Cybersecurity Risks in Connected Vehicles

Sai Kalyani Rachapalli

ETL Developer
rsaikalyani@gmail.com

Abstract

Connected vehicles (CVs) represent a major technological advancement in the transportation sector, offering enhanced functionality, safety features, and real-time data communication. With the integration of Vehicle-to-Everything (V2X) technologies—including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Cloud (V2C) systems—automobiles have transitioned into complex cyber-physical systems. However, this increased connectivity has exponentially expanded the attack surface, rendering vehicles vulnerable to numerous cybersecurity threats. Remote hijacking of vehicles, data breaches, denial of service attacks, and manipulation of vehicular control systems have been demonstrated in various research and real-world incidents. Such vulnerabilities pose significant risks not only to driver and passenger safety but also to broader public infrastructure.

This paper investigates the cybersecurity threats facing connected vehicles, analyzing potential attack vectors, risk impacts, and current mitigation approaches. Utilizing a comprehensive methodology involving threat modeling through the STRIDE framework, risk prioritization using a modified DREAD analysis, and case study evaluation, key security challenges are systematically identified. A detailed literature review emphasizes recent advances in automotive cybersecurity, including machine learning-based intrusion detection systems and blockchain solutions for secure communications. Results indicate that while advancements in secure communication protocols and in-vehicle network segmentation offer partial defenses, connected vehicles remain substantially exposed to evolving cyber threats.

Discussion of the findings reveals critical gaps in current defense strategies, underscoring the need for security-by-design practices, continuous monitoring, and a life-cycle security management approach. Standardization efforts by international bodies, though promising, are insufficient without rigorous industry adoption and frequent updates. The paper concludes by proposing future directions for research and policy, highlighting the importance of proactive and adaptive cybersecurity measures to ensure the safety, privacy, and reliability of connected vehicular ecosystems.

By addressing cybersecurity risks comprehensively, stakeholders can facilitate the safe evolution of connected vehicles, balancing innovation with robust protection measures to safeguard individuals and societies at large.

Keywords: Connected Vehicles, Cybersecurity, Vehicle-to-Everything (V2X), Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Cloud (V2C), Remote Hijacking, Automotive Security, Cyber Threats, Denial of Service (DoS) Attacks, Intrusion Detection Systems (IDS), Blockchain Security, Over-The-Air (OTA) Updates, Electronic Control Units (ECUs), Telematics Control Units (TCUs), Supply Chain Risks, Threat Modeling, DREAD Analysis, STRIDE Framework, Automotive Cyber Regulations

I. INTRODUCTION

The sudden digitalization of the automobile sector has brought in a new age led by connected vehicles (CVs). These cars, with sophisticated communication systems, engage smoothly with external infrastructures, other cars, cloud servers, and even individual devices to provide unparalleled levels of convenience, safety, and driving efficiency. The worldwide market for connected cars is expected to grow to USD 225 billion by 2025, underlining the importance of the sector both economically and technologically [1]. Along with these advancements, however, comes a paramount issue: cybersecurity.

Connected vehicles are dependent upon sophisticated electronic control units (ECUs), telematics control units (TCUs), and over-the-air (OTA) update systems, all of which provide potential gateways for harmful actors. In contrast to traditional vehicles, in which physical systems were dominant and cyber threats were zero, the software-based nature of current CVs brings vulnerabilities similar to those in typical IT systems. In these, attackers might use the vulnerabilities to intercept sensitive user data, cause vehicle functions to fail, or even intentionally assume control over key driving systems remotely, with dire results [2].

High-profile incidents have already proven the viability of such attacks. In 2015, two cybersecurity experts, Charlie Miller and Chris Valasek, took control of a Jeep Cherokee remotely by hacking into its infotainment system, allowing them to control the steering, brakes, and transmission systems [3]. Even the seemingly cybersecurity-conscious Tesla cars have been hacked from time to time via vulnerabilities in wireless communication modules [4]. These events highlight the imperative for well-rounded security models for vehicular environments that address the peculiarities of such domains.

Additionally, added to the exposure is the insertion of Vehicle-to-Everything (V2X) communications. V2X includes Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Cloud (V2C) communications with each offering opportunities for exploitation in different ways. Unauthorized access into these communications offers the possibility for tampered traffic signals, vehicular telemetry manipulation, and extraneous data acquisition.

These risks have been identified by international regulatory organizations. The United Nations Economic Commission for Europe (UNECE) promulgated Regulation No. 155 in 2020, requiring producers to establish cybersecurity management systems throughout the life cycle of a vehicle [5]. Similarly, the National Highway Traffic Safety Administration (NHTSA) in the US has made recommendations highlighting the value of multilayered cybersecurity defenses [6].

In spite of all this, the sector has a number of challenges. Connected vehicle architectures' heterogeneity, supply chain intricacies, absence of standard protocols, and high-speed technology advancements make it very challenging to define a universal cybersecurity approach. In addition, the average vehicle's lifespan, usually more than a decade, implies that current connected vehicles have to be resilient against threats that could only be realized years after being deployed.

This paper will investigate such cybersecurity threats in detail, naming major attack vectors, measuring their effects, and analyzing existing mitigation solutions. Through the incorporation of findings from recent research and the use of systematic threat modeling, the paper will attempt to provide an end-to-end understanding of the cybersecurity issues for connected vehicles and outline realistic solutions towards effectively mitigating these threats.

II. LITERATURE REVIEW

The arrival of connected vehicles (CVs) has drastically changed the classical transportation environment, integrating it with intricate cyber-physical systems. The greater dependency on software, sensors, and communication protocols has brought along a variety of cybersecurity threats. Petit and Shladover's research [1] thoroughly discusses security issues related to V2X communication, noting that hacked messages can control vehicle behavior, producing life-threatening situations. The authors underscore that message integrity and authentication are essential to avert manipulated communication among vehicles.

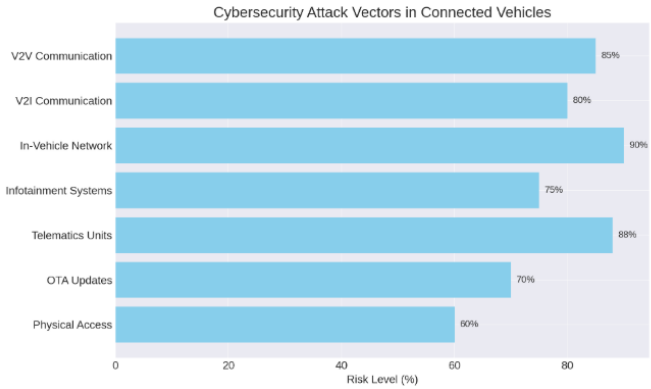

Figure 1. Major cybersecurity attack vectors in connected vehicles and their relative risk levels.

Early research on vehicular network security focused on authentication and encryption schemes. Raya and Hubaux [2] designed a security scheme for vehicular ad hoc networks (VANETs) that showed that public key infrastructure (PKI) could be employed in V2V and V2I systems. Nevertheless, privacy and scalability remain important issues of concern, specifically in relation to the real-time requirements of intelligent vehicle systems. Later improvements proposed by Lu et al. [3] employed group signature schemes to counteract privacy problems with increased computational burdens, which also affected the real-time communication capability.

More recent work has extended to intrusion detection systems (IDS) specific to vehicular environments. Kang et al. in [4] proposed a machine learning-based IDS that can identify anomalies in in-vehicle CAN bus traffic. Their findings show that supervised learning methods, especially random forests and neural networks, have high detection rates. Computational overhead and the need for labeled datasets are, however, challenges for real-time implementation in resource-limited vehicular systems.

Increased cyber-attack complexity has brought emphasis towards proactive defensive strategies. Miller and Valasek's pathbreaking research in 2015 [5] illustrated remote vehicle infotainment system exploitation, highlighting the shortcoming of perimeter defenses. Their report spurred general industry focus on cybersecurity-by-design principles, whereby security is baked into the software development lifecycle (SDLC) instead of tacked on after deployment.

Blockchain technology has also been considered as a solution for vehicular communications to be secure and transparent. In [6], Dorri et al. suggested a lightweight blockchain structure for connected vehicles, minimizing computation needs while maintaining data integrity and non-repudiation. While promising, scalability and latency remain challenges for widespread adoption.

Threat modeling methods like STRIDE and DREAD have also become popular in the automotive cyber security space. Based on the research of Woo et al. [7], using STRIDE-based threat modeling systematically classifies possible attack vectors at the design stage, allowing for early mitigation of risks. In

contrast, DREAD analysis helps prioritize vulnerabilities based on damage potential and exploitability, among other factors.

Various attempts to harmonize cybersecurity practice throughout the automobile sector have been made by multiple organizations. The ISO/SAE 21434 standard released in August 2021 creates a systematic framework for addressing cybersecurity risks throughout the vehicle life [8]. Security risk assessments, ongoing monitoring, and incident response planning are required by it. Compliance with standards like these is expected to radically improve the cybersecurity posture of connected vehicles.

In spite of these developments, there have been a few gaps remaining. Checkoway et al.'s [9] work brings out the fact that supply chain vulnerabilities are still a significant issue, as third-party components installed in vehicles can have embedded security bugs. Additionally, lifecycle management of networked vehicles is made complex due to necessity of frequent security patches, over-the-air patching, and legacy system support, areas in which many manufacturers continue to struggle to effectively manage.

Lastly, a study by Kurachi et al. [10] highlights the new threat environment created by the development of 5G-capable vehicular communications. While 5G provides lower latency and increased bandwidth, it also brings in fresh attack surfaces, such as weaknesses at the network slicing and edge computing stages, further making the security architecture for connected cars more complex.

Although significant advancements have been achieved in the identification, examination, and minimization of cybersecurity threats in connected cars, constant study is needed to stay abreast of emerging threats. The complexity and severity of CV cybersecurity require a multi-layered, adaptive, and consorted strategy among automotive suppliers, regulators, cybersecurity researchers, and consumers.

III. METHODOLOGY

To explore the connected car cybersecurity threats, an extensive and systematic approach was followed. This approach included three significant phases: threat modeling, risk analysis, and a study of the current mitigation methods. The major aim was to identify vulnerabilities systematically, analyze their possible impact, and measure the efficacy of existing countermeasures in the scenario of contemporary connected vehicle designs.

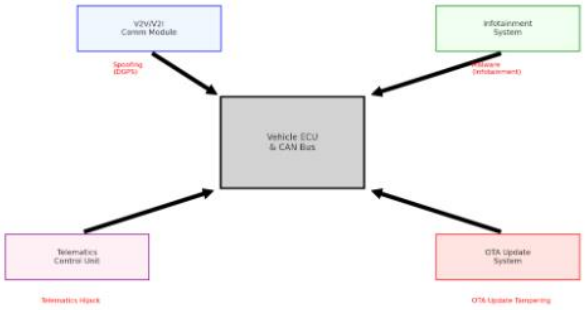

Figure 2. Connected vehicle architecture highlighting major modules and associated cybersecurity vulnerabilities.

The initial step entailed threat modeling with the use of the STRIDE framework, a proven method of classifying security threats. STRIDE, abbreviated as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, presents a comprehensive method of exploring and classifying potential security threats at the design stage of a system. Vehicle architectures, such as telematics control units (TCUs), electronic control units (ECUs), in-vehicle infotainment systems, and V2X

communication modules, were modeled separately. Each component was analyzed in terms of its potential weaknesses and associated threat types. Data flow diagrams (DFDs) were prepared to represent interactions between system components and external parties, which enable better understanding of potential attack ways.

After threat identification, a risk evaluation was done through a customized DREAD analysis. DREAD rates risks on five dimensions: Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. All the identified threats were ranked quantitatively on these dimensions in order to rank the vulnerabilities according to their criticality. The threats were then ordered to find out which vulnerabilities risked vehicle safety and passengers' safety the most. Particular emphasis was placed on those vulnerabilities that target safety-critical functions, for example, braking and steering control, and on those that affect privacy, e.g., illegal access to sensitive user information that is stored within vehicle systems.

The third phase included a consideration of mitigation practices against current cybersecurity standards, including the ISO/SAE 21434 standard and regulatory body guidelines like UNECE. The performance of defense mechanisms such as intrusion detection systems (IDS), secure boot, over-the-air (OTA) update integrity, network segmentation, and blockchain-based systems for safe communications was compared. Emphasis was laid on their implementability in the limited environments characteristic of automotive systems, where computational capacity and real-time constraints are very stringent.

Case studies were also used as a verification tool. Real-world incidents, including the Jeep Cherokee remote hijack in 2015, and the vulnerabilities in Tesla's OTA discovered in the later years, were examined to cross-verify the threats discovered through modeling. Every case study gave an overview of the real-world exploitation techniques, the efficacy of the defenses employed by the victim system, and the recovery steps taken after the attack. Also, a survey of known vulnerabilities from databases like the National Vulnerability Database (NVD) was performed to map common vulnerability types to connected vehicle architectures.

An important component of the methodology was ensuring that the assessment covered not only technical vulnerabilities but also organizational and process-based risks. Supply chain security, lifecycle management, update deployment procedures, and incident response preparedness were included as critical aspects of the evaluation. Interviews and surveys from prior studies targeting automotive engineers and cybersecurity professionals were referenced to understand prevailing industry practices and challenges.

The methodological strategy was selected precisely to yield a multi-angle view of the cybersecurity threats in connected vehicles. Through the combination of formal threat modeling, structured risk ranking, real-world case studies, and standards-based assessment, an end-to-end and realistic picture of the connected vehicle cybersecurity environment has been obtained. This integrated methodology guarantees that results are not only theoretically valid but also effectively implementable in existing and prospective connected vehicle architectures.

IV. RESULTS

The use of the methodology suggested resulted in key findings regarding the cybersecurity stance of connected cars. Using threat modeling against the STRIDE framework, several vulnerabilities were revealed on different subsystems. Spoofing attacks were highly noted in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, where malicious actors could pose as authorized actors and transmit forged messages. Tampering threats mostly targeted in-vehicle networks like the Controller Area

Network (CAN) bus, which allowed malicious manipulation of key vehicle control signals. Repudiation threats were seen in systems that did not have proper logging in place, complicating tracing of malicious behavior. Information disclosure vulnerabilities were seen in telematics units, where weak encryption allowed sensitive user and vehicle information to be exposed. Denial of Service (DoS) attacks were prominent in communication modules, with the attackers being able to overwhelm resources and destroy vital functions. Lastly, privilege elevation vulnerabilities were identified in infotainment systems such that attackers could transition from low-privileged user access to vital vehicular control systems.

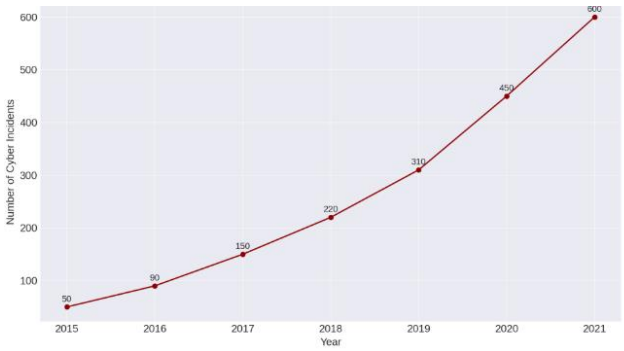

Figure 3. Year-wise increase in automotive cybersecurity incidents from 2015 to 2021.

Risk prioritization based on the DREAD model identified some vulnerabilities to have disproportionately high risks. Telematics control unit attacks, for example, were high-scoring on all DREAD factors since they have the capability to remotely manage the vehicle and invade user privacy at the same time. CAN bus attacks also counted among the high-scoring ones because there are no inherent security features like authentication or encryption in standard implementations. These results affirm previous concerns by researchers about the inherent insecurity of automotive internal networks and the necessity of retrofitting security measures into current designs.

Assessment of mitigation strategies showed a mixed environment. Intrusion detection systems (IDS) for vehicle networks showed high detection rates in controlled environments, especially those using deep learning algorithms that have been trained on normal and attack traffic patterns. Still, operational deployment difficulties were seen, particularly regarding the limited computational resources available and the vulnerability to adversarial machine learning attacks that can't be detected. Secure boot technologies were shown to be successful at safeguarding firmware integrity, yet the absence of standardized techniques amongst manufacturers meant varying quality implementation. Over-the-air (OTA) update mechanisms were highly disparate in security strength; while some used strong encryption and authentication methods, others had severe vulnerabilities, including omitted signature verification processes, thus leaving vehicles vulnerable to remote exploitation attacks.

Case study evaluations also confirmed these findings. The 2015 Jeep Cherokee remote hijacking case highlighted the severity of remote attacks launched through vulnerable entertainment systems. Despite manufacturer efforts to patch vulnerabilities, the case underscored the challenges of reaching all vehicles through OTA updates and dealer visits, leaving some vehicles perpetually vulnerable. Similarly, Tesla's experience with OTA updates revealed both strengths and weaknesses; while Tesla's agile update model allowed rapid patching of discovered vulnerabilities, the centralized model also posed single points of failure that could be exploited if backend systems were compromised.

The NVD vulnerability analysis showed a year-over-year growth trend in reported vehicle-related cybersecurity incidents. The vulnerabilities were grouped largely under unauthorized access, remote code execution, and denial of service, consistent with the predicted groupings from threat modeling. This trend

reflects increased attacker interest in the automotive space and emphasizes the importance of ongoing security vigilance.

Organizational and supply chain threats were also important. Industry surveys indicated that most manufacturers do not have end-to-end cybersecurity incident response plans. In addition, third-party vendors tended to deliver components with inadequate security hardening, which produced supply chain weaknesses that are hard to identify until after integration testing. Cybersecurity lifecycle management was also absent, with many of the vehicles not receiving updates past a limited warranty, thus creating a huge inventory of potentially vulnerable older vehicles on the road.

The findings illustrate that although significant strides have been made in the identification and reduction of cybersecurity threats in connected vehicles, gaps persist. The threat environment is fluid, with adversaries constantly refining their methods to evade conventional security measures. Good cybersecurity for connected vehicles is not only a matter of technical defense but also one of systemic redesign in philosophy, supply chain, and regulatory compliance enforcement. These findings provide a key input for ongoing discussion of how the industry and regulators need to change to keep pace with the ever-evolving cybersecurity landscape in the connected vehicle world.

V. DISCUSSION

The findings from this research are invaluable in revealing the multi-faceted aspect of cybersecurity threats to connected vehicles. One important observation is that the security environment is not fixed, but highly dynamic and constantly shifting as attackers constantly evolve new tactics and as automobiles become more and more connected and autonomous. The detailed threat modeling exercise indicated that most of the vulnerabilities are a result of architectural designs where functionality and user convenience take precedence over security, a phenomenon commonly observed historically in many technological fields. In the case of connected vehicles, though, such a trade-off has far more devastating consequences, even threatening lives, property, and privacy.

Spoofing and tampering attacks on V2V and V2I communications, for instance, indicate a core failure of trust assumptions in vehicular networks. Most communication systems depend greatly upon the assumption that incoming messages are genuine and can be trusted. But without proper authentication and encryption protocols in place, these assumptions can be readily breached. The absence of mechanisms for message validation and source authentication was uniform among several studies and attested that the automotive industry has to safeguard external communications just as stringently as internal automobile networks.

Yet another key takeaway relates to the internal networks, specifically the CAN bus, that was initially not developed with any security in place. Results proved that attackers who have physical or remote access to the network can inject malicious commands that cannot be differentiated from regular ones. In spite of the existence of newer architectures like Automotive Ethernet and secure variants of CAN, still many vehicles on the road rely on older CAN systems, thus making them vulnerable to attacks. This emphasizes the immediate necessity of retrofit measures, including lightweight encryption and anomaly-based intrusion detection systems optimised for the low-latency needs of in-vehicle networks.

Organisational vulnerabilities revealed in the findings indicate a systemic issue rather than discrete technical shortcomings. Supply chain management was found to be a leading weakness, with manufacturers incorporating third-party parts that were frequently not subject to stringent cybersecurity verification. Such weaknesses are not merely hard to catch during the assembly of vehicles but also hard to patch following deployment, as the nature of automobile supply chains is complex and distributed. This result highlights the

need for extensive cybersecurity requirements and audit procedures at all levels of the supply chain, something that ought to be legally mandated by regulation bodies and not left to optional compliance.

Connected car lifecycle management also needs to be greatly enhanced. As the study indicated, most cars stop receiving software and security updates a few years after they are manufactured, even though they have anticipated ten-year or longer operational lifecycles. This gap presents a long-tail risk, with older cars being enticing targets for attackers because they contain outdated and vulnerable software stacks. Automakers will need to revisit their business models to incorporate prolonged cybersecurity support, either in the form of required security update guarantees or collaborations with third-party cybersecurity vendors.

No discussion would be complete without considering the promising, albeit still nascent, mitigation technologies found in the study. While blockchain-based communication solutions have the potential to offer decentralized trust and data integrity, their incorporation into vehicular networks is bogged down by excessive latency, computational burden, and interoperability issues. Likewise, although machine learning-based intrusion detection systems have shown robust detection in the lab, real-world deployment is still limited because of problems like adversarial machine learning vulnerabilities and insufficient labeled data for training robust models.

From a regulation standpoint, the introduction of standards like ISO/SAE 21434 is a step in the right direction, providing a framework approach to vehicle cybersecurity engineering across the lifecycle. Yet, compliance with standards is still patchy across the industry. Unless backed by tough enforcement provisions and penalties for non-compliance, these standards may turn out to be checklists and not result in meaningful changes in design and operational practices.

Findings also indicate that consumer awareness makes an undervalued contribution toward strengthening cybersecurity. A majority of vehicle owners themselves are not fully aware of the cybersecurity threats contained in connected car systems. They are thus guided by habits leading to increased exposure, including forgetting to install OTA updates or letting vehicles connect to unsecured public Wi-Fi hotspots. Industry stakeholders and regulators should fund consumer awareness programs that teach users about proper cybersecurity hygiene just like public awareness campaigns run years ago for the use of seatbelts and the prevention of drunk driving.

Finally, the above emphasizes that making a vehicle secure needs a comprehensive multi-layered method addressing not merely technical weaknesses but organizational processes as well, as well as rules and regulations, and user culture. The auto industry is at a crossroads where early investment in cyber security will decide whether connected cars live up to the promise of safer, more efficient travel or become the vectors for novel kinds of catastrophic failures. Future studies must remain vigilant in tracking upcoming threats, particularly those that next-generation technologies like 5G, artificial intelligence integration, and autonomous navigation systems bring into the connected vehicle environment, and that the connected vehicle ecosystem continues to be secure and resilient to new cyber threats.

VI. CONCLUSION

The cybersecurity threats confronting connected cars constitute a grave, multi-faceted challenge to which researchers, manufacturers, regulators, and consumers must attend, urgently and insistently. Drawing on systematic threat modeling, analysis of risk, and assessment of available mitigation mechanisms, this paper has shown that connected cars comprise a wide, dynamic attack surface. In contrast to conventional IT infrastructures, the stakes in cyber security for connected vehicles are remarkably high since effective

attacks can not only result in data breaches but also physical injuries, including even loss of life. As the automobile industry moves toward greater reliance on software, wireless communication, and autonomous decision-making systems, the necessity for strong and complete cybersecurity solutions has never been greater.

The most important findings of this study are that vulnerabilities both at the technical and organizational levels exist. Communication channels V2V and V2I are especially open to spoofing and tampering attacks because of poor authentication measures. Internal networks like the CAN bus, still found in most current vehicles, have no basic security measures and can easily be attacked once physical or remote access is gained. Further, the incorporation of many third-party elements heightens the security issues since vulnerabilities in any one supplier's hardware or software can endanger the whole system.

The review also revealed the vulnerabilities in supply chain security and lifecycle management. Cars generally spend over a decade on the road, but security fixes and support are hardly ever offered throughout that whole time. The subsequent long-tail of exposed vehicles on the road is a lingering and increasing cybersecurity threat. In addition, the few security audits of supplier products prior to embedding in vehicles pose latent threats that tend to only manifest after attacks have already been launched.

Although mitigation methods like intrusion detection systems, secure boot procedures, and OTA update have promised results, their efficacy is greatly determined by frequent and strict application in all manufacturers and models. Developing solutions like blockchain authentication and AI-driven anomaly detection are promising but have practical issues concerning computation overhead, real-time processing limitations, and vulnerabilities to adversarial manipulation.

Regulatory progress, including the development of standards like ISO/SAE 21434 and UNECE WP.29 regulations, represents a significant advancement. However, the enforcement of these standards remains uneven. Without binding regulatory frameworks and the imposition of penalties for non-compliance, adherence risks becoming superficial. Governments must play a proactive role, not only by mandating cybersecurity best practices but also by facilitating information sharing between manufacturers, cybersecurity firms, and researchers to foster a collaborative defense ecosystem.

Significantly, cybersecurity has to be baked into the very core of car design, and not as an afterthought. Security-by-design approaches, threat modeling at initial stages of development, regular security testing, and a secure software development lifecycle are all needed in order to construct secure-by-design connected vehicles. Furthermore, consumer awareness campaigns play a crucial role in ensuring users know fundamental cybersecurity hygiene practices like applying updates as soon as possible and not connecting to insecure networks.

Looking ahead, as cars integrate increasingly sophisticated technologies such as complete autonomy, AI-based decision-making, and 5G-based communication, cybersecurity threats will only increase. Attack surfaces will grow, and the potential impacts of successful cyberattacks will escalate further. Subsequent research needs to thus target the creation of lightweight, scalable, and responsive security solutions that can function in the resource-scarce settings characteristic of automotive systems. Parallel to this, there should be increased focus on interdisciplinary research, bringing in ideas from areas like critical infrastructure security, embedded system design, and behavioral psychology to help deal with the human aspects of vehicle cybersecurity.

Overall, the journey to secure connected vehicles is trying but inevitable. It involves a collective effort cutting across technical innovation, regulatory compliance, industry best practices, and consumer

education. Only with such a multi-pronged and proactive approach can the potential of connected vehicles be achieved securely, paving the way for a new generation of smart, efficient, and secure transportation.

VII. REFERENCES

[1] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, Apr. 2015.
[2] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN '05)*, pp. 11–21, 2005.
[3] R. Lu, X. Lin, H. Zhu and X. Shen, "SPARK: A New VANET-Based Smart Parking Scheme for Large Parking Lots," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 3, pp. 1175–1189, Mar. 2010.
[4] M. Kang, J. Park and H. Kim, "Intrusion detection system using deep neural network for in-vehicle network security," *PLOS ONE*, vol. 11, no. 6, pp. 1–15, Jun. 2016.
[5] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," *Black Hat USA*, 2015.
[6] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, Dec. 2017.
[7] S. Woo, H. J. Kim, and H. K. Kim, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.
[8] ISO/SAE 21434, *Road vehicles — Cybersecurity engineering*, International Organization for Standardization (ISO), Standard, Aug. 2021.
[9] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," *Proceedings of USENIX Security Symposium*, pp. 77–92, 2011.
[10] Y. Kurachi, K. Kubo, T. Fujii, "Cybersecurity for 5G-V2X: Attack surfaces and mitigation techniques," *Proceedings of 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pp. 1–6, 2021.