Defence Technology 42 (2024) 31–58

Contents lists available at ScienceDirect

Defence Technology

journal homepage: www.keaipublishing.com/en/journals/defence-technology

A comprehensive survey of cyberattacks on EVs: Research domains, attacks, defensive mechanisms, and verification methods

Tawfiq Aljohani [a], Abdulaziz Almutairi [b, *]

[a] Department of Electrical Engineering, College of Engineering at Yanbu, Taibah University, Yanbu, 41911, Saudi Arabia
[b] Department of Electrical Engineering, College of Engineering, Majmaah University, Almajmaah, 11952, Saudi Arabia

ARTICLE INFO

Article history:
Received 13 March 2024
Received in revised form
15 May 2024
Accepted 16 June 2024
Available online 18 June 2024

Keywords:
Cybersecurity
Electric vehicles
Charging stations
Cybersecurity of energy systems
Cyberattacks

ABSTRACT

With the continuous development of transportation electrification, the cybersecurity of energy infrastructure has become increasingly prominent. Explicitly, EVs resemble a significant tool to carryout cyberattacks since EVs are not only seen as dynamic loads but also as mobile energy sources that establish two-way communications with several players in the grid. This taxonomy aims to provide a comprehensive overview of cyberattacks against EVs from four distinct perspectives. The first is the research domains of EVs application, which investigates the different fields of research related to the development and application of EVs and how they are susceptible to cyber threats. The second is the CIA-based attacks, which examines the threats to the confidentiality, integrity, and availability of EVs' sensitive information and critical systems. The third taxonomy discusses the countermeasures and defensive mechanisms to secure the EVs against cyberattacks, including preventive measures, detection algorithms, response strategy, and recovery techniques. The fourth taxonomy is the verification and validation methodologies, which explores the software tools and hardware testbeds used to test and evaluate the security of EVs against cyber threats. Finally, this taxonomy presents an understanding of the current state of cyberattacks against EVs and serves as a valuable resource for researchers and practitioners in the fields of cybersecurity and electric mobility.

1. Introduction

Transportation electrification is critical to combat climate change and Greenhouse Gases (GHG) emissions. While electric vehicles (EVs) are pivotal to achieving sustainability goals via cutting the emissions from the two primary emitting industries, namely the electric power and transportation sectors, their large-scale integration into the energy grid poses indefinite cyber-physical security challenges. Not only do such threats impose disastrous impacts on the power and energy infrastructure, but they could also lead to life-threatening scenarios for the EVs owners.

The emergence of the smart grid concept requires the establishment of extensive communication infrastructures, paving the way toward more vulnerabilities due to heavy reliance on digital integration. The idea of a self-healing and -aware energy grid, with thousands of integrated components possessing two-way communication channels, is nothing short of futuristic [1]. The main objective is to create an intelligent grid that provides fully optimized energy consumption and management, resulting in reliable, affordable, and scalable energy services. But this utopian vision comes with a significant challenge, as the smart grid's dependence on networking and millions of information exchanges leaves it vulnerable to cyber threats. Minor intrusion attacks by adversaries can have devastating effects on smart grid components, putting its consumers at high risk [2]. The integration of millions of EVs into power grids further exacerbates the cybersecurity risks, where hackers can exploit them as new attack vectors, posing significant threats to the smart grid's security. The desire to disrupt energy grids using cyberattacks may have political, social or military goals behind them Refs. [3,4].

In contrast to internal combustion vehicles (ICVs), EVs pose novel challenges in the realm of cyber-physical systems as connected devices. Research in cybersecurity of EVs remains highly underexplored and still in its early stages. However, recent

* Corresponding Author
E-mail address: ad.almutiri@mu.edu.sa (A. Almutairi).
Peer review under responsibility of China Ordnance Society

https://doi.org/10.1016/j.dt.2024.06.009

attention has been given to this topic due to the potential catastrophic outcomes for both drivers and service providers. In addition to compromising personal privacy and safety, such attacks may destabilize the energy grid, posing a series threat to the overall viability of EVs as a reliable and promising technology. Additionally, cybersecurity measures are crucial for the widespread adoption of EVs as cyberattacks may result in significant economic loss, energy manipulation, and data piracy, potentially putting lives at risk and eroding trust in EVs. Therefore, investing in robust and secure EV infrastructure that can detect and mitigate cyber threats is a necessity [4,5].

While recent literature started recently to address the cybersecurity within EVs domains, there remains a significant gap in comprehensive analysis of cyberthreats across the entire EV paradigm. Many survey studies tend to focus on specific applications without offering an overarching view. For instance, the focus might be narrowly placed on intrusion detection systems (IDS) within vehicle networks [6]; vulnerabilities associated with EV charging processes, particularly on-board charging modules [7–10]; cyber challenges in powertrain systems [11]; intra-vehicle communications [12] or V2X communications [13]. Recognizing this gap, this work contributes a detailed, multifaceted four-way taxonomic analysis of the cybersecurity challenges specific to EVs. The study is driven by the crucial need for a structured and comprehensive taxonomy that categorizes and clarifies in an organized fashion the diverse cybersecurity issue within various EVs domains, addressing the evident lack of such structured analysis in existing research. This approach not only highlights the breadth and depth of potential cyberthreats but also systematically organizes them, providing a clear path forward in this field. Hence, the major contribution of this work is as follow:

1) Research Domains Exploration: Comprehensive investigation into the multifaceted cybersecurity-related research domains associated with EVs:
   - Charging infrastructure dynamics and vulnerabilities.
   - The intricacies of communication infrastructure and security protocols tailored for EVs.
   - Detailed examination of powertrains and power electronics components integral to EV operation.
   - Probing into pertinent data privacy issues surrounding EVs.
   - Scrutiny of the evolving landscape of standardization and established protocols for EVs.
2) CIA-based Threat Analysis: A meticulous assessment of threats targeting the confidentiality, integrity, and availability (CIA) within EVs' critical systems and sensitive information, laying the groundwork for potential countermeasures.
3) Defensive Techniques and Countermeasures: Formulation of a holistic taxonomy detailing defense mechanisms against cyberattacks on EVs. The defensive spectrum encompasses preventive measures, detection algorithms, strategic response frameworks, and advanced recovery techniques.
4) Verification and Validation Framework: Exploration of both software tools and hardware testbeds. These are the tools employed in reported literature to rigorously test, verify, and validate the security robustness of EVs against looming cyberthreats.

To ensure a thorough exploration of existing literature on cybersecurity issues in EVs, the search, covering literature from 2008 to 2024, used keywords like "Electric Vehicles Cybersecurity", "EV Charging Stations Security", "Vehicle-to-Grid (V2G) Security", "EV Cyberattacks" in addition to famous list of cyberattacks like Sybil Attacks, Denial of Service (DoS), False Data Injection (FDI), Spoofing, Replay, Man-in-the-Middle (MITM), and so on. Academic databases such as ScienceDirect, IEEE Xplore, SpringerLink, ACM Digital Library, Web of Science, and Google Scholar were utilized. An initial set of 340 papers was identified and then screened through a multi-step process. After title and abstract screening, and a full-text review focusing on relevance to the EV cybersecurity paradigm, 204 papers were selected. Fig. 1 presents a roadmap of the discussed taxonomy, visualizing the paper's structure and discussed topics, while Fig. 2 presents an illustration of the topics covered in the first taxonomy, the cybersecurity of the EV-related research domains.

2. Taxonomy of the cybersecurity threats within the electric vehicles applications

2.1. First taxonomy: research-domains taxonomy

2.1.1. Charging infrastructure

The Electric Vehicle Charging Station (EVCS) is the interface that allows EVs to integrate to the power grid for either charging or discharging processes. A cyberattack on EVCS may take the following scenarios: 1) an EV is plugged-in for either charging or discharging in an EVCS that is either a stand-alone station or a station connected to the local power grid; then, 2) the EV is compromised by a cyberattack of which the hacker successfully gain control over the EV. In such a situation, the following security concerns may arise:

i) Using the compromised EV, the hacker may have the capacity to gain access to the local energy grids or could hold the EV ransom by taking control over one or more of the EV's functionalities.
ii) The hacker might manipulate the charging process of the EV, which leads to horrendous consequences such as equipment failure, thermal runaway, energy requirements manipulation …, etc.
iii) The attacker might consider obstructing the charging/discharging process of the EV via the successful launch of a Denial of Service (DoS) attack, which may lead to destabilization of the local grid if the attack is achieved considering many EVs at once.

The EVCS can be described in terms of its physical and cyber layers. The physical layer of EVCS is comprised of power protection equipment, controllers, sensors, communication devices that support the vehicle charging requests such as power line communication (PLC), power electronics circuits, advanced metering infrastructure devices, to name a few. While the physical layer is not vulnerable to cyberattacks, the communication links that govern the cyber layer of EVCS are highly susceptible to cyberthreats. These threats can cause significant damage to the physical layer components. The cyber interdependencies that integrate the EV with the power grid via EVCS include communication links, internet services portals, in-vehicle embedded electronics devices, on-board charging controller (OBC), conventional power factor correction (PFC) circuits, human-machine interfaces (HMIs), radio interference devices, and original equipment manufacturers (OEMs). The primary goal of hackers targeting EVCS is to manipulate the performance of the charging/discharging process or lead to severe damage to the involved components.

The On-Board Charger (OBC) is a critical component of EVs, primarily responsible for converting the AC input from the EVCS into the DC voltage required to charge the battery pack. The OBC is structured in two stages: a Power Factor Correction (PFC) stage followed by an isolated DC-DC converter. Cyber vulnerabilities of the OBC are categorized into hardware-based and control-based

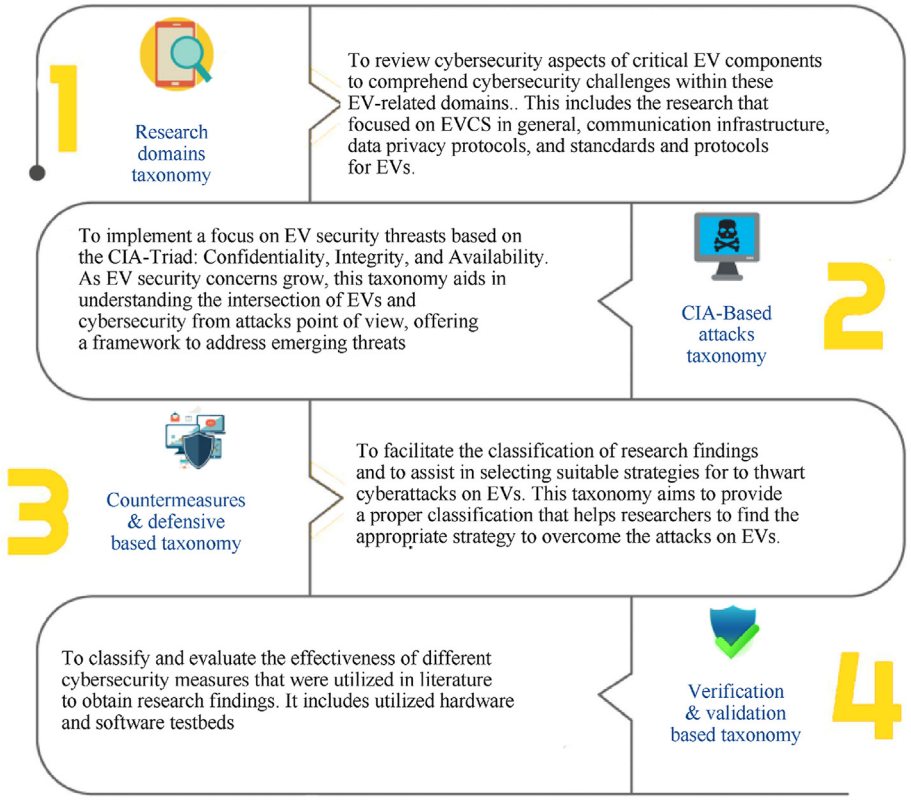

Fig. 1. Roadmap of the taxonomy presented in this work.

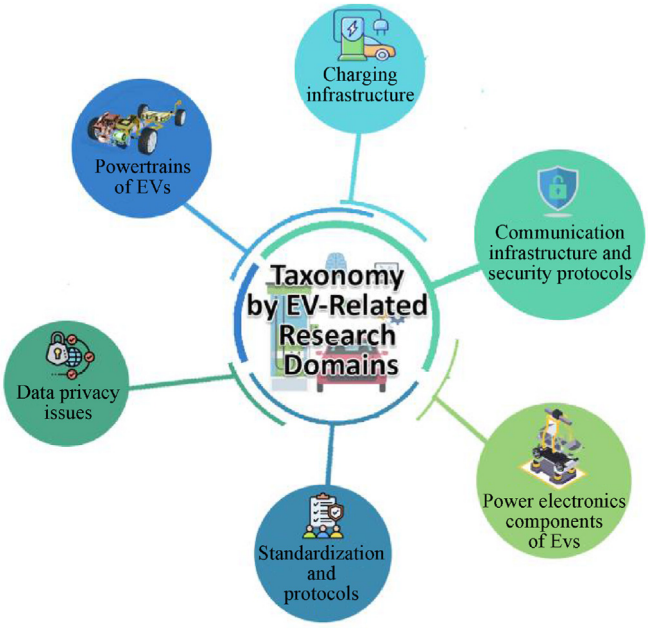

Fig. 2. Classification of the research domains-based taxonomy.

issues. The latter focuses on the Field Programmable Gate Array (FPGA), crucial for maintaining continuous power supply and optimal component temperature [8]. A key vulnerability lies in the Controller Area Network (CAN) protocol, which, despite its widespread use for in-vehicle communications, lacks effective message authentication, making it prone to cyberattacks. To address this, researchers in Ref. [14] developed an enhanced bat algorithm to optimize anomaly detection in CAN traffic. Moreover, attackers targeting the OBC might corrupt its data integrity, leading to unauthorized manipulations of EV charging data. Such attacks could alter battery charging protocols, inject false data into controllers or sensors connected to the OBC circuit. An empirical investigation detailed in Ref. [15] highlighted severe impacts of these threats, where data tampering led to a sharp decrease in battery efficiency, shown by a 70% increase in harmonic distortion and a 300% rise in torque and speed ripples. These disruptions not only degrade the OBC's performance but may also pose significant safety risks.

Power converters are essential in EVCS, converting AC power from the grid into DC power for EV batteries. Typically, primary-side power converters in EVCS shut off post-charging, ensuring a safe vehicle disconnect on the secondary side. This sequence depends crucially on the communication between the OBC and the station's converters. Yet, external interference with these communications can pose substantial risks. Cyber threats might manipulate disconnection timings or falsely indicate the presence of EVs, potentially causing extensive damage. To explore these risks, researchers in Ref. [16] conducted a study on the vulnerabilities of wireless, fast-charging EVCS. Their findings highlighted severe potential damages from cyberthreats at the controller level, which could critically harm the converters. To counteract these threats, a load-independent LCC-tuned topology was proposed by the authors to safeguard the power converters against cyberattacks. Further analysis of fast-charging EVCS vulnerabilities was undertaken in Ref. [17], where the authors applied the STRIDE model—a mnemonic for six security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Services, and Elevation of Privilege. This model helped identify and assess vulnerabilities, leading to the development of attack-mitigation strategies utilizing

the Viterbi Algorithm.

Verifying and validating the cybersecurity risks for EVCS is crucial, necessitating a hardware-based platform that simulates EVCS operations. Such a platform enables vulnerability assessments of EVCS, focusing on its communication links and logic control systems. In this regard, the authors of Ref. [18] developed an adaptive co-simulation model that allows for the simulation and visualization of potential cyberattack impacts on EVCS devices and cloud servers. While no real attacks were executed, the built-in model proved effective in analyzing cyberattack impacts and system responses. The platform also facilitates the emulation of cyber-energy scenarios, enhancing understanding of cyberthreat consequences on EVCS. Additionally, it incorporates an Open Charge Point Protocol (OCPP) client-server setup for cybersecurity tests and uses an XFC infrastructure grid to explore the complexities of Distributed Energy Resources (DERs), their connections to legacy grid components, and vendor clouds. The platform's capability to simulate and analyze responses to cyber events marks progress toward a more secure and resilient charging infrastructure.

As a key component of smart electrical infrastructure within the IoT framework, EVCS are crucial in integrating automated EVs (AEVs) securely. The authors in Ref. [19] proposed an IoT-based architecture employing a hybrid of dynamic programming and deep learning neural networks. This allows for real-time decision-making, enabling AEVs to adeptly navigate complex environments while proactively identifying potential anomalies. Moreover, as EVCS protocols operate over web server domains, the authors of Ref. [20] used the Internet Protocols (IPs) of the EVCS to pinpoint its location, and subsequently gained remote control. They manipulated charging schedules by creating traffic bottlenecks and disrupted power flow in the local distribution grid through bi-directional power discharge from EV batteries, leading to severe frequency variations and component damage on the grid. This action also triggered load disconnections due to protective relay operations. Notably, the authors launched one of the first attacks on the switchgear of EVCS that manage synchronous charging and discharging of connected vehicles, extending previously known cyberthreat tactics [21,22]. Addressing these remote manipulations, the authors of Ref. [23] developed a state-feedback-based algorithm to detect cybersecurity issues that could hinder power grid operations. Their model, leveraging publicly available EVCS and grid data, assesses the risk under realistic security assumptions, focusing on data acquisition, electric utility layout replication, and cyberattack design on system vulnerabilities. The work in Refs. [23,24] highlights the security flaws and vulnerabilities as potential entry points for data-driven and demand-side cyber threats, illustrating that large-scale EV integration might introduce security vulnerabilities that necessitate detection methodologies considering observability and demand-side constraints.

For effective coordination of charging demands from numerous EVs, the operation of EVCS requires swift and centralized oversight akin to Supervisory Control and Data Acquisition (SCADA) systems. In this framework, the rapid communication needs for EVCS are ideally met by 5G technology, owing to its sub-millisecond latency, which enables it to manage communication with a multitude of devices efficiently. To address challenges in this area, Basnet and Ali [25] introduced an innovative, 5G-enabled, solar-powered, independent EVCS structure, overseen by a centralized SCADA system. This study explores the consequences of False Data Injection (FDI) and Distributed Denial of Service (DDoS) attacks on EVCS operations, formulating covert FDI attack strategies and SYN-flood DDoS tactics within the proposed architectural design. Additionally, the authors recommend implementing deep learning-driven local intrusion detection systems (IDS) at the infrastructure/physical level, rather than the network/cyber level, for enhanced attack identification. Their approach simulates FDI and DDoS assaults on the SCADA, which governs the EVCS's solar photovoltaic controller, Battery Energy Storage (BES) system, and the EV controller. In this setup, an IDS consistently records control signals through the Data Acquisition System. Simultaneously, the Data Wrangling unit isolates, processes, and delivers feature sets to a layered Long Short-Term Memory (LSTM) network in a suitable format. The authors assert that this method, boasting near-perfect detection accuracy, can identify covert cyberattacks that typically bypass cyber safeguards and remain unnoticed in standard monitoring systems. They discovered that a low-frequency FDI attack on the photovoltaic controller's duty cycle could generate fluctuations, potentially causing physical harm to downstream devices and leading to a permanent direct current shift in their operational current and voltage. The study suggests that incorporating a variety of attack data in its training could enhance the model's capacity to identify a broader range of attacks.

The study in Ref. [26] examines potential cyberattack scenarios and their impacts when Distributed Energy Resources (DERs) are integrated into rapid-charging stations and suggests possible countermeasures. Utilizing the Cyber-Energy Emulation Platform (CEEP) from Ref. [18], the research crafted reproducible, system-level scenarios to analyze interactions between virtual and physical components. The primary framework comprises an EV rapid-charging unit, an OCPP client/server, a site-specific controller, a meter, an energy storage system (ESS), and a PV system, all interconnected through power and communication networks. Three scenarios involving attacks and their mitigations were examined concerning DER systems and rapid chargers. In the first scenario, a Man-In-The-Middle (MITM) attack was simulated on an ESS, presumed to be incorrectly set up and lacking protective measures like encryption and authentication. This attack altered the energy storage settings and the target state of charge (SoC). The countermeasure involved updating the ESS to incorporate authentication and encryption using Hypertext Transfer Protocol Secure (HTTPS). The second scenario focused on securing Modbus communication between the site controller and meter. An intrusion involved injecting a harmful Modbus-write command to the site controller, altering the power supplied to the fast charger. Mitigation was achieved by implementing a bump-in-the-wire solution, Module-OT, functioning as a client/server at each site meter and controller, with encrypted Modbus communications between them. In the third scenario, the focus was on the protocol conversion process, where messages from the OCPP server were converted by the MQ Telemetry Transport broker. This translation process was found vulnerable to hijacking attacks. The mitigation strategy implemented a token-based authentication server between the MQTT broker and OCPP server, safeguarding it with TLS 1.3 to encrypt the data from the OCPP server. In summary, these scenarios revealed the effects of cyberattacks on both unprotected and mitigated systems, emphasizing the importance of encryption and authentication in safeguarding DER integration at EVCS. The outcomes confirmed that employing such security measures could effectively shield against cyberattacks, mitigating significant risks associated with EVCS.

In their study [27], the authors explore the risk of cyberthreats targeting the charging and discharging mechanisms of EVs, which could destabilize the grid's stability index. They introduce a concept known as malicious mode attack (MMA), exploiting the coordinated charging load control system (CCLCS) to create continuous sinusoidal power disruptions by simultaneously compromising numerous EV charging stations. As a countermeasure, the authors suggest a multi-index information active disturbance rejection control (MIADRC) strategy to enhance the stability and disturbance resistance of affected power systems. The study constructs a

mathematical model to analyze the CCLCS under MMA influence, employing stochastic process analysis and complex modal superposition methods for theoretical deductions. The proposed MIADRC strategy is developed using multi-index non-linear coordinated control to tailor input signals for each generator, incorporating a second-order active disturbance rejection control. This includes an extended state observer (ESO), a multi-index information input tracking-differentiator (TD), and nonlinear state feedback (NSF) output. The effectiveness of MIADRC is assessed by monitoring errors induced in the CCLCS by the ESO part of MIADRC and compensating for the MMA with the NSF component. Experimentally, different MMA frequencies were tested, identifying 0.62 Hz as particularly harmful due to its potential to cause large amplitude oscillations. The MIADRC demonstrated high efficiency, with a 91.8% suppression rate, quickly reacting to MMA and maintaining effectiveness until the oscillations were subdued. The authors of Ref. [28] investigate the effectiveness of resilient distributed coordination (RDC) of EVCS in mitigating cyberattacks through an artificial approach comprising detection, isolation, updating, and recovery. They propose a charging scheduling scheme integrated into the distributed architecture, which includes detecting cyberattacks by comparing electricity prices (EP) between a reference EV and its neighbors. This detection uses the difference in EPs to authenticate correct price signals. In the isolation step, a reference EV evaluates the integrity of its neighbors using a Bayesian Reputation function, based on the ratio of verifiable, correct EPs. A decrease in confidence level indicates a misbehaving EV, which is then disconnected. The recovery phase updates and recovers the distributed consensus protocol, adjusting the electricity prices of EVs and maintaining their connection to the network after isolation. This process is supported by a proposed algorithm (A1) that factors in parameters like aggregate demand and allowable deviations. Additionally, the authors simulate the impact of cyberattacks using a proposed algorithm (A2), which applies an optimal charging strategy. Simulation results under a replay attack showed severe impacts with a fake EP of $0.9/kWh, yet implementing A2 rescued a total cost of $31.84/day compared to a system cost of $177.82/day. Under a ransom attack, A2 effectively isolates infected EVs, setting a weight of zero on the affected edges by the 9th iteration.

The authors of Ref. [29] propose an online mode learning algorithm to assist EV owners in making optimal decisions regarding insurance against cyber manipulation during charging. This algorithm uses mathematical simulations to minimize average costs by optimizing vector parameters determining its efficiency. The cyber-insurance model involves collecting energy price data from EVCS, transmitting it via V2G communication, selecting an appropriate EVCS based on battery level, choosing an insurance policy with favorable charging and discharging rates, and charging the EV at a cost-effective rate when V2G communication is unavailable. To evaluate the model, the study considered a 10×10 km^2 area with 20 fixed charging stations and an EV battery charge/discharge capacity of 60 kWh. Prices for travel, charging, and discharging were set at 0.15, 0.2, and 0.25 monetary units (MUs), respectively. The algorithm's efficiency was tested across four time periods, under two insurance statuses (insured or not insured), with variables including energy consumption rate (0.6), risk probability (0.1), and premium cost (1 MU). Findings indicate that the learning algorithm reduced the average cost for EV users by about 34.5% compared to standard insurance policies. Moreover, a decrease in the insurance purchasing rate was noted when information unavailability probability was 0.1 and the premium was higher than 5 MUs, highlighting the effectiveness of the proposed cyber insurance scheme in mitigating cyber risks and enhancing profitability for EV users during charging.

Other studies that focuses on the cybersecurity of EVs charging include Ref. [30] that navigates through the impact of cyberattacks on charging coordination considering single point of failure; cyberattacks that target distributed large-scale charging of EVs [31]; hacking encrypted wireless charging [32]; manipulation of EVs demand [33]; event-triggers for distributed EVs charging considering cyberthreats [34]; mitigation against cyberattacks during charging process [35]; charging protection using residual generation technique [36]; robust V2G control scheme against cyberthreats [37]; fuzzy machine learning-based cloud for secure charging [38]; recommendation to secure EVs charging stations [39–41]; using dynamics of charging to conduct attacks on the grids [42]; real-time co-simulation and HIL environment for cybersecurity of EVs charging infrastructures [43–45]; a copula-based attack prediction model for V2G [46]; disrupting the power grids via SMS phishing within EVCS [47]; security analysis for EV charging ecosystem [48].

2.1.2. Communication infrastructure and security protocols

The integration of a smarter grid is implausible without the involvement of extensive communication infrastructure in the form of thousands of remotely controlled IoT devices. Such increased dependency on Information and Communication Technologies (ICTs), while yields operational efficiency, poses significant threats on the privacy and security of the energy grid. Furthermore, the menace of cybersecurity in the energy domains is relatively new and unexplored, in contrast to the cybersecurity of other domains (e.g., banking, healthcare, and aviation systems). To add more complexity to the situation, the communication infrastructure of the energy-domain differs in many aspects from those of other fields. Firstly, it was precisely limited to only handful locations that have only cyber layers with no to very-few alterations with physical layers (e.g., SCADA). Secondly, the flow of information exchange in traditional power networks was exclusively a one-way direction: from sources to loads. Thus, cyberthreats were less severe than in the case of bidirectional flow of information. Thirdly, domains like banking and healthcare systems consist of only cyber interfaces in contrast to energy domain, which is presented as a cyber-physical system. Hence, a cyber threat on communication channels can lead to actual physical damages. Fig. 3 presents a system architecture of EVCS integration with various players in the electrical grid.

Large-scale integration of EVs requires support from a robust and resilient power grid that can efficiently and securely meet real-time energy requirements of thousands of EVs. The charging of EVs is achieved via established communication between controllers that oversee the power converters at EVCS, and the electronic sensors attached to the battery management system (BMS) of the EVs. A cyberthreat on EVs does not require the hacker to have physical access to the vehicle itself. Proximity within miles of the targeted EVs is sufficient to perform cyberattack and assume control of part of its functionalities [49]. Communication architecture of EVs oversees relative exchange of information both internally (between EVs' various internal components), and externally (EVs interaction with other devices or systems). Such interconnection is achieved via wireless communication through WIFI connection (3G, 4G, and 5Gs) and Bluetooth, or wired communication through universal serial buses (USBs). However, while such extensive communication infrastructure is expected to increase operational efficiency of the vehicle, its increasing number of point-to-point connections makes the EVs vulnerable to many levels of cyberthreats. As a result, careful coordination to protect communication endpoints is needed, not only to ensure proper and safe operation, but also to eliminate any duplicate security measures.

In Ref. [50], the authors investigate the dynamics of DDoS attacks on the routers in EVCS, emphasizing their potential to

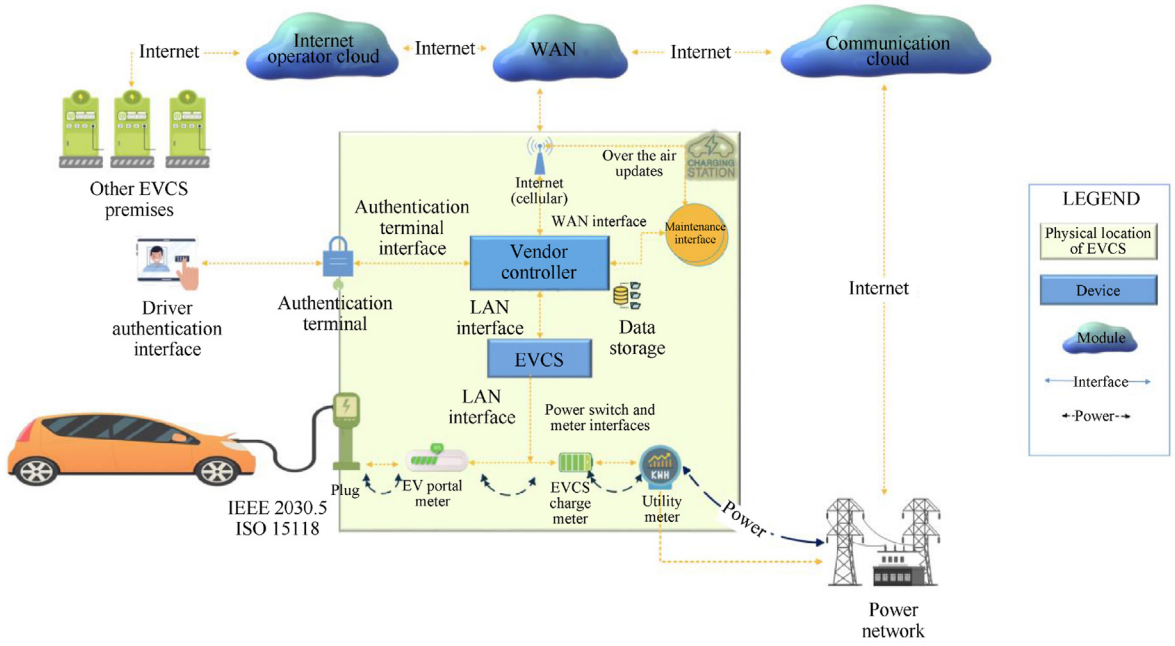

Fig. 3. System architecture of EVCS integration with various players in the smart grid.

destabilize grid operations. Specifically, the authors introduce a statisitcal mathematical model that simulates these attacks using a time-variant Poisson process, capturing the behavior of attack bots and their aggregated effects on denial of charging. The model adapts the Ornstein-Uhlenbeck process to detail the temporal variation and intensity of attacks, integrating queueing theory to assess the resultant traffic dynamics and service disruptions. The study leverages the IEEE 33 test system and Python simulations to explore the consequential impacts on both dynamic and steady-state grid performance, highlighting the critical need for fortified cybersecurity measures. Moreover, the study referenced in Ref. [51] analyzes the issue of packet losses in communication channels due to cyberattacks, an area that remains relatively unexplored. The authors introduce a novel distributed state estimation and stabilization algorithm, designed to address attacks at local estimation levels. The algorithm is capable of assessing the likelihood of packet loss occurrences within these communication channels. Additionally, the research introduces a convex optimization algorithm aimed at minimizing estimation errors, thereby ensuring that the estimated states more accurately mirror the actual states of the system, even when considering packet losses. The efficacy of this approach is validated through simulation results, which show that the proposed algorithm significantly reduces estimation errors. As a result, the estimated states closely align with the actual system states within a rapid timeframe of 0.03 s. Furthermore, when this controller is implemented, it demonstrates an effective capability to stabilize the system states in most scenarios, typically within the standard timeframe for estimation and stabilization, which ranges from 1 to 3 s.

Real-time data communication is essential for proper monitoring and controlling of large-scale EVs integration. The authors of Ref. [52] proposes a method for detecting cyber manipulation to the wavelet signals in the communication infrastructure of EVCS using the Discrete Wavelet Transform (DWT). Specifically, the proposed detection method aims to identify FDIAs that distort the actual EV penetration levels by comparing measurement residuals. Anomalies in the exchanged signals can be identified by verifying that the measured residual is larger than the estimated detection threshold (confidence intervals). The article proposes two approaches for implementing the detection methodology: anomaly detection and misuse of data detection methods. The proposed detection methodology is used to identify corruption in communication signals that establish the charging and discharging capacity at an EVCS. This results in malicious EV penetration levels that can manipulate the operational cost, EV charging requirements, and the local grid stability levels. To validate the proposed detection method, several outcomes were discussed by using the Chi-square test and DWT in identifying cyber manipulation on the EVs communication network. These outcomes include the normal distribution of charge that can be verified by the Lilliefors test, a 5% confidence interval in the normal distribution, the statistical properties of malicious and actual data of EV penetration level, and a comparison of malicious and normal data levels per given threshold levels. Once the threshold levels are exceeded, an alert is sent to the operator indicating that anomalies have been detected. While the authors assert that there is no guarantee for identifying false data values, they recommend further improvements in the methods that identify and detect anomalies in EVCS.

Addressing the cybersecurity of the CAN bus is pivotal for ensuring the performance of EVs, given its critical role in inter-vehicle communication. To enhance CAN bus security, the authors in Ref. [53] introduce a method combining WDT and support vector machine (SVM) for one-class detection, which differentiates between normal and abnormal message frames. The wavelet transforms, by splitting message frequencies into low and high sub-frequencies, extracts key data insights. The CAN bus anomaly-based model employs SVM for security. The model's effectiveness is quantified using four indices: miss rate (MR), false alarm rate (FR), hit rate (HR), and correct reject rate (CR). The authors further enhance the model's accuracy with a crow search algorithm (CSA)-based meta-heuristic optimization technique. Their findings show this modified model surpassing traditional SVM approaches, with a HR of 97.6% and CR of 95.14%. They propose this model's applicability extends to various industrial devices for cyber-attack

detection and sophisticated anomaly classification in the CAN bus. In Ref. [54], the focus shifts to CAN security challenges, where a deep learning-based model is proposed for assessing message exchange security within a vehicle. This model utilizes message frame frequency and ID number, training a generative adversarial network (GAN) for both offline use and online CAN bus message traffic monitoring. Empirical studies on recorded CAN traffic demonstrate the model's high accuracy in detecting genuine cyberattacks and abnormal activities within vehicle communication. Furthermore, Ref. [14] presents an anomaly detection model against CAN bus cyberattacks, built on a modified one-class support vector machine (OCSVM). The model employs a Modified BAT Algorithm (MBA) for reducing false positives and enhancing hit rates in anomaly detection. Experimental data from an unmodified licensed vehicle were used for evaluation, comparing conventional OCSVM, Isolation Forest, and MBA-OCSVM. The study includes a training phase to log normal CAN bus traffic behavior and a second phase using this data to detect anomalous behaviors. The OCSVM algorithm, which employs the Lagrange equation for optimization, outperformed other methods with hit rates above 95% for various datasets. In Ref. [55], researchers tackle DoS and replay attacks (RAs) on the CAN protocol in EVs. They modify the CAN data frame to include user authentication, data integrity, confidentiality, and availability features, using symmetric key cryptography for message authentication. The algorithm integrates a counter byte for message sequence verification and employs encryption tools like advanced encryption standard and RC4. For DoS resilience, a timeout mechanism per message and a unique pseudocode for ECU session management are introduced. Tested in simulated environments and with practical implementations, the algorithm proved effective in user authentication, mitigating RAs and DoS threats, and reducing encryption overhead time to 600 μs, surpassing previous methods like the Advanced Encryption Standard-128.

The authors of Ref. [56] address the vulnerability of EVs to replay attacks on the GB/T 27930-2015 Communication Protocol in China, proposing Rivest-Shamir-Adleman (RSA) Digital Signature and Addition of Random Numbers (ARN) as defense mechanisms. Initially, a comprehensive analysis of message data frames during the charging process was conducted using C++. The RSA algorithm hashes the sender's message with MD5 to produce a 128-bit digest, then encrypts it using the sender's private key with SHA256 to create a signature, verified through reverse decryption. Conversely, the ARN algorithm involves generating random numbers (RNs) in JAVA, associating each message with a corresponding RN, and ensuring the receiver can detect and match these RNs. Simulations of a normal EV charging process, using a JAVA-written program, tested both defense methods against a stimulated replay attack. The RSA algorithm halted the charging process as the voltage dropped to zero V under a forced increase to 50 V, mimicking the effects of a replay attack. Meanwhile, the ARN method restored normal charging by adjusting the voltage, effectively countering the replay attack. However, the ARN method increased database overhead due to the storage of RNs and ran at a low rate, prompting the authors to recommend further research to enhance ARN efficiency, compare it with other anti-replay attack algorithms, and reduce storage and query overhead.

In Ref. [57], researchers present a response model tailored to optimize security risks and enhance smart grid availability against infectious attacks stemming from EVCS. Using a Mixed Integer Linear Programming (MILP) methodology, they address cyberattack propagation within the EVCS and associated communication networks. The model introduces two algorithms: the threat level and the attack propagation model. The former quantifies the potential compromise risk of an EVCS over time, adjusted by the movement of EVs between compromised stations. The latter gauges threat levels when detecting compromised units, factoring in hop distance and two key probabilities—attack propagation via communication relays and successful compromise upon reaching the destination. Performance validation spanned two test systems, with 5 EVs and 20 EVs respectively. The smaller system shed light on the cyberattack propagation dynamics, whereas the larger evaluated the methodology's efficacy. Assessments incorporated variables like EVs movement between EVCS, hop distances, and charging capabilities. Under a 2-min inspection timeframe and a threshold of 0.05 for cyberattack probability, the model curtailed threat levels by neutralizing compromised EVs while maximizing smart grid availability. On a more extensive 100 EV network, the model gauged threat levels in 9.2 s and optimized in 3.3 s.

In their study [58], the authors introduce a method to enhance communication security in random cellular-Vehicle-to-Vehicle (V2V) heterogeneous systems within the automotive network, relevant to future EVs systems. Utilizing random geometry theory, they develop a cellular V2V system model featuring a 5G base station (BS), cellular network users (CU), V2V users (VU), potential eavesdroppers (Eve), and an autopilot floating vehicle (PB), with entities distributed according to Poisson Point distribution. This model enables the evaluation of autonomous driving communication safety through a downlink that integrates the autopilot vehicle as a beacon emitting signals that disrupt eavesdroppers. The study assesses safe transmission probability using the Wyner model to ensure V2V communication integrity, focusing on the instantaneous channel capacity exceeding the data transmission rate for reliability. The model calculates eavesdropping interruption probability and secure transmission probability using V2V connection probabilities and random geometry theory. Simulation results demonstrate the model's efficacy in optimizing safe transmission probability, indicating that increased PB transmit power and reduced distance between the VU and PB enhance security.

Other studies in the literature that cover the cybersecurity of the communication infrastructure of EVCS include the work of Ref. [59] that investigate the impact of vulnerabilities of the OCPP of the charging stations on the security of the smart grid; analysis on the cybersecurity of IEC 61850 standard that defines the communication protocols of IEDs at the substations [60]; a DAG-based smart contract approach to secure the 6G wireless EVCS [61]; GNS3-based analysis for emulating communication networks to test substation protection schemes based on GOOSE (Generic Object-Oriented Substation Event) protocol [62]; a survey that navigates through cybersecurity of the intra-vehicle communications [63,64]; a survey that explores the cybersecurity problems in 5G-enabled EVCS [65]; exploring the integration of vehicles with the power grid using open communication protocols within the context of V2G [66]; a survey that navigates through cybersecurity of and potential challenges in the OCPP [67]; an automated cybersecurity testing approach designed for digitalized substations based on IEC 61850 [68]; a time-series state analysis method for detecting and analyzing cyberattacks on the network of Internet of EVs [69]; investigation of the security aspects related to wireless communication in EVCS [70]; an authentication protocol for Combined Charging and Wireless Power Transfer (CWD-WPT) charging systems in a cloud environment [71]; exploration of the attacks and security measures concerning the exchanged information in the charging infrastructure for EVs [72]; Discussion on the modeling of the communication layer based on the IEC 61850 standard and its extensions for EVs charging and discharging processes [73]; a comprehensive framework for establishing agreements between EVs and the grid to ensure secure communication and data exchange within the context of V2G [74]; a secure and resilient authentication mechanism to protect the privacy of EVs while enabling trustworthy interactions with the grid system [75]; a

examination of the wireless physical layer (PHY) vulnerabilities in EVs charging systems, which highlights potential security weaknesses and risks associated with wireless communication protocols used in EVCS [76]; and a secure wireless communication system to ensure secure and reliable communication between EVs and EVCS [77,78]. Table 1 presents communication requirements and interactions necessary for efficient and effective integration of EVs within the local grid.

2.1.3. Powertrains of EVs

As EVs become more prevalent on the roads, there is growing concern about the potential cybersecurity risks to their powertrains. The powertrain is a crucial component that regulates the EV's performance and movement. A cyberattack targeting the powertrain can pose serious safety risks and threaten the privacy and security of the drivers and passengers. Hackers could exploit vulnerabilities in the electronic control units (ECUs) that manage the powertrain and manipulate them to cause the vehicle to malfunction or even worse cause accidents. Therefore, it is critical to comprehend the nature of these threats and implement appropriate security measures to mitigate the associated risks.

Guo and Ye [79] introduce a cyberattack detection and defense model specifically tailored for the powertrain systems of EVs. The model employs various index metrics to assess the impact of cyberattacks on the lateral stability control system (LSCS) and the four motor drives integral to an EV's operation. The study's primary objective is to conduct a vulnerability analysis and establish a coordinated detection mechanism, thereby improving the cyber-physical security of EVs equipped with advanced motor drives, a key aspect of modern power electronics. The proposed defensive strategies are divided into two main categories. The first strategy focuses on bolstering the in-vehicle network's safety by incorporating measures to thwart malicious activities. This includes the implementation of secure software updates and the integration of secure hardware components. The second strategy involves the creation of a reliable and autonomous monitoring device designed to mitigate the effects of cyberattacks during vehicle operation. A notable contribution of the authors is the enhancement of a driver-in-the-loop steering system, paired with a model-predictive control (MPC)-based driver model. This advancement underscores the growing complexity involved in executing steering actions in modern vehicles. The effectiveness of the proposed detection method was validated through its ability to identify a variety of cyberattacks, including replay, DoS, and data integrity attacks.

The authors of Ref. [80] utilizes backpropagation (BP) technique to assess the impact of cyberattacks on the SoC estimation of the EV's battery. Specifically, cyber manipulation on the battery may influence its functionality to either over- or under-estimation of its SoC predication. The proposed BP technique was implemented in a hardware-in-the-loop (HIL) considering different case scenarios that consider both normal and abnormal (under cyberthreat) operations. The root mean square (RMS) and mean absolute percentage error (MAPE) were considered as statistical tools to measure the accuracy of the NN method. Results show that MAPE data value got noticeably higher under the attack scenario, indicating the ability of the proposed BP method to detect cyber manipulation on the EVs battery.

Reinforcement learning (RL) has emerged as a promising approach for addressing the cybersecurity challenges in intelligent transportation systems (ITS). Despite its potential, accurately modeling RL algorithms remains a challenge. In this context, Wang et al. [81] proposed two value-based deep reinforcement learning (DRL) algorithms to examine the effects of adversarial examples on a well-behaved DRL-based Energy Management System (EMS) in an EV's powertrain. Adversarial examples, commonly used in computer vision applications, can create perturbed images that can fool a well-trained classifier and, therefore, are of concern in the context of ITS where safety and robustness are critical. The proposed model employs a simulation method based on real-world historical delivery trips and an accurate vehicle model to optimize fuel use and maintain battery health. The study highlights the need for effective security measures to ensure the cyber-physical security of EVs and emphasizes the significance of considering adversarial examples in handling safety issues.

The design of Li-ion battery systems often overlooks security threats during the initial phase, which puts them at risk of cyberattacks. In response, Kim et al. [82] propose using both traditional BMS architecture and an intelligent BMS in cyber-physical environments to detect and prevent potential attacks. The work examines potential security vulnerabilities and defense strategies, as well as the use of blockchain technology as a basic cybersecurity reference for BMS developers. By implementing blockchain technology, the authors argue that BMS developers can safeguard their systems against malicious cyber-physical attacks, ensuring the safe use of battery systems across a wide range of applications in cyber-physical environments.

Automated EVs face a wide range of digital threats [19], including traditional eavesdropping, DoS and MITM attacks that can degrade vehicle performance. To address this issue, Guo et al. [83] developed a systematic vulnerability assessment model for connected and automated electric vehicles (CAEVs). The model provides a framework for analyzing the impact of cyber-physical

Table 1
Communication requirements for EV integration to the power grids.

Types of network communication	Function	Other devices used with	Coverage
Wide Area Network (WAN)	Establishes constant services amongsubstations and utility control centers incities and multiple regions through whichthe demand response and scheduling signalscan be communicated.	Service provider networkslike Cellular Network or aUtility Network e.g. WiMax	Large geographical areas like cities andregions
Neighbourhood Area Network (NAN)	Connects smart meters and grid datacollectors in a distribution automation system.	Wireless Mesh Networks, Power Line Communicationor Ethernet.	Within a residential community
Field Area Network (FAN)	Monitors information exchange betweenPEV charging stations and the controlcenters in the distribution system.	Wireless Mesh Networks. Power Line Communicationor Ethernet.	Within a field of known size
Home Area Network (HAN)	Facilitates the operation of the smart grid byenabling smart meters to manage customer-based demands. Monitors how much electrical energy isexchanged within a time. Prompts control response on diversecustomer-side appliances	Connection with PEVs, smart meters, and energy management systems (EMS).	Within premises of houses, buildings or a residence.
Control Area Network (CAN)	Provides reads about the PEV attributes ofthe car and links this information to thecharge controller and charging station.	Engine Control Unit, othercontrol devices and wire orwireless protocols such as Zigbee.	Within the vehicle or car.

security on the core control systems of CAEVs, with a specific focus on the security and resiliency of electric motor systems (EMSs) in response to cyberthreats. The EMSs is primarily attacked by data tunnels and wheel speed sensors that include DoS, repetitive and fraud attacks in its simulated impact analysis, which aims to render system resources inaccessible at a constant value. Repetitive attacks involve repeated or delayed measurements, while fraud attacks modify signals across physical boundaries because of EMS hard cuts. The authors found that such attacks can cause the electric drive system to malfunction in continuously monitoring the thrust demand. The study structured various synchronized cyberattacks with the same intensities to provide a balanced contrast between attack types and cases. The study highlights that data integrity attacks can degrade the vehicle's overall effectiveness, and all evaluation metrics, including recovery time and resilience indices, could help in assessing the impact of various cyberattacks on EMSs. The authors concluded that evaluation metrics and index-based criteria could be used to evaluate the EMSs' vulnerability, performance, and serve as a prerequisite in cyberthreat detection.

To mitigate the cyber risks against powertrains, it is essential to establish precise metrics and models that ensure its proper security and isolate potential physical responses to cyberattacks. The authors of Ref. [15] addresses this challenge by investigating different data integrity attacks on EDS and correlating the interaction between physical and cyber systems using a cyber-physical system (CPS) model. To evaluate the impact of these attacks on the electric drive system, the study constructed a model based on a 50 kW IPM in MATLAB Simulink and defined five performance metrics for evaluation: torque ripple (S1), speed ripple (S2), current distortion (S3), torque tracking error (S4), and the current unbalanced component (S5). The study considered three types of attacks, including a Decreasing Attack that modifies the sensor signal, a White Noise Attack that introduces white noise and random signal variation, and a Mixed Attack that combines both attacks. The simulation performed in demonstrates that cyberthreats can have a significant impact on the EDS components of EVs. For instance, when a decreasing attack signal was introduced to the system, the total harmonic distribution, and the torque ripple (S5) increased by over 70% and 300%, respectively. Similarly, a white noise attack introduced to the system caused an obvious change in the current unbalance component (S5), torque ripple (S1), and tracking error (S4). Furthermore, a mixed attack generated more ripples and distortion, leading to a severe increase in the current unbalanced component (S5). The results of this study emphasize the need for robust metrics and models to diagnose and detect cyberthreats on EDS to ensure proper security and reliability and mitigate the risks associated with cyberattacks.

The necessity to distinctly separate physical and cyber elements for prompt cyberattack detection on traction motor drives is highlighted in the study conducted by the authors of Ref. [84]. They introduce a rapid, binary-classifier-based method utilizing four sensor signals to identify cyber threats targeting electric vehicle traction motor drives, with a particular focus on device-level risks that can significantly affect motor drive systems. This method relies on four sensor signals isolated from the vehicle's network: three-phase current readings (ia, ib, and ic) and the rotor position encoder signal (φr), all transformed using the Park transformation for reliable physical data. Binary Classifiers extract time-domain features from the traction drives' current data, selecting 16 features based on sample moments (mean, variance, skewness, kurtosis) within a sliding window for their simplicity and interpretative ease, facilitating reduced online computation. Multiple binary classifier options, including random forest (RF), k-nearest-neighbor (KNN), and adaptive boosting (AdaBoost), were evaluated for sensitivity to feature-based attacks, with RF and AdaBoost showing high sensitivity while KNN was less effective. Using K-fold cross-validation and a majority vote mechanism, the study assessed the detection performance from multiple perspectives: effectiveness during vehicle cycles, online memory efficiency, computational complexity, and detection speed. The RF and AdaBoost classifiers triggered attack alarms rapidly and with less computational effort, proving efficient for cyberattack detection on traction motor drives.

It is very clear research on the cybersecurity of EVs' powertrains are still highly underdeveloped and lacks significant contribution to secure a component that, if attacked successfully, may yield fatal consequences. While Ref. [85] presents a survey work that investigates against data integrity attacks targeting dynamic route guidance in transportation-based cyber-physical systems, application-based studies are absent in this field. A suggested future study could focus on the how attacks can be performed to interrupt and influence EVs route navigation through internet-fed real-time metadata such as those presented in Refs. [86,87]. Securing the navigation process against cyber manipulation is urgent to avoid GPS- based fooling attacks that could results in hefty costs both in safety and privacy.

2.1.4. Power electronics components of EVs

Recent advancements in power electronics (PE) devices have been crucial for the electrification of transportation sectors, playing a vital role in the structure of EVCS and contributing significantly to the deployment of extremely fast-charging stations. Fig. 4 shows how power electronic components integrate within an EV, highlighting the vulnerabilities these devices might face from cyber manipulations. The authors of Ref. [88] provide a comprehensive review of various power electronics circuit topologies used in fast-charging EVCS. On the other hand, Ref. [89] introduces a real-time HIL cybersecurity testbed platform for power electronics in EVCS, combining the cyber-physical aspects of PE components within industrial control systems (ICS), SCADA systems, and HIL simulation capabilities. This platform evaluates the resilience of PE systems against FDIA and Packet Drop Denial of Service (DoS) attacks by integrating a PE simulator, a cyber system testbed emulated with actual network systems and cloud servers, and penetration testing tools. It assesses the impacts of these attacks through data monitoring, communication data modifications using Ettercap, and penetration tests with massive ACK packet transmissions, revealing

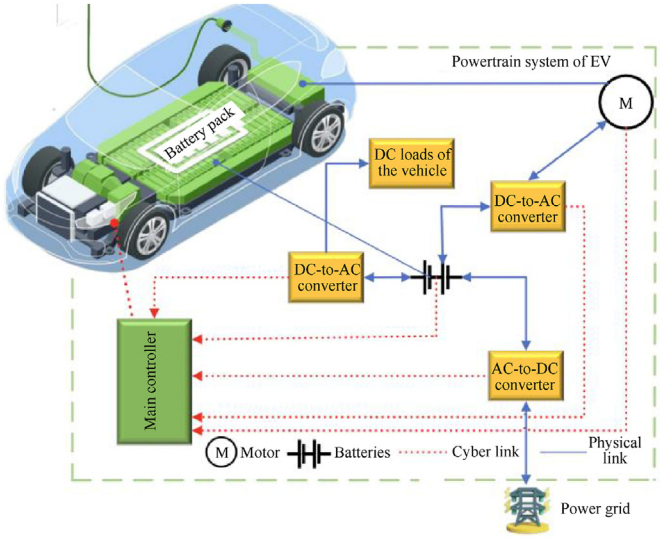

Fig. 4. Communication and physical links of PEs within an EV.

vulnerabilities such as altered real-time monitoring data and manipulated control commands. During ACK DoS attacks, significant increases in CPU and network usage led to server inactivity, affecting cloud-based monitoring data management. Packet Drop DoS attacks demonstrated how communication disruptions can cause a smart inverter to lose active power data receipt within 5 s. This testbed serves as a valuable tool for identifying potential cyber threats to PE systems and developing strategies to mitigate the impacts of cyber-physical attacks.

The advent of extremely fast chargers (XFC) and Battery Management Systems (BMS) in EVs has raised security concerns, particularly in the context of their vulnerability to cyberattacks. Such attacks could lead to overcharging of EV batteries or even grid instability, potentially causing widespread blackouts. In response to these risks, the authors of Ref. [90] have developed a strategy focusing on electromagnetic-based non-intrusive attacks, specifically targeting AC-to-DC converters and BMS power converters. The primary objective of their research is to assess the susceptibility of XFC chargers and BMS to Intentional Electromagnetic Interference (IEMI) attacks and to understand the possible repercussions on EVs. The study presents both simulation and experimental data, examining attacks on critical system components, such as sensors and actuators. It particularly highlights the vulnerability of voltage and current sensor outputs in power converters. The research introduces an analytical model demonstrating how these components can be manipulated using IEMI, which is challenging to shield against. Additionally, the study recommends several design modifications at the hardware level to counteract these threats, identifying three primary attack points for the threat model. The first attack point involves manipulating the voltage sensor data by inducing voltage on the cable connecting the analog sensor output to the Control Voltage (CV) controller's Analog-to-Digital Converter (ADC) input. The second attack point targets the current sensor output, focusing on the PCB trace between the analog current sensor output and the controller ADC's input. The third point of attack aims at altering the input voltage of the gate driver to control the switch. The study identifies that IEMI attacks on voltage sensor outputs pose a significant threat to converters due to the low power nature of such attacks. It suggests that PCB level countermeasures are essential for ensuring system security. One proposed solution is the use of via-fenced strip-lines for analog sensor outputs and gate driver signals. In summary, this research emphasizes the pressing need for enhanced security measures in EVs, particularly with the growing adoption of XFC chargers and BMS. It provides critical insights into potential vulnerabilities to IEMI attacks and outlines possible strategies for their mitigation, contributing valuable knowledge to the field of EV security.

Other studies in the literature that cover the cybersecurity of power electronics components within the infrastructure of EVCS include the work of Ref. [91] who proposes a deep learning algorithm to detect and mitigate cyberattacks in synchronous buck converters; discussion on the importance of implementing effective security measures to safeguard power electronic systems from potential cyberthreats [92–95]; development of a smart inverter communication model and analyzes the impact of cybersecurity attacks on its operation [96]; intrusion detection method for detecting and mitigating cyberattacks involving the manipulation of inverters' power quality (PQ) set-points [97].

2.1.5. Data privacy issues

Smart charging requires a significant amount of data exchange between EVs and the grid. This data includes sensitive information such as EVs energy request, location, payment information, and exchanged texts. These data points are potential targets for cyber criminals who could use them to manipulate the EVCS network, compromise data integrity and breach privacy. Attacks on EV-related information may cause physical damages, identity theft and other harmful consequences. Furthermore, in a digitalized smart grid, invasion of privacy is a major challenge that can arise, particularly within the EVs paradigm. The potential unauthorized access to data, such as personal details, payment specifics, frequently visited charging stations, and battery performance metrics, underscores pressing privacy concerns.

The critical need for robust cryptography to safeguard EV information from cyber manipulation is undeniable, especially given the current dearth of efficient privacy-preserving solutions. Addressing this gap, the authors of Ref. [98] developed a privacy-preserving framework aimed at securing EV information during the charging process. This framework incorporates the Matching Market concept for identifying suitable charging stations and employs lattice-based cryptography to ensure secure communication. The framework is designed to consider various factors for optimal allocation of charging stations, prioritizing both security and privacy preservation. A key aspect of the proposed model is its focus on optimizing EV allocation to charging stations, leveraging a multi-factor payoff-based matching market. Additionally, the model integrates lattice signcryption in EV infrastructure communication, which not only reduces the time needed for cryptographic processes but also resists quantum attacks. When compared to existing methods, the proposed framework demonstrates a notable enhancement in user satisfaction for EV users. It also achieves a reduction in both the cumulative computation cost and latency, making it a more efficient option. The authors assert that their framework is particularly effective in combating confidentiality-authentication attacks, underscoring the vital role of proper cryptography implementation in protecting the privacy of EV information. This approach offers a significant step forward in ensuring the security and privacy of EVs, particularly in the context of the charging process.

Ensuring the protection of data and privacy is a crucial concern in modern societies yet remains an area that is significantly underexplored. There is a dire need for proper protections scheme for charging station reservation that prioritizes privacy and fairness for EV owners, safeguarding their information from potential adversaries. In this regard, the authors of Ref. [99] proposes an authentication scheme that not only considers fairness among EVs but also protects drivers' privacy and prevents any selfish reservation of charging slots. The study adopts a network model consisting of EVs, offline trusted authority (OTA), roadside units (RSUs), charging service providers (CSP), and EVCS, along with an adversary and threat model. The proposed anonymous credential is divided into four phases, including system initialization (SI), primary charging permission/reply (PCP), fair charging reservation (FCR), and EV battery charging (EVBC). The authors claim that the proposed scheme maintains EV owners' privacy using bilinear pairings for anonymous credentials, which enable legitimate EVs with valid credentials to authenticate themselves to the CSP without revealing their identities. Furthermore, the use of an encrypted ticket establishes a secure session between the CSP and the EV to encrypt sensitive charging details without revealing any link between charging requests. The performance of the proposed scheme is evaluated based on communication and computation overhead, which estimate the size of exchanged charging packets and the times of cryptographic operations. The authors report that their scheme significantly enhances EV user satisfaction and reduces computation costs and latency when compared to existing approaches while effectively preventing confidentiality-authentication attacks.

In the research presented in Ref. [100], the focus is on the optimal scheduling and secure management of hybrid AC-DC

microgrids, which include an array of energy sources and storage solutions such as wind turbines, fuel cells, energy storage devices, micro-turbines, photovoltaic units, and EVs. The study approaches the operation of these hybrid AC-DC microgrids (MGs) as a unified optimization challenge and applies the Whale Optimization Algorithm (WOA), a metaheuristic algorithm, for identifying the most efficient operational strategy. In addition to optimizing microgrid operations, the study introduces an IDS designed to identify identity-based cyberattacks targeting advanced metering infrastructure (AMI) within microgrids. This IDS operates by collecting and storing data on the received signal strength associated with specific IP addresses. This information is then utilized to create a binary sample that aids in the detection of cyber threats. The practicality and efficacy of the proposed system architecture were evaluated using a hybrid MG, modeled on the IEEE 33-bus test system. The authors claim that results not only demonstrated the effectiveness of their algorithm in managing the operations of hybrid microgrids but also successful in safeguarding the privacy of EVs.

The blockchain technology has emerged as a promising solution for enhancing energy and data transactions in a secure manner. It allows for processing transactions by multiple agents and nodes within a system, which are then collected into data blocks and broadcasted across the network. The data blocks are linked together securely using cryptography and sealed via a hash code, minimizing the chances of any unauthorized malicious activity. The use of blockchain for securing microgrid operation with EVCS was proposed in Ref. [101]. To protect the privacy and authenticity of financial transactions between EVCS owners, the authors utilized a directed acyclic graph (DAG)-based security framework [102]. The EVCS were treated as nodes within the system that broadcast their transaction data through data blocks of the blockchain. The authors argued that the system's security would be enhanced under the blockchain concept, but the issue of hash address calculation may complicate the process. To overcome this issue, the authors utilized the DAG approach to allow proper transactions via public, private, and transaction blockchains, respectively. The public blockchain allowed some information to be collected and displayed in a transparent and open environment, while the private blockchain was established such that only certain information would be accessible to a few trusted agents within the system. The transaction blockchain managed transactions data and broadcasted them only to the transaction blockchain. The authors claim that the proposed framework provides a secure power management scheme that allowed the network's main agents to perform effective energy transactions within EVCS.

In their study [103], the authors propose a approach to enhance the reliability and security of EVs charging systems by integrating consortium blockchain with fog computing. This innovative scheme involves several key components: a trusted authority (TA), a cloud center, Fog Computing Nodes (FCNs), and charging piles. The TA plays a crucial role as a key generator, verifying and authorizing both EVs and FCNs, and identifying malicious nodes. The cloud center handles complex computations, while the FCNs manage requests from EVs and charging piles. The blockchain component includes a smart contract, TransStorage, facilitating scalable data storage and efficient data management within the blockchain framework. The performance evaluation focused on computational overhead and communication costs, with proper efficiency observed. The average runtime for each request was 21.88 ms for 50 threads and 15.23 ms for 150 threads, with low memory consumption and minimal CPU usage. Regarding data storage, the blockchain recorded only hash results of non-sensitive information, while sensitive data was securely encrypted and stored in the cloud. Overall, the authors attest that the proposed scheme offers a robust solution for improving the charging process, providing decentralized storage for charging records, enhancing transaction verification efficiency and reducing resource consumption.

In Ref. [104], the authors propose a security scheme that utilizes iris recognition and k-Nearest Neighbors (KNN) as an encryption algorithm to prevent fraudulent identities, man-in-the-middle attacks, and unauthorized access to EVCS. The scheme involves a network model with charging companies (CCs), cloud servers (CLS), an offline trusted authority (TA), and EVCS. The system model enables the encryption of authentication queries with the user's iris data to the CLS for verification. The proposed methodology is evaluated in a Python environment and an appropriate server to determine its communication and computational overhead, encryption scalability, and search time. The experimental results show that the KNN-based iris-recognition scheme is quite simple in its application and achieves promising efficiency by ensuring a recognition time of 2 ms. The authors also highlight four design goals for evaluating the scheme, including scalability, efficiency, confidentiality, and unlikability of authentication queries. The methodology achieves the design goals through the transmission of the trapdoor into multiple ciphertexts repeatedly, preservation of authentication query confidentiality, and adjustment of the EVCS to use one TA key to search all the iris data and a significant number of indices from different CCs. Overall, the proposed security scheme presents a promising solution to prevent fraudulent identities, MITM attacks, and unauthorized access to EVCS.

Other studies in the literature that cover the privacy within EVCS include the discussion in Refs. [105–107] of potential vulnerabilities and risks that can compromise the security and privacy of EV charging systems; a privacy-preserving authentication protocol for IoT-enabled charging systems [108]; implementation of a secure data aggregation framework and cryptographic mechanisms to secure communication and data privacy during EVs charging [109]; privacy-preserving and secure authentication mechanism using Elliptic Curve Qu-Vanstone (ECQV) cryptography [110] and divisible electronic payments [111]; authentication and billing process in Internet of Electric Vehicles (IoEV) charging [112]; utilization of the blockchain to secure transactions involving EVs charging [113,114]; identity-based cryptography to enable secure and efficient authentication during EV charging [115]; examination of different privacy-preserving methods employed in EV charging systems and assessment their effectiveness in protecting user privacy [116]; a secure and efficient protocol that enables key agreement between vehicles and the grid while preserving user privacy [117]; a location privacy enhancement scheme for EVs via a concept called "at the right time", where EVs can selectively disclose their location information only when necessary [118].

2.1.6. Standardization and protocols

As the electrical infrastructure is evolving toward a highly interconnected and automated environment, standardization of security protocols has become an integral part to allow successful erection of the concept of the smart grid [4]. Among the very few documentations in this manner are the National Institute of Standards and Technology Interagency Report number 7628, simply known as the NISITR 7628 [119]. Released by the Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee in 2014, this technical report provides analytical framework for the involved stakeholders in the energy industry to sustain proper definition of cybersecurity-related vulnerabilities and issues in the smart grid. While the report is seen as heavily and lengthy technical documentation that not any reader may exhibit the capability to fully understand, the authors of Ref. [120] provides methods for visualizing its complexities, aiding readers to better synthesize the

presented information.

In Ref. [121], the authors examine smart grid standardization efforts, with a focus on cybersecurity. They discuss the Interoperability Framework and Roadmap of the National Institute of Standards and Technology (NIST) and its accompanying document, "Guidelines for Cyber Security in the Smart Grid" (NISTIR 7628), which provides comprehensive coverage of cybersecurity challenges in the smart grid. The authors conclude that while other standardization strategies have been discussed, only few address cybersecurity issues in a meaningful way. The NISTIR 7628 document covers seven domains that make up the smart grid, with interfaces between actors in each domain. Furthermore, the authors discuss two approaches for risk assessment and security analysis: top-down and bottom-up. The top-down approach involves grouping actor interfaces into categories that have common security requirements, while the bottom-up approach covers attacks not reliably included in the NISTIR 7628 framework. However, the authors note that the bottom-up approach can be unclear in specifying attacks, especially when attackers outsmart security designers. To counter such deficiencies, the authors propose a logical interface model that disintegrates the smart grid domains into smaller details without specifying existing interface requirements and data types. More than 130 logical interfaces have been identified, and an individual interface can identify security requirements with ease given its assignment to one out of 22 categories. This model can help organizations assess risks and apply commensurate security requirements to combat cybersecurity issues unique to their smart-grid systems. By employing the NISTIR 7628 top-down approach, securing the EVCS requires that:

(1) Logical interfaces unique to certain application scenarios are defined by using the Meter Data Management System (MDMS):
(2) Already identified logical interfaces are assigned to appropriate categories, for instance placing interfaces between back-office systems under a common management authority.
(3) Two unique steps are executed to ensure that: the preference among the objectives of the CIA (confidentiality, integrity, availability) is searched out; the baseline security requirements are chosen based on the logical interface categories which might involve the following: Session lock, Permitting unidentified and unauthenticated actions, dentification and authentication of the user, Isolation of security function, protection against denial of service, prioritizing the resource, Integrity in communication, confidentiality of static information, software and information integrity.

In their research [122], the authors propose an object-oriented modeling approach to standardize power system communications, focusing on the implementation of IEC 61850-based information models for Vehicle-to-Grid (V2G) communication between EVs and EVCS. Additionally, they map out the steps of a smart charging algorithm onto corresponding messages within this framework. The approach begins with the development of an information model for EVCS, which includes the integration of two logical nodes from IEC 61850, namely DEEV and ZBAT, into the EV model. This integration facilitates communication between EVs and smart grid systems, incorporating V2G interactions into the communication domain using IEC 61850-based models. The operation of a smart charging algorithm is then mapped onto three specific types of IEC 61850 messages: Manufacturing Messaging Specification (MMS), Generic Object-Oriented Substation Event (GOOSE), and Sampled Values (SV). This mapping process takes into account various factors such as SoC of the EV, its range based on this charge, the desired destination, the distance to different EVCS, and the availability of charging slots. The mapping process includes several key steps:

(1) The EV sends an initial power supply request to the EVCS using an MMS message.
(2) The EVCS acknowledges this request and asks for the EV's SOC.
(3) The EVCS sends a GOOSE message to initiate charging.
(4) The EV responds with an SV message indicating its SOC.
(5) The EVCS monitors the EV's SOC until charging stops at a predetermined level.

The authors also present a hardware implementation of these information models through intelligent electronic devices (IED) Capacity Description files, representing both the EV and EVCS. This implementation involves initiating smart charging and capturing all messages chronologically. It includes the transmission of regular SV messages from the EV to keep the EVCS updated on its SOC, and a GOOSE message to signal the EV to stop charging once full charge (100%) is achieved. The effectiveness of the IEC 61850-based solution is validated through the following observations:

(1) Successful sending and receiving of MMS messages for SoC acquisition.
(2) Repetitive forwarding of GOOSE messages by the EVCS to initiate charging.
(3) Regular transmission of SV messages by the EV to update the EVCS on its SOC, and the EVCS's response with a GOOSE message to signal the EV to cease charging at full charge.

In their study [123], the authors conduct a thorough analysis of the security requirements and threats associated with IEC 61850 communication, highlighting its vulnerability to cyberattacks. This vulnerability is primarily due to two factors: the ease of connecting through Ethernet and the interoperable nature of its standardized message structures. The messages of IEC 61850 include GOOSE, SV, Routable-GOOSE (R-GOOSE), Routable-SV (R—SV), and MMS. The study points out that cyberattacks on IEC 61850 substations often target specific protocols or devices, either by disrupting services through data modification or gaining access to confidential information. Attacks on GOOSE messages, which include status and sequence numbers, can take the form of high-status number attacks, high-rate flooding, or semantic attacks where spoofed messages mislead subscribers. Other threats to the system's security involve MITM attacks, FDIA, DoS, replays, password cracking, integrity violations, masquerading, and hardware trojans. The security requirements for IEC 61850 message exchanges are categorized into three main areas:

I. GOOSE and SV Messages: Securing the confidentiality of these messages, which have a strict delivery requirement of 3 ms, is crucial. The authors suggest using the Message Authentication Code (MAC) algorithm for encryption, as it meets the time constraint.
II. R-GOOSE and R—SV Messages: These messages, which are mapped over User Datagram Protocol (UDP) and IP layers, require authenticity and integrity. MAC algorithms are recommended for generating digital signatures, with AES-128 and AES-256 algorithms suggested for optional encryption.
III. MMS Client-Server Messages: The MMS message exchange process consists of a handshake phase and a data transfer phase. IEC 62351-4 ensures authentication and integrity during the handshake and data encryption during data transfer. The authors recommend transport layer security for

the transport profile and a combination of peer-to-peer and end-to-end security for the application profile, executed over Open System Interconnection (OSI) or IP stack.

The comprehensive analysis by the authors of Ref. [123] highlights the critical need for robust security measures in the implementation of IEC 61850 to protect against various potential cyber threats. Similarly, the authors of Ref. [124] shed the light on some of the most important protocols that are of interest to the cybersecurity of EVCS, the most important are the ETSI and OCPP protocols, as follows:

(1) **European Telecommunications Standards Institute (ETSI) Protocol**

In recent years, the IoT sector has witnessed substantial improvement which pave the way for more spread of EVCS on the sides of the roads. However, with lots of IoT devices involved in the charging process come the risks of cyberthreat due to IoT vulnerabilities to cyber manipulation. A technical specification for cybersecurity issues peculiar to the IoT of consumers was published by ETSI. By compiling security guidelines for IoT consumer devices like smart energy gadgets fit into a set of high-level provisions, they guide consumer IoT manufacturers in the development process. Below is a list of high-level provisions defined by ETSI:

- Keep universal default password non-existent.
- Implement how reports of vulnerabilities are managed.
- Update software regularly.
- Storing credentials and security-sensitive data in a secured mode.
- Constantly protect individual data and ensure communication is secured.
- Build resilience of systems to outages.
- Keep installation and maintenance of devices simple.

In addition to this effort, three high-level considerations specific to the cybersecurity and privacy risks of IoT components, in comparison to conventional IT components, have been established by NIST [125]:

a) Several IoT devices relate to the physical world in ways unique and different from that of conventional IT devices.
b) Accessibility, management or monitoring of various IoT devices differs from that of conventional IT devices.
c) IoT devices differ from their conventional counterparts in terms of availability, efficiency, and effectiveness of cyber security and privacy capabilities.

Besides, NIST has identified three key mitigation objectives crucial for the cybersecurity and privacy of IoT devices: device security, data security, and individual privacy. The standards established by NIST align well with those set by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Several of these standards are particularly applicable to cybersecurity and risk assessment within the EV ecosystem. These include NISTIR 7628, which provides guidelines for Smart Grid cybersecurity; NIST.SP 800-30, a guide for conducting risk assessments; IEC 31010:2019, focusing on risk management and assessment techniques; and NIST.SP 800-53.

(2) **Open Charge Point Protocol (OCPP)**

OCPP is a protocol that makes no-cost or no-license provisions for accessible, compliant and identical communications transiting among EVs and Charging Station Management Systems (CSMS). It is gaining prominence as the de-facto standard protocol enabling customers to change the charging network while keeping the charging station constant. In the UK, by 2019, the application of OCPP 1.6 has become mandatory for new charging stations. An upgrade of OCPP 1.6, in comparison to previous versions, has incorporated JSON over WebSocket to support smart charging and the connecting of charging stations to home-based broadband. With the inclusion of internet connection by OCPP 1.6, a critical concern is its security. Hence, by adopting Transport Layer Security (TLS) and public-key cryptography using X.509 certificates, OCPP initiates security considerations. Three security profiles are supported by OCPP 2.0.1 and OCPP 1.6 and are highlighted below:

a) Unsecured Transport with a Basic Authentication Profile: this provides little security to the communication channel because the authentication of charging stations is executed via username and password while providing no authentication for the CSMS. Consequently, it only finds its application in trusted networks that harbor a VPN connection between the CSMS and the charging station.
b) The TLS with a Basic Authentication Profile: this profile uses TLS to offer optimum security to communication channels. While the CSMS is authenticated using a TLS server certificate, the charging stations employ the HTTP Basic Authentication for their verification. Transmission of an encrypted password is enabled by the TLS of this profile.
c) The TLS with Client-Side Certificates Profile: this profile offers maximum security to communication channels using the TLS in comparison to the previous profiles. Authentication of the charging station and CSMS is carried out individually using certificates. However, the charging stations are authenticated by the CSMS via the TLS client certificate.

Other studies in the literature that cover the aspect of standardization efforts of EVCS include a survey on various standards that cover various aspects such as charging components, communication protocols, power management and safety strategies [4]; a lightweight security protocol called EV-PUF for the dynamic charging system of EVs utilizing Physical Unclonable Functions (PUFs) [126]; a secure protocol that ensures authentication between EVs and EVCS that protect against various security threats [127]; a threat analysis of the charging protocol ISO 15118, where the authors address potential security issues, identify potential attack vectors, and suggest countermeasures to mitigate these risks [128]; threat analysis of the OCPP protocol [129,130]; implementation of R-GOOSE messages to identify potential vulnerabilities and risks on the IEC 61850 standard [131]; investigation of the security implementations of the ISO 15118 standard [132,133]; challenges and considerations related to NISTIR 7628 [134]; examination of the vulnerabilities and potential security threats associated with EV charging protocols with various security measures and mechanism [135,136]. Table 2 shows different standardization efforts made to secure EVs and EVCS. Fig. 5 provides a system architecture on the physical and cyber links as well as the charging protocols used to integrate the EVs with the charging stations.

2.2. Second taxonomy: CIA-based attacks taxonomy

As EVs becomes more widespread, the risk of cyberattacks on the underlying domains also grows. These domains include charging stations, battery management systems, and V2G communication systems, among others, and are susceptible to various types of attacks, such as DoS, spoofing, and MITM attacks. A

Table 2
Common international standards and protocols for secure integration of EV's to the energy networks.

Standards for communications	Specific regions of use	Description	Reference
ISO 15118	International (e.g., EU, USA, S.Korea)	A standard for communication between EVs and EVCS. A unique protocol for AC and DC charging by facilitating features like plug & charge. Enables automatic start and stop of charging without authentication requirement.	[137]
OCPP(Open Charge Point Protocol)	International (e.g., the Netherlands)	An open-source protocol that prompts communication between AC and DC charging stations and backend systems. Enables features such as remote monitoring, billing, and firmware updates.	[138]
IEC 61850	International (e.g., EU, Russia, China, Korea, Japan, N. and S. America)	A standard for communication in power systems. Enables communication between EVCS & the grid. Allows features such as grid integration, load management, and demand response.	[139]
GB/T 32960	China	A communication standard between EVs and EVCS. It serves as a protocol specific for AC and DC charging by facilitating features such as remote monitoring and vehicle diagnostics.	[140]
DIN SPEC 70121	Germany	A communication standard between EVs and EVCS. A specific protocol for AC and DC charging with features such as plug & charge and bi-directional power flow. Allows EVs to feed energy back into the grid.	[141]
CHAdeMO 2.0	International (e.g., EU, the Caribbean, India, Indonesia, South Africa, and Thailand)	An updated version of the CHAdeMO communication standard for DC fast charging. Enables bi-directional power flow, allowing EVs to discharge power back into the grid, with features such as authentication and billing, status reporting, and emergency stop.	[142]
CCS 2.0	International (e.g., EU)	An updated version of the Combined Charging System (CCS) standard for DC fast charging. Enables bi-directional power flow and features such as authentication and billing, status reporting, and emergency stop.	[143]
IEC 62351	International	A series that defines cybersecurity requirements for implementing security technologies in the operational environment. It includes objects for network and system management (e.g., with SNMP), role-based access control (RBAC), cryptographic key management, and security event logging.	[144]
GB/T 20234.3	China	A communication standard between EVS and EVCS in China. Enables features such as authentication and billing, status reporting, and emergency stop.	[145]
SAE J2293	International (e.g., N. America)	A standard defining the message requirements for communication using wireless power transfer technology. Provides a common interface for different types of electric vehicles allowing interoperability between different manufacturers.	[146]
SAE J2836	International (e.g., N. America)	A standard that specifies the application of OCPP and other industry-standard communication protocols such as the ISO 15118 and IEC 61850. Defines and facilitates the communication and exchange of data elements and messages between the EV and the EVCS.	[147]
ISO/SAE 21434	International (e.g., N. America)	A joint standard developed by the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) Focuses on cybersecurity of EVs and charging infrastructure. Provides guidance on risk assessment, vulnerability management, secure software development and testing, incident response, and security awareness and training.	[148]

DoS attack can render a charging station or other EV-related system unavailable by overwhelming it with traffic [50]. Conversely, a MITM attack involves intercepting and modifying communications, potentially resulting in data theft or tampering. Spoofing attacks enable cybercriminals to impersonate legitimate users, thereby gaining unauthorized access to sensitive information. Moreover, EVs battery is vulnerable to attacks, as battery draining attacks can rapidly deplete its charges. Malware is yet another type of attack that can infect EV systems, granting unauthorized access to vehicle controls or data, leading to disastrous consequences. Phishing and social engineering attacks also present significant threats to EV owners and charging station operators, as they can trick users into disclosing sensitive information or accessing critical systems. An attacker could effortlessly masquerade as a charging station operator and deceive EV owners into providing their credit card details, which could then be used for fraudulent purposes. As the use of EVs and charging networks continues to expand, the need for robust cybersecurity measures becomes increasingly vital. This entails regular software updates, data encryption, multi-factor authentication, and employee training programs to prevent phishing and social engineering attacks. The increasing complexity and sophistication of cyberattacks on information and communication systems highlight the need for advanced infrastructures to detect and recognize different types of possible attacks.

In this regard, the authors of Ref. [149] proposed an attack pattern detection system that involves designing and implementing real-time detection, analysis, modeling, and visualization of attack patterns, ultimately resulting in a labeled dataset of attack events. The proposed system, called APDMAVS, utilizes attack event correlation and fusion techniques in combination with an attack-based data visualization system that is provided by various security devices. The system is composed of three subsystems: Attack Event Detection Subsystem (AEDS), Attack Pattern Analysis and Modeling Subsystem (APMAS), and Attack Pattern Visualization Subsystem (APVS). It has significant flexibility from both software and hardware perspectives, addressing data integration, complexity, and throughput issues within common and extensible architectures. The transformed and optimized data obtained from potential attack patterns is processed by the attack pattern modeling and analysis subsystem. The detector interface is generic and independent of any particular technology, making it adaptable for future improvements such as new attack detectors, services, and architectural enhancements. The authors claim that the results of an attack carried out over six months under various assumptions allow the creation of a dataset of attack events labeled according to their attack patterns. The proposed real-time system provides organizations with highly realistic situational awareness about cybersecurity threats, enabling them to respond quickly in the face of any attack. Building datasets through attack-pattern modeling and computer code analysis is a critical step in the development of artificial intelligence.

The expanding use of cognitive radio (CR) technology in wireless networks highlights security vulnerabilities, particularly against primary user emulation (PUE) attacks. To counter this, the authors of Ref. [150] developed a localization-based defense (LocDef) scheme. This scheme utilizes a network consisting of TV signal transmitters as primary users, a mobile ad hoc network of secondary users equipped with self-localization capabilities, and

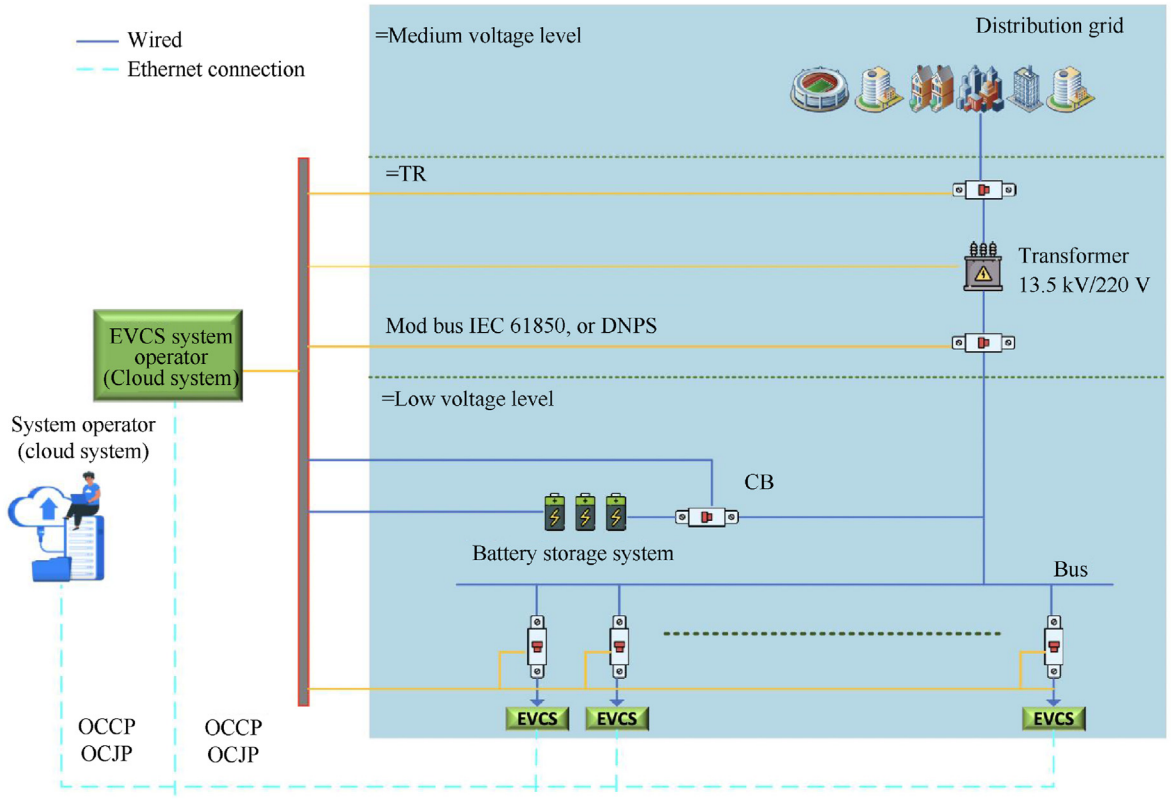

Fig. 5. Physical, cyber links and charging protocols & standards for EVs integration to the grid.

attackers capable of modifying modulation mode and transmission power. The LocDef scheme, which leverages a wireless sensor network (WSN) for synchronized RSS measurements and employs a smoothing technique to pinpoint RSS peaks, efficiently distinguishes between PUE attackers and legitimate primary users without altering the primary users for dynamic spectrum access (DSA). Simulation tests with 300 secondary users over 24 h demonstrated LocDef's robustness in identifying PUE attackers, even with transmitters within 500 m of each other. However, the greatest localization errors and computational times occurred when the primary transmitter was at the WSN's edge, and the use of directional antennas further increased these challenges by reducing sensor detection range. This LocDef scheme offers a viable strategy to bolster wireless network security, vital for sectors like EVCS, where the cognitive radio network is susceptible to such security threats. Implementing such defensive measures is essential for safeguarding the integrity of EV charging networks and ensuring the safety of users.

In Ref. [151], the authors introduce an analytical method to establish the lower bound on the probability of a successful primary user emulation attack (PUEA) on secondary users within a cognitive radio network, marking the first analytical exploration of PUEA feasibility. Utilizing Fenton's approximation and the Markov inequality, the study models the risk posed by coordinated malicious users. The research employs a system model where malicious and legitimate secondary users are uniformly distributed within a circular grid of a specific radius, with a primary transmitter fixed at a certain distance. This setup uses an energy detection method for spectrum sensing by secondary users, employing both a free space propagation model for primary signals and a two-ray ground model for malicious transmissions. Key findings reveal that the lower bound on the likelihood of PUEA is dependent on the distance between the primary transmitter and secondary users, with significant risk variations observed at distances of 2 km and 8 km. Specifically, the study notes negligible PUEA chances at 2 km with received powers ranging from 0.1 mW to 7.5 mW but sees a substantial increase in PUEA probability at 8 km due to a 10 mW discrepancy in received powers between primary and malicious sources. This research provides a valuable analytical framework for assessing PUEA risks in cognitive radio networks and suggests that increasing the circular grid radius could effectively reduce the probability of successful attacks by diminishing the power received from malicious transmissions. These insights are crucial for developing robust defense mechanisms against PUEA in scenarios similar to charging systems at EVCS.

In Ref. [152], the authors investigate into the concept of optimal sensing disruption within a CR technology network, carried out by a power-limited intelligent adversary, and its potential impact on EVCS. This adversary, neither a primary nor secondary user in the CR network, disrupts the system by emitting spoofing signals within the frequency bands used by secondary users. The goal of the adversary is to create the most detrimental effect on the CR system in the event of a spoofing attack. The study examines a scenario in a CR network where secondary users utilize energy detection to ascertain the availability of spectral bands. They employ a radiometer to detect disruptions in sensing, which occur when the adversary targets unused bands and introduces energy into them. This action misleads secondary users into perceiving a reduced number of available bands, a phenomenon referred to as false detections. To evaluate the effectiveness of optimal sensing disruption, the authors explore a strategy where the adversary uses equal power distribution across a partial band to conduct noise spoofing. This approach aims to maximize the average number of false detections, effectively minimizing the available bandwidth for

the CR system within the power limitations of the adversary. The analysis incorporates both thermal noise and spoofing signals to calculate the probability of false detection, defined as the likelihood of secondary users mistakenly sensing an available band as busy. Additionally, the study defines the false alarm probability as the chance that a vacant band is incorrectly identified as busy by secondary users. Key findings of the research include the observation that an increase in the average number of false detections corresponds to a rise in the number of spoofed bands and a decrease in detection threshold. Furthermore, enhancing the time-bandwidth product leads to improved spectrum sensing performance by secondary users. Overall, this study sheds light on the potential for sensing disruptions in CR networks caused by power-limited intelligent adversaries. It underscores the necessity of developing and implementing robust countermeasures to safeguard against such threats, particularly in contexts like EVCS where reliable communication and sensing are critical.

Automatic speaker verification systems, soon to be integral to modern vehicles including EVs, face vulnerabilities to cyberattacks such as replay and spoofing attacks. Such systems could be manipulated with minimal technical effort, posing risks like unauthorized transactions or access to personal information. In Ref. [153], the authors address spoofing attacks where attackers mimic a user's voice to deceive voice recognition systems. They propose WIVO, a device that enhances security by authenticating voice inputs alongside mouth movements. Additionally, the study suggests utilizing microphones that introduce non-linearity through inter-modulation distortion, which helps in distinguishing original voices from tampered ones. Effective countermeasures can exploit detectable patterns in distorted audio, utilizing metrics such as the minimum energy in high frequencies from the audio's short time Fourier transform. Moreover, employing Higher-Order Spectral Analysis (HOSA) features can further secure systems against replay attacks. As voice-driven interfaces grow common in vehicles, recognizing these cybersecurity threats becomes essential, urging the development of sophisticated defenses to protect user data and prevent misuse.

The increasing prevalence of modern vehicles and associated telematic services has heightened their vulnerability to remote control, particularly in terms of masquerade attacks. Such situation necessitates the creation of secure message authentication protocols for CAN networks to bolster defences against such threats. Existing protocols, however, are often inadequate in providing the required level of security. To address this, the authors of Ref. [154] introduce MAuth-CAN, a message authentication protocol tailored to shield against masquerade attacks. This protocol enhances the security of electronic control units (ECUs) against bus-off attacks and employs tamper-resistant hardware like SMART and TrustLite, or secret key-based access control to secure JTAG access to the authenticator. MAuth-CAN operates through four phases: initialization, message transmission, authentication, and parameter update. Initially, the authenticator distributes seeds and initial values for verification and creates session keys. During transmission, ECUs send periodic CAN messages which are authenticated in the subsequent phase, discarding any unverified messages. The final phase updates the protocol parameters as needed. The implementation demonstrated that MAuth-CAN effectively blocks fake CAN-IDs from compromised ECUs, mitigating masquerade attacks and enhancing protocol freshness, thereby reducing the risk of replay and message flooding attacks. However, the protocol's message authentication delay could affect real-time applications, prompting future research to minimize these delays and assess impacts on system performance.

Additionally, cyberattacks can exploit the EVCSs to establish a botnet that could overload the grid, resulting in congestion, line failures, and outages. To demonstrate the possibility of such an attack, previous research simulated a cyberattack on the power distribution and transmission networks by manipulating EVs as a botnet. The researchers revealed that EVs and their charging stations are vulnerable to various types of cyberattacks that can be exploited to establish a botnet. Here, we summarize these vulnerabilities, which include:

(1) The use of a mobile application by an EV user to communicate with a Mobility Service Provider (MSP) to locate a nearby charging station, which can be targeted by a hacker to gain access to the user's personal information.
(2) The communication of information between the EVs and EVCS, facilitated by the connector ports of the charging cable, creates a potential outlet for the transmission of malicious software. The EV and the charging station can both become compromised with malware that can proliferate to other EVs that subsequently utilize the same charging station.
(3) Attacking the charging station to prevent the EV from charging to its specified SoC or charging it at a pace that exceeds the EV's capacity, which can cause intentional damage to the EV.
(4) Targeting the Charge Point Operator (CPO) to manipulate the amount of charge received by the EV or to terminate the charging process before the user's requirements are met.
(5) Using a MITM attack to intercept or modify information between the EV and the charging station.

To demonstrate the potential impact of such attacks, the researchers in Ref. [155] employed the IEEE 33 bus system to simulate an attack on the distribution network, leveraging data from the Toronto Parking Authority to mimic EV availability in a commercial parking lot on bus 24 of the test system. They set the initial SoC of each EV to be uniformly distributed between 20% and 30%, targeting full charges before departure. Using MATPOWER, they modeled the network to pinpoint areas of significant voltage drop, identifying bus 17 as the most vulnerable, closely followed by bus 16, where 50 Fast Charging Direct Current (FCDC) stations were integrated. Further simulations on the IEEE 39 bus system explored cyberattacks broader ramifications, revealing that a mere 5% increase in load from an EV botnet could congest power networks and erroneously trigger protection systems. Such load-altering attacks could cause power outages and grid misoperations due to the distorted measurements from the EV botnet.

Effective monitoring and control of EV system states during cyberattacks on communication channels are pivotal in autonomous vehicle control. In this context, researchers in Ref. [156] introduced a state estimation and control algorithm that utilizes information to manage EV states under cyber threat conditions. The algorithm, based on a state-space model, captures vehicle dynamics and vision system interactions, focusing on four essential state variables: the slip angle, camera, front-wheel angle, and yaw moment, critical for managing the EV in both normal and automated driving. To enhance state monitoring, IoT-enabled smart sensors are employed. However, during data transmission to the control center, the risk of data manipulation by attackers exists. To counter this, a state estimation algorithm was developed to determine the EV's optimal state using mean square error principles and posterior estimation theorems. This algorithm continuously refines the state and error covariance with each iteration, improving the accuracy of vehicle state estimations over time. For state regulation during cyberattacks, the authors crafted a control algorithm employing semidefinite programming. This includes a feedback control law based on the separation principle and the semidefinite programming variable, $\xi > 0$, aiming to minimize estimation error

variance. The optimal gain, G, is computed using a linear matrix inequality approach. The algorithms proposed offer effective solutions for tracking and estimating system states amid cyber threats, proving capable of stabilizing system states within 1600 iterations and determining optimal feedback gain.

The authors in Ref. [157] presents methodology that leverages simulation modeling of a variety of realistic scenarios of replay and bogus information attacks in Vehicular Ad-hoc Networks (VANETs). The proposed methodology also includes the creation of an open dataset that can be used by other researchers to develop and evaluate machine learning-based solutions for detecting and mitigating malicious threats to connected and automated vehicles (CAVs). The research focuses on Dedicated Short-Range Communication (DSRC), which is a crucial aspect of VANETs. The researchers examine the basic safety message (BSM), probe vehicle data message (PVD), traveler information message (TIM), map data message, and signal phase and timing message (SPaT) in DSRC. The proposed methodology uses message sequence numbers to detect replay attacks and considers changes in sender position to detect bogus information attacks. To simulate the attacks, the researchers used the Eclipse MOSAIC simulation framework, which allowed for the integration of several simulation tools such as OMNET++, Urban Mobility, and SUMO. The MOSAIC scenario-converter tool was also utilized to create a database that contained all map-related tasks. The vehicle-to-everything (V2X) communication was performed using Corporate Awareness Messages (CAM) in the attack scenarios. To evaluate the proposed methodology, three datasets were generated, one without attacks, one with a replay attack, and a third with a bogus information attack. The authors argue that their proposed methodology and open dataset provide a valuable resource for researchers to develop and evaluate machine learning-based solutions for securing the intra-communications of vehicles. Furthermore, the proposed methodology could be effectively used to simulate malicious threats against EVs, with the open dataset serving as a benchmark for developing and evaluating machine learning-based solutions for proper detection and mitigation.

The amplifying reliance on EVCS for powering an increasingly transportation fleet necessitates unflagging attention to their cybersecurity, prompted by a spectrum of threats from unauthorized access to manipulation of the charging procedures. The pivotal aspect lies in the categorization of the causes of these attacks into high and low applicability based on their likelihood and frequency, as shown in Fig. 6. Predominantly, high applicability causes are the vulnerabilities routinely encountered due to the systematic oversight or negligence in system design and maintenance.

For instance, the use of outdated software, inadequate security mechanisms, or unencrypted network connections, are tantamount to leaving the proverbial doors wide open for the cyber adversaries. These vulnerabilities, frequently exploited, necessitate an expansive and standardized countermeasure approach encapsulating robust encryption techniques, secure network architecture, and regular system updates, thereby forming a formidable first line of defense. On the other end of the spectrum, low applicability causes represent relatively infrequent yet equally potent attack vectors. These may include insider threats or supply chain disruptions, requiring a higher degree of resources, specialized expertise, and often, unique circumstances for exploitation. Although these scenarios are rarer, their potential impact can be cataclysmic and must not be discounted. Countering such threats necessitates tailored approaches involving meticulous employee background checks and comprehensive supply chain auditing. The differentiation of high and low applicability should be perceived through the lens of frequency and feasibility rather than the severity of the attack, thereby profoundly influencing the blueprint of cybersecurity implementation strategies.

The repercussion of these attack causes on EVCS cybersecurity cannot be understated. An attacker capitalizing on a high applicability cause, such as an unpatched vulnerability, could manipulate charging processes or pilfer user data. Simultaneously, an attack stemming from a low applicability cause, for example, an insider threat, could dismantle the system's integrity, leading to significant data breaches and irreversible reputational damage. Implementing the requisite countermeasures is a multi-pronged undertaking. The need for staunch cybersecurity practices must be ingrained within the organization's ethos, permeating from the executive leadership to the operational personnel. Technically, this involves consistent system updates, rigorous password policies, encrypted communications, secure network protocols, and exhaustive vulnerability testing. Concurrently, employee training on cybersecurity best practices, regular system audits, and rapid incident response protocols form the human facet of this cybersecurity strategy.

Other studies that navigates through the cyberthreats within the EVs paradigm include the discussion of vulnerabilities and potential risks associated with cyberattacks in next-generation cars [158–160]; investigation of the vulnerabilities and consequences of FDI attacks on the reliability and security of EV charging systems [161]; risk analysis of cyber-physical distribution systems, including cyberattacks against the V2G system [162,163]; modeling and simulation of cyberattacks against vehicles through the application of the Meta Attack Language (MAL) [164]. Table 3 shows different types of attacks that could take place within various applications of EVs. Fig. 7 present classification on various cyberthreats on potential attacks on EVs per its type, whereas Fig. 8 illustrates different types of intra-vehicles communication-related threats on EVs.

2.3. Third taxonomy: defensive, countermeasures and detections algorithms taxonomy

Without adequate protection, cyberattacks on EVCS could have far-reaching and significant consequences, impacting not only the charging infrastructure but also the safety and security of users. Consequently, it is essential to develop defensive countermeasures to safeguard EVCS from cyberattacks. In particular, the development of detection algorithms to identify and mitigate potential threats has emerged as a critical aspect of securing EVCS. Considered as an underexplored area of research, only few works in literature have proposed approaches to developing detection algorithms for EVCS. These approaches ranged from ML algorithms to statistical analysis techniques. Nonetheless, the efficiency of these approaches varies depending on the specific characteristics of the EVCS system. Thus, it is crucial to identify the most effective detection algorithm for each EVCS system and continually enhance its performance through testing and refinement.

As the frequency and complexity of cyberattacks escalate, the vulnerabilities of cyber-physical systems, particularly EVs, are increasingly exposed. To counter these threats, researchers have developed various protective mechanisms and algorithms. Among these, encryption techniques like the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are prominent. AES uses a single secret key for encryption and decryption, ensuring secure data exchanges, while RSA employs a public key for encryption and a private key for decryption, enhancing communication security.

Intrusion Detection and Prevention Systems (IDPS) serve as another critical defense, analyzing network flows to detect and prevent cyber breaches. Artificial intelligence (AI) and machine learning techniques, such as neural networks and SVM, are trained to quickly identify malicious activities, protecting various aspects of

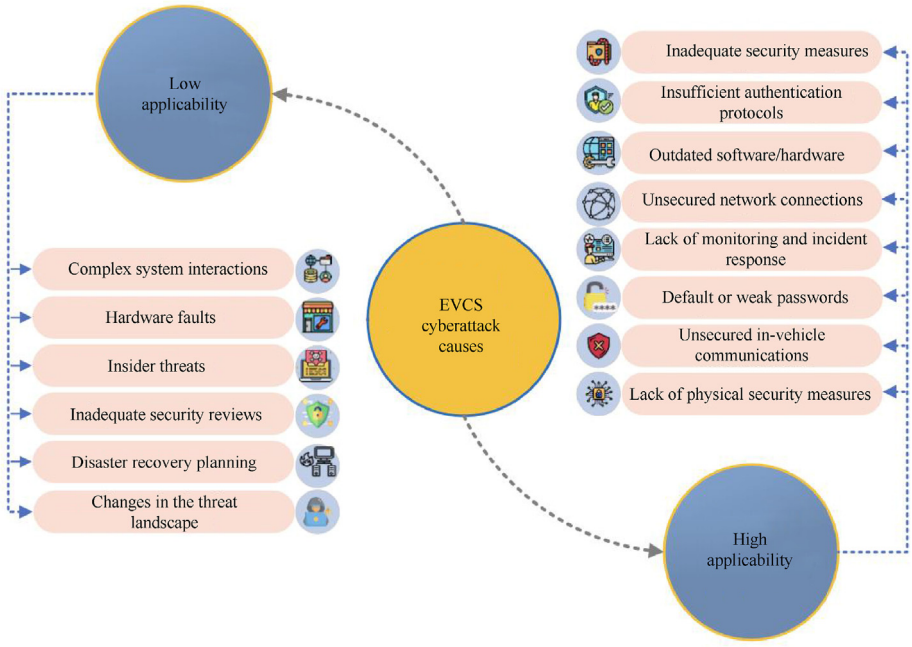

Fig. 6. Low- and high-level applicability of cyberthreats against EVCS.

Table 3
Potential cyberattacks against EVCS with their explanations.

Attack type	Brief description	Potential threats on EV
Denial-of-service (DOS) attack	In this attack, a system is overwhelmed with requests or traffic by an attacker resulting in its unavailability to legitimate users.	By overwhelming the charging station with requests, other electric vehicles are prevented from using the charging station.
Replay attacks	This type of attack occurs when legitimate conversion between two devices is recorded and replayed repeatedly back to one of the devices.	The EV is deceived into receiving unauthorized commands when a communication between it and a charging station is recorded and replayed back to it.
Side-channel attacks	Take advantage of unintended channels like electromagnetic radiation or power consumption, this attack involves extracting sensitive data.	An attacker can possibly eavesdrop on a communication ongoing between the EV and the EVCS by extracting the private key applied to encrypt communication.
Phishing attacks	Such attacks trick a user into revealing private information or downloading malicious software.	The owner can be prompted to download a software update that contains malware when it receives a false email appearing to have come from the manufacturer.
Jamming attacks	A jamming attack where an attacker swarm wireless networks with noise or interference, leading to interrupted communication.	Wireless signals used by the vehicle's systems can be jammed making the vehicle potentially less functional than expected.
GPS spoofing attacks	This type of attack leads to possible misdirection or crashing of a vehicle's GPS system by manipulating its function.	The vehicle receives false GPS signals that says it islocated somewhere different from its original location which could force an accident and even loss of lives.
MitMM attacks	In this attack, exchange of information between two devices is interrupted and twisted.	The attacker is able to steal private data or introduce malicious commands by interrupting the communication between the EV and EVCS
Buffer overflow attacks	In this attack, a system receives more data than its reception capacity or expectation causing a potential crash or execution of unplanned code.	Taking advantage of a buffer overflow vulnerability in the vehicle's systems can lead to its breakdown or malfunction.
SQL injection attacks	This kind of attack gains unauthorized access to the database or manipulate its contents by injecting malicious code into a database query.	An attacker is capable of stealing private data or overrunning the vehicle system by inserting malicious code into its firmware or software.
Electromagnetic pulse (EMP) attacks	Generate an intense eruption of electromagnetic radiation, an EMP attack induces potential damage or inactivates the electronic system.	The vehicle becomes non-functional when an EMP device is used to inactivate its electronics.

EVs from battery systems to communication networks. Additionally, anomaly detection methods analyze data streams to spot unusual behavior, aiding in the early detection of new threats. Security measures like secure booting verify digital signatures on firmware and software, preventing unauthorized access. Communication security is further bolstered by protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which encrypt data transfers between EVs, charging stations, and cloud platforms.

Hardware Security Modules (HSMs), which are specialized cryptographic units, ensure the safe management of keys and data storage, providing a hardened defense against targeted attacks on cryptographic assets. Despite the robustness of these defenses, no system is entirely impervious to attacks. Therefore, a comprehensive cybersecurity strategy for EVs must integrate these technologies and continuously refine and assess them to ensure they remain effective against evolving cyber threats.

In Ref. [165], the authors present a metaheuristic-based detection algorithm called Spider-Monkey Time Synchronization (SMTS), crafted to identify Sybil Security threats in Vehicular Ad

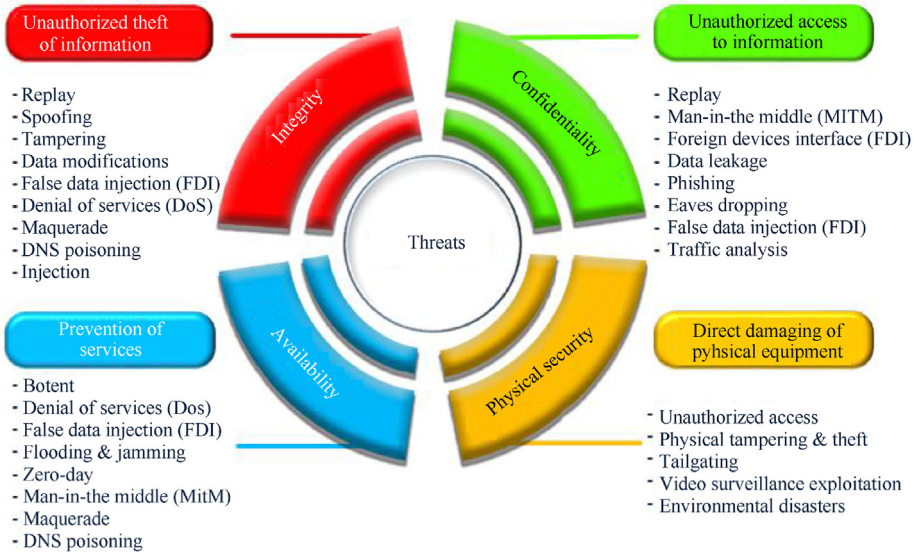

Fig. 7. Classifications of cyberthreats against EVCS.

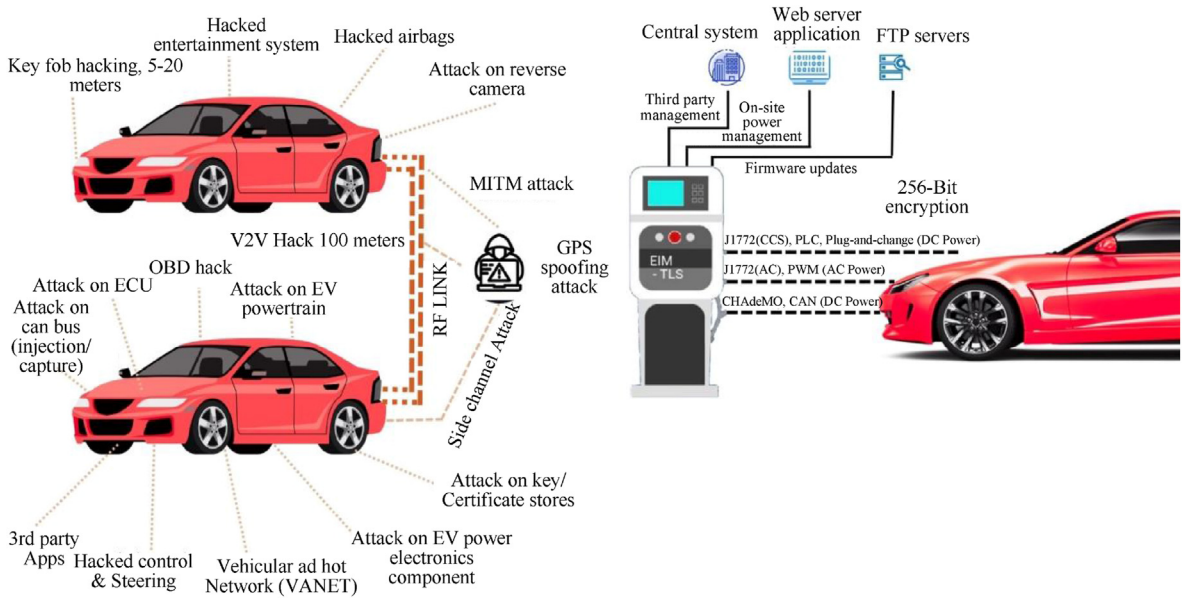

Fig. 8. Potential Cyberthreats targeting intra-communication for EVs.

Hoc Networks (VANETs). The SMTS algorithm is designed to synchronize packet delivery times and minimize energy consumption while detecting Sybil attacks, which involve communication interference and the creation of fake identities. The algorithm consists of three core components: the Spider Monkey Detection Technique (SMDT), Spider Inter-Vehicle Time Synchronization (SIVTS), and Spider Intra-Vehicle Time Synchronization (SInVTS). SMDT uses a meta-heuristic approach to locate malicious nodes conducting Sybil attacks. SIVTS manages the transmission of beacon messages across vehicles in the network, specifically from sensors in honest vehicles to a base station. SInVTS, on the other hand, employs a reference broadcast method for message exchange between cluster heads and vehicle members. Both SIVTS and SInVTS aim to eradicate errors along the transmission path, improving synchronization efficiency. The SMTS operates by measuring legitimate vehicle counts within set confidence intervals and identifying sensor nodes of nearby malicious vehicles by releasing an alarming pheromone when discrepancies are detected. This involves comparing beacon message times from the source vehicle to the packet information received at the destination, analyzing clock offset and propagation delays to effectively detect Sybil attacks. Detection thresholds are set at 90%, 95%, and 98% to catch malicious vehicles operating under multiple identities. Simulation results show that SMTS surpasses existing protocols like P2DAP, SKC, and EAPDA in detecting Sybil attacks, particularly over extended distances and with minimal energy consumption per sensor node during beacon interference. pheromones.

The use of metaheuristic-based techniques in detections of cyber manipulation continues with the work of Ref. [166], where the authors present an algorithm to detect cyberattacks in DC microgrids and DERs. The authors propose the utilization of the Krill Herd Optimization (KHO) algorithm along with the Hilbert-

Huang Transform (HHT) and deep learning to extract signal features and identify Fault Detection and Isolation Attacks (FDIAs) in the DC network, including vulnerabilities in EVCS. Deep autoencoders are constructed with SAE, DAE, and Linear decoders to learn hidden issues, and the KHO algorithm is used to optimize thresholds.

To bolster the security of distributed frequency estimation in multi-EV frequency regulation scenarios, the authors of Ref. [167] introduced a credibility-based load frequency control (DLFC) scheme aimed at detecting and isolating EVs compromised by FDIA attacks. The DLFC is executed through a four-step process: initially, it establishes credibility metrics for frequency estimates of neighboring EVs, calculating the average of collected measurements from EVCS. Next, the energy management system (EMS) updates the credibility coefficients for neighboring EVs based on these metrics. In the third step, the scheme employs an iteration-time-dependent threshold to isolate affected EVs, followed by extensive simulations to test the adaptive threshold functions for efficacy. The DLFC scheme also features a rule that dynamically adjusts local estimates using data from neighboring EVs and EVCS. If an EV is deemed compromised, the EMS disconnects its link and zeroes its estimated weight, aligning well-behaving EVs with their assigned EVCS's average measurements for seamless integration into DLFC operations with conventional generators. This approach has been validated through simulations in a four-area power system model and two case studies—one with a strongly connected and another with a non-strongly connected interaction topology. Results demonstrate that the proposed method enhances frequency regulation efficiency and speed in isolating compromised EVs compared to conventional methods, particularly under similar load disturbances.

In Ref. [168], the authors tackle the security of EVCS using deep neural network (DNN) and long-short term memory (LSTM) algorithms to detect and classify DoS attacks effectively. The study develops a three-layered DNN with two hidden layers featuring the ReLu activation function and L1-L2 regularization to optimize parameters, addressing the vanishing gradient problem with the introduction of LSTM. Extensive data preprocessing and normalization were conducted, including Min-Max scaling and hot encoding, distributing the data as 50% for training, 20% for validation, and 30% for testing. The evaluation demonstrated that LSTM was exceptionally effective in identifying DoS attacks, showing a training accuracy of about 99.95% in just 10 periods, significantly outperforming the DNN, which required up to 70 periods to achieve comparable results. This comparative analysis between LSTM-based and DNN-based IDS in EVCS, assessing metrics like accuracy, precision, recall, and F1-score, underscores the advanced neural network algorithms' capability, particularly LSTM, in boosting EVCS cybersecurity and mitigating DoS attack risks.

In Ref. [169], the authors implemented a machine learning-based IDS to identify spoofing attacks in EVCS. The IDS leverages probabilistic cross-layer metrics, incorporating both physical (PHY) and application (APP) layer data to detect malicious nodes. This system was tested under scenarios involving 50–200 EVs using either a static charging station (SCS) or a combination of SCS with a Mobile Energy Discriminator (MED). The proposed ML-based IDS captures beacon messages from entering nodes, which contain data such as location, speed, and MAC addresses, updating the MED and SCS. Metrics like RSSI, SINR, PDR, relative speed, and GPS coordinates are utilized for detection. The system employs K-NN and RF algorithms, with data split 70% for training and 30% for testing, achieving an accuracy of approximately 91%, improved by 6% when integrating the Position Verification Relay System (PVRS) metric. Performance was assessed using detection rate, ROC curve, AUC, and accuracy measures. The IDS's capability to differentiate between legitimate and spoofed beacon messages effectively pinpoints spoofing attackers within the system. The authors credit the use of cross-layer metrics and a data fusion approach for the robust detection outcomes.

In Ref. [170], the authors present a multi-detector framework aimed at detecting and mitigating cyberattacks on autonomous EV sensors, specifically targeting GPS and Light Detection and Ranging (LiDAR), which is used to provide accurate, real-time 3D information about the vehicle's surroundings, for secure vehicle localization. The framework incorporates a rule-based isolation scheme to identify the sources of anomalous sensor readings, validated using actual vehicle data. Given the susceptibility of GPS and LiDAR to various cyber threats—including DoS, FDIA, stealthy, and replay attacks—the framework utilizes a systematic approach to monitor and analyze sensor data for attack detection, structured as follows:

(1) Online Measurements Analysis: The framework analyzes real-time data from GPS and LiDAR using three distinct attack detectors.
(2) Integration with Extended Kalman Filter (EKF): These detectors incorporate an EKF-based pose estimator combined with a Cumulative Sum (CUSUM) discriminator to evaluate the data.
(3) Individual Sensor Analysis: The first two detectors independently assess the position and orientation based on GPS and LiDAR data, respectively. Concurrently, the CUSUM discriminator identifies discrepancies between the sensor measurements and the predicted states.
(4) Cross-Sensor Analysis: The third detector focuses on detecting inconsistencies between GPS and LiDAR readings, integrating data from both sensors to enhance detection accuracy.

This structured approach allows the framework to effectively identify malicious activities affecting sensor data, thereby enhancing the security and reliability of sensor-based systems in autonomous EVs. The framework also includes protocols for responding to detected threats, ensuring the safety of the vehicle using alternative sensor readings and, if necessary, switching to manual driving mode. These features make the framework particularly valuable for maintaining the safety and security of AEVs, which rely heavily on accurate sensor information for their operation.

In Ref. [171], the authors present a data trust framework aimed at identifying and categorizing false battery sensor data within Battery Energy Storage Systems (BESS) used in EVs and power grids. This framework leverages a Convolutional Neural Network (CNN) diagnostic platform focusing on key parameters like voltage, current, and state of charge (SoC). The core of the proposed work is the CNN-based False Battery Data Detection and Classification (FBD2C) algorithm, which uses AI and deep learning to enhance the accuracy of online battery data. The algorithm simulates various faults using a lithium-cobalt rechargeable (ICR) 18650 26F cell, employing MATLAB/Simulink. The proposed FBD2C algorithm includes three 1-dimensional convolution layers and a max-pooling layer for feature extraction, plus additional layers for processing and output. It is validated using datasets from different battery cells, achieving training accuracy of 99.5% and validation accuracy of 98% over 100 epochs, outperforming other AI algorithms like LSTM and GRU. This demonstrates its effectiveness in detecting and classifying false battery data in BESS, significantly enhancing the reliability and security of EV and power grid systems.

Recent advancements in wireless sensor networking technologies have enabled the integration of EVs and other components into the smart grid, necessitating secure communication protocols to

efficiently and securely manage connected devices. In this context, the authors of Ref. [172] developed a mitigation scheme that utilizes the inherent connectivity capabilities of EVs to manage charging loads effectively. This scheme employs wireless ad-hoc networks to facilitate safe communication between EVs, Roadside Units (RSUs), and other intelligent transportation systems within the smart grid, including EVCS. The proposed scheme leverages the IEEE Wireless Access in Vehicular Environments (WAVE) standard and the IEC 61850 power utility automation and communication standard to ensure consistent data assembly across all component applications—critical for robust power utility communication. Additionally, a new Logical Node (LN) class, the EVs Control (EVCT), is introduced to manage EVs. This LN acts as a sub-function within the network, defining the data and parameters exchanged in the V2G process and monitoring the critical functions and states of the charging process.

The authors of Ref. [173] propose a novel approach to the energy trading process (ETP) between EVs and distribution networks (DN) using blockchain technology. The study addresses the issue of malicious attacks on the ETP by validating the Byzantine based consensus algorithm as a security defensive measure. The ETP involves communication between DN and EVs in the parking lot, with only EVs having more than 75% SoC allowed to participate. Encrypted data is transferred as hashed messages, with each node of the peer-to-peer (P2P) network verifying local blocks via the Byzantine based consensus algorithm. The authors proposed Byzantine Fault Tolerance (BTF) algorithm, implemented via SCADA system, to secure the ETP between the EVs and DN. The algorithm is validated using the standard IEEE 33 bus system, with findings indicating that the BTF provides over 33% security against false data communicated between DN and EVs, and less than 0.1 probability of an attack on P2P nodes. Compared to the Proof-of-Work (PoW) consensus, the BTF centralized node identity management, better satisfied finality, accommodated a wider range of transactions, and could tolerate the most corrupted nodes. Overall, the proposed approach provides a secure and efficient means of energy trading between EVs and DN, addressing the issue of malicious attacks on the ETP.

To continue the discussion around defensive mechanisms, Dey and Khanra [174] developed two algorithms to detect cyberattacks during EV charging. The static detector uses measurement variables, while the dynamic detector employs both system dynamics knowledge and quantification parameters. This model focuses on overcharging and denial-of-charging (DoC) threats and aims to provide a framework for detecting cyberattacks that may affect EV battery packs during charging. The proposed approach utilizes diagnostic security modules (DSM) installed in both the EV and supply equipment of the EVCS. If a possible threat is identified, the EVCS instantly dismisses charging or initiates corrective action. Although the dynamic detector outperforms the static detector in detecting attacks, its integration comes with an additional computational cost. Thus, creating a filter-based design with a multi-objective criterion, including stability, robustness, and attack sensitivity, is necessary for dynamic detectors.

Su et al. [175] developed a defensive algorithm to address privacy and security concerns in the volatile energy markets of smart communities (SC). They introduced a 'contract-based energy blockchain for secure EV charging' and an energy allocation mechanism to tailor EV charging schedules according to varied energy consumption preferences, aiming to maximize benefits for both operators and consumers. This multifaceted approach is structured into four stages:

(1) Integrating trustworthy charging with smart contracts on a permissioned energy blockchain.
(2) Introducing a 'reputation-based delegated Byzantine fault tolerance (DBFT) algorithm' for achieving consensus on the blockchain.
(3) Optimizing contracts through contract theory to align with EVs' energy needs and improve operator utility.
(4) Proposing a method to allocate limited renewable energy to EVs, optimizing resource distribution

The proposed blockchain framework features an aggregator that oversees EV charging, equipped with smart meters to monitor energy usage, and a microgrid enhanced with solar panels. The implementation of the energy blockchain smart contract progresses through three phases—Init, Create, and Invoke—which support energy and cryptocurrency transactions between the EV and aggregator. This contract-based method not only optimizes EV charging within the SC but also effectively mitigates security and privacy issues inherent in uncertain energy markets, providing significant advantages to operators and EV owners alike.

As previously noted, the CAN network is a fundamental element in modern connected vehicles but is susceptible to various cyber threats affecting driver and passenger safety and privacy. The authors in Ref. [176] suggest the implementation of a Decentralized Security Exchange (DSE) system, featuring a cost-effective diagnostic security monitoring (DSM) computer for vehicles that can identify and analyze vehicular cyberattacks. Unlike the CAN system, the DSM maintains lists of verified (whitelist) and malicious (blacklist) data, facilitating the real-time exchange of these lists, along with alerts and updates on malicious activities. Moreover, the DSE system enhances V2V communication, addressing gaps in vehicular infrastructure resilience. The authors report that over 55% of vehicles at an intersection can successfully complete V2V data exchanges, ensuring that emergency detections are comprehensive and that vehicles requiring updates receive them promptly. The system is implemented on a Raspberry Pi connected to the vehicle's CAN bus, configured for encrypted data exchanges via WiFi or WiMax, optimizing for low latency. However, the authors acknowledge potential vulnerabilities where high latency or disasters could be exploited by hackers.

The authors of Ref. [177] tackle the increasing challenges in information security and traffic network management for charging piles by proposing a self-learning intrusion attack detection method that leverages deep learning algorithms, specifically LSTM neural networks. This approach addresses the shortcomings of traditional IDS by providing a dynamic, closed-loop system that adapts continuously, enhancing the ability to detect a broad spectrum of attacks and enabling smarter detection capabilities. The proposed system focuses particularly on Sybil attacks, where malicious vehicles manipulate multiple false identities to disrupt network integrity. The detection method is structured into three critical steps: packet inspection, identification of Sybil nodes, and isolation. Optimized for analyzing vehicular data in VANET, the LSTM model performed well in processing time-series data, making it highly effective for anomaly detection and thus, ideal for identifying Sybil nodes. The system is designed to identify malicious vehicles when their trust value falls below a predefined threshold, quickly and accurately pinpointing various types of malicious nodes and outperforming existing models. Overall, the proposed approach provides a robust security solution for the V2V communication environment, ensuring the safety and security of charging pile operations and effectively safeguarding against cyber threats.

In Ref. [178], the authors introduce a cyberattack detection and diagnosis algorithm that uses model-based, data-driven residuals to monitor long-term cyberattacks on the EMS controller and signal measurements. This method involves a three-step detection process that evaluates controller performance in real-time, correlates

feedback signals with output control input, and generates residuals to detect cyberattacks using long-term data. Tested against two types of cyberattacks on both the sensor and controller of the BMS, the algorithm quickly identified controller and SoC attacks during online testing, proving its effectiveness in securing Hybrid EVs powertrain systems against malicious cyber-physical attacks. Similarly, the authors of Ref. [179] developed a counter-attack security measure aimed at protecting the OBC systems of EVs from data integrity-based cyberattacks. The proposed threat-detection algorithm (TDA) utilizes sensor data and a moving average calculation to detect cyberattacks and provide real-time isolation signals. This process helps regulate the master decision signal, which in turn stops the gate pulses during an attack. Simulation tests demonstrated that reducing the number of points in the moving average calculation allowed the TDA to respond faster and with less voltage overshoot, effectively safeguarding the OBC systems from loss of load attacks and reisolating compromised components. This algorithm has been shown to be a reliable and efficient security measure for combating cyber threats in EV's OBC systems.

As outlined earlier, power electronics (PE) circuits are critical components in modern vehicles and require connectivity to external networks for optimal functionality, exposing modern EVs to increased cyber risks. Guo et al. [180] introduced a defensive strategy that utilizes physics-guided machine learning to detect cyberattacks on EVs' PE circuits across various driving conditions. This strategy integrates physics-based and data-driven models to enhance the detection of cyber threats, such as FDI and replay attacks, which manipulate real-time data. The proposed model combines recurrent neural networks with physics-based modeling to improve prediction accuracy and response to cyberattacks. It incorporates both developed physic-guided data characteristics and raw system data to enhance the robustness against data tampering. Additionally, the model employs vehicle-level signals and a machine learning-based classifier, coupled with real-time monitoring, to bolster training accuracy and enhance the detection of cyber threats. The driving model within the powertrain system utilizes a Proportional-Integral-Derivative (PID) controller for velocity tracking, allowing the EMS to equitably distribute torque. Surveillance systems gather and analyze signals to facilitate early threat detection. To capture the vehicle's dynamic physical attributes, the model leverages raw data from both device and vehicle levels, trained offline and subsequently deployed for real-time operations. Validated in an OPAL-RT HIL simulation testbed, the model demonstrated robust performance across various driving scenarios, showcasing its efficacy in securing EVs against cyberattacks.

In Ref. [181], the authors propose an anomaly-based detection technique to counter Distributed Denial of Charge (DDoC) attacks that target the spatial-temporal coordination mechanism in EVCS, which can cause long waiting times at charging stations. The authors use CNNs to detect anomalous charging request patterns that deviate from normal demand patterns for EVCS. Since there is no publicly available dataset for EVCS demand, the authors created a hypothetical dataset that mimics the charging needs of taxi fleet vehicles. The authors then augmented this dataset using adaptive synthetic sampling (ADASYN) to escalate the number of benign samples to equalize the malicious samples. The CNN-based algorithm takes the EVs demand vector as input, and a set of filters is utilized to extract time-series information to preserve the temporal feature of demand vectors of various EVCS. This allows navigation across input data to train and learn certain features that allow detection of deviation in charging requests patterns from normal values. The authors conducted experiments to test the performance of their proposed method when a single and multiple EVCS are under cyberattack. For a single EVCS under attack, the CNN-based method recorded a 93.9% detection rate (DR) with a 1% false alarm rate (FA). However, the detection rate reduced when multiple EVCS were under attack. For instance, the DR for two EVCS under attack is recorded as 88.4%, and a FA of 1.7% is recorded.

Other studies in the literature that navigates through detection algorithms within the context of EVs include Ref. [182] where the authors propose a deep reinforcement learning-based framework to enhance the resilience and security of EV charging stations against cyber-attacks; a Wasserstein Conditional Generative Adversarial Network (WCGAN) detection algorithm that classify cyberattacks targeting EVCS [183]; detection of cyberthreats against fast charging stations [184]; anomaly detection algorithm [185] and ML-based intrusion detection algorithm [186] to detect cyberattacks against EVCS; a ransomware detection of cyberthreats within SCADA system of EVs using ML-based algorithm [187]; detection against FDIA against EVCS [188,189]; a two-stage protection scheme for the detection and mitigation of coordinated Electric Vehicle Supply Equipment (EVSE) switching attacks [190]; a detection and localization framework that enhances the security of EVCS via identifying and localizing adversarial oscillatory load attacks [191]; a detection strategy for EVs during charging via the Combination of Ensemble Empirical Mode Decomposition with Adaptive Noise (CEEMDAN) and Broad Learning System (BLS) [192]; and a method that analyzes the timing behavior of CAN bus packets to detect potential cyberattacks [193]. On the other hand, studies that focus on the defensive strategies within the EV-paradigm include the work in Ref. [194] which navigates through potential vulnerabilities posed by quantum computing advancements via integrating post-quantum cryptographic algorithms into the EVCS; an anonymous authentication protocol to facilitate efficient communications in V2G networks [195]; a protocol that utilizes pairing-based cryptography to enable secure authentication between EVs and the grid [196]; a wireless authentication solution and a TTCN-3 based test framework for ISO-15118 wireless for Vehicle-to-Grid V2G communication [197]; a robust V2G control algorithm against cyberattacks [198]; novel IDS against attacks on Internet of vehicles [199,200]; quantum computing-based detection algorithm against DoS attacks in EVs [201]; and IDS algorithm to detect cyberattacks in intra-vehicles network [202].

2.4. Fourth taxonomy: verification and validation through software- and hardware-implementation

Verifying the EV-related cybersecurity studies using software and hardware tools is very central to achieve secure operation of EVs. The verification and validation enable researchers and developers to evaluate the effectiveness of various security measures and identify potential vulnerabilities systematically and comprehensively. The insights gained from such studies can help stakeholders develop effective strategies for detecting cyberthreats and implementing countermeasures to safeguard EVs against them. The significance of verification and validation through rigorous software and hardware implementation cannot be overstated, as it plays a crucial role in ensuring the safety and security of EVs, which are expected to serve millions around the globe within few years. Fig. 9 depicts the arrangement of various software employed in the verification studies pertaining to the cybersecurity of EVs. The diagram highlights that a significant portion of these studies relied on the utilization of MATLAB, hardware-in-the-loop, and Python for simulation purposes. However, it is worth noting that approximately 25% of the surveyed works did not specify the software or hardware utilized to obtain their research results. It is important to mention that survey papers lacking any simulation or hardware implementation were not included in the categories presented in the diagram. Lastly, a seminal contribution in the domain of

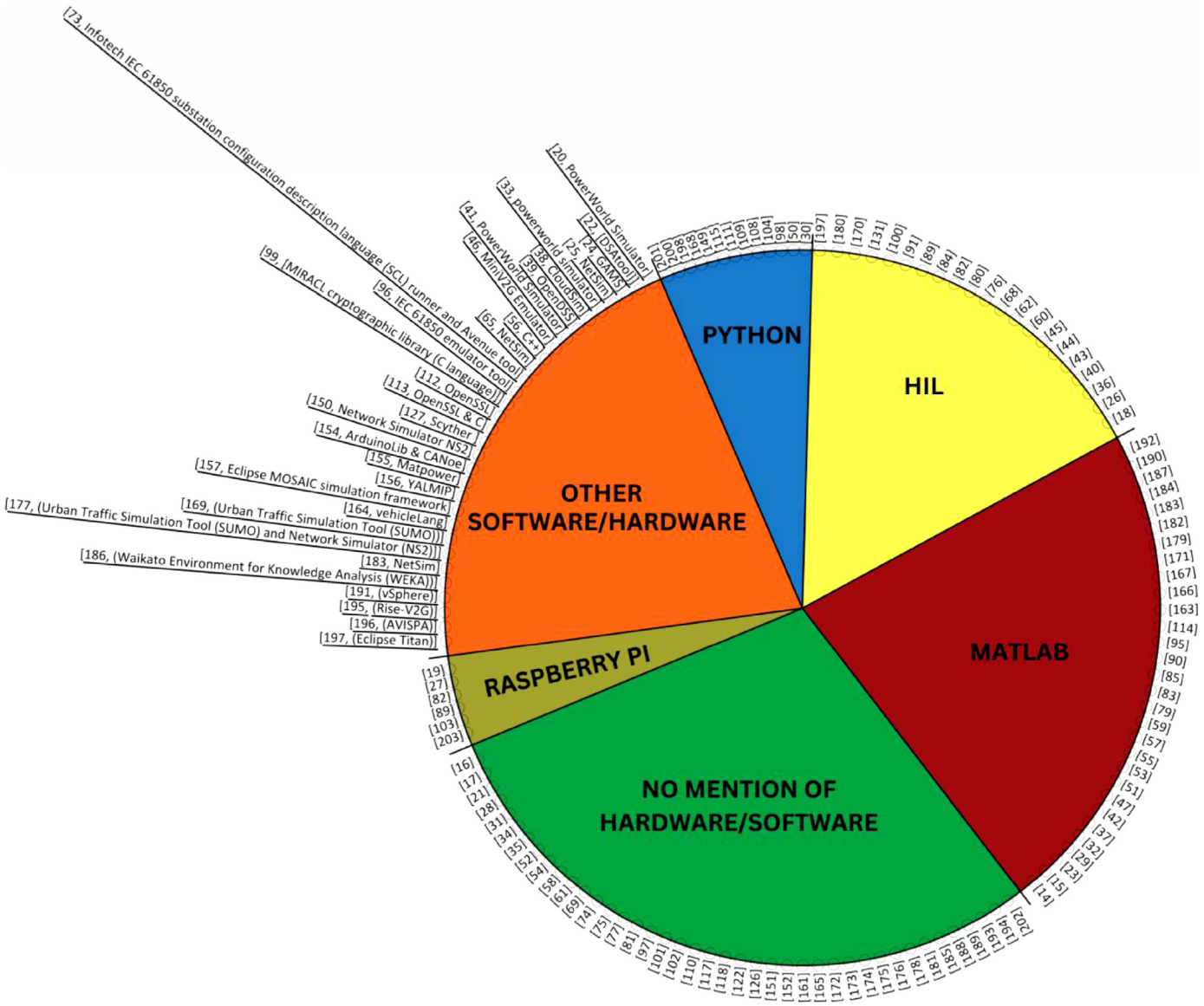

Fig. 9. Classification of various hardware equipment and software programs used in literature for EVCS cybersecurity-related studies.

cybersecurity in electric vehicles is the study by Koscher et al. (2010) [203]. This work stands out for being among the first to conduct empirical experiments related to the cybersecurity of ECU in modern cars, providing valuable insights into the vulnerabilities of contemporary vehicle systems. Its significance lies in laying the groundwork for subsequent research endeavors, effectively advancing the understanding and mitigation of cybersecurity threats in the field of EVs.

3. Conclusions

In the contemporary landscape of transportation electrification, the cybersecurity of energy infrastructures stands as a central concern. This is true as millions of EVs are expected to be on the roads in the upcoming years, with their integration to the grid requiring extensive communication infrastructure to allow efficient coordinated control and real-time decision making [204]. This paper highlights the dual role of EVs—not only as dynamic loads but also as critical vectors for cyber threats due to their bi-directional communication with various smart grid stakeholders. The motivation for this comprehensive survey is to fill the gap in literature, primarily due to the prevailing deficiency in public awareness and research traction in the cybersecurity within the EV paradigm. Through a detailed taxonomy, this work organizes and clarifies the complex cybersecurity issues prevalent in this field. Each section begins with an in-depth discussion that lays a solid foundation, preparing readers to dive into the more complex aspects of the research. The exploration covers several vital research domains essential to EVs, including the intricacies of charging infrastructure, communication protocols, and the vulnerabilities of powertrains and power electronic components. Moreover, the study thoroughly examines CIA-based threats, shedding light on potential safeguards against them. It also presents a broad spectrum of defensive strategies, including preventive measures, detection algorithms, and response mechanisms. Furthermore, this work discusses methodologies for verification and validation, highlighting approaches to test and ensure the robustness of EV cybersecurity in the reported literature. This structured approach not only enhances understanding but also guides future research directions in securing EV infrastructures against growing cyber

threats.

In closing, as the realm of electric mobility continues its ascendancy, ensuring its cyber-resilience becomes indispensable. This taxonomy aim to serve as an essential guidance map for researchers and practitioners in navigating the different terrains of cybersecurity within electric mobility.

Declaration of competing interest

The authors declare no competing interest.

Acknowledgements

This work was supported by the Deanship of Postgraduate Studies and Scientific Research at Majmaah University under Project (Grant No R-2024-1183).

Glossary

EVs	Electric Vehicles
EVCS	Electric Vehicle Charging Station
ICVs	Internal Combustion Vehicles
IDS	Intrusion Detection Systems
IoT	Internet-of-Things
CIA	Confidentiality, Integrity, and Availability
DoS	Denial of Service attacks
OBC	On-board Charging Controller
HMI	Human-Machine Interface
CAN	Controller Area Network
SoC	State of Charge
OCPP	Open Charge Point Protocol
DERs	Distributed Energy Resources
IPs	Internet Protocols
SCADA	Supervisory Control and Data Acquisition
FDI	False Data Injection attacks
DDoS	Distributed Denial of Service attacks
MITM	Man-In-The-Middle attacks
BES	Battery Energy Storage System
HTTPS	Hypertext Transfer Protocol Secure
MUs	Monetary Units
ICTs	Information and Communication Technologies
ECUs	Electronic Control Units
BMS	Battery Management System
USBs	Universal Serial Buses
DWT	Discrete Wavelet Transform
SVM	Support Vector Machine
ADN	Addition of Random Number
MILP	Mixed Integer Linear Programming
V2V	Vehicle-to-Vehicle
V2G	Vehicle-to-Grid
V2X	Vehicle-to-Everything
Eve	Potential Eavesdroppers
HIL	Hardware-in-the-loop
RL	Reinforcement Learning
EMS	Energy Management System
ITS	Intelligent Transportation Systems
CAEVs	Connected and Automated Electric Vehicles
ICS	Industrial Control Systems
PE	Power Electronic Circuits
XFC	Xtreme Fast Charging EVCS
EMI	Electromagnetic Interference
FCNs	Fog Computing Nodes
MMS	Manufacturing Messaging Specification
GOOSE	Generic Object-Oriented Substation Event
NIST	National Institute of Standards and Technology
MDMS	Meter Data Management System
IED	Intelligent Electronic Devices
MAC	Message Authentication Code
UDP	User Datagram Protocol
OSI	Open System Interconnection
ETSI	European Telecommunications Standards Institute
CSMS	Charging Station Management Systems
TLS	Transport Layer Security
CR	Cognitive Radio technology
PUE	Primary User Emulation
PUEA	Primary User Emulation Attacks
VANETs	Vehicular Ad-hoc Networks
AES	Advanced Encryption Standard
RSA	Rivest-Shamir-Adleman
SSL	Secure Socket Layer
HSMs	Hardware Security Modules
DNN	Deep Neural Network
LSTM	Long-Short Term Memory
CNN	Convolutional Neural Network
RSUs	Roadside Unit
ETP	Energy Trading Process
DSE	Decentralized Security Exchange
TDA	Threat-Detection Algorithm
DDoC	Distributed Denial of Charge

References

[1] Usman A, Shami SH. Evolution of communication echnologies for smart grid applications. Renew Sustain Energy Rev 2013;19:191–9.
[2] Chin WL, Li W, Chen HH. Energy big data security threats in IoT-based smart grid communications. IEEE Commun Mag 2017;55(10):70–5.
[3] Aljohani TM. Cyberattacks on energy infrastructures as modern war Weapons —Part I: analysis and motives. IEEE Technology and Society Magazine. IEEE Technol. Soc. Mag. 2024;43(2). https://doi.org/10.1109/MTS.2024.3395688. Jun. 2024.
[4] Aljohani TM. Cyberattacks on energy infrastructures as modern war weapons —Part II: gaps, standardization, and mitigation measures. IEEE Technol Soc Mag 2024;43(2). https://doi.org/10.1109/MTS.2024.3395697. Jun. 2024.
[5] Said D. A survey on information communication technologies in modern demand-side management for smart grids: challenges, solutions, and opportunities. IEEE Eng Manag Rev 2022;51(1):76–107.
[6] Loukas G, Karapistoli E, Panaousis E, Sarigiannidis P, Bezemskij A, Vuong T. A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. Ad Hoc Netw 2019;84:124–47.
[7] Acharya S, Dvorkin Y, Pandžić H, Karri R. Cybersecurity of smart electric vehicle charging: a power grid perspective. IEEE Access 2020;8:214434–53.
[8] Chandwani A, Dey S, Mallik A. Cybersecurity of onboard charging systems for electric vehicles—review, challenges and countermeasures. IEEE Access 2020;8:226982–98.
[9] Ronanki D, Karneddi H. Electric vehicle charging infrastructure: review, cyber security considerations, potential impacts, countermeasures and future trends. IEEE Journal of Emerging and Selected Topics in Power Electronics 2023.
[10] Babu PR, Palaniswamy B, Reddy AG, Odelu V, Kim HS. A survey on security challenges and protocols of electric vehicle dynamic charging system. Security and Privacy 2022;5(3):e210.
[11] Ye J, Guo L, Yang B, Li F, Du L, Guan L, Song W. Cyber–physical security of powertrain systems in modern electric vehicles: vulnerabilities, challenges, and future visions. IEEE Journal of Emerging and Selected Topics in Power Electronics 2020;9(4):4639–57.
[12] Rathore RS, Hewage C, Kaiwartya O, Lloret J. In-vehicle communication cyber security: challenges and solutions. Sensors 2022;22(17):6679.
[13] Alnasser A, Sun H, Jiang J. Cyber security challenges and solutions for V2X communications: a survey. Comput Network 2019;151:52–67.
[14] Avatefipour O, Al-Sumaiti AS, El-Sherbeeny AM, Awwad EM, Elmeligy MA, Mohamed MA, Malik H. An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning. IEEE Access 2019;7:127580–92.
[15] Yang B, Guo L, Li F, Ye J, Song W. Impact analysis of data integrity attacks on power electronics and electric drives. In: 2019 IEEE transportation electrification conference and expo (ITEC). IEEE; 2019, June. p. 1–6.
[16] Park Y, Onar OC, Ozpineci B. Potential cybersecurity issues of fast charging stations with quantitative severity analysis. In: 2019 IEEE CyberPELS (CyberPELS). IEEE; 2019, April. p. 1–7.
[17] Girdhar M, Hong J, Lee H, Song TJ. Hidden Markov models-based anomaly correlations for the cyber-physical security of EV charging stations. IEEE

Trans Smart Grid 2021;13(5):3903–14.
[18] Sanghvi A, Markel T. Cybersecurity for electric vehicle fast-charging infrastructure. In: 2021 IEEE transportation electrification conference & expo (ITEC). IEEE; 2021, June. p. 573–6.
[19] Bergies S, Aljohani TM, Su S-F, Elsisi M. An IoT-based deep-learning architecture to secure automated electric vehicles against cyberattacks and data loss. IEEE Transactions on Systems, Man, and Cybernetics: Systems 2024.
[20] ElHussini H, Assi C, Moussa B, Atallah R, Ghrayeb A. A tale of two entities: contextualizing the security of electric vehicle charging stations on the power grid. ACM Transactions on Internet of Things 2021;2(2):1–21.
[21] Farraj AK, Kundur D. On using energy storage systems in switching attacks that destabilize smart grid systems. In: 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT). IEEE; 2015, February. p. 1–5.
[22] Liu S, Chen B, Zourntos T, Kundur D, Butler-Purry K. A coordinated multi-switch attack for cascading failures in smart grid. IEEE Trans Smart Grid 2014;5(3):1183–95.
[23] Acharya S, Dvorkin Y, Karri R. Public plug-in electric vehicles+ grid data: is a new cyberattack vector viable? IEEE Trans Smart Grid 2020;11(6):5099–113.
[24] Wang Y, Zhao Z, Qi B, Cheng Y, Tang K, Li B. Vulnerability analysis of an electric vehicle fleet for car-sharing service under cyber attacks. Sustainable Energy, Grids and Networks 2024;37:101207.
[25] Basnet M, Ali MH. Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning. IET Generation, Transmission & Distribution 2021;15(24):3435–49.
[26] Sanghvi A, Markel T, Granda S, Nagarajan A, Jun M. Identification and testing of electric vehicle fast charger cybersecurity mitigations (No. NREL/TP-5R00-80799). Golden, CO (United States): National Renewable Energy Lab.(NREL); 2021.
[27] Zhou Y, Liu W, Ma J, Zhen X, Li Y. Malicious mode attack on EV coordinated charging load and MIADRC defense strategy. 2021. arXiv preprint arXiv: 2110.13681. Chicago.
[28] Weng S, Li Y, Ding X. Resilient distributed coordination of plug-in electric vehicles charging under cyber-attack. Electronics 2020;9(5):770.
[29] Hoang DT, Wang P, Niyato D, Hossain E. Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: a cyber insurance-based model. IEEE Access 2017;5:732–54.
[30] Gumrukcu E, Arsalan A, Muriithi G, Joglekar C, Aboulebdeh A, Zehir MA, et al. Impact of cyber-attacks on EV charging coordination: the case of single point of failure. In: 2022 4th global power, energy and communication conference (GPECOM). IEEE; 2022, June. p. 506–11.
[31] Fard MF, Hou X, Liu M. Exploration of for-purpose decentralized algorithmic cyber attacks in EV charging control. 2023. arXiv preprint arXiv:2303.03535.
[32] Wang H, Tashakor N, Jiang W, Liu W, Jiang CQ, Goetz SM. Hacking encrypted frequency-varying wireless power: cyber-security of dynamic charging. IEEE Trans Energy Convers 2024.
[33] Nisar F, Ramachandran G, Vilathgamuva M, Jurdak R. Manipulation of actual demand in electric vehicles (MaD EV): a cyber-security perspective. In: 2022 IEEE 7th southern power electronics conference (SPEC). IEEE; 2022, December. p. 1–8.
[34] Wu K, Weng S, Sun Z. Resilient event-triggered distributed electric vehicles charging scheduling against cyber attacks. In: 2022 41st Chinese control conference (CCC). IEEE; 2022, July. p. 4543–50.
[35] Girdhar M, Hong J, Yoo Y, Song TJ. Machine learning-enabled cyber attack prediction and mitigation for EV charging stations. In: 2022 IEEE power & energy society general meeting (PESGM). Chicago: IEEE; 2022, July. p. 1–5.
[36] Anvaripour M, Alavi SM, Hayes M, Saif M. Cybersecurity of electric vehicles charging systems by using residual generation technique. 2022.
[37] An H, Yi J, Zhang G, Bamisile O, Li J, Huang Q. A robust V2G voltage control scheme for distribution networks against cyber attacks and customer interruptions. IEEE Trans Smart Grid 2024.
[38] Yang P. Electric vehicle based smart cloud model cyber security analysis using fuzzy machine learning with blockchain technique. Comput Electr Eng 2024;115:109111.
[39] Johnson J, Anderson B, Wright B, Quiroz J, Berg T, Graves R, et al. Cybersecurity for electric vehicle charging infrastructure (No. SAND2022-9315). Albuquerque, NM (United States): Sandia National Lab.(SNL-NM); 2022.
[40] Li C, Li B, Sun H. Research on cybersecurity protection strategy of electric vehicles charging systems. In: International conference on internet of things and machine learning (IoTML 2021), vol 12174. SPIE; 2022, April. p. 138–43.
[41] Nasr T, Torabi S, Bou-Harb E, Fachkha C, Assi C. Power jacking your station: in-depth security analysis of electric vehicle charging station management systems. Comput Secur 2022;112:102511.
[42] Sayed MA, Ghafouri M, Debbabi M, Assi C. Dynamic load altering EV attacks against power grid frequency control. In: 2022 IEEE power & energy society general meeting (PESGM). IEEE; 2022, July. p. 1–5.
[43] Sarieddine K, Sayed MA, Jafarigiv D, Atallah R, Debbabi M, Assi C. A real-time cosimulation testbed for electric vehicle charging and smart grid security. IEEE Security & Privacy; 2023.
[44] Attanasio L, Conti M, Donadel D, Turrin F. MiniV2G: an electric vehicle charging emulator. In: Proceedings of the 7th ACM on cyber-physical system security workshop, Hong Kong, China; 7 June 2021.
[45] Hosseinzadehtaher M, Tiwari D, Kouchakipour N, Momeni A, Lelic M, Wu Z. Grid resilience assessment during extreme fast charging of electric vehicles via developed power hardware-in-the-loop. In: 2022 IEEE transportation electrification conference & expo (ITEC). IEEE; 2022, June. p. 929–34.
[46] Nonvignon TZ, Boucif AB, Mhamed M. A copula-based attack prediction model for vehicle-to-grid networks. Appl Sci 2022;12(8):3830.
[47] Soykan EU, Bagriyanik M, Soykan G. Disrupting the power grid via EV charging: the impact of the SMS Phishing attacks. Sustainable Energy, Grids and Networks 2021;26:100477.
[48] Antoun J, Kabir ME, Moussa B, Atallah R, Assi C. A detailed security assessment of the EV charging ecosystem. IEEE Network 2020;34(3):200–7.
[49] Eiza MH, Ni Q. Driving with sharks: rethinking connected vehicles with vehicle cybersecurity. IEEE Veh Technol Mag 2017;12(2):45–51.
[50] Aljohani TM, Almutairi A. Modeling time-varying wide-scale distributed denial of service attacks on electric vehicle charging stations. Ain Shams Engineering Journal 2024;15(7):102860.
[51] Rana MM. Attack resilient wireless sensor networks for smart electric vehicles. IEEE sensors letters 2017;1(2):1–4.
[52] Abedi S, Arvani A, Jamalzadeh R. Cyber security of plug-in electric vehicles in smart grids: application of intrusion detection methods. Plug In Electric Vehicles in Smart Grids: Integration Techniques 2015:129–47.
[53] Kavousi-Fard A, Jin T, Su W, Parsa N. An effective anomaly detection model for securing communications in electric vehicles. IEEE Trans Ind Appl 2020.
[54] Kavousi-Fard A, Dabbaghjamanesh M, Jin T, Su W, Roustaei M. An evolutionary deep learning-based anomaly detection model for securing vehicles. IEEE Trans Intell Transport Syst 2020;22(7):4478–86.
[55] Abd El-Gleel M, El-Zawawi AMO, El-Habrouk M. Secure lightweight CAN protocol handling message loss for electric vehicles. In: 2021 international conference on communication, control and information sciences (ICCISc), vol. 1. IEEE; 2021, June. p. 1–6.
[56] Li Y, Wang Y, Wu M, Li H. Replay attack and defense of electric vehicle charging on GB/T 27930-2015 communication protocol. J Comput Commun 2019;7(12):20.
[57] Mousavian S, Erol-Kantarci M, Wu L, Ortmeyer T. A risk-based optimization model for electric vehicle infrastructure response to cyber attacks. IEEE Trans Smart Grid 2017;9(6):6160–9.
[58] Wang C, Song R, Liu Z. Simulation of vehicle network communication security based on random geometry and data mining. IEEE Access 2020;8: 69389–400.
[59] Gandhi K, Morsi WG. Impact of the open charge point protocol between the electric vehicle and the fast charging station on the cybersecurity of the smart grid. In: 2022 IEEE Canadian conference on electrical and computer engineer ing (CCECE). IEEE; 2022, September. p. 235–40.
[60] Palahalli H, Hemmati M, Gruosso G. Analysis of cyber security threat of using IEC61850 in digital substations involving DERMS. In: 2022 international symposium on power electronics, electrical drives, automation and motion (SPEEDAM). IEEE; 2022, June. p. 948–53.
[61] Razmjouei P, Kavousi-Fard A, Dabbaghjamanesh M, Jin T, Su W. DAG-based smart contract for dynamic 6G wireless EVs charging system. IEEE Transactions on Green Communications and Networking 2022;6(3):1459–67.
[62] Alrashide A, Abdelrahman MS, Kharchouf I, Mohammed OA. GNS3 communication network emulation for substation GOOSE based protection schemes. In: 2022 IEEE international conference on environment and electrical engineering and 2022 IEEE industrial and commercial power systems europe (EEEIC/I&CPS europe). IEEE; 2022, June. p. 1–6.
[63] Kim S, Shrestha R, Kim S, Shrestha R. Vehicle communication and cyber security. Automotive Cyber Security: Introduction, Challenges, and Standardization 2020:67–96.
[64] El-Rewini Z, Sadatsharan K, Selvaraj DF, Plathottam SJ, Ranganathan P. Cybersecurity challenges in vehicular communications. Vehicular Communications 2020;23:100214.
[65] Manoj B, Hasan Ali MD. Exploring cybersecurity issues in 5G enabled EV charging station with deep learning. IET Gener Transm Distrib 2021;15: 3435–49.
[66] Neaimeh M, Andersen PB. Mind the gap-open communication protocols for vehicle grid integration. Energy Informatics 2020;3:1–17.
[67] Garofalaki Z, Kosmanos D, Moschoyiannis S, Kallergis D, Douligeris C. Electric vehicle charging: a survey on the security issues and challenges of the open charge point protocol (OCPP). IEEE Communications Surveys & Tutorials 2022.
[68] Hong J, Song TJ, Lee H, Zaboli A. Automated cybersecurity tester for iec61850-based digital substations. Energies 2022;15(21):7833.
[69] Li Q, Wang Y, Pu Z, Wang S, Zhang W. Time series association state analysis method for attacks on the smart internet of electric vehicle charging network. Transport Res Rec 2019;2673(4):217–28.
[70] Köhler S, Birnbach S, Baker R, Martinovic I. On the security of the wireless electric vehicle charging communication. In: 2022 IEEE international conference on communications, control, and computing technologies for smart grids (SmartGridComm). IEEE; 2022, October. p. 393–8.
[71] Roman LF, Gondim PR. Authentication protocol in CTNs for a CWD-WPT charging system in a cloud environment. Ad Hoc Netw 2020;97:102004.
[72] Nedyalkov I, Arnaudov D. Attacks and security measures of the exchanged information in the charging infrastructure for electromobiles. In: 2019 IEEE XXVIII international scientific conference electronics (ET). IEEE; 2019, September. p. 1–4.
[73] Aftab MA, Hussain SS, Ali I, Ustun TS. IEC 61850-based communication layer modeling for electric vehicles: electric vehicle charging and discharging processes based on the international electrotechnical commission 61850

standard and its extensions. IEEE Industrial Electronics Magazine 2020;14(2):4–14.
[74] Khan AA, Kumar V, Ahmad M, Jangirala S. A secure and energy efficient key agreement framework for vehicle-grid system. J Inf Secur Appl 2022;68:103231.
[75] Kilari VT, Yu R, Misra S, Xue G. Robust revocable anonymous authentication for vehicle to grid communications. IEEE Trans Intell Transport Syst 2020;21(11):4845–57.
[76] Baker R, Martinovic I. Losing the car keys: wireless PHY-layer insecurity in EV charging. USENIX; 2019, August.
[77] Su H, Qiu M, Wang H. Secure wireless communication system for smart grid with rechargeable electric vehicles. IEEE Commun Mag 2012;50(8):62–8.
[78] Hybrid Committee. Use cases for communication between plug-in vehicles and the utility grid. In: SAE international, detroit. Michigan; 2010. Standard J2836/1, Jan 2010.
[79] Guo L, Ye J. Cyber-physical security of electric vehicles with four motor drives. IEEE Trans Power Electron 2020;36(4):4463–77.
[80] Rahman S, Aburub H, Mekonnen Y, Sarwat AI. A study of EV BMS cyber security based on neural network SOC prediction. In: 2018 IEEE/PES transmission and distribution conference and exposition (T&D). IEEE; 2018, April. p. 1–5.
[81] Wang P, Li Y, Shekhar S, Northrop WF. Adversarial attacks on reinforcement learning based energy management systems of extended range electric delivery vehicles. 2020. arXiv preprint arXiv:2006.00817.
[82] Kim T, Ochoa J, Faika T, Mantooth HA, Di J, Li Q, Lee Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE Journal of Emerging and Selected Topics in Power Electronics 2020;10(1):1270–81.
[83] Guo L, Yang B, Ye J, Chen H, Li F, Song W, et al. Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles. IEEE Trans Ind Inf 2020;17(5):3335–47.
[84] Yang B, Ye J, Guo L. Fast detection for cyber threats in electric vehicle traction motor drives. IEEE Transactions on Transportation Electrification 2021;8(1):767–77.
[85] Lin J, Yu W, Zhang N, Yang X, Ge L. Data integrity attacks against dynamic route guidance in transportation-based cyber-physical systems: modeling, analysis, and defense. IEEE Trans Veh Technol 2018;67(9):8738–53.
[86] Aljohani TM, Ebrahim A, Mohammed O. Real-Time metadata-driven routing optimization for electric vehicle energy consumption minimization using deep reinforcement learning and Markov chain model. Elec Power Syst Res 2021;192:106962.
[87] Aljohani TM, Mohammed O. A real-time energy consumption minimization framework for electric vehicles routing optimization based on SARSA reinforcement learning. Vehicles 2022;4(4):1176–94.
[88] Deb N, Singh R, Brooks RR, Bai K. A review of extremely fast charging stations for electric vehicles. Energies 2021;14(22):7566.
[89] Choi J, Narayanasamy D, Ahn B, Ahmad S, Zeng J, Kim T. A real-time hardware-in-the-loop (HIL) cybersecurity testbed for power electronics devices and systems in cyber-physical environments. In: 2021 IEEE 12th international symposium on power electronics for distributed generation systems (PEDG). IEEE; 2021, June. p. 1–5.
[90] Dayanikli GY, Hatch RR, Gerdes RM, Wang H, Zane R. Electromagnetic sensor and actuator attacks on power converters for electric vehicles. In: 2020 IEEE security and privacy workshops (SPW). IEEE; 2020, May. p. 98–103.
[91] Banda MK, Koduru SS, Machina VSP, Madichetty S. A deep learning based cyber attack detection and mitigation scheme in synchronous buck converter. In: 2022 IEEE international conference on power electronics, drives and energy systems (PEDES). IEEE; 2022, December. p. 1–6.
[92] Sahoo S. Cyber security in power electronic systems. In: Control of power electronic converters and systems. Academic Press; 2021. p. 199–220.
[93] Balda JC, Mantooth A, Blum R, Tenti P. Cybersecurity and power electronics: addressing the security vulnerabilities of the internet of things. IEEE Power Electronics Magazine 2017;4(4):37–43.
[94] Surya S, Srinivasan MK, Williamson S. Technological perspective of cyber secure smart inverters used in power distribution system: state of the art review. Appl Sci 2021;11(18):8780.
[95] Zhang J, Ye J, Guo L, Li F, Song W. Vulnerability assessments for power-electronics-based smart grids. In: 2020 IEEE energy conversion congress and exposition (ECCE). IEEE; 2020, October. p. 1702–7.
[96] Hussain SS, Ustun TS. Smart inverter communication model and impact of cybersecurity attack. In: 2020 IEEE international conference on power electronics, drives and energy systems (PEDES). IEEE; 2020, December. p. 1–5.
[97] Khan A, Hosseinzadehtaher M, Shadmand MB, Saleem D, Abu-Rub H. Intrusion detection for cybersecurity of power electronics dominated grids: inverters PQ set-points manipulation. In: 2020 IEEE CyberPELS (CyberPELS). IEEE; 2020, October. p. 1–8.
[98] Kumar G, Saha R, Rai MK, Buchanan WJ, Thomas R, Geetha G, et al. A privacy-preserving secure framework for electric vehicles in IoT using matching market and signcryption. IEEE Trans Veh Technol 2020;69(7):7707–22.
[99] Rabieh K, Aydogan AF. A fair and privacy-preserving reservation scheme for charging electric vehicles. In: 2019 international symposium on networks, computers and communications (ISNCC). IEEE; 2019, June. p. 1–6.
[100] Lei M, Mohammadi M. Hybrid machine learning based energy policy and management in the renewable-based microgrids considering hybrid electric vehicle charging demand. Int J Electr Power Energy Syst 2021;128:106702. Chicago.
[101] Gong X, Dong F, Mohamed MA, Abdalla OM, Ali ZM. A secured energy management architecture for smart hybrid microgrids considering PEM-fuel cell and electric vehicles. IEEE Access 2020;8:47807–23.
[102] Wang B, Dabbaghjamanesh M, Kavousi-Fard A, Mehraeen S. Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach. IEEE Trans Ind Appl 2019;55(6):7300–9.
[103] Li H, Han D, Tang M. A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing. IEEE Syst J 2020;15(3):3189–200. Chicago.
[104] Hataba M, Sherif A, Elsersy M, Nabil M, Mahmoud M, Almotairi KH. Privacy-preserving biometric-based authentication scheme for electric vehicles charging system. In: 2021 3rd IEEE Middle East and north africa COMMunications conference (MENACOMM). IEEE; 2021, December. p. 86–91.
[105] Muhammad Z, Anwar Z, Saleem B, Shahid J. Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability. Energies 2023;16(3):1113.
[106] Aghapour R, Zeraati M, Jabari F, Sheibani M, Arasteh H. Cybersecurity and data privacy issues of electric vehicles smart charging in smart microgrids. In: Electric vehicle integration via smart charging: technology, standards, implementation, and applications. Cham: Springer International Publishing; 2022. p. 85–110.
[107] Colangelo G, Ennis SF. Energy data sharing and the case of electric vehicles smart charging. CERRE report. 2022.
[108] Parameswarath RP, Gope P, Sikdar B. Privacy-preserving user-centric authentication protocol for IoT-enabled vehicular charging system using decentralized identity. IEEE Internet of Things Magazine 2023;6(1):70–5.
[109] Islam S, Badsha S, Sengupta S, Khalil I, Atiquzzaman M. An intelligent privacy preservation scheme for EV charging infrastructure. IEEE Trans Ind Inf 2022;19(2):1238–47.
[110] Almuhaideb AM, Algothami SS. Efficient privacy-preserving and secure authentication for electric-vehicle-to-electric-vehicle-charging system based on ECQV. J Sens Actuator Netw 2022;11(2):28.
[111] Nabil M, Bima M, Alsharif A, Johnson W, Gunukula S, Mahmoud M, Abdallah M. Priority-based and privacy-preserving electric vehicle dynamic charging system with divisible e-payment. In: Smart cities cybersecurity and privacy. Elsevier; 2019. p. 165–86.
[112] ElGhanam E, Ahmed I, Hassan M, Osman A. Authentication and billing for dynamic wireless EV charging in an internet of electric vehicles. Future Internet 2021;13(10):257.
[113] Baza M, Sherif A, Mahmoud MM, Bakiras S, Alasmary W, Abdallah M, Lin X. Privacy-preserving blockchain-based energy trading schemes for electric vehicles. IEEE Trans Veh Technol 2021;70(9):9369–84.
[114] Li Y, Hu B. A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles. IEEE Trans Ind Inf 2020;17(3):1968–77.
[115] Asokraj S, Bianchi T, Brighente A, Conti M, Poovendran R. Identity-based authentication for on-demand charging of electric vehicles. 2022. arXiv preprint arXiv:2208.02857.
[116] Unterweger A, Knirsch F, Engel D, Musikhina D, Alyousef A, de Meer H. An analysis of privacy preservation in electric vehicle charging. Energy Informatics 2022;5(1):1–27.
[117] Shen J, Zhou T, Wei F, Sun X, Xiang Y. Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things. IEEE Internet Things J 2017;5(4):2526–36.
[118] Liu JK, Au MH, Susilo W, Zhou J. Enhancing location privacy for electric vehicles (at the right time). In: Computer security–ESORICS 2012: 17th European symposium on research in computer security, pisa, Italy, september 10-12, 2012. Proceedings, vol 17. Springer Berlin Heidelberg; 2012. p. 397–414.
[119] Pillitteri V, Brewer T. Guidelines for smart grid cybersecurity, NIST interagency/internal report (NISTIR). Gaithersburg, MD: National Institute of Standards and Technology; 2014. https://doi.org/10.6028/NIST.IR.7628r1 [online].
[120] Harvey M, Long D, Reinhard K. Visualizing nistir 7628, guidelines for smart grid cyber security. In: 2014 power and energy conference at Illinois (PECI). IEEE; 2014, February. p. 1–8.
[121] Chan ACF, Zhou J. On smart grid cybersecurity standardization: issues of designing with NISTIR 7628. IEEE Commun Mag 2013;51(1):58–65.
[122] Ustun TS, Hussain SS. Implementation of IEC 61850 based integrated EV charging management in smart grids. In: 2019 IEEE vehicle power and propulsion conference (VPPC). IEEE; 2019, October. p. 1–5.
[123] Hussain SS, Ustun TS, Kalam A. A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. IEEE Trans Ind Inf 2019;16(9):5643–54.
[124] Pourmirza Z, Walker S. Electric vehicle charging station: cyber security challenges and perspective. In: 2021 IEEE 9th international conference on smart energy grid engineering (SEGE). IEEE; 2021, August. p. 111–6.
[125] NIST. Considerations for managing internet of things (IoT) cybersecurity and privacy risks. In: National Institute of standards and technology, US department of commerce; 2019.
[126] Babu PR, Reddy AG, Palaniswamy B, Das AK. EV-PUF: lightweight security protocol for dynamic charging system of electric vehicles using physical unclonable functions. IEEE Transactions on Network Science and

Engineering 2022;9(5):3791–807.
[127] Babu PR, Amin R, Reddy AG, Das AK, Susilo W, Park Y. Robust authentication protocol for dynamic charging system of electric vehicles. IEEE Trans Veh Technol 2021;70(11):11338–51.
[128] Bao K, Valev H, Wagner M, Schmeck H. A threat analysis of the vehicle-to-grid charging protocol ISO 15118. Comput Sci Res Dev 2018;33(1–2):3–12.
[129] Alcaraz C, Lopez J, Wolthusen S. OCPP protocol: security threats and challenges. IEEE Trans Smart Grid 2017;8(5):2452–9.
[130] Garofalaki Z, Kosmanos D, Moschoyiannis S, Kallergis D, Douligeris C. Electric vehicle charging: a survey on the security issues and challenges of the open charge point protocol (OCPP). IEEE Communications Surveys & Tutorials 2022.
[131] Kharchouf I, Alrashide A, Abdelrahman MS, Mohammed OA. On the implementation and security analysis of routable-GOOSE messages based on IEC 61850 standard. In: 2022 IEEE international conference on environment and electrical engineering and 2022 IEEE industrial and commercial power systems europe (EEEIC/I&CPS europe). IEEE; 2022, June. p. 1–6.
[132] Berg A, Svantesson F. Is your electric vehicle plotting against you?: an investigation of the ISO 15118 standard and current security implementations. 2021.
[133] Lee S, Park Y, Lim H, Shon T. Study on analysis of security vulnerabilities and countermeasures in ISO/IEC 15118 based electric vehicle charging technology. In: 2014 International conference on IT convergence and security (ICITCS). IEEE; 2014, October. p. 1–4.
[134] Chan ACF, Zhou J. On smart grid cybersecurity standardization: issues of designing with NISTIR 7628. IEEE Commun Mag 2013;51(1):58–65. 2013.
[135] Van Aubel P, Poll E. Security of EV-charging protocols. 2022. arXiv preprint arXiv:2202.04631.
[136] Xu J, Huang J, Liu C, Tian L, Yu X, Wang J, Zhou L. The security of charging protocol between charging piles and electric vehicles. In: 2019 IEEE sustainable power and energy conference (iSPEC). IEEE; 2019, November. p. 1315–20.
[137] Van Den Bossche P. Iec 61851-1: electric vehicle conductive charging system-Part 1: general requirements. IEC; 2010. p. 1–99. In 2, https://www.iso.org/obp/ui/#iso:std:iso:15118: 20:ed-1:v1:en.
[138] Open Charge Alliance". https://www.openchargealliance.org/protocols/ocpp-201/.
[139] IEC. Iec 61850:2021 ser. Retrieved from, https://iec61850.dvl.iec.ch/; 2021.
[140] GB Standards. GB/T 32960.2-2016: PDF in English (Standard No.: GB/T 32960.2-2016). Retrieved from, https://www.chinesestandard.net/PDF.aspx/GBT32960.2-2016; 2016.
[141] DIN SPEC 70121. Retrieved from https://www.en-standard.eu/din-spec-70121-electromobility-digital-communication-between-a-d-c-ev-charging-station-and-an-electric-vehicle-for-control-of-d-c-charging-in-the-combined-charging-system-text-in-english/.
[142] CHAdeMO. https://www.chademo.com.
[143] Combined Charging System 1.0 Specification. https://tesla.o.auroraobjects.eu/Combined_Charging_System_1_0_Specification_V1_2_1.pdf.
[144] IEC 62351: Cybersecurity for IEC 61850 – IEC 61850. (n.d.). IEC 62351: Cybersecurity for IEC 61850 – IEC 61850.https://iec61850.dvl.iec.ch/what-is-61850/technical-principles/61850-cybersecurity/.
[145] GB/T 20234.3-2015: PDF in English. (189760, January 1). GB/T 20234.3-2015: PDF in English. https://www.chinesestandard.net/PDF.aspx/GBT20234.3-2015.
[146] SAE International. Sae j2293-/1-200807: energy transfer system for electric vehicles-part-I: functional requirements and system architectures. Retrieved from, https://www.sae.org/standards/content/j2293/1_200807; 2008.
[147] SAE International. SAE J2836_1/201907: use cases for communication between plug-in vehicles and utility grid. Retrieved from, https://www.sae.org/standards/content/j2836/1_201907/; 2019.
[148] ISO. ISO/SAE 21434:2021. Retrieved from, https://www.iso.org/standard/70918.html; 2020, November 17.
[149] Higuera JRB, Higuera JB, García JLT, Montalvo JAS, Rubio MS. Building a dataset through attack pattern modeling and analysis system. Comput Electr Eng 2022;97:107614.
[150] Chen R, Park JM, Reed JH. Defense against primary user emulation attacks in cognitive radio networks. IEEE J Sel Area Commun 2008;26(1):25–37.
[151] Anand S, Jin Z, Subbalakshmi KP. An analytical model for primary user emulation attacks in cognitive radio networks. In: 2008 3rd IEEE symposium on new frontiers in dynamic spectrum access networks. IEEE; 2008, October. p. 1–6.
[152] Peng Q, Cosman PC, Milstein LB. Optimal sensing disruption for a cognitive radio adversary. IEEE Trans Veh Technol 2010;59(4):1801–10.
[153] Malik KM, Malik H, Baumann R. Towards vulnerability analysis of voice-driven interfaces and countermeasures for replay attacks. In: 2019 IEEE conference on multimedia information processing and retrieval (MIPR). IEEE; 2019, March. p. 523–8.
[154] Jo HJ, Kim JH, Choi HY, Choi W, Lee DH, Lee I. Mauth-can: masquerade-attack-proof authentication for in-vehicle networks. IEEE Trans Veh Technol 2019;69(2):2204–18.
[155] Khan OGM, El-Saadany E, Youssef A, Shaaban M. Impact of electric vehicles botnets on the power grid. In: 2019 IEEE electrical power and energy conference (EPEC). IEEE; 2019, October. p. 1–5.
[156] Rana MM. IoT-based electric vehicle state estimation and control algorithms under cyber attacks. IEEE Internet Things J 2019;7(2):874–81.
[157] Iqbal S, Ball P, Kamarudin MH, Bradley A. Simulating malicious attacks on VANETs for connected and autonomous vehicle cybersecurity: a machine learning dataset. In: 2022 13th international symposium on communication systems, networks and digital signal processing (CSNDSP). IEEE; 2022, July. p. 332–7.
[158] Khan SK, Shiwakoti N, Stasinopoulos P, Chen Y. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accid Anal Prev 2020;148:105837.
[159] Ahmed S, Dow FM. Electric vehicle technology as an exploit for cyber attacks on the next generation of electric power systems. In: 2016 4th international conference on control engineering & information technology (CEIT). IEEE; 2016, December. p. 1–5.
[160] Payne BR. Car hacking: accessing and exploiting the can bus protocol. Journal of Cybersecurity Education, Research and Practice 2019;2019(1):5.
[161] Piperigkos N, Lalos AS. Impact of false data injection attacks on decentralized electric vehicle charging protocols. Transport Res Procedia 2021;52:331–8.
[162] Girdhar M, Hong J, You Y, Song TJ, Govindarasu M. Cyber-attack event analysis for EV charging stations. 2022. arXiv preprint arXiv:2211.08530.
[163] Haoyang Y, Dong L, Jiaming W. Risk analysis of cyber physical distribution system considering cyber attacks on V2G system. In: The 10th renewable power generation conference (RPG 2021), vol 2021. IET; 2021, October. p. 841–6.
[164] Katsikeas S, Johnson P, Hacks S, Lagerström R. Probabilistic modeling and simulation of vehicular cyber attacks: an application of the meta Attack Language. ICISSP 2019, February:175–82.
[165] Iwendi C, Uddin M, Ansere JA, Nkurunziza P, Anajemba JH, Bashir AK. On detection of Sybil attack in large-scale VANETs using spider-monkey technique. IEEE Access 2018;6:47258–67.
[166] Cui H, Dong X, Deng H, Dehghani M, Alsubhi K, Aljahdali HMA. Cyber attack detection process in sensor of DC micro-grids under electric vehicle based on Hilbert–Huang transform and deep learning. IEEE Sensor J 2020;21(14):15885–94.
[167] Hu Z, Liu S, Wu L. Credibility-based distributed frequency estimation for plug-in electric vehicles participating in load frequency control. Int J Electr Power Energy Syst 2021;130:106997.
[168] Basnet M, Ali MH. Deep learning-based intrusion detection system for electric vehicle charging station. In: 2020 2nd international conference on smart power & internet energy systems (SPIES). IEEE; 2020, September. p. 408–13.
[169] Kosmanos D, Pappas A, Maglaras L, Moschoyiannis S, Aparicio-Navarro FJ, Argyriou A, Janicke H. A novel intrusion detection system against spoofing attacks in connected electric vehicles. Array 2020;5:100013.
[170] Wang Y, Liu Q, Mihankhah E, Lv C, Wang D. Detection and isolation of sensor attacks for autonomous vehicles: framework, algorithms, and validation. IEEE Trans Intell Transport Syst 2021;23(7):8247–59.
[171] Lee H, Kim K, Park JH, et al. Convolutional neural network-based false battery data detection and classification for battery energy storage systems. IEEE Trans Energy Convers 2021;PP(99):1. 1.
[172] Nsonga P, Hussain SS, Ali I, Ustun TS. Using IEC 61850 and IEEE WAVE standards in ad-hoc networks for electric vehicle charging management. In: 2016 IEEE online conference on green communications (OnlineGreenComm). IEEE; 2016, November. p. 39–44.
[173] Sheikh A, Kamuni V, Urooj A, Wagh S, Singh N, Patel D. Secured energy trading using byzantine-based blockchain consensus. IEEE Access 2019;8:8554–71.
[174] Dey S, Khanra M. Cybersecurity of plug-in electric vehicles: cyberattack detection during charging. IEEE Trans Ind Electron 2020;68(1):478–87.
[175] Su Z, Wang Y, Xu Q, Fei M, Tian YC, Zhang N. A secure charging scheme for electric vehicles with smart communities in energy blockchain. IEEE Internet Things J 2018;6(3):4601–13.
[176] Darby P, Gottumukkala R. Decentralized computing techniques in support of cyber-physical security for electric and autonomous vehicles. In: 2019 IEEE green technologies conference (GreenTech). IEEE; 2019, April. p. 1–5.
[177] Zhang YY, Shang J, Chen X, Liang K. A self-learning detection method of Sybil attack based on LSTM for electric vehicles. Energies 2020;13(6):1382.
[178] Guo L, Yang B, Ye J. Detection and diagnosis of long-term cyber-attacks for predictive energy management system in hevs. In: 2021 IEEE applied power electronics conference and exposition (APEC). IEEE; 2021, June. p. 842–8.
[179] Dey S, Chandwani A, Mallik A. Real time intelligent data processing algorithm for cyber resilient electric vehicle onboard chargers. In: 2021 IEEE transportation electrification conference & expo (ITEC). IEEE; 2021, June. p. 1–6.
[180] Guo L, Ye J, Yang B. Cyberattack detection for electric vehicles using physics-guided machine learning. IEEE transactions on transportation electrification 2020;7(3):2010–22.
[181] Shafee A, Nabil M, Mahmoud M, Alasmary W, Amsaad F. Detection of denial of charge (DoC) attacks in smart grid using convolutional neural networks. In: 2021 international symposium on networks, computers and communications (ISNCC). IEEE; 2021, October. p. 1–7.
[182] Basnet M, Ali MH. Deep reinforcement learning-driven mitigation of adverse effects of cyber-attacks on electric vehicle charging station. Energies 2023;16(21):7296. Chicago.
[183] Basnet M, Ali MH. WCGAN-based cyber-attacks detection system in the EV charging infrastructure. In: 2022 4th international conference on smart power & internet energy systems (SPIES). IEEE; 2022, December. p. 1761–6.

[184] Warraich ZS, Morsi WG. Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids. Sustainable Energy, Grids and Networks 2023;34:101027.
[185] Cumplido J, Alcaraz C, Lopez J. Collaborative anomaly detection system for charging stations. In: Computer security–ESORICS 2022: 27th European symposium on research in computer security, Copenhagen, Denmark, september 26 –30, 2022, proceedings, Part II. Cham: Springer Nature Switzerland; 2022, September. p. 716–36.
[186] ElKashlan M, Elsayed MS, Jurcut AD, Azer M. A machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs). Electronics 2023;12(4):1044.
[187] Basnet M, Poudyal S, Ali MH, Dasgupta D. Ransomware detection using deep learning in the SCADA system of electric vehicle charging station. In: 2021 IEEE PES innovative smart grid technologies conference-Latin America (ISGT Latin America). IEEE; 2021, September. p. 1–5.
[188] Said D, Elloumi M. A new false data injection detection protocol based machine learning for P2P energy transaction between CEVs. In: 2022 IEEE international conference on electrical sciences and technologies in maghreb (CISTEM), vol. 4. IEEE; 2022, October. p. 1–5.
[189] Said D, Elloumi M, Khoukhi L. Cyber-attack on P2P energy transaction between connected electric vehicles: a false data injection detection based machine learning model. In: IEEE access, vol 10; 2022. p. 63640–7. https://doi.org/10.1109/ACCESS.2022.3182689.
[190] Kabir ME, Ghafouri M, Moussa B, Assi C. A two-stage protection method for detection and mitigation of coordinated EVSE switching attacks. IEEE Trans Smart Grid 2021;12(5):4377–88.
[191] Sarieddine K, Sayed MA, Torabi S, Atallah R, Assi C. Edge-based detection and localization of adversarial oscillatory load attacks orchestrated by compromised EV charging stations. Int J Electr Power Energy Syst 2024;156:109735.
[192] Yi J, An H, Xing Y, Li J, Zhang G, Bamisile O, et al. A cyber attack detection strategy for plug-in electric vehicles during charging based on CEEMDAN and Broad Learning System. Energy Rep 2023;9:80–8.
[193] Tomlinson A, Bryans J, Shaikh SA, Kalutarage HK. Detection of automotive CAN cyber-attacks by identifying packet timing anomalies in time windows. In: 2018 48th annual IEEE/IFIP international conference on dependable systems and networks workshops (DSN-W). IEEE; 2018, June. p. 231–8.
[194] Kern D, Krauß C, Lauser T, Alnahawi N, Wiesmaier A, Niederhagen R. QuantumCharge: post-quantum cryptography for electric vehicle charging. Cryptology ePrint Archive; 2023.
[195] Belkaaloul A, Bensaber BA. Anonymous authentication protocol for efficient communications in vehicle to grid networks. In: 2021 IEEE symposium on computers and communications (ISCC). IEEE; 2021, September. p. 1–5.
[196] Roman LF, Gondim PR, Lloret J. Pairing-based authentication protocol for V2G networks in smart grid. Ad Hoc Netw 2019;90:101745.
[197] Jakó Z, Knapp Á, El Sayed N. Wireless authentication solution and TTCN-3 based test framework for ISO-15118 wireless V2G communication. Infocommunications Journal 2019;11(2):39–47.
[198] Verma A, Saha R, Kumar G, Conti M. PETRAK: a solution against DDoS attacks in vehicular networks. Comput Commun 2024.
[199] Alsaleh A. A novel intrusion detection model of unknown attacks using convolutional neural networks. Comput Syst Sci Eng 2024;48(2).
[200] Korium MS, Saber M, Beattie A, Narayanan A, Sahoo S, Nardelli PH. Intrusion detection system for cyberattacks in the Internet of Vehicles environment. Ad Hoc Netw 2024;153:103330.
[201] Said Dhaou. Quantum computing and machine learning for cybersecurity: distributed denial of service (DDoS) attack detection on smart micro-grid. Energies 2023;16(8):3572.
[202] Kristianto E, Lin PC, Hwang RH. Sustainable and lightweight domain-based intrusion detection system for in-vehicle network. Sustainable Computing: Informatics and Systems 2024;41:100936.
[203] Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, et al. Experimental security analysis of a modern automobile. In: 2010 IEEE symposium on security and privacy. IEEE; 2010, May. p. 447–62.
[204] Aljohani T, Mohamed MA, Mohammed O. Tri-level hierarchical coordinated control of large-scale EVs charging based on multi-layer optimization framework. Elec Power Syst Res 2024;226:109923.