2023

# Cybersecurity and Digital Privacy Aspects of V2X in the EV Charging Structure

Umit Cali

Murat Kuzlu
*Old Dominion University*, mkuzlu@odu.edu

Onur Elma

Osman Gazi Gucluturk

Ahmet Kilic

*See next page for additional authors*



## Original Publication Citation

Cali, U., Kuzlu, M., Elma, O., Gucluturk, O. G., Kilic, A., & Catak, F. O. (2023) Cybersecurity and digital privacy aspects of V2X in the EV charging structure. In A. Mileva, S. Wendzel, V. Franqueira (Eds.), *EICC '23 Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference* (pp. 174-180). Association for Computing Machinery. https://doi.org/10.1145/3590777.3591406

# Cybersecurity and Digital Privacy Aspects of V2X in the EV Charging Structure


Umit Cali
umit.cali@ntnu.no
Department of Electric Energy,
Norwegian University of Science and Technology
Trondheim, Norway

Murat Kuzlu
mkuzlu@odu.edu
Engineering Technology,
Old Dominion University
Norfolk, VA, USA

Onur Elma
onurelma@comu.edu.tr
Department of Electrical and Electronics Engineering,
Canakkale Onsekiz Mart University
Canakkale, Turkiye

Osman Gazi Gucluturk
osman.gucluturk@boun.edu.tr
Faculty of Law,
Bogazici University
Istanbul, Turkiye

Ahmet Kilic
ahmet.kilic@nisantasi.edu.tr
Department of Electrical and Electronics Engineering,
Nisantasi University
Istanbul, Turkiye

Ferhat Ozgur Catak
f.ozgur.catak@uis.no
Department of Electrical Engineering and Computer Science,
University of Stavanger
Stavanger, Norway



## ABSTRACT

With the advancement of green energy technology and rising public and political acceptance, electric vehicles (EVs) have grown in popularity. Electric motors, batteries, and charging systems are considered major components of EVs. The electric power infrastructure has been designed to accommodate the needs of EVs, with an emphasis on bidirectional power flow to facilitate power exchange. Furthermore, the communication infrastructure has been enhanced to enable cars to communicate and exchange information with one another, also known as Vehicle-to-Everything (V2X) technology. V2X is positioned to become a bigger and smarter system in the future of transportation, thanks to upcoming digital technologies like Artificial Intelligence (AI), Distributed Ledger Technology, and the Internet of Things. However, like with any technology that includes data collection and sharing, there are issues with digital privacy and cybersecurity. This paper addresses these concerns by creating a multi-layer Cyber-Physical-Social Systems (CPSS) architecture to investigate possible privacy and cybersecurity risks associated with V2X. Using the CPSS paradigm, this research explores the interaction of EV infrastructure as a very critical part of the V2X ecosystem, digital privacy, and cybersecurity concerns.



## CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

## KEYWORDS

data privacy, cybersecurity, cyber-physical-social systems, Electric vehicle, V2X





*EICC 2023, June 14–15, 2023, Stavanger, Norway*



ACM ISBN 978-1-4503-9829-9/23/06.
https://doi.org/10.1145/3590777.3591406

**ACM Reference Format:**
Umit Cali, Murat Kuzlu, Onur Elma, Osman Gazi Gucluturk, Ahmet Kilic, and Ferhat Ozgur Catak. 2023. Cybersecurity and Digital Privacy Aspects of V2X in the EV Charging Structure. In *European Interdisciplinary Cybersecurity Conference (EICC 2023), June 14–15, 2023, Stavanger, Norway.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3590777.3591406


## 1 INTRODUCTION

Connected vehicles, also known as connected cars, are vehicles that are equipped with internet connectivity and the ability to communicate with other vehicles and infrastructure on the road. This communication is often referred to as Vehicle-to-Everything (V2X) technology. Within the smart grid, V2X is not only used for vehicle-to-communication but also vehicle-to-power. Thus, V2X is defined under the cyber-physical-social system with resilient and secure power and communication process. For the security of the V2X process, the blockchain is one of the preferable methods [13, 15]. The energy trading and/or management in the EV environment need a secure and fast communication structure. The new communication technologies with V2X, such as 5G/6G, are studied in the literature [3, 16]. Another study discussed discuss some existing blockchain-integrated architectures in diverse V2X communications to develop more robust security mechanisms with 5G-enabling technologies [12]. Also, a new Cybertwin is proposed between vehicle and edge server based on proxy ring signature technique for V2X communication [14].

V2X technology allows connected vehicles to share information with each other, as well as with traffic lights, road signs, and other infrastructure, in order to improve safety, reduce congestion, and make the driving experience more efficient. For example, a connected vehicle may receive a warning from another vehicle about a potential accident ahead or information from a traffic light about when it will change to green [10]. However, as with any technology that relies on data collection and sharing, there are concerns about digital privacy and cybersecurity. Because connected vehicles are constantly sending and receiving information about their location, speed, and other data, there is a risk that this data could be accessed or used by unauthorized parties and that the systems of the vehicle

could be hacked. Besides, V2X data security and privacy protection are big issues in the automotive industry. V2X information security not only affects property security, and personal safety but also even social stability and national security. To solve this issue, the security test method for V2X Communication has been proposed [11].

This risk is increased in the case of electric vehicles (EVs), as they have a strong dependence on communication and connectivity, are connected to charging stations, and have more advanced features like remote control and monitoring. To address these concerns, several measures have been proposed, such as the use of encryption and secure communication protocols to protect data, as well as regulations and standards to govern the collection and use of data. Additionally, manufacturers and service providers may also offer features like data deletion and data sharing opt-out to give consumers more control over their data. To keep the car and its systems from being hacked, the software should be updated regularly, secure network communication should be used, and strong authentication methods should be used. AI and machine learning (ML) can be used as integral subsystems of the communication network operation [4].

Furthermore, connected vehicles and V2X technologies, particularly in the case of EVs, have the potential to increase safety, minimize congestion, and improve driving efficiency. However, it is also critical to evaluate possible digital privacy issues alongside the cybersecurity threats, as well as make efforts to safeguard customer data and car systems. Since EV charging behavior patterns of EV users may reveal some information about their private and family lives, the linked data must be managed in accordance with the appropriate cyberlaw framework. The main contribution of this article is to address the digital privacy and cybersecurity issues pertaining to the integration of V2X technologies in electric cars (EVs). The study explores the potential digital privacy and cybersecurity concerns in the V2X ecosystem, concentrating primarily on the interaction of the EV infrastructure, by proposing a multi-layer Cyber-Physical-Social Systems (CPSS) architecture tailored for the proposed study. The article also suggests a number of solutions to safeguard consumer data and vehicle systems, including encryption and secure communication protocols, legislation and standards, data deletion and data sharing opt-out choices, and frequent software upgrades with strong authentication mechanisms. Furthermore, the study emphasizes the significance of AI and machine learning in the functioning of communication networks. The contribution is supplemented further by the inclusion of an overview of the EU and US domains, which emphasize cyberlaw elements relating to privacy and cybersecurity problems in the context of V2X and EVs.

## 2 CYBER-PHYSICAL-SOCIAL SYSTEMS AND VEHICLE TO EVERYTHING (V2X)

CPSS utilizes data from three different sources: social, physical, and cyber spaces. Each of these spaces is interconnected in its own way. In the social space, people are connected through social networks; in the physical space, things are connected through networks such as sensor networks and machine networks; and in cyberspace, computing is connected through computing networks. Data is collected through various means, such as social sensors, physical sensors, and information systems databases. Fig. 1 illustrates the Cyber-Physical-Social Systems Layers of V2X. This figure is derived from [7].

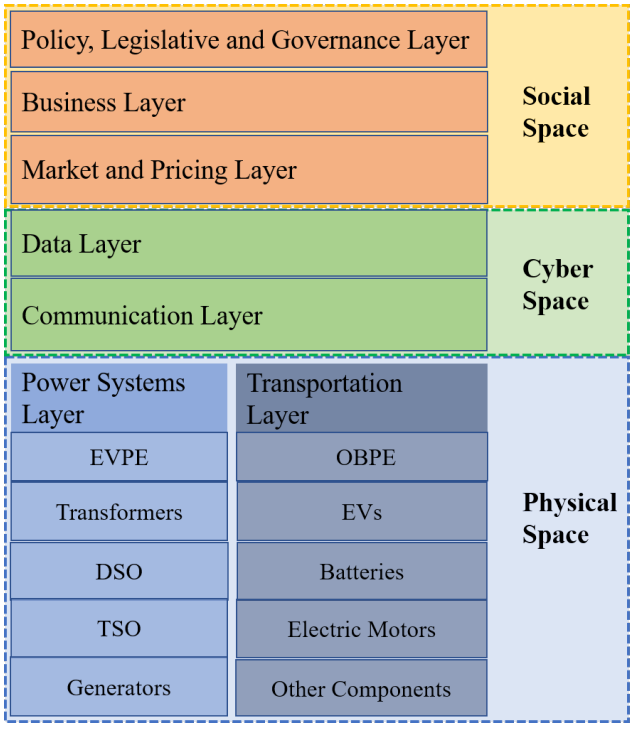


**Figure 1: Cyber-Physical-Social Systems Layers of V2X**

### 2.1 Physical Space

Electricity is more than energy needs, and it is the way to resilient and reliable power that is indispensable for the economy, civilization, better health, education, and technology. In another word, electrical energy has significant potential as a game changer for the technological improvement of society. Besides, the transition of electrification is the main focus to control climate change and for green deals. For this purpose, EVs have key roles in rising socio-technological processes with environmental concerns, and V2X structure is one of the most important parts of this relation. V2X is a socio-technical design with power and communication systems under a cyber-physical-social system (CPSS), as demonstrated in Fig. 1.

The CPSS integration is the state-of-art area to implement the communication with the internet of things, energy management, and bidirectional power flowing in the power systems [7]. Thus, V2X can be categorized under the CPPS to analyze and implement bi-directional energy-flowing opportunities. CPSS can be used to manage these mobile energy sources to supply any energy need things. The interaction between EVs and anything under cyber-physical-social systems has been shown in Fig. 2.

The physical space of the EV environment has been categorized into two sub-layers which are the power system layer and the transportation layer. The power system layer is related directly

power network and has electric vehicle power exchange equipment (EVPE), transformers, a distribution system, a transmission system, and power plants. With smart grid technology and renewable resources, distributed generation is also part of this layer [6]. The transportation layer is related to EVs and their inside physical components, which are onboard power exchange (OBPE) unit, EV batteries, electric motors, and other communication and control components. EVPE and OBPE are the critical parts of the bidirectional power exchange which have a critical role in more effective communication with the social space and more functional use of EVs.

## 2.2 Cyber Space

Cyberspace, also known as the Internet of Services (IoS), is responsible for data sensing, resource management, and computing services. Data processing is a crucial part of this layer, with the goal of converting data into information, knowledge, and wisdom. Cyberspace is a key part of CPSS and has two sub-layers: data collection and data transmission. The data collection sub-layer, which is connected to the physical layer through sensing devices, digitizes analog values, such as AC voltage and current, obtained from sensors and measurement devices.

The data transmission sub-layer then transmits information through various wired and wireless communication technologies, such as AI, DLT, and IoT. Data collection and transmission security in CPSS is a significant challenge, as it is important to protect the confidentiality and privacy of users' data during transmission. To protect personal information during the data processing and transmitting process, various security protocols, such as authentication, authorization, and encryption methods, are used to protect the identity privacy of communicating units and reduce security concerns in CPSS. Furthermore, DLT can play a crucial role in removing unnecessary third parties and enabling more secure transactions connected to EV charging, billing, and payment settlement. Furthermore, AI-based apps can be utilized to detect anomalies in order to ensure secure and dependable V2X operations.

Vehicles, components, drivers, and the environment are communicating more frequently and are becoming increasingly important. Communication is a critical factor for the technological basis of future cooperative intelligent transportation systems. It enables new and improved functions to inform and support the driver, leading to increased road safety, improved traffic efficiency, energy efficiency, and greater personal comfort and convenience. However, the number and severity of attacks on vehicles and industrial components are increasing rapidly, and the potential attack surface is also increasing due to the increasing network connectivity. The high risk and high attack surface are due to the wireless connectivity of vehicles with the environment, such as Smartphone wireless connectivity (e.g., Bluetooth, Wi-Fi), Vehicle to infrastructure communication (e.g., ITS-G5, LTE), Communication with the cloud (e.g., LTE), and Vehicle to charging station communication (e.g., Bluetooth, Wi-Fi). Furthermore, to enable advanced communication security, the Cybertwin-driven 6G network architecture for the V2X ecosystem has garnered academic interest. This framework proposes proxy ring signature handover authentication and a security reference architecture that fits very well with the demonstrated CPPS approach [14].

## 2.3 Social Space

The Cyber-Physical-Social System (CPSS) is an expansion of the current Cyber-Physical-System (CPS) that includes social space as well as cyber and physical space. Human society, comprising entrepreneurship, markets, economics, governance, law, policy, and legal elements, is referred to as social space. Social Space is divided into three layers. The Policy, Legislative, and Governance Layer refers to the involvement of states in policymaking in crucial areas such as energy, health, transportation, and digitalization. Legislative and legal features connect to the state's legislative and judicial systems. In this context, digital privacy, cyber security, and sectoral legal frameworks relevant to the energy and transportation sectors will be addressed collaboratively to give a more comprehensive study. The Business Layer also handles the firms' economics, such as their profitability and other economic indicators. Market Layer also includes market, price formation, and other market-related operations.

# 3 DIGITAL PRIVACY AND CYBER SECURITY ASPECTS

The intricacy of Cyber-Physical-Social Systems (CPSS) and Vehicle-to-Everything (V2X) connectivity raises digital privacy and cybersecurity issues. The seamless interconnectedness of cars, infrastructure, devices, and social networks creates vast volumes of data that may be used by criminal actors or endanger user privacy if not adequately safeguarded.

Encryption, authentication, and authorization secure data transmission and storage in CPSS and V2X. Advanced security protocols, including blockchain, AI, and ML, can identify and prevent cyberattacks in real time.

Governments and regulators must create comprehensive legislative frameworks to handle privacy and cybersecurity in CPSS and V2X settings. This involves creating data ownership, use, and sharing regulations and enforcing privacy and cyberattack sanctions. In the increasingly integrated transportation world, cross-border collaboration is essential for uniform legislation and enforcement.

Moreover, CPSS and V2X communication digital privacy and cybersecurity issues demand a multifaceted strategy that combines cutting-edge technology solutions with strong regulatory frameworks. This balancing unlocks intelligent transportation system capabilities while protecting user privacy and providing a secure environment.

## 3.1 General Regulatory Framework

Privacy or cybersecurity aspects of EV charging infrastructures are not specifically regulated in a single legislative text either in the EU or the US. The regulatory steps are mostly taken to reach policy goals to spread and standardize EV charging stations. "Fit for 55 in 2030 package" and "The Infrastructure Investment and Jobs Act", which is also known as "The Bipartisan Infrastructure Law," are examples of texts containing such goals and steps in the EU and the US, respectively[2, 5].

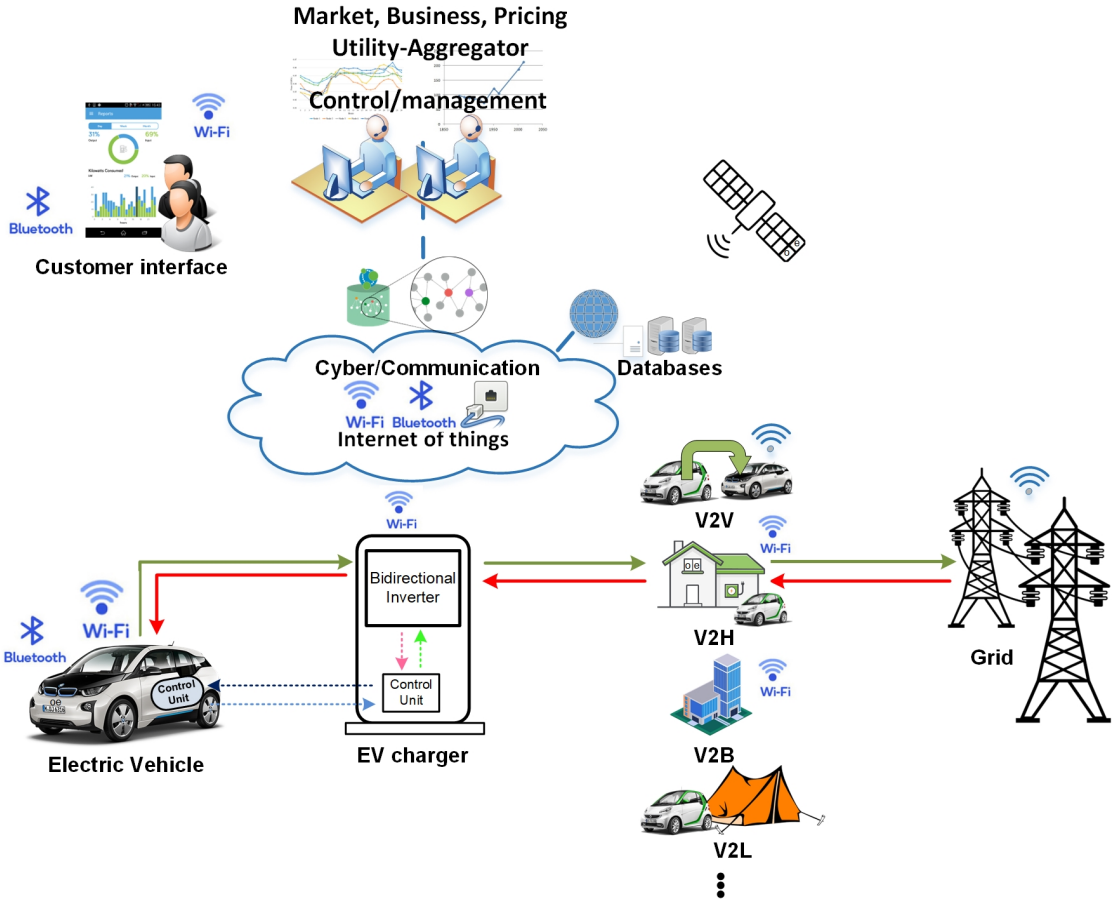


**Figure 2: Cyber-Physical-Social Systems structure of V2X**

There are also calls for standalone regulation from different entities such as ChargeUp Europe. ChargeUp Europe is created to establish communication between the sector and the EU institutions in order to render the roll-out of EV charging infrastructure expeditious and effortless[9]. Its foundational values include the commitment to ensure "the highest level of data protection and cybersecurity in their ecosystems". ChargeUp Europe calls for a standalone regulation of EV charging infrastructures for different reasons, including, but not limited to, meeting decarbonization goals and uniforming as well as harmonizing sporadic rules applicable to EV charging infrastructures in different legislative texts governing the electricity market or alternative fuels.

On the other hand, there are general frameworks applicable to digital privacy and cybersecurity, as well as secondary rules or guidelines, some of which shall be referred to below, along with certain associated risks.

## 3.2 Digital Privacy Aspects

The continuous collection and exchange of data raise the risk of unwanted access or use, which is one of the primary reasons why digital privacy is becoming an increasingly pressing issue in EVs. The more connected vehicles become, the more personal data is created and processed. The use of EV charging infrastructure as a hub for cars to connect to a charging network in different structures increases not only the amount of personal data processed but also the privacy risks.

In the EU, there are two major pieces of legislation on digital privacy: The General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD). GDPR, which became effective in 2018, is the legal framework that governs data protection and privacy in the European Union (EU). It establishes stringent standards for the acquisition, storage, and use of personal data, which is defined as "any information relating to an identified or identifiable natural person". The data gathered from connected automobiles will be either directly (location, plate number, etc.) or indirectly (journey details, driving style) related to an identifiable person; thus, personal data. Under GDPR, businesses (data controllers) processing personal data are either required to obtain the consent of individuals (data subjects) prior to the collection and use of their data or rely on one of the other grounds set forth under Article 6. Additionally, pursuant to the provisions under Chapter III, businesses are required to provide individuals with the right to access, correct, and delete any personal data that the company has collected about them. Also, as per Article 32, businesses are required to put in place appropriate

technological and organizational safeguards to keep the personal data of customers from being accessed or used without permission.

EV charging infrastructures are, in fact, connection hubs through which EVs connect to a network and share data, which may raise different concerns from the perspective of GDPR. There is no single universal EV charging infrastructure. The charging stations may be constructed as a closed network or connected directly to the grid. Communication with the driver may be established via an app, an RFID card, or both. Some stations may also offer fast charging, which affects the time during which EVs remain connected to the infrastructure and also, indirectly, the period during which data sharing takes place. Risks associated with EV charging infrastructure should be determined and addressed on a case-by-case basis, taking the specific features of the respective infrastructure into account. However, some common risks may be identified.

First, the data collected by EVs may be important for the privacy of individuals. EVs collect real-time location data and, through IoT services and devices, link this data to or share this data with other persons or services. Indeed, The European Data Protection Board (EDPB) considers the continuous location data processing in connected vehicles intrusive and emphasizes that specific measures should be implemented to protect individuals from the constant surveillance and the misuse of personal data [17]. Second, data-sharing arrangements in EV charging infrastructures may cause the loosening of the control of data subjects over their data. This is particularly important since an interconnected and interoperable network is promoted in both the EU and the US for the establishment of an efficient market in EV charging infrastructure. Third, in cases where the processing is based on consent, the augmented data-sharing and processing may undermine the validity of the consent. Hence, it should be examined whether data subjects understand the nature and the scale of the processing they consent to.

ePD, on the other hand, as explicitly stated under Article 1, supplements GDPR in ensuring "an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services." Particularly, ePD applies to components of EV charging infrastructure that are "terminal equipment" within the sense of Directive 2008/63/EC, meaning that for the storing of information, or the gaining of access to information already stored, in these components, prior consent shall be required.

In addition to GDPR and ePD, there are other existing or upcoming European legislative texts, such as the newly adopted Data Governance Act or the famous upcoming EU AI Act and the Data Act, that may affect digital privacy in EV charging infrastructures. Unsurprisingly, and in accordance with the risks mentioned above, all these texts contain provisions aimed at governing data sharing and ensuring that individuals retain some degree of control over the data that is related to or created by them.

In the US, a combination of federal and state legislation governs the protection of digital privacy. The Federal Trade Commission (FTC), which is responsible for the protection of consumers, including the privacy thereof, at the federal level, has published recommendations for the connected car sector. These recommendations emphasize providing customers with a notice that is both explicit and obvious about the acquisition and use of their data, as well as providing customers with the option to exercise control over the collection, use, and sharing of their data. Also, businesses are required to take measures to keep personal information about customers from being accessed or used in an inappropriate way.

In light of the above, it is clear that the regulatory framework concerning digital privacy and applicability to EV charging infrastructure is quite dynamic. It would be fair to expect that the number of provisions will increase over time, even in the near future. Businesses that are involved with EVs in either the EU or the US are required to comply with these and implement appropriate safeguards to keep personal data from being accessed or used inappropriately and, more generally, to CAN ensure a certain level of protection for digital privacy. Appropriate safeguards should be identified and implemented, taking risks associated with the given EV charging infrastructure setting and its features into consideration. These include but are not limited to, the encryption of data, the use of secure communication protocols, and routine security.

### 3.3 Cybersecurity Aspects

The real-time or almost real-time communication and connection of EVs make them potential targets for cyber attacks, which is why cybersecurity is also a crucial component in the connected vehicle business. Regulatory steps have been taken, again, in both the EU and the US in order to address these problems and answer the concerns of consumers.

In the EU, the Network and Information Systems Directive (NIS), which became effective in 2018, is the main legislation on cybersecurity. Directive (EU) 2022/2555 (NIS2) has been published in the Official Journal, and it is currently in force. However, pursuant to Article 44, NIS will be repealed with effect from 18.10.2024. Thus, for the purposes of the near future, both NIS and NIS2 provisions shall be relevant for cybersecurity.

Both NIS and NIS2 are collections of principles that ensure the safety of network and information systems, including EVs. Businesses that are active in this sector are required to put in place suitable safeguards, both technological and organizational, to prevent their networks and information systems from being accessed or used illegally. In addition, organizations are obligated to disclose certain kinds of cybersecurity events to the appropriate authorities.

In the US, the regulatory framework is much frictional, consisting of certain federal and state regulations. Guidelines for the connected car sector have been released by the National Highway Traffic Safety Administration (NHTSA) and the Federal Bureau of Investigation (FBI). These rules stress how important it is to protect the EV systems, networks, and communication protocols, as well as to provide regular software updates and security patches and follow industry standards for keeping data safe and making sure communications are secure. The most important development in the US is, however, The Bipartisan Infrastructure Law, which contains specific provisions on EV charging infrastructure and provides an organizational framework to spread, standardize, and ensure access to EV chargers while simultaneously maintaining the security of the network.

Companies that are active in the connected car sector in either the EU or the US are required to comply with these requirements for cybersecurity and adopt adequate steps to secure their systems and data from access or use that is not permitted. This means updating software on a regular basis, talking over a secure network, using strong authentication methods, and doing regular security audits.

# 4 V2X REQUIREMENTS AND FUTURE DIRECTIONS

## 4.1 V2X requirements

The European Commission published a strategy to promote the development of V2X communications and cooperative intelligent transport systems (CITS) in 2016 [1]. CITS describes vehicles exchanging messages that not only lead to the output of warning messages to the driver. It also aims to adjust the vehicle's driving behavior from information received via V2X message. This can result in potentially safety-critical behavior. Therefore, familiar data must be exchanged. Thus, the information contained in the received V2X messages can be trusted. This requires clear measures such as intelligent transport systems (ITS) stations to detect whether authorized ITS stations send the received V2X messages and whether a sending station is authorized to send particular data. For ITS stations to trust the legitimacy and authenticity of the V2X messages, the European approach to ITS relies on digital certificates and public key infrastructure (PKI). Vehicles or Roadside Units, as well as other entities, can participate at IST stations; for example, pedestrians sending or receiving mobile devices to the ITS messages. ETSI TR 102 638 [8, 18] defines a number of basic ITS applications, e.g., Emergency Vehicle Warning or Traffic light optimal speed advisory. With ETSI ITS specifications, it is not only about V2X communication but also about security and trusted aspects of intelligent transport systems (ITS), telematics, and all kinds of communication in vehicles and between vehicles and fixed locations. Information security for V2X is critical and requires multiple mutual recognition between vehicles and the cloud. Information security depends on different parameters, e.g., the performance of security chips and edge or backend. By introducing the edge server or backend other entities into the communication path, V2X messages and functions are exposed to attackers and potential attacks, which is not the case for direct V2V and V2I communication. However, depending on risks with the specific messages and functions, the security requirements for V2X communication involving edge or backend systems differ significantly [19]. Security with ITS for privacy and trust refers to adopting a relatively closed system. ITS stations must be registered in the respective PKI system. Registration must be in ETSI described specifications and regulations. The inclusion of edge and backend systems in the ITS is associated with these technical and organizational challenges. To protect a possible against the manipulation of V2X messages, mutual authentication and authorization of the communication partners must be used. There are requirements for conformance testing specifications published by the Connected Vehicle Certification Operating Council for test structures and procedures. All major V2X standards are based on the ISO standard for conformance testing methodology and the ETSI rules for conformance testing and test specifications, such as Wireless Access in Vehicular Environments (WAVE) 802.11 for MAC, Networking Services, SAE J2945-1 - On-board System Requirements for V2V Safety Communications. The requirements (components or system) for V2X must be defined and tested. For this purpose, there is a basic system profile in the EU, which enables interoperability between subsystems, e.g., warning of emergency vehicles and congestion warnings. Since 2016, there has been SAE International in the USA standard J2945-1 On-Board System Requirements for V2V Safety Communications. This document describes the V2X system and the selected safety applications and is based on exchanging basic safety messages like the EU.

## 4.2 Future Directions

The current situation regarding IT security in the automotive industry requires further improvement of existing IT security measures. The open character of the V2X network brings enormous challenges in terms of security and data protection in order to limit the number of participants in the V2X network and to prevent interference from unauthorized senders. All messages are cryptographically signed, and only messages containing a valid signature are processed. In order to exclude vehicles from the network that have been damaged due to a technically detected or by deliberate manipulation, messages with a valid signature. If it is possible to have no or less interference with the privacy of users, the support of anonymous or pseudonymous communication should not be enabled. The exchanged data must be protected from manipulation and deletion and accepted by legitimate participants. The exchanged data should not be disclosed to any party that is not authorized to receive the information. It must be ensured that the exchanged data can be processed enough efficiently and accurately. The secure equipment of the vehicle and environment for secure and safe communication must be affordable and avoid high costs. The existing V2X specification and standards must meet security and privacy requirements to some degree for integrity protection as measures for the realization of safe and secure communication with V2X can enable through terminals. This allows for the improvement of the capabilities of existing traffic subsystems. Thus, the coordination of applications and the improvement of systems can promote the new transport infrastructure construction, new use case, and support drivers.

# 5 CONCLUSION

V2X technology plays a critical role in boosting energy mobility, safety, and comfort for EV owners as EVs are ready to disrupt our everyday lives. If V2X becomes more widespread, it will affect a variety of industries, including transportation and energy systems. EVs have the ability to perform several functions in our daily lives, comparable to the varied usefulness of cell phones. The growth of electric vehicles will expedite the digitalization of power systems and other businesses, making power flow flexibility a vital component of contemporary power systems. It is anticipated that the next generation of EV charging infrastructure and V2X operations will support bidirectional power and data exchange. This paper investigates the concerns related to the potential privacy and cybersecurity risks associated with V2X in the context of the CPSS framework in a systematic manner, with particular emphasis on the EV charging infrastructure. It intends to explore the concerns surrounding digital privacy and security in V2X implementations. Furthermore,

this study highlights the need for implementing a comprehensive strategy that combines innovative technology solutions with solid legislative frameworks to solve digital privacy and cybersecurity problems in CPSS and V2X contexts. By finding this balance, it can be maximized the promise of intelligent transportation systems while protecting user privacy and promoting a safe environment for future mobility solutions. It is anticipated that policymakers and legislators will revise their agenda, taking into account the potential threats connected with this sector, while developing the next generation of legislative requirements for cybersecurity and digital privacy in the sphere of e-mobility and EVs.

## REFERENCES


[1] 2016. A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. COM(2016) 766 final, 30.11.2016. http://aei.pitt.edu/96134/

[2] 2021. Infrastructure Investment and Jobs Act (IIJA) (Public Law 117-58). https://www.congress.gov/117/bills/hr3684/BILLS-117hr3684enr.pdf

[3] Waqar Anwar, Norman Franchi, and Gerhard Fettweis. 2019. Physical layer evaluation of V2X communications technologies: 5G NR-V2X, LTE-V2X, IEEE 802.11 bd, and IEEE 802.11 p. In *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. IEEE, 1–7.

[4] Maria Christopoulou, Sokratis Barmpounakis, Harilaos Koumaras, and Alexandros Kaloxylos. 2022. Artificial Intelligence and Machine Learning as key enablers for V2X Communications: A Comprehensive Survey. *Vehicular Communications* (2022), 100569.

[5] European Council. 2023. Fit for 55: The EU plan for a green transition. https://www.consilium.europa.eu/en/policies/green-deal/fit-for-55-the-eu-plan-for-a-green-transition/. Accessed: 2023-04-06.

[6] Onur Elma. 2020. A dynamic charging strategy with hybrid fast charging station for electric vehicles. *Energy* 202 (2020), 117680.

[7] Onur Elma, Umit Cali, and Murat Kuzlu. 2022. An overview of bidirectional electric vehicles charging system as a Vehicle to Anything (V2X) under Cyber-Physical Power System (CPPS). *Energy Reports* 8 supp 14 (2022), 25–32. https://doi.org/10.1016/j.egyr.2022.10.008

[8] T ETSI. 2009. Intelligent transport systems (its); vehicular communications; basic set of applications. *Definitions. Technical Report 102 638, Tech. Rep.* (2009).

[9] ChargeUp Europe. 2023. What is ChargeUp Europe? https://www.chargeupeurope.eu/what-is-chargeup-europe. Accessed: 2023-04-06.

[10] Sohan Gyawali, Shengjie Xu, Yi Qian, and Rose Qingyang Hu. 2021. Challenges and Solutions for Cellular Based V2X Communications. *IEEE Communications Surveys & Tutorials* 23, 1 (2021), 222–255. https://doi.org/10.1109/COMST.2020.3029723

[11] Kexun He and Baotian Li. 2022. Automotive V2X Communication Security Key Technology and Test Method Research. In *2022 7th International Conference on Cyber Security and Information Engineering (ICCSIE)*. IEEE, 40–43.

[12] Eranda Jayatunga, Avishek Nag, and Anca Delia Jurcut. 2022. Security Requirements for Vehicle-to-Everything (V2X) Communications Integrated with Blockchain. In *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*. IEEE, 208–213.

[13] Myeonghyun Kim, Joonyoung Lee, Jihyeon Oh, Kisung Park, Youngho Park, and Kilhoum Park. 2022. Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers. *Applied Energy* 322 (2022), 119445.

[14] Guanjie Li, Chengzhe Lai, Rongxing Lu, and Dong Zheng. 2021. Seccdv: A security reference architecture for cybertwin-driven 6g v2x. *IEEE Transactions on Vehicular Technology* 71, 5 (2021), 4535–4550.

[15] Long Luo, Jingcui Feng, Hongfang Yu, and Gang Sun. 2021. Blockchain-enabled two-way auction mechanism for electricity trading in internet of electric vehicles. *IEEE Internet of Things Journal* 9, 11 (2021), 8105–8118.

[16] Md Noor-A-Rahim, Zilong Liu, Haeyoung Lee, Mohammad Omar Khyam, Jianhua He, Dirk Pesch, Klaus Moessner, Walid Saad, and H Vincent Poor. 2022. 6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities. *Proc. IEEE* 110, 6 (2022), 712–734.

[17] European Data protection Board. 2021. Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. (2021). https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

[18] Cong Wang, Yiying Zhang, Xi Chen, Kun Liang, and Zhiwei Wang. 2019. SDN-based handover authentication scheme for mobile edge computing in cyber-physical systems. *IEEE Internet of Things Journal* 6, 5 (2019), 8692–8701.

[19] Jun Wu. 2021. Security and intelligent management for fog/edge computing resources. *Fog/Edge Computing For Security, Privacy, and Applications* (2021), 213–234.