 4739–4744.
[34] T. Harighi, R. Bayindir, S. Padmanaban, and L. Mihet-Popa, "An overview of energy scenarios, storage systems and the infrastructure for vehicle-to-grid technology," *Energies*, 2018.
[35] A. Alsharif, C. W. Tan, R. Ayop, and A. A. A. Ahmed, "Energy management strategy for Vehicle-to-grid technology integration with energy sources: Mini review," *African Journal of*, 2022.
[36] 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.
[37] 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.

[38] 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.
[39] A. Aljarbouh and B. Caillaud, "Robust simulation for hybrid systems: chattering path avoidance," *arXiv preprint arXiv:1512.07818*, 2015.
[40] T. Baumeister, "Literature review on smart grid cyber security," *Development Laboratory at the University of …*, 2010.
[41] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.
[42] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Secur. Priv.*, vol. 7, no. 3, pp. 75–77, May 2009.
[43] H. M. Khalid, S. M. Muyeen, and I. Kamwa, "An improved decentralized finite-time approach for excitation control of multi-area power systems," *Sustainable Energy, Grids and Networks*, vol. 31, p. 100692, 2022.
[44] S. Iqbal *et al.*, "Aggregated Electric Vehicle-to-Grid for Primary Frequency Control in a Microgrid- A Review," in *2018 IEEE 2nd International Electrical and Energy Conference (CIEEC)*, 2018, pp. 563–568.
[45] C. Rodríguez, C. Vidal, M. Díaz, E. Contreras, G. Guggisberg, and I. Rivas, "An Overview of Challenges and Benefits Associated to the Development of Vehicle to Grid Technology," in *2021 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, 2021, pp. 1–6.
[46] M. Taiebat and M. Xu, "Synergies of four emerging technologies for accelerated adoption of electric vehicles: Shared mobility, wireless charging, vehicle-to-grid, and vehicle automation," *J. Clean. Prod.*, 2019.
[47] A. Duracz *et al.*, "Advanced hazard analysis and risk assessment in the ISO 26262 functional safety standard using rigorous simulation," 2020, pp. 108–126.
[48] V. Timmers and P. A. J. Achten, "Non-exhaust PM emissions from electric vehicles," *Atmos. Environ.*, 2016.
[49] J. De Santiago, H. Bernhoff, and B. Ekergård, "Electrical motor drivelines in commercial all-electric vehicles: A review," *IEEE Transactions*, 2011.
[50] S. Pelletier, O. Jabali, and G. Laporte, "50th anniversary invited article—goods distribution with electric vehicles: review and research perspectives," *Transportation science*, 2016.
[51] H. Vijayakumar, "Business Value Impact of AI-Powered Service Operations (AIServiceOps)," *Available at SSRN 4396170*, 2023.
[52] S. Jahandari, "Graph-theoretic Identification of Dynamic Networks." University of Minnesota, 2022.
[53] A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.
[54] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, Fourthquarter 2014.
[55] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Secur. Priv.*, vol. 8, no. 1, pp. 81–85, Jan. 2010.
[56] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 468–483, Dec. 2018.
[57] J. Mullan, D. Harries, T. Bräunl, and S. Whitely, "The technical, economic and commercial viability of the vehicle-to-grid concept," *Energy Policy*, vol. 48, pp. 394–406, Sep. 2012.

[58] S. Cundeva and A. Dimovski, "Vehicle-to-grid system used to regulate the frequency of a microgrid," in *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, 2017, pp. 456–460.
[59] A. Hashmi and M. T. Gul, "Integrating E-vehicle into the power system by the execution of vehicle-to-grid (V2G) terminology — A review," in *2018 International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, Pakistan, 2018, pp. 1–5.
[60] A. Aljarbouh, A. Duracz, Y. Zeng, B. Caillaud, and W. Taha, "Chattering-free simulation for hybrid dynamical systems," *HAL*, vol. 2016, 2016.
[61] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in Smart Grids," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2011, pp. 1–8.
[62] K. G. Boroojeni, M. Hadi Amini, and S. S. Iyengar, *Smart Grids: Security and Privacy Issues*. Springer International Publishing, 2017.
[63] A. R. Metke and R. L. Ekl, "Smart Grid security technology," in *2010 Innovative Smart Grid Technologies (ISGT)*, 2010, pp. 1–7.
[64] H. M. Khalid, S. M. Muyeen, and J. C.-H. Peng, "Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2054–2065, 2019.
[65] I. Lee and Wallarm Inc, "What is Eavesdropping Attack and How to prevent it?," 2023. [Online]. Available: https://www.wallarm.com/what/what-is-eavesdropping-attack-definition-types-and-prevention. [Accessed: 2023].
[66] S. Goel, R. Sharma, and A. K. Rathore, "A review on barrier and challenges of electric vehicle in India and vehicle to grid optimisation," *Period. Polytech. Trans. Eng.*, 2021.
[67] S. Tirunagari, M. Gu, and L. Meegahapola, "Reaping the Benefits of Smart Electric Vehicle Charging and Vehicle-to-Grid Technologies: Regulatory, Policy and Technical Aspects," *IEEE Access*, vol. 10, pp. 114657–114672, 2022.
[68] W. Choi *et al.*, "Reviews on grid-connected inverter, utility-scaled battery energy storage system, and vehicle-to-grid application - challenges and opportunities," in *2017 IEEE Transportation Electrification Conference and Expo (ITEC)*, 2017, pp. 203–210.
[69] S. Jahandari and D. Materassi, "Optimal observations for identification of a single transfer function in acyclic networks," 2021, pp. 852–857.
[70] A. S. Rajasekaran and M. Azees, "A comprehensive survey on security issues in vehicle-to-grid networks," *Journal of Control and*, 2023.
[71] M. Kumar, S. Vyas, and A. Datta, "A Review on Integration of Electric Vehicles into a Smart Power Grid and Vehicle-to-Grid Impacts," in *2019 8th International Conference on Power Systems (ICPS)*, 2019, pp. 1–5.
[72] T. A. Lehtola and A. Zahedi, "Electric vehicle battery cell cycle aging in vehicle to grid operations: A review," *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 9, no. 1, pp. 423–437, Feb. 2021.
[73] W. Hammad, T. O. Sweidan, M. I. Abuashour, H. M. Khalid, and S. M. Muyeen, "Thermal management of grid-tied PV system: A novel active and passive cooling design-based approach," *IET Renew. Power Gener.*, vol. 15, no. 12, pp. 2715–2725, 2021.
[74] K. Thiagarajan, C. K. Dixit, M. Panneerselvam, C. A. Madhuvappan, S. Gadde, and J. N. Shrote, "Analysis on the Growth of Artificial Intelligence for Application Security in Internet of Things," 2022, pp. 6–12.
[75] K. M. Tan, V. K. Ramachandaramurthy, and J. Y. Yong, "Integration of electric vehicles in smart grid: A review on vehicle to grid technologies and optimization techniques," *Renewable Sustainable Energy Rev.*, vol. 53, pp. 720–732, Jan. 2016.
[76] N. Naik and C. Vyjayanthi, "Optimization of Vehicle-to-Grid (V2G) Services for Development of Smart Electric Grid: A Review," in *2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, 2021, pp. 1–6.

[77] H. Yu, S. Niu, Y. Shang, Z. Shao, Y. Jia, and L. Jian, "Electric vehicles integration and vehicle-to-grid operation in active distribution grids: A comprehensive review on power architectures, grid connection standards and typical applications," *Renewable Sustainable Energy Rev.*, vol. 168, p. 112812, Oct. 2022.
[78] 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.
[79] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Trans. Power Delivery*, 2010.
[80] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," *IEEE PES general meeting*, 2010.
[81] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 981–997, 2012.
[82] 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.
[83] S. Ruj and A. Nayak, "A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 196–205, Mar. 2013.
[84] T. M. Chen, "Survey of cyber security issues in smart grids," *visual analytics for homeland defense and security …*, 2010.
[85] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," *2010-Milcom 2010 Military*, 2010.
[86] 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.
[87] S. Habib and M. Kamran, "A novel vehicle-to-grid technology with constraint analysis-a review," in *2014 International Conference on Emerging Technologies (ICET)*, 2014, pp. 69–74.
[88] M. A. Hannan *et al.*, "Vehicle to grid connected technologies and charging strategies: Operation, control, issues and recommendations," *J. Clean. Prod.*, vol. 339, p. 130587, Mar. 2022.
[89] A. Alsharif, C. W. Tan, R. Ayop, A. Dobi, and K. Y. Lau, "A comprehensive review of energy management strategy in Vehicle-to-Grid technology integrated with renewable energy sources," *Sustainable Energy Technologies and Assessments*, vol. 47, p. 101439, Oct. 2021.
[90] H. M. Khalid and J. C.-H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 697–707, 2015.
[91] A. Sharma and S. Sharma, "Review of power electronics in vehicle-to-grid systems," *Journal of Energy Storage*, vol. 21, pp. 337–361, Feb. 2019.
[92] S. Habib, M. Kamran, and U. Rashid, "Impact analysis of vehicle-to-grid technology and charging strategies of electric vehicles on distribution networks – A review," *J. Power Sources*, vol. 277, pp. 205–214, Mar. 2015.
[93] B. W. Zhou, T. Littler, and H. F. Wang, "The impact of vehicle-to-grid on electric power systems: A review," in *2nd IET Renewable Power Generation Conference (RPG 2013)*, 2013, pp. 1–4.
[94] 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.
[95] K. Thiagarajan, M. Porkodi, S. Gadde, and R. Priyadharshini, "Application and Advancement of Sensor Technology in Bioelectronics Nano Engineering," 2022, pp. 841–845.

[96] A. Alamin, H. M. Khalid, and J. C.-H. Peng, "Power system state estimation based on Iterative Extended Kalman Filtering and bad data detection using normalized residual test," 2015, pp. 1–5.
[97] F. Mwasilu, J. J. Justo, E.-K. Kim, T. D. Do, and J.-W. Jung, "Electric vehicles and smart grid interaction: A review on vehicle to grid and renewable energy sources integration," *Renewable Sustainable Energy Rev.*, vol. 34, pp. 501–516, Jun. 2014.
[98] H. Khayyam, H. Ranjbarzadeh, and V. Marano, "Intelligent control of vehicle to grid power," *J. Power Sources*, vol. 201, pp. 1–9, Mar. 2012.
[99] 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.
[100] Y. Zhou and X. Li, "Vehicle to grid technology: A review," in *2015 34th Chinese Control Conference (CCC)*, 2015, pp. 9031–9036.
[101] B. Kramer, S. Chakraborty, and B. Kroposki, "A review of plug-in vehicles and vehicle-to-grid capability," in *2008 34th Annual Conference of IEEE Industrial Electronics*, 2008, pp. 2278–2283.
[102] D. Lauinger, F. Vuille, and D. Kuhn, "A review of the state of research on vehicle-to-grid (V2G): Progress and barriers to deployment," in *Proceedings of European Battery, Hybrid and Fuel Cell Electric Vehicle Congress*, 2017.
[103] A. J. Albarakati *et al.*, "Real-time energy management for DC microgrids using artificial intelligence," *Energies*, vol. 14, no. 17, p. 5307, 2021.
[104] 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.
[105] C. Liu, K. T. Chau, D. Wu, and S. Gao, "Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies," *Proc. IEEE*, 2013.
[106] M. Yilmaz and P. T. Krein, "Review of the Impact of Vehicle-to-Grid Technologies on Distribution Systems and Utility Interfaces," *IEEE Trans. Power Electron.*, vol. 28, no. 12, pp. 5673–5689, Dec. 2013.
[107] B. K. Sovacool, J. Kester, L. Noel, and G. Zarazua de Rubens, "Are electric vehicles masculinized? Gender, identity, and environmental values in Nordic transport practices and vehicle-to-grid (V2G) preferences," *Transp. Res. Part D: Trans. Environ.*, vol. 72, pp. 187–202, Jul. 2019.
[108] H. M. Khalid and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, 2016.
[109] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct.*, 2019.
[110] A. Anwar and A. N. Mahmood, "Cyber security of smart grid infrastructure," *arXiv preprint arXiv:1401.3936*, 2014.
[111] Z. Ni and S. Paul, "A Multistage Game in Smart Grid Security: A Reinforcement Learning Solution," *IEEE Trans Neural Netw Learn Syst*, vol. 30, no. 9, pp. 2684–2695, Sep. 2019.
[112] M. Coffman, P. Bernstein, and S. Wee, "Electric vehicles revisited: a review of factors that affect adoption," *Transp. Rev.*, vol. 37, no. 1, pp. 79–93, Jan. 2017.
[113] G. Harper *et al.*, "Recycling lithium-ion batteries from electric vehicles," *Nature*, vol. 575, no. 7781, pp. 75–86, Nov. 2019.
[114] M. Ehsani, Y. Gao, and J. M. Miller, "Hybrid Electric Vehicles: Architecture and Motor Drives," *Proc. IEEE*, vol. 95, no. 4, pp. 719–728, Apr. 2007.
[115] S. Jahandari and A. Srivastava, "Adjusting for Unmeasured Confounding Variables in Dynamic Networks," *IEEE Control Systems Letters*, vol. 7, pp. 1237–1242, 2023.

[116] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali, "Smart grid cyber security: Challenges and solutions," in *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, 2015, pp. 170–175.
[117] I. L. G. Pearson, "Smart grid cyber security for Europe," *Energy Policy*, 2011.
[118] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of Security Advances in Smart Grid: A Data Driven Approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, Firstquarter 2017.
[119] A. Aljarbouh, "Accelerated simulation of hybrid systems: method combining static analysis and run-time execution analysis." Rennes 1, 2017.
[120] E. Aljdaeh *et al.*, "Performance enhancement of self-cleaning hydrophobic nanocoated photovoltaic panels in a dusty environment," *Energies*, vol. 14, no. 20, p. 6800, 2021.
[121] M. İnci, M. M. Savrun, and Ö. Çelik, "Integrating electric vehicles as virtual power plants: A comprehensive review on vehicle-to-grid (V2G) concepts, interface topologies, marketing and future prospects," *Journal of Energy Storage*, vol. 55, p. 105579, Nov. 2022.
[122] M. Yilmaz and P. T. Krein, "Review of benefits and challenges of vehicle-to-grid technology," in *2012 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2012, pp. 3082–3089.
[123] B. K. Sovacool, L. Noel, J. Axsen, and W. Kempton, "The neglected social dimensions to a vehicle-to-grid (V2G) transition: a critical and systematic review," *Environ. Res. Lett.*, vol. 13, no. 1, p. 013001, Jan. 2018.
[124] B. K. Sovacool, J. Axsen, and W. Kempton, "The Future Promise of Vehicle-to-Grid (V2G) Integration: A Sociotechnical Review and Research Agenda," *Annu. Rev. Environ. Resour.*, vol. 42, no. 1, pp. 377–406, Oct. 2017.
[125] S. S. Devi, S. Gadde, K. Harish, C. Manoharan, R. Mehta, and S. Renukadevi, "IoT and image processing Techniques-Based Smart Sericulture Nature System," *Indian J. Applied & Pure Bio*, vol. 37, no. 3, pp. 678–683, 2022.
[126] S. Jahandari, A. Kalhor, and B. N. Araabi, "Online forecasting of synchronous time series based on evolving linear models," *IEEE Trans. Syst. Man Cybern.*, vol. 50, no. 5, pp. 1865–1876, 2018.
[127] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia Comput. Sci.*, 2014.
[128] Y. Wang, D. Ruan, D. Gu, J. Gao, and D. Liu, "Analysis of smart grid security standards," *2011 IEEE*, 2011.
[129] E. Bou-Harb, C. Fachkha, and M. Pourzandi, "Communication security for smart grid distribution networks," *IEEE*, 2013.
[130] H. M. Khalid and J. C.-H. Peng, "Tracking electromechanical oscillations: An enhanced maximum-likelihood based approach," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 1799–1808, 2015.
[131] 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.
[132] H. M. Khalid *et al.*, "WAMS operations in power grids: A track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks," *IEEE Syst. J.*, 2023.
[133] H. M. Khalid, F. Flitti, M. S. Mahmoud, M. M. Hamdan, S. M. Muyeen, and Z. Y. Dong, "Wide area monitoring system operations in modern power grids: A median regression function-based state estimation approach towards cyber attacks," *Sustainable Energy, Grids and Networks*, vol. 34, p. 101009, 2023.
[134] S. Gadde, E. Karthika, R. Mehta, S. Selvaraju, W. B. Shirsath, and J. Thilagavathi, "Onion growth monitoring system using internet of things and cloud," *Agricultural and Biological Research*, vol. 38, no. 3, pp. 291–293, 2022.

[135] N. Osman, H. M. Khalid, O. S. Tha'er, M. I. Abuashour, and S. M. Muyeen, "A PV powered DC shunt motor: Study of dynamic analysis using maximum power Point-Based fuzzy logic controller," *Energy Conversion and Management: X*, vol. 15, p. 100253, 2022.
[136] A. Aljarbouh, "Non-standard zeno-free simulation semantics for hybrid dynamical systems," 2019, pp. 16–31.
[137] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Syst. J.*, vol. 13, no. 1, pp. 710–719, 2017.
[138] E. Santacana, G. Rackliffe, and L. Tang, "Getting smart," *IEEE Power Energ. Mag.*, 2010.
[139] F. Skopik and P. D. Smith, "Smart grid security: Innovative solutions for a modernized grid," 2015.
[140] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *SoutheastCon 2015*, 2015, pp. 1–6.
[141] M. Sathanapriya *et al.*, "Analysis of Hydroponic System Crop Yield Prediction and Crop IoT-based monitoring system for precision agriculture," 2022, pp. 575–578.
[142] H. M. Khalid, Q. Ahmed, J. C.-H. Peng, and G. Rizzoni, "Pack-level current-split estimation for health monitoring in Li-ion batteries," 2016, pp. 1506–1511.
[143] 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.
[144] D. Al Momani *et al.*, "Energy saving potential analysis applying factory scale energy audit–A case study of food production," *Heliyon*, vol. 9, no. 3, 2023.
[145] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on Smart Grid," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2011, pp. 1–7.
[146] F. Dalipi and S. Y. Yayilgan, "Security and privacy considerations for IoT application on smart grids: Survey and research challenges," *Conference on Future Internet of Things …*, 2016.
[147] A. Sanjab, W. Saad, I. Guvenc, and A. Sarwat, "Smart grid security: Threats, challenges, and solutions," *arXiv preprint arXiv*, 2016.
[148] S. Jahandari and D. Materassi, "How Can We Be Robust Against Graph Uncertainties?," 2023, pp. 1946–1951.
[149] H. M. Khalid, Q. Ahmed, J. C.-H. Peng, and G. Rizzoni, "Current-split estimation in Li-ion battery pack: An enhanced weighted recursive filter method," *IEEE Transactions on Transportation Electrification*, vol. 1, no. 4, pp. 402–412, 2015.
[150] N. Sharmili *et al.*, "Earthworm Optimization with Improved SqueezeNet Enabled Facial Expression Recognition Model," *Computer Systems Science & Engineering*, vol. 46, no. 2, 2023.
[151] 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.
[152] L. Kotut and L. A. Wahsheh, "Survey of Cyber Security Challenges and Solutions in Smart Grids," in *2016 Cybersecurity Symposium (CYBERSEC)*, 2016, pp. 32–37.
[153] G. N. Sorebo and M. C. Echols, *Smart grid security: An end-to-end view of security in the new electrical grid*. Boca Raton, FL: CRC Press, 2011.
[154] S. Goel, Y. Hong, V. Papakonstantinou, and D. Kloza, "Smart grid security," 2015.
[155] S. Jahandari, A. Kalhor, and B. N. Araabi, "A self tuning regulator design for nonlinear time varying systems based on evolving linear models," *Evolving Systems*, vol. 7, pp. 159–172, 2016.

[156] 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.
[157] 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.
[158] J. Sakhnini, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," *Internet of things*, 2021.
[159] Z. El Mrabet, N. Kaabouch, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Electr. Eng.*, 2018.
[160] K. G. Boroojeni, M. H. Amini, and S. S. Iyengar, "Overview of the security and privacy issues in smart grids," *Smart grids: security and*, 2017.
[161] 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.
[162] R. Vargas, A. Mosavi, and R. Ruiz, "Deep learning: a review," 2017.
[163] X.-W. Chen and X. Lin, "Big Data Deep Learning: Challenges and Perspectives," *IEEE Access*, vol. 2, pp. 514–525, 2014.
[164] E. Lee, F. Rabbi, H. Almashaqbeh, A. Aljarbouh, J. Ascencio, and N. V. Bystrova, "The issue of software reliability in program code cloning," 2023, vol. 2700.
[165] H. Vijayakumar, A. Seetharaman, and K. Maddulety, "Impact of AIServiceOps on Organizational Resilience," 2023, pp. 314–319.
[166] 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.
[167] Z. Niu, G. Zhong, and H. Yu, "A review on the attention mechanism of deep learning," *Neurocomputing*, vol. 452, pp. 48–62, Sep. 2021.
[168] W. Wang, M. Zhang, G. Chen, H. V. Jagadish, B. C. Ooi, and K.-L. Tan, "Database Meets Deep Learning: Challenges and Opportunities," *SIGMOD Rec.*, vol. 45, no. 2, pp. 17–22, Sep. 2016.
[169] D. Ghelani, "Cyber Security in Smart Grids, Threats, and Possible Solutions," *Authorea Preprints*, 2022.
[170] Y. Mo *et al.*, "Cyber–Physical Security of a Smart Grid Infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
[171] C. Clastres, "Smart grids: Another step towards competition, energy security and climate change objectives," *Energy Policy*, vol. 39, no. 9, pp. 5399–5408, Sep. 2011.
[172] M. Coşkun *et al.*, "An overview of popular deep learning methods," *Eur. J. Tech.*, vol. 7, no. 2, pp. 165–176, Dec. 2017.
[173] X. Hu, L. Chu, J. Pei, W. Liu, and J. Bian, "Model complexity of deep learning: a survey," *Knowl. Inf. Syst.*, vol. 63, no. 10, pp. 2585–2619, Oct. 2021.
[174] X. Wang, Y. Zhao, and F. Pourpanah, "Recent advances in deep learning," *International Journal of Machine Learning and Cybernetics*, vol. 11, no. 4, pp. 747–750, Apr. 2020.
[175] H. Vijayakumar, "Revolutionizing Customer Experience with AI: A Path to Increase Revenue Growth Rate," 2023, pp. 1–6.
[176] S. Yonbawi *et al.*, "Modified Metaheuristics with Transfer Learning Based Insect Pest Classification for Agricultural Crops," *Computer Systems Science & Engineering*, vol. 46, no. 3, 2023.
[177] T. Serre, "Deep Learning: The Good, the Bad, and the Ugly," *Annu Rev Vis Sci*, vol. 5, pp. 399–426, Sep. 2019.
[178] H. Wang and B. Raj, "On the Origin of Deep Learning," *arXiv [cs.LG]*, 24-Feb-2017.

[179] Z. Rafique, H. M. Khalid, and S. M. Muyeen, "Communication systems in distributed generation: A bibliographical review and frameworks," *IEEE Access*, vol. 8, pp. 207226–207239, 2020.
[180] A. Voulodimos, N. Doulamis, A. Doulamis, and E. Protopapadakis, "Deep Learning for Computer Vision: A Brief Review," *Comput. Intell. Neurosci.*, vol. 2018, p. 7068349, Feb. 2018.
[181] A. C. Mater and M. L. Coote, "Deep Learning in Chemistry," *J. Chem. Inf. Model.*, vol. 59, no. 6, pp. 2545–2559, Jun. 2019.
[182] 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.
[183] Y. Liang and W. Liang, "ResWCAE: Biometric Pattern Image Denoising Using Residual Wavelet-Conditioned Autoencoder," *arXiv preprint arXiv:2307.12255*, 2023.
[184] J. Schmidhuber, "Deep learning in neural networks: an overview," *Neural Netw.*, vol. 61, pp. 85–117, Jan. 2015.
[185] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.
[186] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, p. 108975, Feb. 2023.
[187] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electric Power Systems Research*, vol. 149, pp. 210–219, Aug. 2017.
[188] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 46–52, Aug. 2012.
[189] S. Jahandari and D. Materassi, "Analysis and compensation of asynchronous stock time series," 2017, pp. 1085–1090.
[190] 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.
[191] Z. Bai, R. Yang, and Y. Liang, "Mental task classification using electroencephalogram signal," *arXiv preprint arXiv:1910.03023*, 2019.
[192] Y. Liang, W. Liang, and J. Jia, "Structural Vibration Signal Denoising Using Stacking Ensemble of Hybrid CNN-RNN," *arXiv e-prints*, p. arXiv-2303, 2023.
[193] F. Liao, E. Molin, and B. van Wee, "Consumer preferences for electric vehicles: a literature review," *Transp. Rev.*, 2017.
[194] T. R. Hawkins, O. M. Gausen, and A. H. Strømman, "Environmental impacts of hybrid and electric vehicles—a review," *Int. J. Life Cycle Assess.*, vol. 17, no. 8, pp. 997–1014, Sep. 2012.
[195] C. C. Chan and Y. S. Wong, "Electric vehicles charge forward," *IEEE Power Energ. Mag.*, vol. 2, no. 6, pp. 24–33, Nov. 2004.
[196] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — the new and improved power grid: A survey," *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 944–980, Fourth 2012.
[197] X. Li, X. Liang, R. Lu, X. Shen, and X. Lin, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications*, 2012.
[198] S. N. Islam, Z. Baig, and S. Zeadally, "Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures," *IEEE Trans. Ind. Inf.*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019.
[199] S. Min, B. Lee, and S. Yoon, "Deep learning in bioinformatics," *Brief. Bioinform.*, vol. 18, no. 5, pp. 851–869, Sep. 2017.

[200] A. Kamilaris and F. X. Prenafeta-Boldú, "Deep learning in agriculture: A survey," *Comput. Electron. Agric.*, vol. 147, pp. 70–90, Apr. 2018.
[201] S. Jahandari and D. Materassi, "Topology identification of dynamical networks via compressive sensing," *IFAC-PapersOnLine*, vol. 51, no. 15, pp. 575–580, 2018.
[202] S. Alahmari *et al.*, "Hybrid Multi-Strategy Aquila Optimization with Deep Learning Driven Crop Type Classification on Hyperspectral Images," *Comput. Syst. Sci. Eng.*, vol. 47, no. 1, pp. 375–391, 2023.
[203] A. Aljarbouh, "Selection of the optimal set of versions of N-version software using the ant colony optimization," 2021, vol. 2094, p. 032026.
[204] H. M. Khalid and J. C.-H. Peng, "Bidirectional charging in V2G systems: An in-cell variation analysis of vehicle batteries," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3665–3675, 2020.
[205] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. M. Muyeen, "Denial-of-service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways," *Sensors* , vol. 21, no. 19, p. 6415, 2021.
[206] M. S. Mahmoud, H. M. Khalid, and M. M. Hamdan, *Cyberphysical infrastructures in power systems: architectures and vulnerabilities*. Academic Press, 2021.
[207] 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.
[208] Z. Said *et al.*, "Intelligent approaches for sustainable management and valorisation of food waste," *Bioresour. Technol.*, p. 128952, 2023.
[209] 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.
[210] J. Y. Kim and Y. Kim, "Benefits of cloud computing adoption for smart grid security from security perspective," *J. Supercomput.*, 2016.
[211] M. K. Hasan, A. Habib, Z. Shukur, and F. Ibrahim, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and*, 2023.
[212] C. P. Vineetha and C. A. Babu, "Smart grid challenges, issues and solutions," *Green Building and Smart Grid …*, 2014.
[213] A. J. Albarakati *et al.*, "Microgrid energy management and monitoring systems: A comprehensive review," *Frontiers in Energy Research*, vol. 10, p. 1097858, 2022.
[214] M. Atalay and P. Angin, "A Digital Twins Approach to Smart Grid Security Testing and Standardization," in *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*, 2020, pp. 435–440.
[215] S. Bera, S. Misra, and J. J. P. C. Rodrigues, "Cloud Computing Applications for Smart Grid: A Survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1477–1494, May 2015.
[216] Q. Wang, G. Zhang, and F. Wen, "A survey on policies, modelling and security of cyber-physical systems in smart grids," *Energy Convers. Econ.*, vol. 2, no. 4, pp. 197–211, Dec. 2021.
[217] 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.
[218] 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.
[219] S. Jahandari and A. Srivastava, "Detection of Delays and Feedthroughs in Dynamic Networked Systems," *IEEE Control Systems Letters*, vol. 7, pp. 1201–1206, 2022.
[220] Y. Zhu *et al.*, "Application of Physics-Informed Neural Network (PINN) in the Experimental Study of Vortex-Induced Vibration with Tunable Stiffness," in *The 33rd International Ocean and Polar Engineering Conference*, 2023.

[221] W. Liang, Y. Liang, and J. Jia, "MiAMix: Enhancing Image Classification through a Multi-stage Augmented Mixied Sample Data Augmentation Method," *arXiv preprint arXiv:2308.02804*, 2023.
[222] A. S. Musleh, M. Debouza, H. M. Khalid, and A. Al-Durra, "Detection of false data injection attacks in smart grids: A real-time principle component analysis," 2019, vol. 1, pp. 2958–2963.
[223] S. Jahandari, A. Kalhor, and B. N. Araabi, "Order determination and robust adaptive control of unknown deterministic input-affine systems: An operational controller," 2016, pp. 3831–3836.
[224] H. M. Khalid, F. Flitti, S. M. Muyeen, M. S. Elmoursi, O. S. Tha'er, and X. Yu, "Parameter estimation of vehicle batteries in V2G systems: An exogenous function-based approach," *IEEE Trans. Ind. Electron.*, vol. 69, no. 9, pp. 9535–9546, 2021.
[225] Y. Boujoudar *et al.*, "Fuzzy logic-based controller of the bidirectional direct current to direct current converter in microgrid," *Int. J. Elect. Computer Syst. Eng.*, vol. 13, no. 5, pp. 4789–4797, 2023.
[226] Z. Rafique, H. M. Khalid, S. M. Muyeen, and I. Kamwa, "Bibliographic review on power system oscillations damping: An era of conventional grids and renewable energy integration," *Int. J. Electr. Power Energy Syst.*, vol. 136, p. 107556, 2022.
[227] P. P. Shinde and S. Shah, "A Review of Machine Learning and Deep Learning Applications," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018, pp. 1–6.
[228] Y. Guo, Y. Liu, A. Oerlemans, S. Lao, S. Wu, and M. S. Lew, "Deep learning for visual understanding: A review," *Neurocomputing*, vol. 187, pp. 27–48, Apr. 2016.
[229] 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.
[230] 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.
[231] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects," *Electronics*, vol. 11, no. 9, p. 1502, 2022.
[232] S. M. Shariff, D. Iqbal, M. Saad Alam, and F. Ahmad, "A State of the Art Review of Electric Vehicle to Grid (V2G) technology," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 561, no. 1, p. 012103, Oct. 2019.
[233] B. K. Sovacool, J. Kester, L. Noel, and G. Zarazua de Rubens, "Actors, business models, and innovation activity systems for vehicle-to-grid (V2G) technology: A comprehensive review," *Renewable Sustainable Energy Rev.*, vol. 131, p. 109963, Oct. 2020.