IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 3, Ser. 2 (May. – June. 2024), PP 21-27
www.iosrjournals.org

Cybersecurity Of Electric Vehicle Smart Charging Management For Supply Chain Transport Operation

Kamalendu Pal[1]
[1](Department Of Computer Science, City University Of London, Northampton Square, London Ec1v 0hb)

Abstract:
Background*: The combination of modern technology and supply chain operations has significantly impacted the freight transportation industry, with electric vehicles (EVs) playing a crucial role in business operations. The increasing use of EVs and charging infrastructures for medium and heavy-duty supply chain transport systems has led to the development of an intelligent charging management system (SCMS), which optimizes the charging of plug-in vehicles. This system also provides various grid services such as voltage control, frequency regulation, peak shaving, renewable energy integration support, spinning reserve, and demand response for auxiliary services. These functions rely on data from plug-in vehicles (PEVs), electric vehicle supply equipment (EVSE), service providers, and utilities. However, SCMS faces challenges, particularly regarding cyber and physical threats, including man-in-the-middle attacks, data intrusion, denial of charging, and physical attacks, due to the interactions and interdependencies between cyber and physical components. While these threats present business challenges, they also create opportunities for researchers and practitioners to develop strategies and methodologies that drive enterprises towards operational excellence in EV-driven operations. This paper provides a reference map that outlines different interface types and categories of EVSE, reviews security and privacy threats associated with these interfaces and relevant components, and highlights security protection issues and solutions from recent academic literature.*

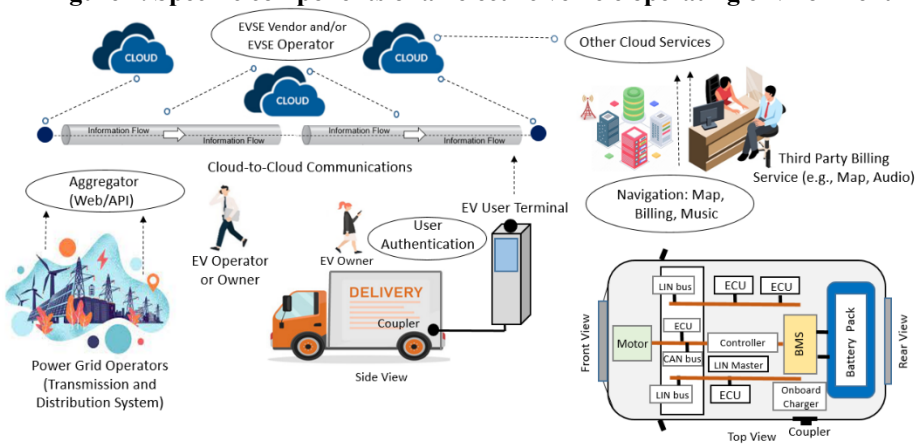
Materials and Methods*: This paper examines EVs' security and privacy issues from a Cyber-Physical System (CPS) point of view in supply chain transportation. Given the high demand for EVs and the increasing number of deployed charging facilities, it is fundamentally necessary to guarantee the security and privacy of both vehicles and drivers [8]. Many literature contributions discuss solely technical aspects of the EV ecosystem without focusing on security issues. Other security-focused works study a single system component (e.g., the vehicle's internal bus, the smart grid, or the communication protocols) without comprehensively analyzing the electric vehicle's whole ecosystem. This paper provides a general overview of EV functioning, focusing on their core components to build the basic knowledge needed to analyze the possible threat vectors. For example, denial of service (DoS) and its effects on BMS: (i) prevent energy delivery, (ii) prevent information communication, and (iii) physically damage the battery. In addition, it also considers malicious code injection, spoofing (i.e., reporting false information to the driver), MitM (Man in the Middle) attacks for reporting false information, tampering (e.g., impairing the charging process), and eavesdropping (e.g., track the user) are the few notable vulnerabilities. The paper then discusses possible attacks, briefly presents countermeasures specific to EVs, and underlines the existing security solutions for fuel vehicles that are also effective in EVs.*
Results*: This paper describes the background knowledge about EV operational ecosystems and reviews relevant literature on EV security. The paper also reviews different categories of EVSE-related cybersecurity and vulnerabilities related to a reference framework based on interface types: (i) vehicle-to-EVSE interfaces, (ii) EV owner access points, (iii) EVSE Internet Interface, and (v) EVSE Maintenance Interface, it includes wireless access (e.g., cellular, Wi-Fi, Bluetooth) and wired ports. In addition, this framework considers cloud services that interact with the EVSE through these interfaces.*
Conclusion: *The paper discusses some countermeasures for EV ecosystem security-related recent research works for individual categories. Finally, the paper concludes with concluding remarks.*
Key Word*: Business Operation; Electronic Vehicles; Freight Transport; Supply Chain Management; Security Vulnerabilities; Security Solutions.*

Date Of Submission: 12-05-2024 Date Of Acceptance: 22-05-2024

I. Introduction

The role of industrial supply chain management is to facilitate smooth operations and generate revenue by manufacturing products, adding value for providing various services, and selling products to consumers [16] [17] [18]. Common to all industrial sectors, supply chain operations must manage raw materials flowing from selective suppliers through value-adding processes and distribution channels to serve ultimate consumers. In order to provide an efficient level of service without producing an undue expenditure burden, all the business processes along the supply chain operations need to be in balance, and often, innovative technologies play essential roles. For example, electric vehicles (EVs) are the means of transporting products, services, and personnel that use electric power rather than the traditional transport systems that depend on fossil fuels. Moreover, fossil-fueled transportation is one of the significant causes of negative environmental impact due to greenhouse gas emissions out of its regular operation. The ongoing climate crisis demands green sources of alternatives to replace technologies with high environmental impact. In this way, EVs have been introduced as a sustainable green source of automobiles, where electric batteries are employed as a power source, and this modern transportation technology provides opportunities to achieve global sustainability objectives in supply chain operation [19].

Figure 1. Specific components of an electric vehicle operating environment



LEGEND –

V2G	- Vehicles to Grid Communication	Battery Pack	- Source of Energy
G2V	- Grid to Vehicle Communication	BMS	- Battery Management System
VANET	- Vehicular Ad-hoc Network	LIN bus	- Local Interconnect Network bus
WAN	- Wide Area Network	ECU	- Electronic Control Unit
CAN bus	- Controller Area Network bus	EVSE	- Electronic Vehicle Supply Equipment
WPT	- Wireless Power Transfer	(EVSE devices support the electrification of the transportation	
industry			

During recent years, the number of people opting for the EV alternative increased to the point where the specific market share of new EV sales reached more than fifty percent in some countries (e.g., Iceland (55.6%) and Norway (82.7%) [3]. Moreover, with the expanding prevalence of electric vehicle use and the charging infrastructure in the passenger vehicle sector, EVs for medium and heavy-duty freight transport applications are also increasing [2]. Consequently, strategic planning for electric vehicle charging infrastructure deployment is essential globally. At the same time, the charging points in the United Kingdom (UK) and other countries within the European Union (EU) have increased phenomenally from 34,000 in 2014 to 250,000 in 2020, and the European Commission initiated a target of one million charging stations by 2025 to reduce greenhouse gas emissions in the environment [1]. Governmental agencies are laying a strategic framework in ushering in issues related to the 'Green Environment, ' and the adoption of EVs is expected to increase soon. Governments are incentivizing the adoption of EVs thanks to the deployment of a large number of Electric Vehicle Supply Equipment (EVSE) in public charging infrastructures [4] and planning to ban sales of fossil-fueled vehicles [5]. Furthermore, technological advancement removes the current barriers to consumers' adoption of EVs, providing extended driving range and uninterrupted charging facilities [6].

The increasing number of EVs demands a thorough analysis of the security of vehicles and the operational infrastructure [7]. Like traditional vehicles, EVs have many electronic control units (ECUs), sensors, and actuators that measure real-time process performances and control stimuli inside and outside the vehicle. At the same time, ECUs are running huge lines of embedded programming code. Individual ECUs control the automobile's particular functionalities (e.g., brakes, lights), and these units intercommunicate using wire

connections. In this way, EV integrates components to govern the hardware and software-defined to manage electric (and sometimes in combination with *hybrid energy* sources) energy smartly. Some of these components are, for example, the Battery Management System (BMS) and the charging system. BMS helps store direct current (DC) as the energy source to drive an automobile unit, and it provides mechanisms to monitor individual batteries in the pack and measure each cell's voltage, current, and temperature. The BMS communicates with the human-machine interface on the dashboard to report the status of the battery system. All functional information of the BMS is communicated via microcomputers (e.g., Controller Area Network (CAN), Local Interconnected Network (LIN)) bus systems. CAN represents the primary network for cost-effective wiring, self-diagnosis, and error correction. Moreover, CAN has been designed to be a reliable solution, avoiding security and privacy-related shortcomings.

This paper examines EVs' security and privacy issues from a Cyber-Physical System (CPS) point of view in supply chain transportation. Given the high demand for EVs and the increasing number of deployed charging facilities, it is fundamentally necessary to guarantee the security and privacy of both vehicles and drivers [8]. Many literature contributions discuss solely technical aspects of the EV ecosystem without focusing on security issues. Other security-focused works study a single system component (e.g., the vehicle's internal bus, the smart grid, or the communication protocols) without comprehensively analyzing the electric vehicle's whole ecosystem. This paper provides a general overview of EV functioning, focusing on their core components to build the basic knowledge needed to analyze the possible threat vectors. For example, denial of service (DoS) and its effects on BMS: (i) prevent energy delivery, (ii) prevent information communication, and (iii) physically damage the battery. In addition, it also considers malicious code injection, spoofing (i.e., reporting false information to the driver), MitM (Man in the Middle) attacks for reporting false information, tampering (e.g., impairing the charging process), and eavesdropping (e.g., track the user) are the few notable vulnerabilities. The paper then discusses possible attacks, briefly presents countermeasures specific to EVs, and underlines the existing security solutions for fuel vehicles that are also effective in EVs.

This paper is organized as follows. Section 2 describes the background knowledge about EV operational ecosystems and reviews relevant literature on EV security. The paper also reviews different categories of EVSE-related cybersecurity and vulnerabilities related to a reference framework based on interface types: (i) vehicle-to-EVSE interfaces, (ii) EV owner access points, (iii) EVSE Internet Interface, and (v) EVSE Maintenance Interface, it includes wireless access (e.g., cellular, Wi-Fi, Bluetooth) and wired ports. In addition, this framework considers cloud services that interact with the EVSE through these interfaces. The paper also discusses some countermeasures for EV ecosystem security-related recent research works for individual categories. Finally, the paper concludes with concluding remarks.

II. Background Information And Review Of Literature

Various technologies constitute the basis of the current EV ecosystem. In this ecosystem, the Internet of Things (IoT), radio frequency identification (RFID) technology, cloud computing, middleware, and wireless sensor networks (WSNs) are the few promising constituent components. Moreover, WANs can use nearfield communications among different low-power and multi-functioning objectives or connect operational data communication nodes in an ad-hoc manner. At the same time, the EV ecosystem consists of uniquely addressable sub-systems connected through communication protocols. Interoperability and technical standards are highly influential in the EV ecosystem, laying the groundwork for security management.

Table 1. Recent literatures on EV security related issues

Research Group	Application Domain	Critical Features
Ye et al. [13], University of Georgia, USA	Cyber-Physical System by Power Electronics in EVs.	Considered security-related attacks; however, they did not consider how these attacks may impact the other components of the EV and did not discuss the issues related to wireless power transfer.
Khalid et al. [10], Ford Motor Company, and USA universities	EV's battery management system highlights the lack of a cybersecurity standard to ensure security.	Presented an overview of the possible standardization framework that could be used to achieve the security assurance of the battery management system.
Chandwani et al. [11], Arizona State University, USA	The onboard charging system of EVs.	Highlighted an overview of the cybersecurity threats associated with the onboard charging system of EVs. However, their contribution did not consider how the security attacks can impact the other components of the EVs.
Acharya et al. [12], New York University, USA and University of Zagreb, Croatia.	Different attacks inside the electric vehicle during communication with the power supplier.	Discussed how various security attacks can be conducted inside the EV and during communication with the power supplier. However, the researchers do not consider the specific components of the EVs, such as the battery management system.
Garofalaki et	Review the Open Charge	A review of OCPP and related security threats and

al.[14], University of West Attica and other Universities.	Point Protocol (OCPP) and the related security threats.	vulnerabilities in the Vehicle-to-Grid (V2G) ecosystem due to its adoption.
Babu et al. [15], National Institute of Technology, AP, India, and other universities.	Analysis of payment and authentication protocols.	Analyzed the security of the main protocols proposed for the EV environment, focusing on the payment methods and the authentication mechanisms.

Various industrial research initiatives have been related to EV security issues in recent years. Schmittner and fellow researchers [9] reviewed the available standards, including EV systems designing and validation-related issues. A group of researchers highlighted an overview of the cybersecurity requirements for the automotive industry, and their work was focused on in-vehicle components [10]. The same research group discussed various technologies and security attacks that were not specific to EVs. Multiple researchers presented technical reviews of the EV ecosystem [10] [11]. However, none of them considered the security aspects in particular.

However, many academics and practitioners presented their experimental ideas and results, concentrating on specific security issues of EV-related components. For example, a research group [10] has their views on the EV's battery management system, explicitly highlighting the lack of a cybersecurity standard to ensure its security and providing an overview of the possible standardization framework that could be used to achieve complete security assurance. The selected research works in some specialized categories are listed in a tabular format, as shown in Table 1, with a brief description of the research group, application area, and critical features.

In recent years, there have been various initiatives to review the risks within the EVSE operation environment. Based on these reviews, threat models, and the potential impacts of cyberattacks on EV charging, the research community has provided guidance on EV charging security requirements. It is worth mentioning that efforts to address security gaps have emerged out of the dedication of some of the research projects.

None of the available literature, as presented in Table 1, focuses on intertwining EVs' different cyber-physical aspects. Unlike the above research, this paper focuses on the EVSE ecosystem, presents the leading security and privacy challenges, and then highlights some mitigative solutions.

III. Security Analysis Structure

Although increased studies have been reported to apply security protection approaches to traffic and EV transportation systems, only a few research address system architectures and the platform issues of heavy-duty freight transport systems and their security. This paper reviews diverse types of EVSE cybersecurity and vulnerabilities based on a reference framework that relates to various interface categories already presented in the last part of section one.

Some research looked at the information exchange between the EV sensors, actuators, and controllers, and it has been allocated high priority for security protection deployment purposes. Generally, it is controlled by a suitable protocol, such as Message Queuing Telemetry Transport (MQTT). In addition to the used protocol, algorithms are built to manage the EVSE ecosystem's information readings and processing procedures. In this way, different software engineering process models play an essential role in the designed systems for improving numerous factors, including the reliability and expandability of EVs. While implementations, topologies, and data exchanges differ between vendors and country-specific controlling authorities, many EVSE devices have some standard features and related protocols. In addition to these protocols, various service provisions are available in modern EVs. For example, cloud services provide music streaming services for the vehicle driver, connecting emergency services at times of need, web surfing and navigation facility, and telematics. Furthermore, assorted services are used for EV's regular operations, including billing and private road toll-charge.

EV Operation Interface Vulnerabilities and Mitigative Solutions: This category of interfaces covers any contact points between EVs and the EVSE ecosystem. For example, connectors (i.e., plugs or couplers) on EVs and battery charging stations come in categories that vary in power intake and intercommunication governing protocols [21]. Due to the global usage of EVs, various categories of couplers, communication protocols, and individual connectors or contact points exist. Scientific specifications are beyond the scope of this paper. However, the individual interface represents a communication capability that can exchange intentionally manipulated charging parameters or security breaching software (commonly known as malware) to the EVSE because current EVs (e.g., semi-autonomous, fully autonomous) vehicles provide a wide range of privacy-related attack vectors into the EV/EVSE ecosystem [20] [22]. These security attacks compromise EV operation systems and provide the attacker an initial entry point in the operating environment that could pivot to the EVSE device through different communication mechanisms (i.e., wired or wireless). In

addition, the connecting cable and intercommunication protocols may also open the door for the charging session to side-channel security breaches. Some of the recent research in EV-EVSE interfaces are described briefly in Table 2.

Table 2. Electric vehicle to EVSE interface vulnerabilities.

Reference	Description of project and vulnerability
[32]	A research group reported credential theft and privacy risks.
[30]	A group of researchers published information on electric vehicle identification spoofing, power stealing, falsifying meter data, and preventing operations-related issues.
[39]	K Rohde published a paper highlighting malware injection between electric vehicles and EVSE.
[31]	Boa and fellow researchers described session hijacking, charging repudiation, MITM, DoS, and masquerading attacks.
[27]	Baker and Martinovic presented the business case of eavesdropping on EV charging sessions with radiated side-channel.
[29]	Dudek and fellow researchers presented their V2G injector software, which can read and write coupler data. This allows the theft of network keys and data injection through replay or MIT attacks.

However, the global research community has presented various security breach mitigation-related experimental outcomes in recent years, including the remote sideband coupler data extraction description [27]. There are other countermeasures reported in the literature, and these included the introduction of chokes and electronic shielding methods to optimize data leakage, enhancing the essential distribution technique, and including new Single-Level Attenuation Characterization (SLAC) initialization step to well-equipped secure coupler communications in the event of public key infrastructure (PKI) system is absent. In another research work, researchers highlighted that coupler sessions need to be re-authenticated after disruptions of the attacks to minimize the side effects on the consumers [28].

EV Operator Interface Vulnerabilities and Mitigative Solutions: At a scientific conference, a researcher presented weak security-related issues in service transactions (e.g., billing practice) and RFID card data storage in the public charging ecosystem [33]. The same researcher also described how RFID cards could be cloned in a similar way that other credit or debit card owner accounts would be billed for charging sessions. Achim Friedland presented the same type of EVSE operator privacy and identification-related issues for RFID and smartphone-based application authorization purposes [34]. In addition, there have also been warnings about credit card skimmers on EVSE operational-related equipment [35]. Another research group reported on the vulnerabilities of iSO, and Android apps deployed to manage customer charging sessions and how reversed-engineered cloud interfaces could be used [36]. In addition, the research group [38] highlighted various security vulnerabilities associated with EVSE firmware, online applications, and web portals. The group's recommended suggestions include addressing issues with EVSE web servers and applications, for example, hard-coded credentials, Structured Query Language (SQL) injection, and programmed credentials for the user interfaces [38].

EVSE Internet Interface Vulnerabilities and Remedies: One essential issue related to EVSE equipment is the presence of vulnerable web service-based applications that can be accessed locally using a smartphone or computer. In addition, most EVSE ecosystem maintenance and configuration applications use Wi-Fi to connect to the appropriate service. Moreover, these service applications are protected by a security system; however, the firewall-based protection can be breached via the EVSE ecosystem. Some of the recent research findings are briefly presented in Table 3.

Table 3. Electric vehicle to EVSE interface vulnerabilities.

Reference	Description of project and vulnerability
[26]	A researcher highlighted vulnerability using an open configuration web service running on EVSE.
[33]	Interception of RFID, credit card, and other near-field communication (NFC) data.
[36]	Researchers were reported to have accessed configuration business data and files using insecure web servers, flat EVSE networking, and inappropriate authentication methods.
[37]	A research report highlighted the issues related to unauthenticated application programming interfaces (APIs), insecure direct object API references, account hijacking, and insecure firmware update techniques.

In order to deploy secure EVSE internet interfaces, many academics and practitioners have suggested providing more robust encryption and TLS technologies. Researchers recommended end-to-end encryption to provisioning meter, service billing, and EV charging data confidentiality and integrity based on specific categories of encryptions (i.e., NISTIR 7628) and key management [41][42]. Other research works have been conducted in network-based security-related intrusion detection systems, security monitoring, and incident response planning [40] [41].

EVSE Maintenance Interface Vulnerabilities and Mitigative Recommendations: Every EVSE device has its maintenance interface. The interfaces could be serial (e.g., RS232, serial over USB), Wireless connections (e.g., Wi-Fi), Ethernet (e.g., SSH, HTTP, Telnet), Bluetooth, or via the front panel/ screen. Cybersecurity researchers have reported various vulnerabilities in the hardware and software running on EVSE. It includes research issues associated with server login and password and unique identification tokens from users [33]. A research report highlighted multiple insecure coding practice experimental results [36].

The National Renewable Energy Laboratory (NREL) recommended various risk prevention measures to mitigate the vulnerabilities and secure physical and remote access to EVSE [43]. Additionally, it has been recommended that data be encrypted with 256-bit cipher suits, all external ports be removed, and tempter alarms be introduced [41].

IV. Research Gaps and Associated Vulnerabilities

This section presents the research gaps and associated vulnerabilities of currently available technologies of various entities of SCMSs, such as PEVs, EVSEs, and smart meters. The research gaps and vulnerabilities identified by various research agencies' technical meetings on electric vehicle and charging station cybersecurity are as follows: (i) Currently available PEV and EVSE charging infrastructures are immature for cybersecurity best practices. Most PEV industries need to have security software and development methodologies and guidelines. Also, buyers of PEVs and EVSEs do not typically specify the cybersecurity-related protection requirements because of limited knowledge, (ii) the trust model for end-to-end communication is in an early stage of development, (iii) cybersecurity-related testing and assessment are not accessible to most of the PEVs and charging infrastructure industries, (iv) the guidelines and guidance on cybersecurity requirements for wireless charging infrastructures for light electric buses, and electric trucks are still in the testing and demonstration phase, and (v) commonly available EVSEs are still struggling with proper physical security guidelines and guidance. The unavailability of such guidance has already affected the consumer's confidence in PEVs.

V. Conclusion

The EVs and their applications in supply chain transportation are attracting attention from academics and practitioners, and the topic has been studied for the last few decades for multiple objectives (e.g., environmental sustainability, innovation in engineering design, mitigating green energy use, and affordability) research projects. Several research themes have been reported in the literature. These research themes propose and investigate different areas of EVs' real-world applications. The research results demonstrate the potential of using different categories of EVs to improve the performance of supply chain transportation systems. Most research applications, however, focus on modelling, system design (e.g., better batter performance, inbuilt embedded software system's security), and simulation experiments to mitigate greenhouse gas emission-related issues. Few real-world applications are developed by research and development (R & D) organizations. Researchers have paid significant attention to EV smart charging solutions worldwide to suitably meet the EVs' power source demands in recent years. Moreover, the increasing demand for EVs in the global market is challenging technology experts for better engineering design and smart charging technology, where the privacy and security of automobile owners are paramount.

In this paper, an overview of the components of an EV automobile has been discussed. It also provides the basic information needed to understand how in-vehicle communication networks work and which devices need to communicate with one another. The security and privacy-related issues of in-vehicle communications and those related to the charging infrastructure are discussed in this paper. The paper also discussed how different security attacks might influence the EV ecosystem, and then the paper presented some countermeasures for EV ecosystem security-related research works. In general, the design, implementation, and application of EV driving experience and security-related issues in traffic and transportation are still immature and need further study. Integrating new technologies, such as blockchain and mobile software agent technologies, should be considered to enhance EV application systems' flexibility and mitigate uncertainty in supply chain transport operations.

References

[1] Strauss. M. “Deployment Of EU Electric Vehicle Charging Station Too Slow, Auditors Say”. Available Online: Https://Www.Reuters.Com/Article/Us-Eu-Autos-Electric-Charging/Deployment-Of-Eu-Electric-Vehicle-Charging-Stations-Too-Slow-Auditors-Say-Iduskbn2c023c/ (Accessed On 15 February 2024).
[2] Geotab. Electric Vehicle Trends In 2020: Top 6 Factors Impacting Fleet Electrification; Geotab: Oakville, ON, Canada, 2020.
[3] Zachary. S. “16 Countries Now Over 10% Plugin Vehicle Share, 6 Over 20%”, Https://Cleantechnica.Com/2021/09/05/16-Countries-Now-Over-10-Plugin-Vehicle-Share-6-Over-20/, 2021.

[4] Madhani A. And Krisher, T. "Biden Pushes Electric Vehicle Chargers As Energy Costs Spike," Https://Www:Usnews:Com/News/Business/Articles/2021-11-17/Biden-Pushes-Electric-Vehicle-Chargers-As-Energycosts-Spike, Nov. 2021.

[5] Gordon, P. "Netherlands Aims To Ban Conventionally-Fueled Vehicles By 2050," Https://Www:Smart-Energy:Com/Industry-Sectors/Electricvehicles/Netherlands-Aim-To-Ban-Conventionally-Fueled-Vehicles-By-2050/, Jan 2019.

[6] Capuder, T. Sprcic, D. M. Zoricic, D. And Pandzic, H. "Review Of Challenges And Assessment Of Electric Vehicles Integration Policy Goals: Integrated Risk Analysis Approach," International Journal Of Electrical Power & Energy Systems, Vol. 119, 105894, 2020.

[7] Miller C. And Valasek, C. "Remote Exploitation Of An Unaltered Passenger Vehicle," Black Hat USA, 2015(91), 2015.

[8] Lin C. W. And Sangiovanni-Vincentelli, A. "Cyber-Security For The Controller Area Network (CAN) Communication Protocol," In 2012 2 International Conference On Cyber Security. IEEE, 2012, 1–7.

[9] Schmittner C. And Macher, G. "Automotive Cybersecurity Standards Relation And Overview," In International Conference On Computer Safety, Reliability, And Security. Springer, 2019, 153–165.

[10] Khalid, A. Sundararajan, A. Hernandez, A. And Sarwat, A. I. "Facts Approach To Address Cybersecurity Issues In Electric Vehicle Battery Systems," In 2019 IEEE Technology & Engineering Management Conference (TEMSCON). IEEE, 2019, 1–6.

[11] Chandwani, A. Dey, S. And Mallik, A. "Cybersecurity Of Onboard Charging Systems For Electric Vehicles—Review, Challenges And Countermeasures," IEEE Access, Vol. 8, 226 982–226 998, 2020.

[12] Acharya, S. Dvorkin, Pandzic, Y. H. And Karri, K. "Cybersecurity Of Smart Electric Vehicle Charging: A Power Grid Perspective," IEEE Access, Vol. 8, 214 434–214 453, 2020.

[13] Ye, J. Guo, L. Yang, B. Li, F. Du, L. Guan, L. And 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, 9(4), 4639–4657, 2020.

[14] Garofalaki, Z. Kosmanos, D. Moschoyiannis, S. Kallergis, D. And 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.

[15] Babu, P. R. Palaniswamy, B. Reddy, A. G. Odelu, V. And Kim, H. S. "A Survey On Security Challenges And Protocols Of Electric Vehicle Dynamic Charging System," Security And Privacy, 5(3), 2022.

[16] Pal, K. Ontology-Based Web Service Architecture For Retail Supply Chain Management, In Proceedings Of 9th International Conference On Ambient Systems, Networks And Technologies (ANT-2018), 9-11 May, Porto, Portugal, 985-990, 2018.

[17] Pal, K. And Yasar, A. Semantic Approach To Data Integration For An Internet Of Things Supporting Apparel Supply Chain Management, In Proceedings Of 17th International Conference On Mobile Systems And Pervasive Computing (Mobispc), August 9-12, Leuven, Belgium, 197-204, 2020.

[18] Pal, K. Privacy, Security And Policies: A Review Of Problems And Solutions With Blockchain-Based Internet Of Things Applications In Manufacturing Industries, In Proceedings Of 18th International Conference On Mobile Systems And Pervasive Computing (Mobispc), August 9-12, 176-183, Leuven, Belgium, 176-83, 2021.

[19] Pal, K. Drivers Of Sustainable Supply Chain Management Using Internet Of Things-Based Blockchain Technology, In The Government Impact On Sustainable And Responsible Supply Chain Management , Professor Atour Taghipour (Edited), Chapter 10, June 2023, The IGI Global Publishing, 701 E Chocolate Avenue, Hershey PA 17033, USA.

[20] Kim, K.; Kim, J.S.; Jeong, S.; Park, J.H.; Kim, H.K. Cybersecurity For Autonomous Vehicles: Review Of Attacks And Defence. Computer Security 2021, 103, 102150.

[21] Harnett, K.; Watson, G.; Brown, G. Government Fleet And Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices And Procurement Language Report; Volpe National Transportation Systems Center: Cambridge, MA, USA, 2019.

[22] Macher, G.; Armengaud, E.; Brenner, E.; Kreiner, C. Threat And Risk Assessment Methodologies In The Automotive Domain. Procedia Computer. Science. 2016, 83, 1288–1294.

[23] Wyglinski, A.M.; Huang, X.; Padir, T.; Lai, L.; Eisenbarth, T.R.; Venkatasubramanian, K. Security Of Autonomous Systems Employing Embedded Computing And Sensors. IEEE Micro 2013, 33, 80–86.

[24] Argyropoulos, N.; Khodashenas, P.S.; Mavropoulos, O.; Karapistoli, E.; Lytos, A.; Karypidis, P.A.; Hofmann, K.P. Addressing Cybersecurity In The Next Generation Mobility Ecosystem With CARAMEL. Transp. Res. Procedia 2021, 52, 307–314.

[25] Vassallo, E.W.; Manaugh, K. Spatially Clustered Autonomous Vehicle Malware: Producing New Urban Geographies Of Inequity. Transp. Res. Rec. 2018, 2672, 66–75.

[26] Shezaf, O. Who Can Hack A Plug? The Infosec Risks Of Charging Electric Cars. In Proceedings Of The Hack In The Box, Amsterdam, The Netherlands, 10–11 April 2013.

[27] Baker, R.; Martinovic, I. Losing The Car Keys: Wireless PHY-Layer Insecurity In EV Charging. In Proceedings Of The 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; 407–424.

[28] Köhler, S.; Baker, R.; Strohmeier, M.; Martinovic, I. Brokenwire: Wireless Disruption Of CCS Electric Vehicle Charging. Arxiv 2022, Arxiv:2202.02104

[29] Dudek, S.; Delaunay, J.-C.; Fargues, V. V2G Injector: Whispering To Cars And Charging Units Through The Power-Line. In Proceedings Of The SSTIC (Symposium Sur La Sécurité Des Technologies De L'information Et Des Communications), Rennes, France,
5–7 June 2019.

[30] 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 Proceedings Of The 2014 International Conference On IT Convergence And Security (ICITCS), Beijing, China, 28–30 October 2014.

[31] 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, 3–12.

[32] Höfer, C.; Petit, J.; Schmidt, R.; Kargl, F. POPCORN: Privacy-Preserving Charging For Emobility. In Proceedings Of The 2013 ACM Workshop On Security, Privacy & Dependability For Cyber Vehicles, Berlin, Germany, 4 November 2013; 37–48.

[33] Dalheimer, M. Ladeinfrastruktur Für Elektroautos: Ausbau Statt Sicherheit (Charging Infrastructure For Electric Cars: Expansion
Instead Of Security). In Proceedings Of The 34th Chaos Communication Congress, Leipzig, Germany, 27–30 December 2017.

[34] Friedland, A. Security And Privacy In The Current E-Mobility Charging Infrastructure. In Proceedings Of The Deepsec,

Vienna, Austria, 31 July 2016.
[35] Wright, A.C.; Street, J.E. Charging In The Crosshairs: How EV Drivers Could Become Cyber Criminals' New Target. 2019. Available Online: Https://Www.Digitalcitizensalliance.Org/Clientuploads/Pdf/Charging_In_The_Crosshairs.Pdf (Accessed On 23 January 2024).
[36] Cyber Security Research And Development: Cyber Assessment Report Of Level 2 AC Powered Electric Vehicle Supply Equipment; INL Technical Report INL/MIS-18-45521; INL: Hong Kong, China, 2018.
[37] Smart Car Chargers. Plug-N-Play For Hackers? Pen Test Partners. Available Online: Https://Www.Pentestpartners.Com/Securityblog/Smart-Car-Chargers-Plug-N-Play-For-Hackers/ (Accessed On 4 January 2024).
[38] 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.
[39] Rohde, K. Cyber Security Of DC Fast Charging: Potential Impacts To The Electric Grid. In Proceedings Of The S4x19, Miami, FL, USA, 14–17 January 2019.
[40] Pratt, R.M.; Carroll, T.E. Vehicle Charging Infrastructure Security. In Proceedings Of The 2019 IEEE International Conference On Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019.
[41] Van Eekelen, M.; Poll, E.; Hubbers, E.; Vieira, B.; Van Den Broek, F. An End-To-End Security Design For Smart EV-Charging For Enexis And Elaadnl; Elaadnl: Arnhem, The Netherlands, 2014.
[42] The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee. NISTIR 7628 Revision 1: Guidelines For Smart Grid Cybersecurity, Volume 1-Smart Grid Cybersecurity Strategy, Architecture, And High-Level Requirements; NIST: Gaithersburg, MD, USA, 2014.
[43] Morosan, A.G.; Pop, F. OCPP Security—Neural Network For Detecting Malicious Traffic. In Proceedings Of The International Conference On Research In Adaptive And Convergent Systems, Krakow, Poland, 20–23 September 2017; 190–195.