International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Software-Defined Vehicle Fleet Management System with Integrated Cybersecurity Measures

Venkata Lakshmi Namburi

Submitted:12/05/2024 **Revised**: 28/06/2024 **Accepted**: 05/07/2024

Abstract: The significance of cybersecurity in today's globally linked world is paramount. Cybercriminals are finding new and more sophisticated ways to compromise fleet management systems, which regulate and track giant groupings of cars. The potential for cyberattacks is rising exponentially due to the increasing data-driven integration of various systems. Security threats, such as cyber vulnerabilities (CVs), have grown in tandem with the potential uses of extensive data-based communication in multiple sectors, including the autonomous car business. Data transmission between autonomous vehicles and Internet of Things devices may be more susceptible to cyberattacks because of the symmetry of extensive data communication networks employed by these vehicles. Both symmetric and asymmetric algorithms can encrypt the data associated with CVs. Proactive cybersecurity solutions for autonomous vehicles, power-based cyberattacks, and dynamic responses are among the many new concerns and opportunities presented by technological breakthroughs and shifting security threats. A lot of big data research has gone into finding ways to lessen the impact of CVs and big data breaches by implementing security solutions. Big data communication, autonomous vehicular networks (AVNs), and DCAVs will face future security challenges, primarily from CVs in data communication, vulnerabilities in AVMs, and cyber threats to network functioning. For this reason, security algorithms and countermeasure models must be efficient if CVs and data breaches are to be minimized. Integrating CV policies and rules with proxy and DMZ servers strengthened the countermeasure's effectiveness. Here, the energy levels of individual attacks are established to determine the information security measures that are reliant on the increasing degrees of assaults and CVs.

Keywords*: cybersecurity, AVNs, DCAVs, DMZ*

Introduction

The information technology teams working with federal fleet managers and the fleet managers themselves must understand the dangers connected with modern vehicles. The risks associated with distracted drivers are shifting to include invasions of privacy and compromised operation as the general safety of vehicles continues to improve. By following the procurement language described in this work, we can ensure that electric vehicle supply equipment (EVSE), connected and automated vehicles (CAVs), telematics, and driver safety can be maintained [1]. The study outlines potential security issues, methods to address them, and procurement language that can be used. Federal fleet managers typically fail miserably when faced with independently implementing mitigating recommendations. They must cooperate with the proper manufacturers and network providers to ensure the technology has enough safety measures. Cars used in trial projects or as additional equipment can have their safety features determined by procurement criteria, which fleet managers can influence [2]. They manage to do this even though they have no control over the factory settings of mass-produced automobiles.

The information contained in the study is intended to guarantee that the occupants of vehicles, additional equipment, and vehicles themselves are adequately protected.

Modern automobiles contain multiple entry points for cybercriminals, even before introducing connected or automated technologies, telematics, or electric vehicle self-evident systems (EVSE). Electronic control units (ECUs) in new automobiles often have one hundred million lines of code written into them. The wipers, airbags, and brakes are just a few of the many functions that these ECUs regulate. Using in-vehicle networks, such as the controller area network (CAN) [3,], is common practice to allow communication between these ECUs. It is

Research Scholar, B.E.S.T Innovation University (BESTIU), Software Systems Engineer, Danlaw Inc. Michigan USA. venkatanamburi91@gmail.com

possible to join or splice these networks into other networks. Potential entry points for hackers outside the vehicle include information and entertainment systems, navigation consoles, cellular and wireless signals, Bluetooth, USB connections, and even devices that monitor tyre pressure [4]. Figure 1 shows some possible entry points for malicious actors in contemporary vehicles. These attack vectors include but are not limited to, automated and networked technologies.

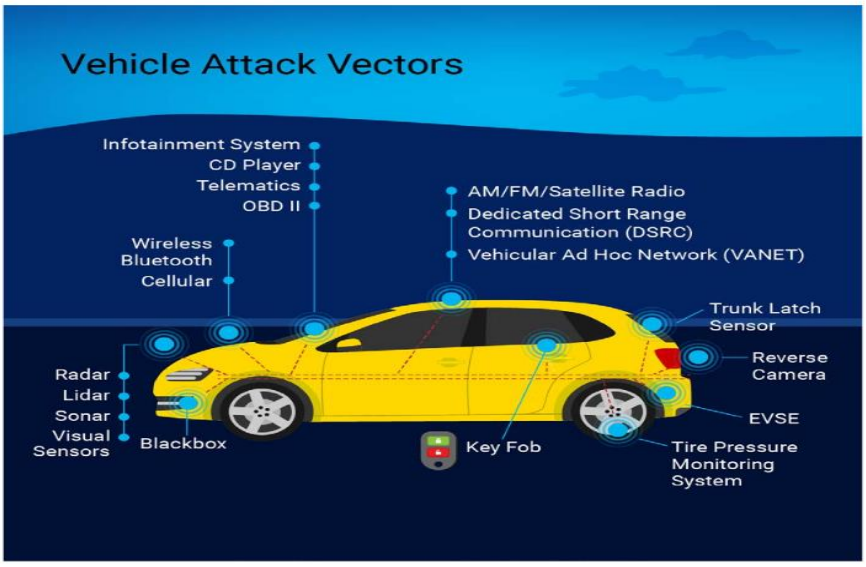

Figure 1. Attack points found in many contemporary vehicles

Since introducing software in automobiles, original equipment manufacturers have incorporated cybersecurity defence. In 2016, there were six million car crashes in the US. According to the US Department of Transportation's Deputy Administrator of the National Highway Traffic and Safety Administration [5]cyberattacks were not a factor in any of these incidents.

In fact, there is substantial evidence that certain vehicle safety features, such as automatic emergency braking, lower the number of accidents and the severity of those incidents [6]. On the other hand, vehicles are becoming increasingly technologically advanced and networked, which causes many issues, some of which are connected to safety and privacy.

Literature review

In the present moment, autos, in their position as essential components of cyber-physical systems (CPS), will be able to handle the issues currently experienced by the automobile industry properly. As the concept of vehicles-to-everything becomes more prevalent, it will increase the complexity and problems associated with self-awareness, adaptability, and dynamism regarding security. Due to the fluidity of these technological advances in intelligent movement, many essential safety improvements have been made possible. At the same time, there is still a need to move away from security methods that depend on techniques and implementations that don't change. As an illustration, the automobiles utilized in this kind of transition demonstrate that open software protocols and connections for the automobile and electric in-vehicle infrastructure are of utmost significance for the safety of the vehicles.

If they were combined with a rising number of sensor platform vehicles [8], they would become fully functional, complicated computers on wheels.

In urban mobility, such capabilities will make it easier to perform tasks such as computing within vehicles, managing fleets [9], synchronizing, telemetry, and transmitting information in both directions [10]. Using embedded technologies, they can also manage transactions involving network traffic [11]. A connected, intelligent, and self-driving car is an example of a social "thing" that can generate enormous amounts of data and serve as virtual data sources on wheels and smart mobile objects [12]. This type of car comes with the ability to drive itself. These characteristics and properties make the vehicle social.

Background

The qualities and attributes of security play an essential part in developing associated technologies, making them atomically necessary for the existence of linked, intelligent, and autonomous cars. Safety concerns are ever-present and significantly impact the evolution of automotive technology, especially as it relates to the relationship between traditional driving and the safety of autonomous driving systems. Cybersecurity solutions, ranging from the most basic to the most advanced, are now within reach for a broad range of industries and occupations, thanks to the general opinion that vehicles must comply with cybersecurity requirements as security controllers. In today's modern automobiles, there are unique security needs that encompass a wide range of topics, including application security, intrusion detection and prevention systems (IDS/IPS), secure over-the-air (OTA) transactions, trusted execution environments (TEE), built-in hardware security, and more [13].

Safety concerns have grown in tandem with visions of autonomous, connected automobiles that may exchange data with smart devices and the IoT, among other potential future transportation infrastructures. According to recent projections, there will be 115 million CVs by 2025. Furthermore, in just three years, the number of offences committed against modern automobiles has increased by 225% [14]. It will be necessary for people, automobiles, intelligent devices, the Internet of Things (IoT), and third-party infrastructure (often referred to as V2X) to collaborate for these networks to function correctly.

Many studies have been done on these security issues, focusing on vulnerability, sophistication, threat modelling, acceptability and influence factors, as well as cybersecurity evaluations and difficulties. In addition, a lot of work goes into fixing these security issues in new cars by implementing security mechanisms like trusted execution environments (TEEs) [15].

Modern Operational FMS Architectures

Fleet management information systems are essential for organizations in the transportation and logistics industry that operate a fleet of vehicles and trailers to transport products. These companies require effective vehicle management. An example of a standard information management system (IMS) architecture is shown here as a model for projecting our recommended security architectures onto it.

Sample Modern FM Functional System Architecture

A typical example of modern FMS architecture is depicted in Figure 2. It is composed of the following components: A vehicle equipped with a global positioning system (GPS) receiver for routing and tracking, as well as a mobile device equipped with the Fleet Management Client (FMC) application that communicates with the electronic control unit (ECU) of the vehicle using the On-Demand Battery Interface (ODB II) [15]. A server in the backend of the fleet management system receives information from the FMC, such as the vehicle's speed, fuel level, and Mass Air Flow (MAF), and then wirelessly transmits that information to the server. The server then stores and processes the data.

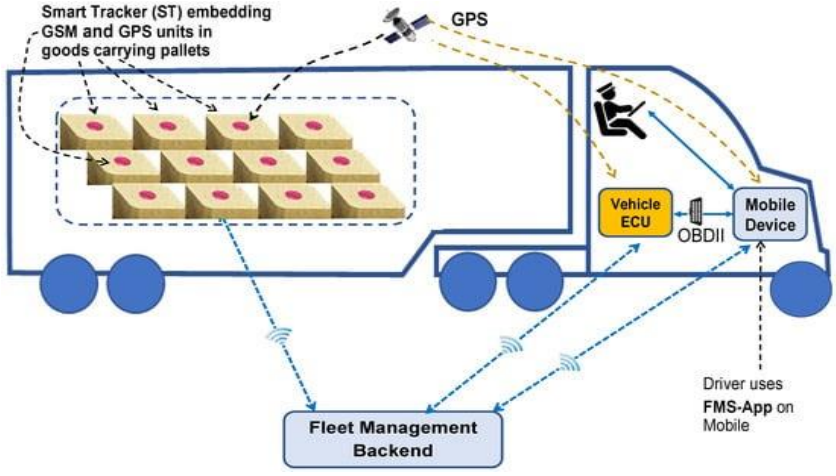

Figure 2. An example of a current fleet management system's structure.

The drivers verify their identities by logging into the FMS using the FMC app on their mobile devices. The authentication process will launch the login session once it is successful. The FMC app uses the GPS data to calculate the IRP and IFTA miles-per-state automatically. In addition to recording their pre- and post-trip inspections, drivers can monitor fuel, toll, and food purchases using the FMC app. Fleet Manager (FM) users can examine, audit, archive, and print trip records that include this information and the duty log, IFTA, IRP, and inspection data. Truck boxes or trailers equipped with Smart Trackers (STs) enable load carriers (pallets) to establish a connection to the FMS. STs include a GPS receiver, which is inexpensive and can connect to a mobile data network using SIM cards. Regularly, every ST updates the FMS with its current location [17,18].

Threat Models and FM-Adversary Types

The first step in securing the FMS is to catalogue all potential attack types, their characteristics, and the extent to which they could compromise the system. It is feasible to classify the potential attackers into the following categories:

- Insiders and Outsiders: FMS-verified users are insiders, while outsiders can only launch limited attacks.
- • Malicious and Reasonable: Bad actors who launch attacks do so solely to disrupt the network's operations; they stand to gain nothing personally. Attackers with rational minds aim to profit themselves.
- There are two main categories: active and passive attackers. In contrast to passive attackers, active attackers actively manipulate messages rather than just monitoring traffic.

Assumed Attack Scenarios on Existing FMS

A wide variety of attacks can compromise FMS deployment and operation because of its open wireless nature and the need to route information from source to destination [20] efficiently:

Impersonation Attack: This attack involves a malicious actor impersonating a legitimate FMS entity and gaining access to its resources. The perpetrators of such an assault are active enemies. Outsiders or insiders, they could be either. An attacker can take advantage of flaws in the network, application, or transport layers in this multilayer assault. An intruder takes something belonging to a valid user and passes it off as that person. An imposter mobile can trick the FMS into thinking it is an official FMS mobile and transmitting inaccurate positions. Impersonation attacks on FMS can take several forms, as seen in Figure 2:

Attack 1: The adversary impersonates the mobile.

Attack 2: The opponent impersonates the vehicle.

Attack 3: The opponent impersonates the ST.

Attack 4: The adversary impersonates the driver.

Because FMS entities do not have physically guarded identities, it is possible for an attacker to gain control of the mobile device and the car's identities. Additionally, the attacker can substitute actual items with fake ones and provide distorted data to the FMS in the form of geolocation, velocity, and other comparable metrics.

Location Tracking Attacks: By utilizing the current location of the FMS entity or the path that has been followed over time, it is feasible to track the automotive vehicle, the mobile device, the intelligent tracker, and the drivers.

Eavesdropping Attacks: These fall under the passive and network-layer attack categories. The primary objective of these assaults is to gain access to sensitive FMS data.

Denial of Service (DoS) Attacks: An FMS denial-of-service attack aims to overload the system's services so legitimate users and entities can access or disrupt the communication channel. This assault renders the system inoperable. Vehicles will not receive time-sensitive information in this manner. Furthermore, if the driver relies on the application's data to make decisions, they could be at risk. For example, a malicious actor could send a deluge of traffic (incorrect messages) to the gateway service to overwhelm the victim's resources and prevent authorized users from accessing them. Anyone launching a denial-of-service assault would target the gateway service well because it is the hub for all publicly mandated communications.

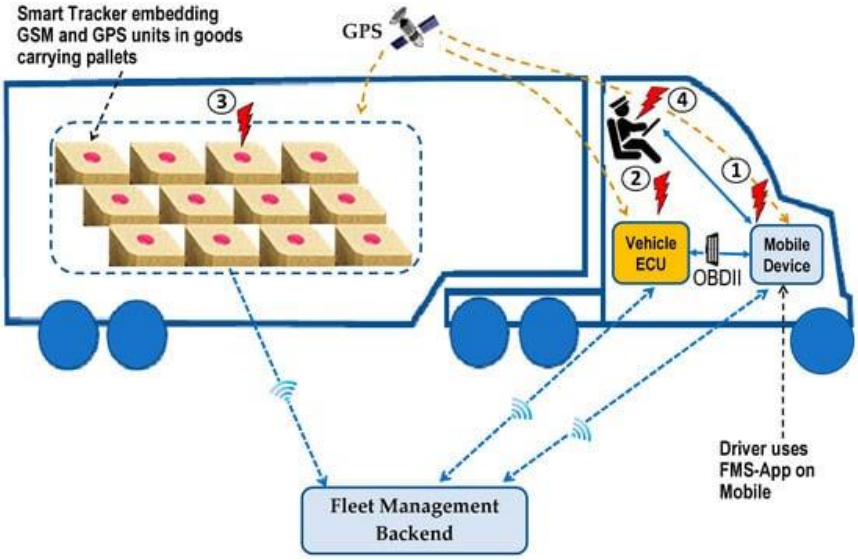

Figure 3. Modelling possible risks to existing fleet management systems.

Figure 3 shows how possible risks to existing fleet management systems are modelled. Physical security is not part of any recognized state-of-the-art treatment that renders physical units irreplaceable. This highlights the importance of developing a system that can reliably detect clone-resistant vehicles, mobiles, products, and drivers. For modern FMSs to have solid security foundations, this identification has to happen in real time. Consequently, additional security measures are required.

Research design

The recommended security design in this study was established after considering various combinations of chosen protocols and energy-efficient algorithms. This research examined preexisting models for developing safe DCAV and AVN. The suggested method ups the ante in defences by deploying an energy-efficient security algorithm.

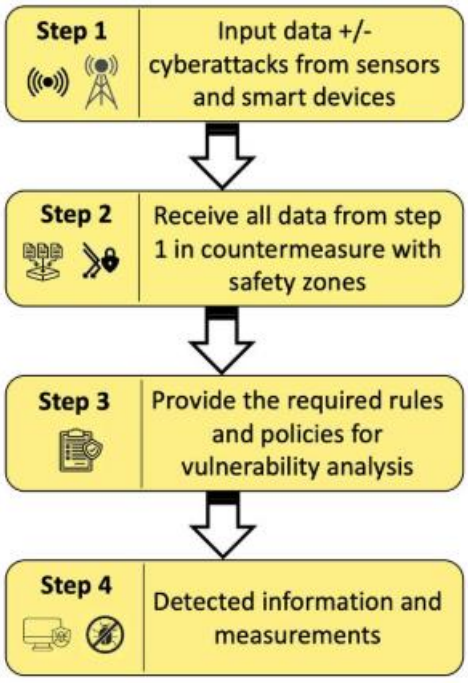

Figure 4. A block diagram of the proposed approach.

Several possible combinations of distinct energy-efficient protocols and algorithms were considered for establishing the security architecture offered in this study. This research looked at current models to see what approaches may be employed to make DCAV and AVN more secure. An algorithm for security that is efficient in terms of energy consumption is implemented in the suggested method to enhance the level of countermeasures.

Results and discussion

It has been determined through study, theoretical results, and analysis that the exchange of large amounts of data between self-driving vehicles would be protected while consuming the least energy possible. In light of this, when society starts to use autonomous cars, there will be a secure environment with low energy prices. This is because there will be a safe environment.

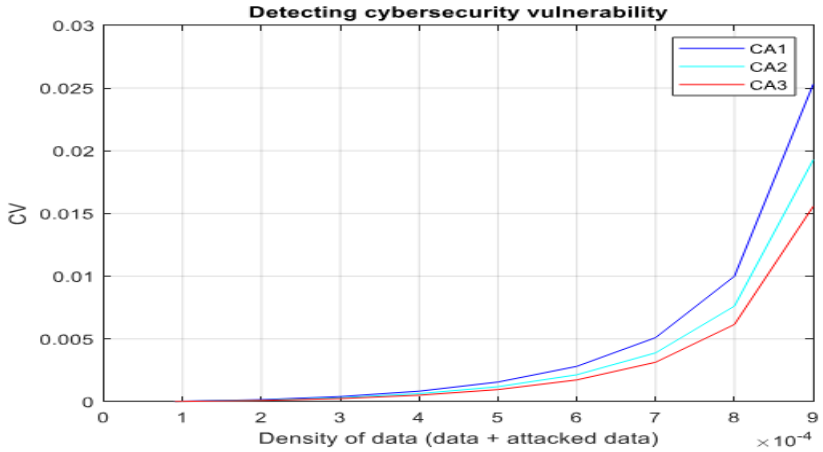

Figure 5. Detection of different cyberattacks

In addition, as shown in Figure 5, the detections are still affected by the types of cyberattacks, even if the countermeasure methods require a robust detection capability. For this experiment, we employed the three types of attacks—light, mild, and strong—identified by the suggested model. Additionally, we utilized a particular algorithm for countermeasures.

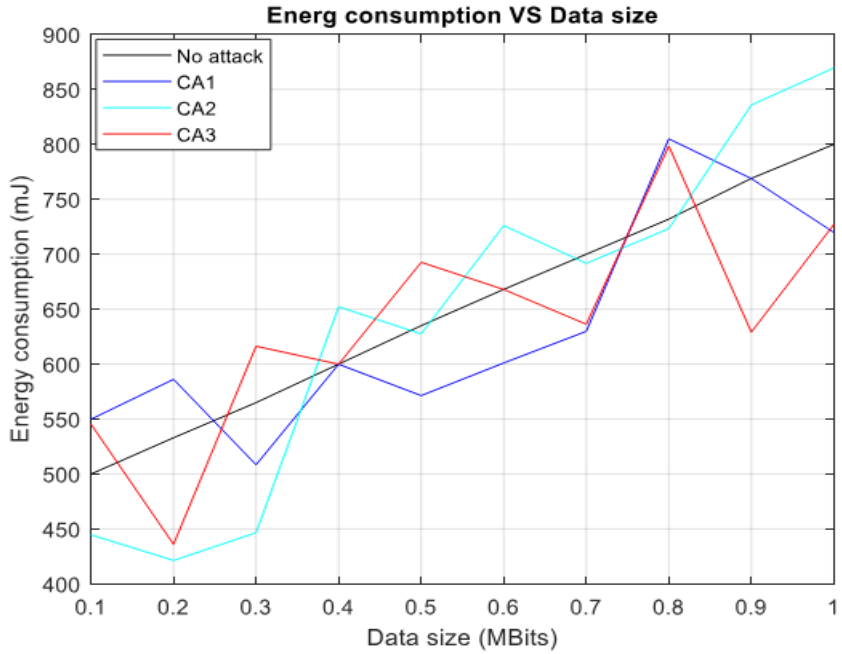

Figure 6. Energy with cyberattacks.

A description of the various energy levels that DCAV experiences in response to cyberattacks or threats is presented in Figure 6, which is broken down into the following categories:

1. Strong threats: Certain onboard diagnostics (OBD) hacks are responsible for these attacks' damage to the DCAV and AVN settings. These hacks prevent interior functions from functioning correctly. Regarding autonomous vehicles (AVs), the power of threats and CVs is increased by V2V hacks, V2I hacks, OBD, GPS spoofing, and MITM.

2. Mild threats: These threats weaken and slow down AVs' inner and exterior systems. When it comes to autonomous services, critical fob hacking on the control area network (CAN) bus and the hackinentertainment system

hacking hinder their efficiency threats: In autonomous vehicles (AVs), some parts, such as the brakes and airbags, might be compromised while the car is moving. This is the case because AVs rely on all the capabilities and services that DCAV and AVN use.

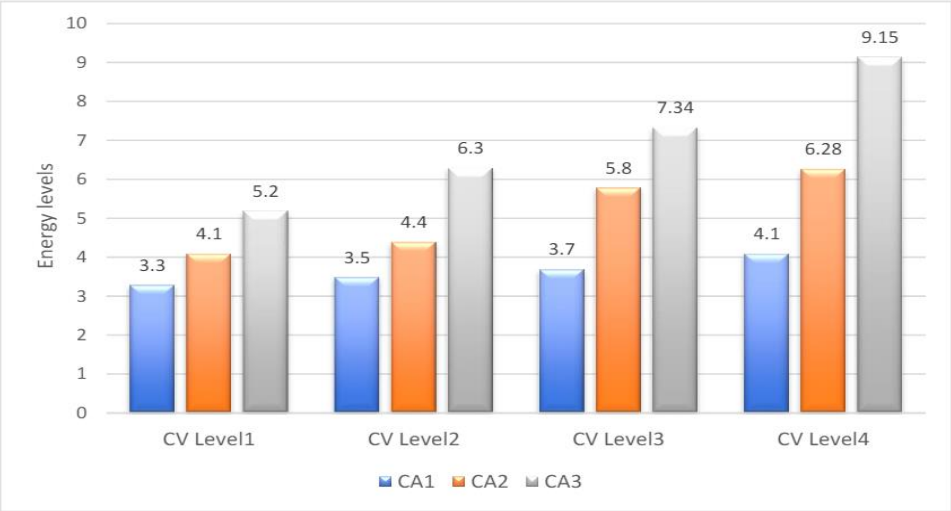

Figure 7. Energy level variations for different cyberattacks.

Figure 7 uses CV levels (CV level 1, CV level 2, CV level 3, and CV level 4) that should have fixed weights to demonstrate the results and comparisons of the energy levels.

Conclusion

This research provided an overarching summary of the CVs that pose a risk to AVN's autonomous driving capabilities and to existing AVs and DCAVs. Cybersecurity was improved due to the symmetry of data exchange and the inherent difficulty of creating security measures for autonomous vehicles. According to research into security analysis, asymmetric key encryption is the most effective solution for countermeasure security. This is because asymmetric key encryption provides significantly more protection than symmetric encryption. An appropriate theoretical model was established to identify CVs and develop countermeasures for big-data transmission, which incorporates the required norms and regulations. The objective was to guarantee the security of data collected by autonomous cars. According to the study, there is a direct correlation between the quality of cybersecurity solutions and the quantity of energy released unintentionally during breaches and irregular operations. After using the analytical method for energy measurements, it was demonstrated that whenever cyberattacks happen in the AVN and massive data transmission, energy consumption goes up. As a defence mechanism, we built and tested a distributed cyber-attack detection architecture for AVNs. The proposed framework was put to the test by executing a defence plan that considered the determination of three distinct assault types: light, mild, and powerful.

References

[1] Alcaraz, Cristina, Javier Lopez, and Stephen Wolthusen. 2017. "OCPP Protocol: Security Threats and Challenges." IEEE Transactions on Smart Grid 8, no. 5 (February 15, 2017): 2452–59. https://doi.org/10.1109/TSG.2017.2669647.

[2] Bao, Kaibin, Hristo Valev, Manuela Wagner, and Hartmut Schmeck. 2018. "A Threat Analysis of the Vehicle-to-Grid Charging Protocol ISO 15118." Computer Science - Research and Development 33, no.1 (September 1, 2017): 3–12. https://doi.org/10.1007/s00450-017-0342-y.

[3] Barker, Elaine. 2016. “Recommendation for Key Management—Part 1: General.” National Institute of Standards and Technology (NIST) Special Publication 800-57 Part 1, Revision 4. January 2016. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf.

[4] Barry, Keith. 2018. “Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair?” Consumer Reports, April 20, 2018. https://www.consumerreports.org/automotivetechnology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair/.

[5] Carlson, Barney, and Ken Rohde. 2018. “Cyber Security of DC Fast Charging: Potential Impacts to the Electric Grid.” Idaho National Laboratory presentation, September 12, 2018. INL/MIS-18- 51289. https://avt.inl.gov/sites/default/files/pdf/presentations/INLCyberSecurityDCFC.pdf.
CHAdeMO. n.d. “What is CHAdeMO.” Accessed May 2019. https://www.chademo.com/aboutus/what-is-chademo/.

[6] Checkoway et al. 2011. “Comprehensive Experimental Analyses of Automotive Attack Surfaces.” USENIX Security, August 10–12, 2011. http://www.autosec.org/pubs/carsusenixsec2011.pdf.

[7] Yu M., Guo Z., Shen S., Ning Y., Liu T., Sun D. An Intelligent Connected Vehicles Information Security Attack Matrix Model; Proceedings of the 2023 IEEE 5th International Conference on Power, Intelligent Computing and Systems (ICPICS); Shenyang, China. 14–16 July 2023; pp. 82–86. [CrossRef] [Google Scholar]

[8] Bouchouia M.L., Labiod H., Jelassi O., Monteuuis J.P., Jaballah W.B., Petit J., Zhang Z. A survey on misbehavior detection for connected and autonomous vehicles. *Veh. Commun.* 2023;**41**:100586. doi: 10.1016/j.vehcom.2023.100586.

[9] Rinaldo R.C., Horeis T.F. *Proceedings of the 4th ACM Computer Science in Cars Symposium (CSCS '20), Feldkirchen, Germany, December 2 2020.* Association for Computing Machinery; New York, NY, USA: 2020. A Hybrid Model for Safety and Security Assessment of Autonomous Vehicles; pp. 1–10. [CrossRef] [Google Scholar]

[10] Varma I.M., Kumar N. A comprehensive survey on SDN and blockchain-based secure vehicular networks. *Veh. Commun.* 2023;**44**:100663. doi: 10.1016/j.vehcom.2023.100663. [CrossRef] [Google Scholar]

[11] Hsu K. An Example of Securing In-Cabin AI Using TEE on a Secure FPGA SoC. 2020. [(accessed on 9 August 2023)]. Available online: https://www.allaboutcircuits.com/industry-articles/an-example-of-securing-in-cabin-ai-using-tee-on-a-secure-fpga-soc/

[12] Tesei A., Lattuca D., Luise M., Pagano P., Ferreira J., Bartolomeu P.C. A transparent distributed ledger-based certificate revocation scheme for VANETs. *J. Netw. Comput. Appl.* 2023;**212**:103569.

[13] Blum B. Cyberattacks on Cars Increased 225% in Last Three Years—ISRAEL21c. 2022. [(accessed on 9 August 2023)]. Available online: https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/

[14] Geppert T., Deml S., Sturzenegger D., Ebert N. Trusted Execution Environments: Applications and Organizational Challenges. *Front. Comput. Sci.* 2022;**4**:930741. doi: 10.3389/fcomp.2022.930741.

[15] Valadares D., Will N., Spohn M., Santos D., Perkusich A., Gorgonio K. *Proceedings of the 11th International Conference on Cloud Computing and Services Science-CLOSER Funchal, Madeira, Portugal, 19–21 March 2018.* SciTePress; Setúbal, Portugal: 2021. Trusted Execution Environments for Cloud/Fog-based Internet of Things Applications; pp. 111–121