Security of Electric Vehicle Charging Stations

Subramaniam Ganesan*, Dhrumil Kamleshbhai Patel, Rhea Chokhalingam
Department of Electrical and Computer Engineering, Oakland University, Rochester, MI 48309, USA.
Email: Ganesan@oakland.edu
** Corresponding author*

Abstract: **The rapid growth of the electric vehicle (EV) market requires a robust and secure charging infrastructure, addressing cyber threats and security issues within Electric Vehicle Charging Stations (EVCS). This paper gives an insight into EV adoption and charging options such as Home-based charging systems, Public-based charging systems, and DC fast charging. An analysis of EVCS vulnerabilities, risks associated with EV user interfaces, network connections, and terminal maintenance are presented. Leveraging the STRIDE threat model, potential cyberattacks including various attack modes are identified and discussed. The paper proposes a range of countermeasures such as secure coding practices, tamper detection sensors, network segmentation, intrusion detection systems, and control mechanisms' role-based access to fortify EV charging systems against these threats. This paper identifies security gaps in EV charging systems and proposes remedies that can be suitably modified for EVCS applications. Innovative solutions like Artificial Intelligence-Based Scheduling Models, Over-the-Air (OTA) Updates, and Vehicle to Grid (V2G) concepts are explored for enhanced security and efficiency. We present the security challenges in EVCS for the reliability, safety, and integrity of these systems and the countermeasures that can be adapted to EVCS.**

Keywords: **Application of AI for monitoring, Battery charging stations, Countermeasures, Cyberattack on the charging systems.**

I. INTRODUCTION

Design and production of Electric vehicles (EVs) are increasing. The automotive industry is building battery charging infrastructure quickly to support EVs.. To encourage EV adoption, the governments offer discounts and incentives such as tax breaks and rebates to electric vehicle customers. The various types of charging options available are home-based charging systems, public-based charging systems, and DC fast charging (DCFC). Each charging method has distinct advantages for EV battery charging [1].
Home-based charging systems use a standard household outlet (120 volts) and deliver a slow charging, which is used by EV owners who can charge their vehicles overnight for limited driving [2]. On the other hand, the public=based charging system utilizes dedicated 240-volt charging stations, providing a faster charging time. Public-based charging systems are commonly found in public areas like shopping centers, workplaces, universities, and public parking, making them suitable for regular use [1]. DC fast charging (DCFC) stands out as the quickest EV charging option, having the potential for 30 minutes to charge nearly 80%. These stations are mostly situated along highways and longer travel routes, making them important for long-distance journeys [1]. Currently, DCFC and Public charging stations are heavily commercially invested. The public-based charging systems are more efficient than the home-based charging systems. Whereas, DCFC stations cater to the needs of long-distance travelers and help alleviate range anxiety [3].
In recent times, considerable investments by public charging networks and automakers have been directed toward expanding DCFC infrastructure, enhancing the practicality and convenience of long-distance travel in EVs.
There were 3.23.2 million public charging stations (including 1.81.8 million slow chargers at the end of 2023. There were 1.41.4 million fast chargers, i.e., with a charging rate of more than 22 kW and up to 350 kW) and almost ten times more home charging stations than public ones [4]. However, the use of millions of BEVs will have significant impacts on the grid [5]. If too many BEVs are charged at the same time, it will cause a system-wide overload.
The declining costs of EVs can be credited to technological advancements in manufacturing processes and the scale-up of production. These improvements have significantly influenced public perception of EVs. Notably, the battery technology revolution has emerged as a potential catalyst for driving EV adoption [3]. There is a great need for more charging stations. We need to construct more charging stations to accommodate the increasing number of EVs on the roads.

II. WHAT IS AN ELECTRIC VEHICLE CHARGING STATION (EVCS)?

Electric Vehicle (EVs) charging systems comprise the smart grid, battery charging circuits/microcontrollers, software, protection circuits, and communication to a central database. Electric AC power from the grid is connected to EVs through Electric Vehicle Charging Stations (EVCS). These EVCS units are self-contained infrastructures enabled with Internet-of-Things functionality. In public charging, cloud servers control the operation of EVCS, offering users guidance to available charging stations, facilitating the setup and management of charging sessions, and tracking consumption statistics. Through Internet Public EVCS users can communicate with a charging management system that allows them to schedule charging sessions, specify billing rates, initiate and terminate charging processes, and monitor their EVs' status through these services.

The functional operation of the power infrastructure is imperative for charging an EV, as EVCS units draw power from the grid. This integration of charging stations into the grid provides safety and required power. To secure the whole system, all exchanges of data between user applications, EVs, and EVCS units must be secured. Various enterprises, national governments, and others have their cybersecurity protocols. A lack of standardization in these security protocols leads to cybersecurity challenges within the EV charging ecosystem [6-11].

III. TYPES OF EV CHARGING STATIONS.

Modes of charging, charging methods, standards, and figures are described nicely in [12].

There are two main types of EV chargers:

- For Home Charging, slow AC chargers,
- For Public charging, a high-power, fast DC charger.

Enhanced Convenience: Setting up a personal charging station at home offers advantages such as time savings and cost. The ease of charging EV vehicles with a home-based Charging system is more. It eliminates the waiting period for searching for and acquiring a charging spot at a public charging station.

Cost Effective: Home-based charging option is cost-efficient because it reduces the overhead cost of a Public Charging station which usually runs to make a profit and charges a significant fee.

Increased Property Value: The presence of EV charging stations at residences could raise the value of a property. Home-based charging leads to savings in terms of time and expenses. Currently, many new houses have pre-installed EV charging to attract Home Buyers. This feature might also result in quicker sales at better prices, thus recovering the initial investment in EV charging stations.

Reduced Wear and Tear, Enhanced Safety: With fewer users, the wear and tear on home charging stations is reduced, resulting in lower repair costs. Additionally, these stations are designed to operate independently of external networks, ensuring a level of safety and control over their usage [2].

Extended Charging Duration: Many EV owners prefer retaining their Home-based charging system chargers for home use. However, these chargers have slower charging rates compared to public options. Installing a Public charging system charger can significantly accelerate the charging process.

Initial Investment Concerns: Those unable to afford personal charging stations would depend on public charging infrastructure.

Lower Initial Costs: This system does not necessitate significant upfront investment from individuals. The users only pay for the electricity consumed during the charging process [2].

Cost-Effective Option for the Public: Public EV charging stations often provide faster charging than most residential setups can offer. This proves advantageous for individuals requiring urgent vehicle charging during their journeys.

Potential for Lengthy Waiting Times: Arriving at a public charging station might result in extended waiting periods. Consequently, many may opt for home charging to minimize the inconvenience of prolonged delays [2].

Challenges in Locating Charging Stations: Even if someone has mapped out the public charging stations along their regular routes, having a personal home charger remains a convenient and reliable option.

Battery Health Concerns: The use of fast chargers could accelerate the deterioration of an EV's battery compared to a home-based charging system or slow public-based charging system. To improve the life of batteries, the recommendation is to limit the use of rapid charging stations and depend more on home charging options [2].

IV. WHY SECURITY IS AN ISSUE?

Consider three various attacks and their consequences:

If an attacker draws off the electricity by masquerading as an authorized customer, then the consequence would be loss of money or energy.

If an attacker tampers with the power lines to steal power, then the consequence would be insufficient power delivery to the EVs [5-7].

If an attacker steals power as a valid customer, then it can have a negative outcome by inducing electric disturbances across the power grid [5-7].

System Security Challenges

Any system connected to the internet is susceptible to cyber-attack. EVCS are connected to the internet or the outside world. It can be considered as an IOT, an Internet of Things. The security attack can be:

- Side-channel attacks
- Software-based attacks
- Network-based attacks

To secure charging stations, implement encryption and authentication measures, limit access to critical functions, implement secure boot processes, and regularly update and patching software. Securing EVCS systems is essential to protect individuals, organizations, and society as a whole.

The IOT/embedded System Security Standards and Requirements can be studied. The DoD provides guidelines for both device security and cybersecurity. The FDA provides cybersecurity best practices for medical device manufacturers at www.fda.gov/medical-devices/digital-health-center-excellence/ cybersecurity. Proof of meeting security requirements can be required to get FDA approval for a connected medical device. National Institute of Standards, NIST provides security standards and guidelines for various embedded segments, including electronics, energy, manufacturing, and transportation. Federal Information Processing Standards, FIPS are U.S. government computer security standards specifying

requirements for cryptographic algorithms. FIPS 140-3 is commonly followed in the embedded industry. Security Technical Implementation Guides, STIGs are configuration standards consisting of cybersecurity requirements for specific technologies.

Software-based attacks are aimed at gaining some or full control of a system. This can be through malware or brute-forcing access methods. It can be done remotely through fake updates, drivers, or security patches. Run updates from known trusted devices. The code and updates should only run if it contains the proper signature. Brute-forcing attacks occur when a hacker tries to guess credentials to access the device. The hacker runs a script that will attempt to log into the device by running through a list full of passwords. The best way to prevent brute forcing attacks is through strong passwords, two-factor authentication, and limiting the number of password attempts.

Network-based attacks include "man-in-the-middle" attacks as well as "distributed denial of service" (DDoS) attacks. Man-in-the-middle attacks are most commonly conducted by spoofing a free WiFi hotspot. More sophisticated approaches involve IP spoofing, in which the attacker alters packet headers in an IP address, DNS cache poisoning, in which an attacker gains access to a DNS server and alters website address information; HTTPS spoofing, in which an attacker uses a fake certificate to imitate a trusted site, and SSL hijacking in which an attacker would send established authenticated keys during a TCP handshake to appear that the user has made a secure connection. a firewall with traffic analysis and filtering can help prevent the attacks or at least detect them in time to take preventative measures to protect the system.

Side channel attacks are hardware attacks. The Attacker has access to the device or infinite time to analyze. Some of the common types of side-channel attacks are caused by power analysis, timing attacks, and electromagnetic analysis. Proper design of the memory system and Wi-Fi connections will prevent such attacks.

Secure Communication Channels

Software obfuscation is also a method to help make an IOT/embedded system more secure. Software obfuscation involves making code that is difficult for humans to understand. This is done to conceal the true purpose of the code and makes it harder to reverse engineer. This can be done manually by the developer or through automated tools.

Life Cycle Support

New hacks and attack methods are continuously being discovered. It is important to keep the products up to date against the latest attack. This can be done through firmware updates and patches, allowing the companies to keep their products protected against the latest threats.

V. EV CHARGING STATION VULNERABILITY POINTS

The vulnerabilities of Charging stations are charging station connectors, authentication of users, internet connection to EVCS and maintenance ports in EVCS.

Security Risks with EV Connectors: Due to the communication protocols and connectivity features EV connectors pose as potential targets for malicious attacks. Exploiting these vulnerabilities, attackers could introduce Various attacks to gain unauthorized access to the Electric Vehicle Charging Stations (EVCS). Such breaches could have adverse security repercussions, as unauthorized access allows malicious actors to further compromise and control the system. Additionally, there are concerns about side-channel threats during the charging process, which need to be addressed[1].

Vulnerabilities in User Terminals: The use of the latest authentication methods like RFID, credit card, or NFC for interconnecting various components of EVCS and Users to aid in billing and tracking. However, the security of these authentication systems is of utmost crucial. Compromised authentication systems could result in significant disruptions, such as deactivating charging sessions, manipulating pricing, or introducing safety risks to EVCS and electric vehicles. The countermeasure is to implement strong encryption, securing communication protocols, regular updates, and vulnerability assessments are crucial for mitigating these risks.

Security Concerns with Internet Connections: The advancement in different services for offering to EVCSs requires Internet connectivity, nevertheless it could compromise security threat to the charging infrastructure, allowing attackers to exploit it as a Launchpad for broader attacks on important parts of the infrastructure. Unauthorized access through the Internet connection could impact the power grid or transportation network, potentially causing severe disruptions in the power supply.

Implementing security measures such as strong authentication controls, protocols for encryption, and intrusion detection systems are vital. Challenges with Maintenance Terminals: More physical ports are used in electric vehicles for various protocols and interfaces like Ethernet. This creates a notable concern for security. There are communication loopholes through which attackers can get unauthorized access. Such physical ports are also used for maintenance purposes. During the maintenance time the attackers can exploit the vulnerabilities to gain unauthorized access. This will affect the integrity and security of vehicles. The countermeasure is to use secure authentication control, intrusion detection, and prevention.

VI. MAPPING OF PROJECT

In the mapping project, a threat matrix [6] is used. The attack is based on the stride concept and it is widely accepted in the automotive industry. It shows the attacks and how it has been manipulated by the charging stations for getting unauthorized attacks. It shows also the impacts that can

happen on the power grid public-based charging stations, and home-based charging stations. The goal is to get the risk analysis and prioritize the countermeasures for overcoming such attacks [6].

VII. CYBERATTACKS (STRIDE THREAT)

STRIDE Threat Modeling is a widely recognized approach to analyzing threats within the industry, initially popularized through its implementation at Microsoft. This method categorizes threats into the following types, each with specific characteristics as outlined in [6]:

Spoofing: This involves impersonating a legitimate user to gain unauthorized access or privileges. The attacker pretends to be someone or something they are not to deceive the system.

Tampering: Tampering occurs when an attacker modifies or edits legitimate information within the system. This unauthorized alteration can lead to data corruption or manipulation.

Repudiation: In cases of repudiation, an attacker denies or disowns an action they have executed within the system. This could include denying responsibility for transactions or activities.

Information Disclosure: This threat involves a breach of confidentiality, where unauthorized access is gained to sensitive or protected information. Attackers may exploit vulnerabilities to access data that they are not authorized to see [3].

Denial of Service (DoS): It degrades the performance of services for legitimate users. Attackers flood the system with requests or overload it, making it inaccessible to those it is intended for.

Elevation of Privilege: Here, an attacker with limited or lower-level access attempts to gain higher privilege access within the system. By exploiting vulnerabilities, they aim to increase their level of authority or control.

By using the STRIDE framework, organizations can assess systematically and address potential threats to their systems. The STRIDE is a threat modeling methodology used to identify and analyze potential security threats in software systems. Developed by Microsoft, it stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. It helps in understanding and addressing security risks during the design and development stages of a system. This identifies vulnerabilities, implements appropriate security measures, and mitigates risks effectively.

VIII. DATA HUNTING

The flow diagram of data in EV is given in [3]. The charging process in electric vehicles involves critical (dark solid) and non-critical (light dotted) data flows. The vehicle, divided into trust domains, includes the "Powertrain Domain" managing power generation and the EV communication controller, BMS (Battery management systems), and CAN bus (Controller area network bus) for communication. External interfaces like OBD (On board diagnostics), WIFI, Bluetooth, and cellular modems expand the vehicle's attack surface. Gateways are crucial for secure communication between domains, performing functions like intrusion detection and key management. V2G Root and subordinate CAs authenticate parties, establishing a trust hierarchy for secure communications. This system aims to secure communication in EV charging, addressing challenges in network security and ensuring trust in data exchanges between vehicles and charging stations [6,10,11].

The data flow diagram is divided into four regions and outlines the vehicle, charging station, service provider, and external entities responsible for charging infrastructure. The station likely houses multiple controllers: the System for overall functionality, the Power module for power electronics, SECC for EV communication, and the cooling controller for thermal management. A human-machine interface aids customer authorization and reports charging metrics. Connectivity to the CSO is via wireless or wired networks, adjusting electric demand based on signals from the distribution system operator. Another model depicts power connections, with HPC stations likely linked to a 480V to 35kV distribution network, metering power usage separately for billing. System models, (combined and analyzed using threat modeling), reveal consequences and threats. Remote threats, executable via the internet, pose higher risks as attackers can strike from anywhere globally—local threats, needing physical presence, target components directly. The models identify vulnerabilities such as power disruption through remote-controllable breakers, local protection circuit tripping, and potential onsite storage or generation to supplement grid supply. This analysis informs strategies to secure EV charging systems against diverse cyber and physical threats, ensuring safe and reliable operations [6, 10-14].

IX. COUNTERMEASURES FOR CYBERATTACKS IN EV CHARGING STATION

Business Network and Operations

Implement secure coding practices including integrity checks of code repositories and version-controlling.

Use separation of privilege for all EVCS-related operations

Ensure cyber security best practices like the NIST cybersecurity framework, which are used for internal assessment of cyber hygiene patching supply chain and its management as well as threat mitigations [10].

EVCS Security and Network:

Implement Tamper detection sensors and alarms on EVSE enclosures. Prioritize alarms and ensure timely actions on critical log events. Encrypt all information storage devices within the EVSE.

Use Network segmentation and VLANs to isolate EVSE installations. Install firewalls and IDs at key network locations. Encrypt all network traffic using a FIPS 140 - 2 compliant cryptographic module. Disable unnecessary services and ports [11].

The development of standardized policies as well as for other assets management in the EVCS. Defensive techniques can include the defense mechanism for various networks like firewalls. Anomaly detection, as well as intrusion detection, are preventive systems that can be additionally added to the current awareness system.

The response mechanisms should be researched more to prevent further adverse actions on the system, such research mechanisms can be considered as non-repudiation technologies as well as dynamic responses.

The contingency plans should be operating modes that would help create hardware and software-based fallback mechanisms [3].

Role-Based Access Control (RBAC)

Implement RBAC mechanisms to enforce least privilege access controls within ECUs, ensuring that only authorized users or processes have access to sensitive functions and data. Define roles and permissions based on the principle of least privilege to minimize the impact of potential security breaches.

Over-the-Air (OTA) Updates

Enable secure OTA update mechanisms to deliver patches, bug fixes, and software updates to automotive ECUs remotely.

Implement encryption, authentication, and integrity verification mechanisms to ensure the authenticity and integrity of updates, reducing the risk of tampering or exploitation.

Intrusion Detection Systems (IDS)

Deploy intrusion detection systems within automotive ECUs to monitor for suspicious activities or unauthorized access attempts. IDS can help detect and respond to security incidents in real time, enhancing the overall resilience of vehicle systems.

X. SCHEDULING MODEL

EV Charging/Discharging and Battery Degradation:

The Smart Charging technique manages EVs and discharging based on real-time energy demand, grid requirements, and grid quality.

Vehicle to Grid (V2G) Concept:

The V2G technology allows EVs to utilize onboard batteries as an energy source for driving and energy storage systems for power grids [12].

Battery Degradation and Charging Efficiency:

The tradeoff between inevitable battery degradation and power loss during battery discharging and the benefit of V2G needs to be further investigated [12].

XI. ACTIVE INFERENCE TO ENHANCE CYBERSECURITY IN EVCS

Active inference helps enhance the cybersecurity of EVCS by solving complex inference tasks using probabilistic models with a large number of latent variables specific to EV charging and infrastructure. This becomes very critical when implementing advanced strategies like real-time threat intelligence sharing, adaptive security perimeters across installations or logical elements, predictive threat analysis, and anomaly detection.

The system in general should process a constant stream of data from various sources such as charging stations, EVs, payment systems, and power grid infrastructure. The data can then be used to update probabilistic models in real time, allowing the system to infer the current state of the environment and potential threats.

1. Transaction Data: Analyzing transaction data using Bayesian inference can help identify anomalous patterns that may indicate fraudulent activities or unauthorized access attempts. For example, if a user typically charges their vehicle during work hours but if there is a transaction emanating from their account late at night and a different location. Bayesian inference updates its prior probability of fraud based on this new data flagging the transaction for further investigation
2. User Behavior Data: If a user authenticates from their phone or car and suddenly there is a login attempt from a new, unknown device, Bayesian inference then updates the probability of unauthorized access and the system can require MFA or suspend the account.
3. System Performance Data: By monitoring system performance metrics such as power delivery and charging station availability, we can help detect anomalies using Bayesian inference that may indicate cyberattacks or physical tampering.
4. Threat Intelligence Data: Using live external threat intelligence data, the Bayesian inference process can help the system anticipate disruptions or increased demand.

XII. MARKOV-BLANKET

Implementing a Markov blanket in the context of an EVCS cybersecurity system is essential because it encapsulates all the information needed to predict the behavior of a node given its local environment. Once we know the states of the nodes in a node's Markov blanket, the node becomes independent of all other nodes in the network.

Identifying the Markov blankets of different components can help in designing efficient ‘message passing ‘algorithms. By focusing on the nodes in a component's Markov blanket, the system can make informed decisions and updates based on the most relevant information, without needing to consider the entire network.

The Markov blanket broadly consists of 3 types of nodes: The parents, the children, and the Spouses. From a system standpoint, this can be represented in a Graph DB with edges and vertices. For example, when updating the beliefs about a user authentication component, the system can focus on the information from its parents (e.g., user input data, authentication server status), children (e.g., access control system, transaction system), and spouses (e.g., network security measures, physical security measures). This local information is sufficient to make accurate inferences about the authentication component's state.

User Authentication Component: Using the Markov blanket of the user authentication component, the system can exchange information about authentication failures or successes with other relevant components, such as access control and transaction systems. This message passing ensures that the system responds coherently to authentication-related events.

Power Delivery System: The Markov blanket of the power delivery system helps identify the key factors influencing its performance, such as grid demand and charging station status. By monitoring these factors and sending messages to other components like the energy transaction ledger, the system can ensure that power delivery remains stable and secure.

Transaction System: The transaction system allows the system to consider the activities of user authentication, power delivery, and external payment gateways when processing transactions. By exchanging messages among these components based on their relationships, the system reacts to potential fraud or inconsistencies in real time.

Incorporating Bayesian inference and message passing using these data points and Markov blanket elements enables the EVCS cybersecurity system to: Continuously update its system about the likelihood of different threats based on new evidence.

Exchange information effectively among interconnected components to ensure a coordinated response. Adapt its security measures dynamically in response to evolving threat landscapes. Detect anomalies and potential attacks in real time by monitoring key performance indicators and user behavior patterns. Incorporate external threat intelligence to track emerging vulnerabilities and attack vectors.

By leveraging these techniques, the EVCS cybersecurity system can provide a robust, adaptive, and proactive defense against cyber threats, ensuring the safety and reliability of the charging infrastructure.

XIII. APPLICATION OF AI

An AC charger is a power switch with communications between the vehicle and the charger. Its chief purpose is electrical safety, with the ability to limit the power that the battery takes [15]. The heart of the Charger circuit is a Microprocessor similar to HT45F5Q-2, which continuously monitors the Battery voltage, charging current, and charging duration. The charging system can be hacked due to malicious software or through the internet connection to the charger. Microprocessors monitor system security in addition to charging characteristics, with Artificial intelligence. With embedded AI, the microprocessor can run AI models at the device level and directly use the results to protect the charger from cyber threats. The most widely adopted charging protocol today is OCPP, known for its standardization. As well as initiating and terminating charging sessions and processing bills, OCPP allows online changes to be made to the charging settings. OCPP supports smart charging by regulating session timing, charging rate, and charging time. Verifying a charging session's legitimacy with a billing system is the primary focus of OCPP's security measures. As a result, attackers may easily hijack the transmission and take control of EV charging since it is conducted in plain text and encryption is not widely used.

Security attacks on EVCS are typically the following: False data injection, the Man-in-the-Middle attack, Denial of Service attack, Malware injection, and Physical attack. The factors that show abnormal behaviors are changes in energy consumption, increases in power consumption, or unusually long time for charging. AI can easily detect these factors and apply countermeasures. AI algorithms detect anomaly detection and predict cyber threats.

XIV. CONCLUSIONS

The fast-growing electric vehicle (EV) market needs a close look at the cybersecurity of Electric Vehicle Charging Stations (EVCS). This paper explained the different ways to charge, from plugging in at home (Home-based charging system) to the speedy charging stations on highways (DC fast charging, DCFC) and the security issues faced by EVCS. An analysis of EVCS vulnerabilities is presented. The paper proposes a range of countermeasures such as secure coding practices, tamper detection sensors, network segmentation, intrusion detection systems, and control mechanisms' role-based access to fortify EV charging systems against these threats. This paper identifies security gaps in EV charging systems and proposes remedies that can be suitably modified for EVCS applications. Innovative solutions like Artificial Intelligence-Based Scheduling Models, Over-the-Air (OTA) Updates, and Vehicle to Grid (V2G) concepts are explored for enhanced security and efficiency.

Using the STRIDE threat model, this paper has explained potential cyber dangers like pretending to be someone else, messing with data, denying actions, leaking information, blocking services, and gaining more access than allowed in EVCS. To protect against these risks, we suggest various strong measures like safe coding, sensors to detect meddling, dividing networks, spotting intruders, and setting access rules. Also, we use smart solutions like AI-based schedules and remote updates to make EV charging safer, faster, and eco-friendly. Future work involves improving AI algorithms to help in the prediction of cyber threats in EVCS. As EVs become more popular, taking these steps is crucial to make sure EVCS are reliable, safe, and trustworthy.

Author Contributions: All three authors have made equal contributions to the conception, and literature search, drafted the paper, revised it collectively and approved the submitted version, and agree to be personally accountable for the accuracy or integrity of the full paper.

Conflicts of Interest: All three authors declare no conflict of interest.

REFERENCES

[1] S. Hamdare, O. Kaiwartya, M. Aljaidi, M. Jugran, Y. Cao, S. Kumar, M. Mahmud, D. Brown and J. Lloret, "Cybersecurity Risk Analysis of Electric Vehicles Charging Stations," *Sensors*, vol. 23, no. 15, pp. 6716, 2023.

[2] S. Holzer, "Public VS. at-Home EV Charging Stations: The Pros and Cons," 2022. Available online: https://www.bonney.com/blog/the-pros-and-cons-of-public-vs-at-home-ev-charging-stations/

[3] V. Sawant and P. Zambare, "DC fast charging stations for electric vehicles: A review," *Energy Conversion and Economics*, vol. 5, pp. 54-71, 2024.

[4] S. M. Muhindo, "Mean Field Game-Based Algorithms for Charging in Solar-Powered Parking Lots and Discharging into Homes a Large Population of Heterogeneous Electric Vehicles," *Energies*, vol. 17, no. 9, pp. 2118, 2024.

[5] W. Su, J. Wang and Z. Hu, "Planning, Control, and Management Strategies for Parking Lots for PEVs. In Plug-in Electric Vehicles in Smart Grids: Integration Techniques," *Power Systems*, Springer: Berlin/Heidelberg, Chapter. 3, pp. 61-98, Germany, 2015.

[6] J. Johnson, B. Anderson, B. Wright, J. Quiroz, T. Berg, R. Graves, J. Daley, K. Phan and M. Kunz, "Cybersecurity for Electric Vehicle Charging Infrastructure," Sandia National Laboratories, 2022.

[7] "Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design," IEC 62443-3-2, 2020.

[8] R. Baker and I. Martinovic, "Losing the car keys: Wireless PHY layer insecurity in EV charging," *Proc. of the 28th USENIX Security Symposium*, pp. 407-422, 2019.

[9] S. Acharya, Y. Dvorkin and R. Karri, "Public Plug-in Electric Vehicles +Grid Data: Is a New Cyberattack Vector Viable?," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020.

[10] M. Brandl et al., "Batteries and battery management systems for electric vehicles," *2012 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, Germany, pp. 971-976, 2012.

[11] F. Sommer, J. Dürrwang and R. Kriesten, "Survey and classification of automotive security attacks," *Information*, vol. 10, no. 4, pp. 148, 2019.

[12] M. S. Mastoi, S. Zhuang, H. M. Munir, M. Haris, M. Hassan, M. Usman, S. S. H. Bukhari and J. Ro, "An in-depth analysis of electric vehicle charging station infrastructure, policy implications, and future trends," *Energy Reports*, vol. 8, pp. 11504-11529, 2022.

[13] R. B. Carlson, K. W. Rohde, M. J. Crepeau, S. C. Salinas, S. E. Cook and A. Medam, "Consequence-Driven Cybersecurity for High Power Electric Vehicle Charging Infrastructure,", INL, 2023. https://www.osti.gov/servlets/purl/1993944

[14] Global EV Outlook 2020, IEA, https://www.iea.org/reports/global-ev-outlook-2020.

[15] Q. Chen and K.A. Folly, "Application of Artificial Intelligence for EV Charging and Discharging Scheduling and Dynamic Pricing: A Review," *Energies*, vol. 16, no. 1, pp. 146, 2023.