EXPLORING THE EV CHARGING ECOSYSTEM AND PERFORMING AN EXPERIMENTAL ASSESSMENT OF ITS CLOUD AND MOBILE APPLICATION INFRASTRUCTURE SECURITY

Pooja Patil[1], Sara Acikkol Dogan[1], Samir Tout[1], and Ranu Parmar[2]

[1]School of Information Assurance and Applied Computing, Eastern Michigan University, Michigan, USA
[2]Hitachi Energy, Michigan, USA

ABSTRACT

The security of Electric Vehicle (EV) charging has gained momentum after the increase in the EV adoption in the past few years. Mobile applications have been integrated into EV charging systems that mainly use a cloud-based platform to host their services and data. Like many complex systems, cloud systems are susceptible to cyberattacks if proper measures are not taken by the organization to secure them. In this paper, we explore the security of key components in the EV charging infrastructure, including the mobile application and its cloud service. We conducted an experiment that initiated a Man in the Middle attack between an EV app and its cloud services. Our results showed that it is possible to launch attacks against the connected infrastructure by taking advantage of vulnerabilities that may have substantial economic and operational ramifications on the EV charging ecosystem. We conclude by providing mitigation suggestions and future research directions.

KEYWORDS

Cloud infrastructure, Electric vehicle charging, Security analysis, Mitigation techniques, mobile application.

1. INTRODUCTION

With the increase in global warming, leaders are moving towards sustainability which is focused on protecting the environment. To reduce pollution and gas emissions, the transportation sector is heavily embracing the idea of putting more electric vehicles (EVs) on the road. Therefore, EVs and their charging points are expected to increase in the coming decade. The U.S. Secretary of Energy has announced a nationwide EV charging plan to support such increases [1]. In addition to chargers, a full-fledged ecosystem was designed around EV charging, which includes, among others, the home chargers, EV manufacturers, charging station manufacturers, EV drivers, cloud service providers, even the power grid, and the EV charging software companies [2]. Cloud infrastructure plays a significant role in efficiently supporting the operation of electric vehicle charging stations. It provides a range of functions, which include authentication, data storage and analysis, remote monitoring and control of charging sessions, and integration with billing and grid management systems. As a result, the use of cloud infrastructure in the operation of electric vehicle charging stations has become increasingly important as the adoption of EVs continues to grow [3]. In essence, cloud infrastructure helps ensure the seamless flow of data and will enable advanced functionalities, such as dynamic pricing, load management, and integration with renewable energy sources. To facilitate the flow of such data, notably to EV users, mobile

DOI: 10.5121/ijcsit.2024.16101

applications were added into the EV charging ecosystem to interact with the EV cloud services and provide a seamless experience for their users. However, due to the variety and intricacy of this ecosystem, there is a greater risk of cybersecurity breaches with the possibility that malicious cyber actors could exploit it at various levels, including using unsecured chargers as a point of entry to compromise vehicles, buildings, grid resources, or other charging equipment [4]. EVs also inherit attack vectors from traditional connected vehicles, under which they fall, which were grouped by [5] into ones related to the cloud, communication, or the vehicles themselves.

In this paper, we provide an overview of the high-level EV charging ecosystem. Then we outline challenges and opportunities that surround this ecosystem, explore resources to support its proper functioning and possibly mitigating the risks that surround it, such as EV standards and protocols. The study then focuses on a selected portion of the ecosystem, namely the mobile application and its communication with the cloud and performs an experimental assessment to demonstrate a potential vulnerability therein. The study concludes by providing a few suggestions and defensive approaches that can be followed to shield organizations from the cyberattacks and help take precautionary measures.

2. BACKGROUND AND MOTIVATION

a. Scaled Down EV Charging Ecosystem

The main categories of components of an EV charging ecosystem are the associated software, hardware, manufacturing and service companies, and the involved people [2]. Figure 1 below depicts representatives of these categories which constitute the main components that this study focuses on. These are: the people, the chargers, the software applications, and the cloud services. From a software standpoint, the ecosystem is divided into two main layers: a frontend and a backend. The former encompasses the software applications that users interact with including, among other things, the mobile application that the driver uses to handle the charging. These typically offer the driver the ability to manage their account, provide a map of available charging points, payment methods, and charging history [2]. The backend software layer, on the other hand, manages the charging infrastructure, including the charging station. This layer must support compliance with ISO 15118, which governs the communication between the charging station and the vehicle. It also must support Open Charge Point Protocol (OCPP) that enables the charging stations to communicate with a charging station management system (CSMS). Both ISO 15118 and OCPP will be addressed next.

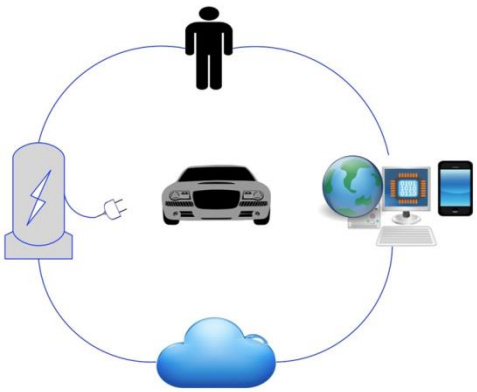

Figure 1. EV ecosystem representative categories

b. ISO 15118

The ISO 15118 standard for EVs focuses on the communication process between the EV, Electric Vehicle Supply Equipment (EVSE), and Central Management System (CMS). It specifies the message exchange between the EV and EVSE, which is implemented over a Power-Line Communication (PLC) [6]. Additionally, it defines the communication between the EVSE and CMS, which is implemented over Ethernet mainly with IPv6 UDP/TCP protocol using the Open Charge Point Protocol (OCPP) [7]. The standard itself is divided into five parts as follows:

Table 1: Sections of ISO 15118 [8]

ISO 15118-1	Presents the overall flow of communication and general use cases
ISO 15118-2	Deals with the requirements of messages exchanged by EV and EVSE over the top 5 layers of the Open System Interconnection (OSI) model.
ISO 15118-3	Deals with the functionalities of the bottom 2 layers of the OSI model which are physical and data link layer requirements.
ISO 15118-4	Includes the conformance tests for ISO 15118-2 only which deals with layers 3 and up and does not consider the power flow between EV and EVSE.
ISO 15118-5	Includes the conformance tests for ISO 15118-3 which deals with layer 2 and below.

ISO 15118 is important for interoperability and consumer acceptance of electric vehicles. It aims to ensure smooth, effective, and reliable charging of EVs by establishing a well-defined communication process [9]. It is also crucial for grid integration of EVs and supports monitoring and control of the charging process. Next it is important to cover the widely known EV charging protocol, OCPP.

c. OCPP

One of the widely known EV charging protocols is the Open Charge Point Protocol (OCPP). A few research studies have addressed possible attacks on this protocol and discussed various security challenges and potential threats associated with OCPP as it is an open-source standard for communication between EVSE and CMS [10]. Security issues related to OCPP are also a significant concern, as vulnerabilities in the protocol can lead to unauthorized access to data and disruptions in the charging infrastructure. The potential impacts of such security issues may have ramifications on power, safety, and other aspects and therefore further research into these topics is critical. There is also a need for state and federal governments to enact legislation that improves the security of EVSE systems [4]. This could lead to defining specific cybersecurity requirements for EVSE, training programs, and establishing incident response strategies for widespread cyberattacks.

d. Challenges and Opportunities

Multiple recent studies address the cybersecurity vulnerabilities of electric vehicle chargers, the potential impacts of these vulnerabilities, and the possible defenses to address them. EV charging platforms typically use a mobile application that communicates with a cloud-based service that enables ease of use and access for customers. As it is known, cloud computing has become popular and accepted due to its many advantages such as cost-effectiveness, scalability, and flexibility. It offers on-demand services, allowing users to access computation, storage, and applications remotely [11]. However, cloud infrastructure for EV charging also faces several

challenges with all the added technological complexities. One of the main challenges pertains to the cybersecurity requirements, which are confidentiality, integrity, availability, authentication, accountability, and privacy that need to be addressed to ensure the security of cloud-supported EV applications [12]. These challenges need to be overcome to fully attain the benefits of cloud computing for EV charging.

3. EVCHARGING APPS AND THEIR VULNERABILITIES

Another important player in the EV charging ecosystem is the accompanying mobile application, which at the same time is a common entry point for various types of attacks, including Man in The Middle (MiTM). The main vulnerabilities of EV charging systems are due to the lack of proper security considerations in the design of the deployed systems, which makes them insecure against cyberattacks [13]. Such vulnerabilities can lead to possible service disruption and even a failure in the power grid system of EVSEs, as demonstrated by the impact of practical cyberattack scenarios [14]. The charging infrastructure is also susceptible to message tampering, spoofing, and delay in acquiring charging points, which can negatively affect the charging services and compromise the underlying power layer [15]. Adversaries can remotely hijack charging sessions and conduct attacks against the cloud infrastructure due to the primary vulnerabilities of EV charging apps, which include illegal authorization for important operations and a lack of user/vehicle authentication [3].

Cyberattacks could also have serious negative effects on users, the distribution network operator, and the charging coordinator by exchanging sensitive information, which could have unavoidable technical and financial repercussions [16]. Researchers have also found flaws that might cause regional or nationwide disruptions in EVSE devices, communications to EVs, and cloud services provided by EVSE vendors, third-party systems, and grid operators [4]. Moreover, complex cyber-physical interdependencies created by the interaction of EVs, EVSEs, and power grids might be maliciously exploited, emphasizing the necessity of improved cybersecurity in the EV charging ecosystem [15]. The next section will provide an overview of an experiment that was conducted as part of this study to expose serious violations of more than one of the previously mentioned cybersecurity requirements: confidentiality, integrity, availability, authentication, accountability, and privacy.

4. ATTACK SCENARIOS AND IDENTIFIED RISKS

As mentioned earlier, EV charging applications face various security threats, such as potential MiTM attacks enabling unauthorized third-party interception and manipulation of network communication, phishing attempts misleading device users into disclosing sensitive information, and Denial of Service (DoS) aiming to disrupt the availability and functionality of the application or the charging infrastructure, and more.

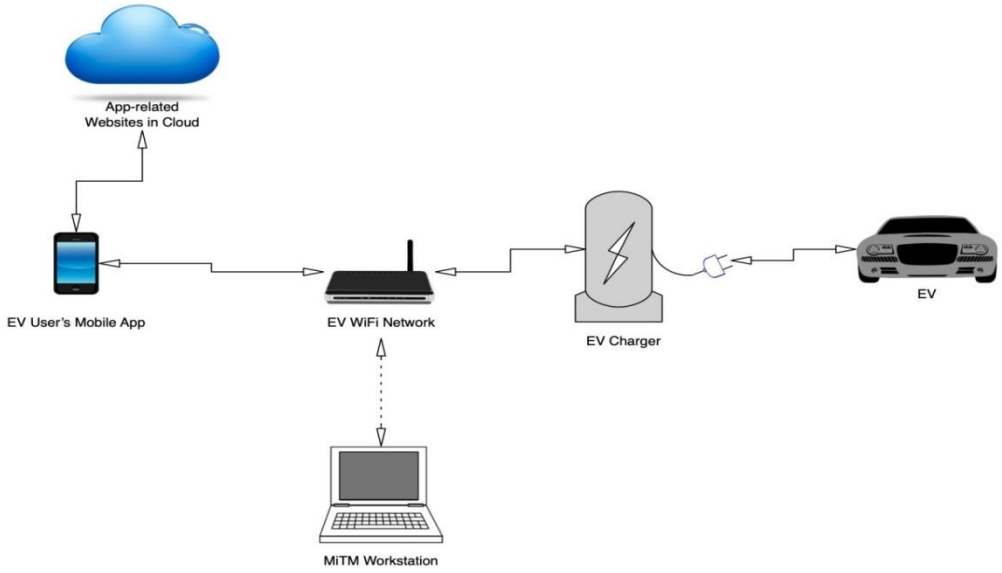

Figure 2. The experimental environment

In a hypothetical scenario, depicted in Figure 2, an external actor infiltrates the EV owner's WiFi to sniff network traffic during the user's interaction with an EV charging app through social engineering tactics. The environment was configured to have a workstation sit in the middle, between the mobile app and the cloud services, where data is sent and fetched. Certain assumptions were formulated for the purpose of risk assessment. The account creation and updating functions were intercepted, revealing a clear-text listing of the username and the password, therefore violating two basic security requirements: confidentiality and privacy. In an operational environment of the EV charging app, where all the authentication requests are processed on the servers in the cloud, if the information is not obfuscated, encrypted, or at least encoded before it is sent to the server, it becomes susceptible to interception by malicious actors. Figure 3 shows a network packet capture during a simulated interception, revealing the cleartext of the user's username and password. In the alternate network packet capture presented in Figure 4, the user's credit card information was exposed when a user incorporated a payment method into their account through the mobile app. Obtaining credit card information by attackers introduces a high risk of fraudulent transactions, identity theft and potentially compromises the cardholder's personal privacy and financial integrity.

```
1  POST /identity/connect/token HTTP/1.1
2  Host: v2-identityserver.azurewebsites.net
3  Cookie: ARRAffinity=[redacted]; ARRAffinitySame
4  Accept: */*
5  Content-Type: application/x-www-form-urlencoded
6  Authorization: Basic[redacted]
7  Content-Length: 93
8  User-Agent:[redacted] (iPhone; iOS 17.1.2; Scale/3.00)
9  Accept-Language: en-US;q=1, tr-US;q=0.9
10 Accept-Encoding: gzip, deflate, br
11 Connection: close
12
13 grant_type=password&password=admin&scope=offline_access%20api&username=admin%40evchargers.net
```

Figure 3. Cleartext confidential data disclosure

Figure 4. Cleartext payment information disclosure

Overall, this configuration of the mobile application poses a significant security risk as attackers could potentially capture and exploit the plaintext Personal Identifiable Information (PII) due to the lack of encrypted client-server communications. It violates, at a minimum, the cybersecurity mandated defense-in-depth approach in protecting critical assets.

Another part of this experiment included the exploration of how secure JSON Web Tokens (JWTs) are when used by the mobile application. JWTs are encoded in base64 and secured through cryptographic algorithms. In Figure 4, we were able to acquire the authorization token from the Application Programming Interface (API) on the client side of the application. While the modification of the JWT was prevented as it is generated exclusively on the authentication server, we decoded that JWT using an open-source tool. Although the app-to-cloud configuration had further protection for the token, without proper robust authentication, this JWT is subject to token sidejacking.

Figure 5. JWT Disclosure

In a scenario where attackers exploit decoded JWTs containing PII data, they can cause users into unwittingly expose confidential information through phishing or social engineering practices. Figure 5 illustrates that a JWT was generated each time a user visited different pages in the app, even though no user-originating change was made onto the app during the user's interaction with the application. As important, it is visible in Figure 5 that the response of each request made on the payment page included the list of credit card information previously added to the user's account. Therefore, it is crucial to treat these tokens with the same level of confidentiality as passwords, as their security depends on limited exposure.

5. MITIGATION APPROACHES

The National Renewable Energy Laboratory (NREL) researched vehicle cybersecurity threats and mitigation approaches and produced a report on "Vehicle Cybersecurity Threats and Mitigation Approaches", which includes a section on EV charging infrastructure [17]. This source provides valuable insights into the specific cybersecurity challenges the EV charging infrastructure faces and it offers mitigation approaches to address associated threats. The National Institute of Standards and Technology (NIST) provides key points for cybersecurity that can be used to protect cloud users from possible vulnerabilities and risks. Proper implementation of security protection measures is also very crucial for cloud computing service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [18, 19]. The extremely fast charging (XFC) Baseline Profile in the recent NIST report outlines a set of security standards and best practices for securing XFC infrastructure in the context of electric vehicles. It covers topics such as access control, data protection, threat mitigation, and other cybersecurity measures specific to the charging infrastructure. It offers guidance on establishing a secure and reliable environment for EV charging, ensuring the safety and integrity of the infrastructure, data, and the charging process [20].

The five main aspects of the cybersecurity framework provided by the NIST are Identify, Protect, Detect, Respond, and Recover. It is advocated by many researchers for more intensive penetration testing of EV Supply Equipment systems, development of tailored network-based and host-based intrusion detection methods, and the adoption of zero-trust principles in this context. We want to suggest focusing on the aforementioned five functions listed in the NIST framework to perform risk management for the cybersecurity of cloud infrastructure.

Figure 6. NIST framework [21]

One of the widely known risk assessment methods in cybersecurity is known as Threat Modeling. It is a process of creating hypothetical cyberattack scenarios and converting them into a system or data flow type diagram to identify vulnerabilities and eventually improve the cybersecurity of an organization. Similarly, we suggest ideas to comply with the five functions of the NIST framework to perform the reconnaissance to identify risks and make the EV applications hosted on a more robust cloud platform and secure from cyberattacks.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Figure 7. NIST five functions framework core categories [21]

1: Identify - The organizations must understand their cloud environment which helps lay the groundwork for the applications using the cloud infrastructure. It helps identify the user, system, and data assets and leads an organization to the desired state of cybersecurity and organizational goals.

To apply this function to address risks in our experiment, we walk through our scenario of the EV charging app backend being hosted on a cloud-based platform. The first step would be to list all the user and system assets.

User assets: Any personally identifiable information such as name, email, credit card details, etc. System assets: data transport security layer, JWT, virtual or storage, and servers, license details, etc.

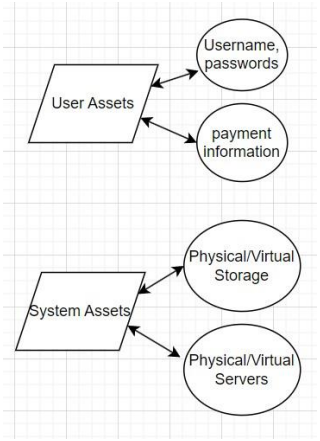

Figure 8. Cloud user and system assets

2: Protect - As a cloud provider, the organization should be heavily invested in cybersecurity. More and more organizations are beginning to transition the data to the cloud platforms and this

trend will only continue to grow. With this trend, there also comes a responsibility to protect the data and information on the cloud provided by users and within the organization itself.

To apply this function to address risks in our experiment, one way to safeguard the information would be to first train and educate the people working in the organization about cybersecurity. Secondly, organizations should apply strict cybersecurity guiding principles, such as zero-trust and trickle these down to strengthening the configuration of communication between the app and the cloud to be obfuscated at multiple layers and associated protocols. They can also make use of artificial intelligence (AI) to explore the vulnerabilities to ensure cyber resilience. Lastly, they must have timely maintenance of the services to keep the applications up to date and establish rules that force users to update the software and change their password regularly.

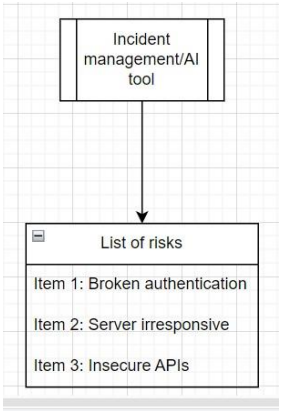

Figure 9. Example of a list of vulnerabilities found by a risk detection tool

3: Detect - As a cloud provider dealing with application security, it is important to detect data breaches as soon as they occur.

For example, a Distributed Denial of Service (DDoS) attack targets one of the cloud services that is supporting the EV app. A DDoS attack happens when multiple hosts concurrently overwhelm the target host with malicious or random traffic, making the target unresponsive or unable to operate.

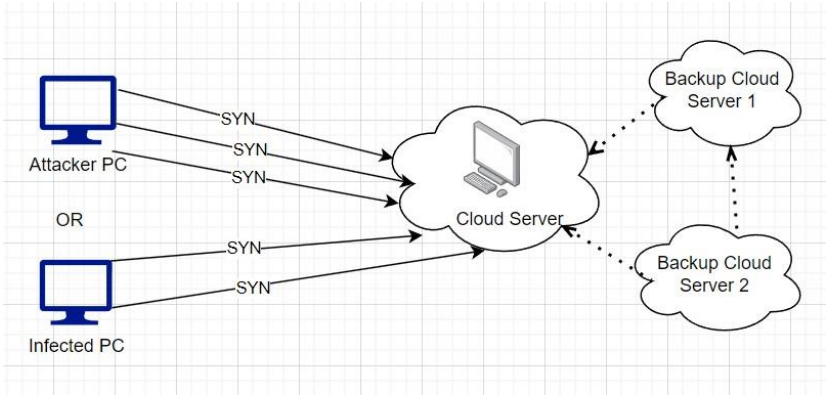

Figure 10. A simple DoS attack with multiple SYN requests to the cloud server

The first step should be to detect the attack as soon as it hits by making use of established incident detection tools. Secondly, it is essential to assemble the intricate details of which physical or virtual servers were attacked and a list of all the services that went down with the DDoS attack.

4: Respond - As it is important to detect security breaches and events as soon as possible, it is equally necessary to be able to contain the impact and take prompt actions. This can be achieved by having an incident response team, paired with an incident response plan in place at the organization.

For example, as soon as a DoS breach is detected, the first step should be to check if the current server that has been breached can be analyzed. If not, then is there a load-balancing cluster set up, and if not then does the organization have a mirror or backup server in place?

It is always important to have a backup server and if the budget supports having more than one backup server to avoid single points of failure which usually small-scale organizations face [22].
5: Recover - The organization must be able to recover from a data breach or a cybersecurity event and bring the services back up. It is also important for an organization to have a recovery strategy that reduces the impact on third parties and stakeholders associated with the organization. This delves into the important concept of business continuity to minimize the disruption of services.
For example: Now is the time to restore the services if the affected server is still functional. Otherwise, a backup server is started, pending that all services and data on the primary server can be shifted to the secondary server. The organizations can also leverage incident management tools which can help pre-configure all the above to ensure a smooth recovery.

6. CONCLUSION

This paper introduced the EV charging ecosystem, some of its relevant challenges and opportunities in relation to cybersecurity, and demonstrated, through a relevant experiment, that even modern components of an existing charging ecosystem expose serious flaws. We discussed a potential set of attack scenarios and showcased possible weaknesses that violated several cybersecurity requirements, mainly through the exposure of the user data in plain text and without basic obfuscation. This underscores the importance of utilizing established standards-based cybersecurity methods such as threat modeling, incident response, and the NIST cybersecurity framework, to mitigate or even avoid such risks. The limited experiments that we performed in this study were geared toward highlighting such flaws and, while they may not have a massive effect, they offer various stakeholders a glimpse into the need for cloud and EV providers to build their threat mitigation plan based on standards-based methods, including threat modeling. We plan to expand these experiments to encompass more components within the EV charging ecosystem, such as the OCPP-related attacks and more advanced cloud-based attacks. Future expansion of this study will also include performing an ISO/SAE 21434-compliant Threat Analysis and Risk Assessment (TARA) on the system at hand [23].

ACKNOWLEDGEMENTS

The authors would like to thank the Cloud Security Alliance (CSA), represented by our co-author Ranu Parmar, for providing insights into topics that are relevant to this study.

REFERENCES

[1] Bui, V. (2023, June). The Road to an Electric Vehicle Future. Department of Energy. https://www.energy.gov/articles/road-electric-vehicle-future.
[2] Zorko, L. (2023). EV charging ecosystem: explaining the big picture behind it. https://tridenstechnology.com/ev-charging-ecosystem/.

[3] Sarieddine, K., Sayed, M. A., Assi, C., Atallah, R., Torabi, S., Khoury, J., ...& Bou-Harb, E. (2023). EV Charging Infrastructure Discovery to Contextualize its Deployment Security. IEEE Transactions on Network and Service Management.

[4] Johnson, J., Berg, T., Anderson, B., & Wright, B. (2022). Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. Energies, 15(11), 3931.

[5] Salek, M Sabbir; Khan, Sakib Mahmud; rahman, Mizanur; Deng, Hsien-wen; islam, Mhafuzul; Khan, Zadid; et al. (2021): A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.17429510.v1.

[6] Madhusudhanan, S., & Sivraj, P. (2022, November). Development of Communication Simulator for Electric Vehicle Charging following ISO 15118. In 2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon) (pp. 1-6). IEEE.

[7] Chaudhari, A., Shegokar, S., Shinde, G., & Shimple, S. (2023, March). Real Time Implementation of OCPP Communication Protocol for Electric Vehicle Supply Equipment. In 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) (pp. 943-948). IEEE.

[8] Smart charging – Vehicle to grid Communication (2018) https://www.kpit.com/insights/smartcharging-vehicle-to-grid-communication/.

[9] Schmutzler, J., Wietfeld, C., & Andersen, C. A. (2012, October). Distributed energy resource management for electric vehicles using IEC 61850 and ISO/IEC 15118. In 2012 IEEE Vehicle Power and Propulsion Conference (pp. 1457-1462). IEEE.

[10] Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D., & Douligeris, C. (2022). Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP). IEEE Communications Surveys & Tutorials.

[11] Sadeem, Hamad, Alrasheed., Majid, Aied, Alhariri., Sulaiman, Abdulaziz, Adubaykhi., Salim, El, Khediri. (2022). Cloud Computing Security and Challenges: Issues, Threats, and Solutions. doi: 10.1109/ciot53061.2022.9766571.

[12] Gongjun, Yan., Ding, Wen., Stephan, Olariu., Michele, C., Weigle. (2013). Security challenges in vehicular cloud computing. IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2012.2211870.

[13] Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., & Assi, C. (2022). Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. Computers & Security, 112, 102511.

[14] Antoun, J., Kabir, M. E., Moussa, B., Atallah, R., & Assi, C. (2020). A detailed security assessment of the EV charging ecosystem. IEEE Network, 34(3), 200-207.

[15] Acharya, S., Dvorkin, Y., Pandžić, H., & Karri, R. (2020). Cybersecurity of smart electric vehicle charging: A power grid perspective. IEEE Access, 8, 214434-214453.

[16] Gumrukcu, E., Arsalan, A., Muriithi, G., Joglekar, C., Aboulebdeh, A., Zehir, M. A., ...& Monti, A. (2022, June). 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) (pp. 506-511). IEEE.

[17] Hodge, C., Hauck, K., Gupta, S., & Bennett, J. C. (2019). Vehicle cybersecurity threats and mitigation approaches (No. NREL/TP-5400-74247). National Renewable Energy Lab.(NREL), Golden, CO (United States).

[18] Tariq, M. I., Tayyaba, S., Ashraf, M. W., & Rasheed, H. (2017). Risk based NIST effectiveness analysis for cloud security. Bahria University Journal of Information & Communication Technologies (BUJICT), 10(Special Is).

[19] Chandramouli, R. (2011, November). Service Model Driven Variations in Security Measures for Cloud Environments. In IADIS International Conference Applied Computing 2011; November 6-8, 2011; Rio de Janeiro, Brazil (pp. 527-530). International Association for Development of the Information Society (IADIS).

[20] McCarthy, J., Grayson, N., Brule, J., Cottle, T., Dinerman, A., Dombrowski, J., & Urlaub, N. (2023). Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure (No.NIST Internal or Interagency Report (NISTIR) 8473). National Institute of Standards and Technology.

[21] National Institute of Standards and Technology (NIST). Retrieved fromwww.nist.gov.

[22] Ghafoor, Kayhan Zrar, Marwan Aziz Mohammed, Kamalrulnizam Abu Bakar, Ali Safa Sadiq, and Jaime Lloret. "Vehicular cloud computing: trends and challenges." Mobile Networks and Cloud Computing Convergence for Progressive Services and Applications (2014): 262-274.

[23] Püllen, D., Liske, J., & Katzenbeisser, S. (2021). ISO/SAE 21434-Based Risk Assessment of Security Incidents in Automated Road Vehicles. In Computer Safety, Reliability, and Security: 40th International Conference, SAFECOMP 2021, York, UK, September 8–10, 2021, Proceedings 40 (pp. 82-97). Springer International Publishing.

AUTHORS

Pooja Patil is a Ph.D. student in Cybersecurity at Eastern Michigan University, holding a Master's degree in computer science. Currently employed in the tech industry, her research focuses on the connected vehicles and related standards, such as ISO/SAE 21434. Her work showcases the synergy between automotive cybersecurity theory and practical applications. She has also presented her innovative projects at various automotive summits and conferences, highlighting her dedication to advancing the field.

Sara Acikkol Dogan is currently pursuing her Ph.D. at Eastern Michigan University and is actively engaged in the field of Automotive Cybersecurity. She holds a Masters degree in information assurance and a Bachelors in mathematics, she specializes in the exploration of security risks associated with Electric Vehicles (EVs) and Autonomous Vehicles (AVs). She also has a keen interest in, and promising contributions to penetration testing methodologies and practices, further enriching her contributions to the field.

Samir Tout is a professor of cybersecurity at Eastern Michigan University. He holds multiple industry certifications, including PMP, ITIL, TOGAF, GREM, GAWN, and GMOB. He serves as a Ph.D. advisor for several students and specializes in mobility cybersecurity and related standards such as ISO/SAE 21434, AI/ML, and is an avid programmer, with a rich industry consulting history. Dr. Tout has occasionally advised prominent automotive/aviation industry players, including major OEMs. He was awarded a collaborative NSF grant in 2014 to study anomaly detection in energy environments. He also earned several scholarly fellowships and industry awards.

Ranu Parmar is the Chief Product Security Officer at Hitachi Energy. She has over 20 years of experience in IT and Enterprise security, risk management, and application security for cloud computing solutions in the banking and energy sectors dedicated to critical infrastructure protection. She has led and specializes in the risk and compliance team, including NERC-CIP standards in the energy sector. Her cybersecurity risk and compliance experience includes policy-driven automation and driving visibility for asset protection, security operations, audit and compliance reporting, and securing industrial products, systems, and services. Ranu is a Certified Information Systems Security Professional with a Master of Science in Information Assurance from Eastern Michigan University. Ranu is one of the co-founders of the CSA Detroit Chapter and Women Security Alliance (Womsa.org).