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

Secure Mobile Platforms for Connected Vehicle Ecosystems: A Synthesis of Threats, Detection, and Governance

Ruturajsinh Kiritsinh Jadeja

Submitted: 05/08/2024 **Revised**: 18/09/2024 **Accepted**: 29/09/2024

Abstract—The modern car is not just a vehicle with an internal Controller Area Network (CAN) bus, but can have a proliferation of smartphone-based vehicle keys, Bluetooth-paired infotainment units, cellular telematics control units, and over-the-air (OTA) update channels, and that has expanded the attack surface. This paper reviews and consolidates the results of 27 peer reviewed publications from the literature on mobile connectivity and its impact on automotive cybersecurity risks and the literature's response in terms of detection, authentication, and governance mechanisms, through to 2023. The CAN bus proved to be a safety-critical asset with no built-in authentication capabilities through early experiments that showed an attacker could stop the vehicle when they could access a single electronic control unit (ECU). Later studies on Bluetooth infotainment pairing have found that phonebook and message information can be recovered from paired devices, and near-field-communication (NFC) key schemes using a smartphone can be suggested as replacements for mechanical and radio-frequency (RF) immobilizers. On the defense side, in this paper, we find that a machine-learning and deep-learning based intrusion detection system (IDS) achieves up to 99.995 percent accuracy when detecting CAN traffic and 99.88-99.99 percent accuracy with intra-vehicle and external network datasets, although the values are dataset dependent and do not necessarily align between studies. The paper also draws parallels between the complementary layers of a secure mobile platform that are the paper's topics, namely blockchain-based credential management, provably secure authentication protocols, Bayesian game-theoretic defense allocation, and the ISO/SAE 21434 risk-engineering standard. To organize these mechanisms, a five-layer reference architecture is proposed, and comparison of the various detection, cryptographic, and governance approaches shows that, despite these advances, there are still challenges with cross-dataset validation, the real-time computational viability of embedded devices, and the harmonization of regulations for OTA software updates. The authors conclude that only a layered approach of combined anomaly detection, paired mutual authentication, and standards-based risk management can provide sufficient security for connected vehicles, as attackers are increasingly coming from paired mobile devices instead of the vehicle itself.

Keywords*—connected vehicles; automotive cybersecurity; Controller Area Network; intrusion detection system; Bluetooth infotainment; over-the-air updates; vehicular ad hoc network; blockchain authentication; ISO/SAE 21434; telematics; mobile vehicle key; risk assessment*

I. INTRODUCTION

Today's cars are mechanically independent systems that are now integrated as computing systems with dozens of electronic control units (ECUs) that communicate with each other over an internal Controller Area Network (CAN) bus as well as with the outside world via Bluetooth, cell phones and the Internet and cloud-based mobile applications [1, 2]. As stated throughout the literature surveyed a defining cybersecurity challenge for the connected-vehicle era is this dual connectivity – both internal and external – with traffic that can be reached indirectly via a paired smartphone, telematics dongle or over-the-air (OTA) software update channel [7], [8]. The basic demonstration of this risk was given by Koscher et al. [14] who were able to demonstrate experimentally that a single invader could compromise the safety-critical functions while performing arbitrary actions on the individual wheel brakes and the engine and disregarding the instructions of the driver. They also found that a corrupted packet could be able to jam a brake even after a power off, which will not be possible when using manual override. By design, this early work found the CAN bus does not offer any authentication for message sources and thus any device with electrical access to the bus (including those accessed via a

Employer: Leela Consultancy LLC

Consult.RuturajJadeja@gmail.com

compromised mobile interface) can insert arbitrary control frames [14, 27]. The paper summarizes the 27 references focusing on intrusion detection, cryptographic key management, authentication using blockchain, vehicular ad hoc network (VANET) architecture and cybersecurity governance to describe secure mobile platforms for connected-vehicle ecosystems.

II. Mobile-Linked Attack Surface Of Connected Vehicles

The smartphone-based digital key, the Bluetooth-compatible infotainment head unit, the cellular telematics control unit and the OTA update channel are the most frequently mentioned mobile interfaces in the reviewed literature that represent main entry points into the vehicle. The results of the quantitative detection are summarized in Fig. 1 and the mobile-linked topology discussed below is summarized in Fig. 2, a separate topology diagram being presented as Fig. 3 in Section III for sequentialness of the figures and tables. In an argument similar to the one offered by Busold et al. [5] for the replacement of the mechanical and RF-based key with an application for a near-field-communication (NFC) enabled smart phone, they propose that a cryptographically secured mobile credential can decrease the relay and cloning attacks that exist in traditional remote keyless-entry systems, while also providing additional convenience features like temporary key sharing. The authors note that the security of the mobile operating system and secure element restrains the security of the vehicle itself—the mobility aspect of the scheme's key strength and its key weakness. Renganathan et al. [20] conducted a systematic security evaluation of the Bluetooth network that was exposed by an automotive infotainment unit, concentrating on the pairing process that is employed to synchronize a personal device with the head unit. When paired together, the Phonebook Access Profile (PBAP) and related object-exchange profiles enable the infotainment system to download and store a driver's contact list and messages, leaving a persistent privacy exposure that persists long after the pairing session is completed, the authors write, which they dub a valet attack because a temporary or unauthorised driver of the car can access the previously synced personal data. They standardise the level of severity of such exposures using a standard rating measurement, and suggest countermeasures that could be implemented, such as tighter profile access control and regular credential expiration.

Table I. Mobile-Linked Attack Surface of Connected Vehicles, Synthesized from References Through 2023

Interface	Principal Risk	Source(s)	Representative Countermeasure
Smartphone / NFC digital key	Relay attack, key cloning, secure-element compromise	Busold et al. [5]	Cryptographic mutual authentication; time-bounded ranging
Bluetooth infotainment pairing	Persistent access to synced phonebook / message data (“valet attack”)	Renganathan et al. [20]	Profile-level access control; credential expiry; severity rating
Cellular telematics unit	Data exfiltration; potential pivot toward CAN gateway	Gao et al. [9]; Joy & Gerla [13]	Network segmentation; encrypted telemetry channels
Over-the-air (OTA) update channel	Malicious or unauthenticated firmware installation, fleet-wide	Mahmood et al. [17]	Signed packages; rollback protection; secure boot

Another outward-facing interface is telematics units for the cellular uplink for remote diagnostics, insurance telematics, and emergency calling. Gao, Meng, and Wüthrich [9] examined the use of telematics-based driving data, traditionally gathered for usage-based insurance, as it is transmitted via mobile-attached equipment and cloud-based pipelines that could be breached, potentially releasing driving-behavior information and, given the level of integration, routes into vehicle systems. Also, Joy and Gerla [13] list some privacy and security concerns that are unique to Internet of Vehicles (IoV) and how the combination of vehicular ad hoc networks and cloud and mobile infrastructure complexify the attacker's

probe of trust boundaries. In particular, Mahmood, Nguyen and Shaikh [17] have studied an OTA update channel in isolation, performing a systematic threat analysis of the automotive OTA mechanisms and believe that a compromised update server or an unauthenticated update package could, in principle, install malicious firmware across the fleet as update pipelines have high privileges to update ECU firmware. Their security-testing strategy focuses on the security minimum of verifying the signing of the update-package, rollback protection and secure boot chaining.

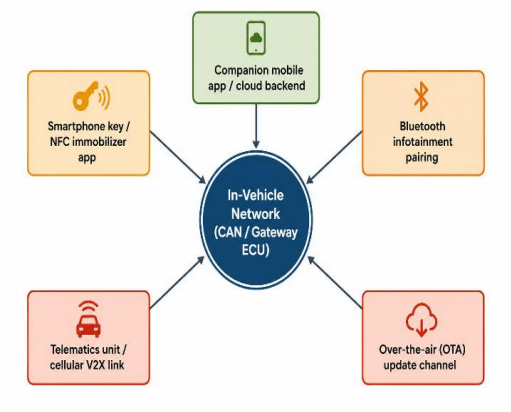

Fig. 1. Mobile-linked interfaces feeding into the in-vehicle Controller Area Network, synthesised from references [5], [9], [13], [17], and [20].

III. Intrusion Detection And Prevention For In-Vehicle Networks

Opportunities for intrusion detection and prevention solutions in the in-vehicle network. As the CAN bus does not have authentication built in, the most common defence approach reported in the surveyed literature is to watch the bus and look for suspicious activity. Among the sources examined, Al-Jarrah et al. [1] offer the most formal taxonomy of such IDSs, which can be broken down into flow-based, payload-based, or hybrid approaches. This taxonomy is reproduced here schematically in Fig. 2. A one-class support vector machine (OCSVM) was applied to real traffic from a Ford Explorer in the flow-based category, with results ranging from Al-Jarrah et al. [1] 0.8720 to 1.0000 depending on the message insertion and deletion rates, showing that the detection rate of this class of methods is not a single value but varies with the composition of the dataset and the intensity of the attack. Later deep-learning methods report significantly higher point-accuracy results on the respective evaluation set. Hossain et al. [12] trained a classifier using LSTM architecture with an optimized Nadam (Nadam Optimizer) and sigmoid activation function on an experimental vehicle with injection of denial-of-service, fuzzing, and spoofing attacks from CAN traffic and reported an overall detection accuracy of 99.995 percent and greater detection rates when compared with a baseline of classifiers created using the survival-analysis method. When testing on the previously unseen, zero-day-style attacks, the proposed multi-tiered hybrid system, MTH-IDS, recorded F1-scores of 0.963 and 0.800 on the CAN-intrusion dataset and the CICIDS2017 dataset of external network traffic respectively, which is a significant drop from the near-perfect accuracy results on the known-attack data sets, highlighting the difficulty of the open problem of generalization to novel attacks. To capture the local features and learn the most important time steps in a message window, the authors of [22] proposed a complementary design that uses one-dimensional convolution to extract the local features, and a bidirectional LSTM and an attention mechanism (CLAM) to determine the most relevant time steps for an anomaly.

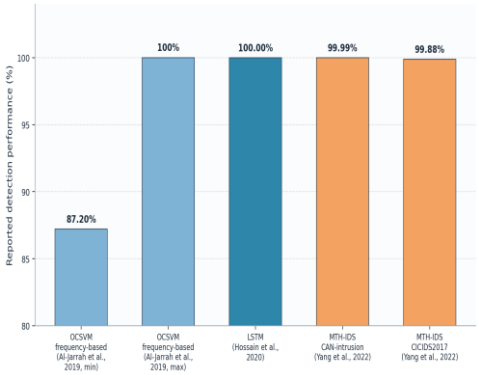

Fig. 2. Reported detection performance of intrusion detection approaches surveyed in Section III, drawn from [1], [12], and [26]. Values are not a controlled cross-study benchmark.

To illustrate the point in a comparative way, the point-accuracy results reported by [1, 12, 26] have been plotted on a common axis in Fig. 3; the three studies differ in the type of vehicle, the type of dataset, and the attack injection protocol and so should not be regarded as a controlled benchmark. This is explicitly formulated by Bozdal et al. [4], who propose the wavelet-based IDS, WINDS, which identifies behavioural change points in CAN transmission patterns, since the thresholding-based IDS methods in both time and frequency domains frequently have high false alarm rates and are tuned to a particular vehicle. To test this cross-vehicle generalisation concern, the real traffic data gathered at two research centres were evaluated for WINDS. Signal-domain and physical-layer options are alternatives to just data-driven CAN

payload analysis. Xun, Zhao and Liu [25] developed an external intrusion detection system that tracks the voltage signals on the bus instead of the content of the messages sent, since an attacking device installed electrically on the bus would alter the voltage signals that a software-based monitor would not be able to detect. The deployment constraint mentioned throughout this literature is that the deep learning models are often accurate but require high computational resources in comparison to the processing resources of a gateway ECU. Bloom [3] introduced an adaptive cumulative sum (CUSUM) algorithm with low computational requirements for the resource-constrained ECU. De Araujo-Filho et al. [6] took this a step further and proposed a low-cost intrusion prevention system (IPS) that would make it more difficult for cyber-attacks to occur in real time as opposed to identifying them only as a post-facto occurrence; this is an important distinction because detection is not enough to prevent an in-progress brake- or engine-control attack like the one demonstrated by Koscher et al. [14]. An earlier structured survey of this design space was given by Young et al [27] who pointed out the trade-off between detection latency and false-positive rate that occurs repeatedly.

A widely used evaluation quantity across this literature is the true positive rate (recall), computed as

$$TPR = TP — (TP + FN) \quad (1)$$

where TP denotes correctly flagged attack frames and FN denotes attack frames the classifier misses; the accuracy and F1 figures reported by [12] and [26] and summarized in Fig. 3 are derived from statistics of this form computed on each study's own held-out test partition.

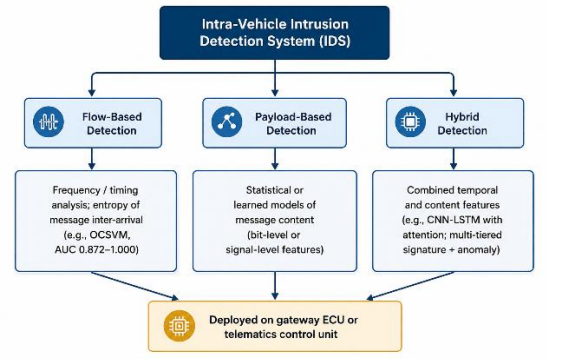

Fig. 3. Taxonomy of intra-vehicle intrusion detection system designs, adapted from the flow-based / payload-based / hybrid classification of Al-Jarrah et al. [1].

Table II. Intrusion Detection Approaches for In-Vehicle Networks Synthesized from the Reviewed Literature

Method	Source	Evaluation Data	Reported Outcome
OCSVM (frequency-based, flow)	Al-Jarrah et al. [1]	Ford Explorer field data	AUC 0.8720–1.0000
LSTM (Vanilla, sigmoid/Nadam)	Hossain et al. [12]	Experimental vehicle, injected DoS/fuzz/spoof	99.995% accuracy
MTH-IDS (signature + anomaly, hybrid)	Yang et al. [26]	CAN-intrusion dataset	99.99% accuracy
MTH-IDS (external network tier)	Yang et al. [26]	CICIDS2017	99.88% accuracy; F1 0.963/0.800 (zero-day)
CNN-Bi-LSTM with attention (CLAM)	Sun et al. [22]	In-vehicle signal data	Qualitative: attention-weighted temporal features
Wavelet-based (WINDS)	Bozdal et al. [4]	Two independent vehicle fleets	Qualitative: cross-vehicle generalization emphasis
Voltage-signal external IDS (VehicleEIDS)	Xun et al. [25]	Physical-layer voltage traces	Qualitative: hardware-level anomaly cues

IV. Authentication, Key Management, and Distributed-Ledger Approaches

Even though a mobile device or external network peer has been detected, there are noways for it to establish an initial connection to the vehicle; a second stream of the surveyed literature deals with how a mobile device or external network peer can prove its

legitimacy to the vehicle before any data exchange, communication or interaction. Nurkifli and Hwang [18] design a provably secure Internet of Vehicles (IoV) authentication protocol by analysing the resistances to impersonation and replay attacks, to enable the mobile client (e.g. a mobile phone key or a fleet-management system) to start a session key with the vehicle without entering the long-term credentials in the wireless channel.

Another blockchain proposal that secures connected and autonomous vehicles (CAVs) is by Rathee et al. [19] who suggest that a distributed ledger could offer tamper-evident logging of credential issuance and revocation events on the network, eliminating the single point of failure that a centralized key-management server would incur in a fleet of CAVs. Since implementing the consensus requires latency and computational resources, the authors place the mechanism for credential governance and audit on the CAN bus itself, which is consistent with the layered architecture recommended in Section VI, where we propose to place the mechanism for real-time message authentication.

Table III. Authentication and Credential-Management Mechanisms Synthesized from the Reviewed Literature

Mechanism	Source	Threat Addressed	Core Principle
Provably secure IoV authentication	Nurkifli & Hwang [18]	Impersonation/replay resistance	Formal cryptographic proof
NFC smartphone digital key	Busold et al. [5]	Key cloning/relay	Mobile secure-element root of trust
Blockchain credential ledger	Rathee et al. [19]	Centralised key-server compromise	Distributed tamper-evident logging
Bayesian Stackelberg defense allocation	Halabi et al. [11]	Advanced persistent threats (APT)	Game-theoretic resource commitment
VANET architecture / QoS survey	Al-Sultan et al. [2]	V2V / V2I routing exposure	Foundational protocol survey

V. Standards, Risk Assessment, and Policy Frameworks

The technical mechanisms, in the literature surveyed, are always described as essential but not enough if they are not coupled with the engineering process and, of course, regulatory structure. Weimerskirch and Wolf [24] present a review of the ISO/SAE 21434 standard for automotive cybersecurity engineering that normalizes the threat analysis and risk assessment (TARA) as a mandatory task in the development lifecycle of a vehicle programme, and makes cybersecurity engineering into a co-equal discipline with functional safety. Luo et al. [16] discuss TARA (threat analysis and risk assessment) techniques more generally, categorizing the qualitative and semi-quantitative scoring schemes (also called threat trees or severity-likelihood matrices) that TARA processes often use, and Sommer, Kriesten and Kargl [21] survey complementary model-based security testing approaches that convert such a risk assessment into concrete test cases that are exercised against a vehicle's mobile and network interfaces before it's released to the public. As noted in Section II, ECU firmware is typically safety-critical and, in the case of firmware accessed via OTA, it is highly desirable to use formal verification techniques that go beyond testing by verifying that a certain class of faults are not present. Liu et al. [15] survey formal verification methods and tools for automotive software and argue that the safety-critical nature of ECU firmware, especially firmware accessed through the OTA channel discussed in Section II, makes formal verification desirable beyond simple testing, since it can prove that a class of faults is not present in the firmware. At a more abstract level, Van der Heijden and Haber [23] provide insight into the policy and regulatory landscape for CPVs, positing that while the rollout of connected vehicles is accelerating, regulatory harmonisation across jurisdictions is following at a slower pace, especially in terms of cross-border OTA update approval and liability assignments when an occurrence is caused by a software update rather than a physical fault.

Table IV. Standards, Risk Assessment, and Policy Frameworks Synthesised from the Reviewed Literature

Framework	Source	Primary Function
ISO/SAE 21434 cybersecurity engineering	Weimerskirch & Wolf [24]	Lifecycle threat analysis and risk assessment (TARA)
Threat analysis and risk assessment survey	Luo et al. [16]	Attack-tree / severity-likelihood scoring
Model-based security testing	Sommer et al. [21]	Test-case generation from risk models
Formal verification of automotive software	Liu et al. [15]	Proof-based defect elimination in firmware
Policy and regulation for cyber-physical vehicles	van der Heijden & Haber [23]	Cross-jurisdiction OTA and liability harmonisation

VI. Toward a Layered Secure Mobile Platform Architecture

The mechanisms developed in Sections II- V don't compete, they occupy different layers of a defence-in-depth architecture. They are grouped into five layers in Fig. 4, starting from the mobile and external interfaces described in Section II at the bottom, followed by network segmentation and intrusion detection, and then cryptographic access control, and finally, at the top, the governance layer defined by ISO/SAE 21434 and the policy literature of Section V. In the reviewed sources, there is a recurring trend that authentication and detection mechanisms are presented and evaluated as engineering controls, whereas standards, like [24] and surveys like [16] and [21] are presented as the process of an organisation choosing, testing, and maintaining the appropriate mix of these controls for a specific vehicle program. These findings align with those of [1], [14] and [27] that the initial and most harmful attacks targeted the lack of separation between the safety-critical and infotainment facing bus segments; Koscher et al. [14] claimed that their test vehicle's primitive separation was overcome by bridging between the subnetworks. IDS is placed above segmentation and not as a replacement for it, because, as also stated by Bloom [3] and De Araujo-Filho et al. [6] some traffic sent by an attacking host will make it to the bus, so detection and prevention systems must rely on this traffic and therefore must be able to detect it in real time.

Fig. 4. Proposed five-layer reference architecture for secure mobile connected-vehicle platforms, synthesising mechanisms from Sections II through V.

VII. Comparative Discussion and Open Challenges

The first observation is comparative, relating to the two. Note that the detection performance numbers are not directly comparable across studies: the 99.995 percent accuracy from [12] is based on a different vehicle, attack-injection protocol, and data set than the 99.99/99.88 percent accuracy reported by [26] and the range of AUCs reported in [1] of 0.8720–1.0000 indicate that high point-accuracy can be obtained under favorable conditions, but should not be interpreted as a leaderboard. Second, literature consistently reports a known-attack detection to zero-day generalisation gap, with the best quantitative evidence for this gap found in [26], which found that the ability to perform and detect novel-attack generalisation was materially more difficult, with F1-scores of 0.963 and 0.800 for the unseen attacks. Third, in the literature on the IDS, the accuracy of lightweight statistical methods, e.g. the CUSUM approach of Bloom [3] is explicitly motivated by ECU resource constraints, whereas the accuracy of deep-learning methods, e.g. [12], [22] and [26] is reported without uniformly reporting inference latency

or memory footprint on representative gateway hardware, leaving real-time deployability an open empirical question across much of this body of work. Fourth, cryptographic and governance mechanisms deal with different failure modes than detection does: authentication protocols like [5] and [18] seek to prevent an unauthorised mobile device from forming a session with the bus in the first place, while blockchain credentialing like [19] focuses on maintaining integrity in the bus's session(s) after the fact. This complementary, not competing, relationship is summarized in Table V in the context of the four mechanism families discussed in the paper.

Table V. Comparative Roles of the Four Mechanism Families Synthesised in This Paper

Mechanism Family	Primary Objective	Comparative Strength / Limitation	Representative Sources
Anomaly / intrusion detection	Detect malicious traffic already on the bus	High point-accuracy achievable; weaker on zero-day attacks; latency/footprint under-reported	[1], [3], [4], [6], [12], [22], [25], [26], [27]
Authentication / key management	Prevent unauthorized session establishment	Strong formal guarantees; dependent on mobile-device secure-element integrity	[5], [18]
Distributed-ledger credentialing	Tamper-evident governance of credentials at fleet scale	Removes single point of failure; adds consensus latency, unsuited to real-time bus messages	[19]
Standards / risk governance	Organizational process for selecting and validating controls	Provides lifecycle assurance; harmonization across jurisdictions incomplete	[15], [16], [21], [23], [24]

VIII. CONCLUSION

The goal of this paper was to capture the essence of research on secure mobile platforms for connected-vehicle ecosystems, ranging from the initial discovery that a single compromised ECU could turn off the brakes and engines of all vehicles in a vehicle-to-infrastructure communication scenario [14] to today's attack surfaces enabled by Bluetooth, telematics, and OTA, and the measures put in place to detect, authenticate, and govern them. The survey of the detection literature highlights the ability of machine-learning and deep-learning IDS to obtain a high point-accuracy on individual evaluation datasets, with reported results of 99.995 percent [12] and 99.99/99.88 percent for intra- and inter-vehicle traffic, respectively, and shows that generalization to unseen attacks and feasibility on embedded devices are comparatively under-explored. Various authentication protocols [5] and [18] as well as distributed-ledger credentialing [19] and ISO/SAE 21434 risk-engineering standard [24], were demonstrated to solve complementary failure modes, which inspired the five-layer reference architecture presented in Section VI. The policy and standards literature examined in this synthesis suggests that future research should focus on three key areas relating to cross-dataset IDS benchmarking, embedded-hardware latency reporting, and harmonised cross-jurisdiction governance of the OTA update channel identified throughout this synthesis as the mobile-linked interface of greatest structural concern.

REFERENCES

[1] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, “Intrusion detection systems for intra-vehicle networks: A review,” IEEE Access, vol. 7, pp. 21266–21289, 2019.

[2] S. AL-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular ad hoc network,” J. Netw. Comput. Appl., vol. 37, pp. 380–392, 2014.

[3] G. Bloom, “Anomaly detection approach using adaptive cumulative sum algorithm for controller area network,” in Proc. ACM Workshop

Automotive Cybersecurity (AutoSec), 2019, pp. 25–30.

[4] M. Bozdal, M. Samie, and I. K. Jennions, "WINDS: A wavelet-based intrusion detection system for controller area network (CAN)," IEEE Access, vol. 9, pp. 58621–58633, 2021.

[5] C. Busold, A. Taha, C. Wachsmann, A. Dmitrienko, H. Seudié, M. Sobhani, and A.-R. Sadeghi, "Smart keys for cyber-cars: Secure smartphone-based NFC-enabled car immobilizer," in Proc. 3rd ACM Conf. Data Appl. Security Privacy, 2013, pp. 233–242.

[6] P. F. De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, "An efficient intrusion prevention system for CAN: Hindering cyber-attacks with a low-cost platform," IEEE Access, vol. 9, pp. 166855–166869, 2021.

[7] A. A. Elkhail, R. U. D. Refat, R. Habre, A. Hafeez, A. Bacha, and H. Malik, "Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses," IEEE Access, vol. 9, pp. 162401–162437, 2021.

[8] C. Gao, G. Wang, W. Shi, Z. Wang, and Y. Chen, "Autonomous driving security: State of the art and challenges," IEEE Internet Things J., vol. 9, no. 9, pp. 7572–7595, 2022.

[9] G. Gao, S. Meng, and M. V. Wüthrich, "What can we learn from telematics car driving data: A survey," Insurance: Mathematics and Economics, vol. 104, pp. 185–199, 2022.

[10] S. Gupta, C. Maple, and R. Passerone, "An investigation of cyber-attacks and security mechanisms for connected and autonomous vehicles," IEEE Access, vol. 11, pp. 90641–90669, 2023.

[11] T. Halabi, O. A. Wahab, R. Al Mallah, and M. Zulkernine, "Protecting the Internet of vehicles against advanced persistent threats: A Bayesian Stackelberg game," IEEE Trans. Rel., vol. 70, no. 3, pp. 1–16, 2021.

[12] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "LSTM-based intrusion detection system for in-vehicle CAN bus communications," IEEE Access, vol. 8, pp. 185489–185502, 2020.

[13] J. Joy and M. Gerla, "Internet of vehicles and autonomous connected car privacy and security issues," in Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN), 2017, pp. 1–9.

[14] K. Koscher et al., "Experimental security analysis of a modern automobile," in Proc. IEEE Symp. Security Privacy, 2010, pp. 447–462.

[15] C. Liu, C. Gu, and M. Guizani, "Formal verification for automotive software: A survey on methods and tools," ACM Comput. Surv., vol. 54, no. 8, pp. 1–30, 2022.

[16] F. Luo, Y. Jiang, Z. Zhang, Y. Ren, and S. Hou, "Threat analysis and risk assessment for connected vehicles: A survey," Security Commun. Netw., vol. 2021, Art. 1263820, 2021.

[17] S. Mahmood, H. N. Nguyen, and S. A. Shaikh, "Systematic threat assessment and security testing of automotive over-the-air (OTA) updates," Veh. Commun., vol. 35, Art. 100468, 2022.

[18] E. H. Nurkifli and T. Hwang, "Provably secure authentication for the Internet of vehicles," J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 8, Art. 101721, 2023.

[19] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," Sensors, vol. 19, no. 14, Art. 3165, 2019.

[20] V. Renganathan, E. Yurtsever, Q. Ahmed, and A. Yener, "Valet attack on privacy: A cybersecurity threat in automotive Bluetooth infotainment systems," Cybersecurity, vol. 5, no. 1, Art. 30, 2022.

[21] F. Sommer, R. Kriesten, and F. Kargl, "Survey of model-based security testing approaches in the automotive domain," IEEE Access, vol. 11, pp. 55474–55514, 2023.

[22] H. Sun, M. Chen, J. Weng, Z. Liu, and G. Geng, "Anomaly detection for in-vehicle network using CNN-LSTM with attention mechanism," IEEE Trans. Veh. Technol., vol. 70, no. 10, pp. 10880–10893, 2021.

[23] R. W. van der Heijden and E. Haber, "Policy and regulation for cyber-physical vehicle systems: State of the art and future directions," Transp. Res. Part A, vol. 136, pp. 252–266, 2020.

[24] A. Weimerskirch and M. Wolf, "Automotive cybersecurity: Review and outlook on ISO/SAE 21434," SAE Int. J. Transp. Cybersecurity Privacy, vol. 4, no. 2, pp. 75–83, 2021.

[25] Y. Xun, Y. Zhao, and J. Liu, "VehicleEIDS: A novel external intrusion detection system based on

vehicle voltage signals," IEEE Internet Things J., vol. 9, no. 3, pp. 2124–2133, 2021.

[26] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles," IEEE Internet Things J., vol. 9, no. 1, pp. 616–632, 2022.

[27] C. Young, J. Zambreno, H. Olufowobi, and G. Bloom, "Survey of automotive controller area network intrusion detection systems," IEEE Design Test, vol. 36, no. 6, pp. 48–55, 2019.