Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Cybersecurity in Autonomous and Connected Vehicles: A Systems-Level Threat Analysis and Resilience Framework

Gopi Krishna Kommineni
Independent Researcher, USA
Corresponding Author: Gopi Krishna Kommineni, **E-mail**: gkrishnakommineni@gmail.com

| ABSTRACT

The rapid evolution of autonomous and connected vehicles has ushered in transformative changes in mobility, enabling real-time data exchange, cooperative driving, and over-the-air feature enhancements. However, this connectivity also exposes vehicles to a vast and complex cyber threat landscape. This article examines the cybersecurity risks inherent in autonomous and connected vehicles, including attacks on vehicle-to-everything communications, electronic control units, sensor spoofing, and remote code execution. It proposes a layered cybersecurity resilience framework based on threat modeling, intrusion detection, and cryptographic security protocols tailored for automotive architectures. The article also addresses implementation challenges related to legacy systems, resource constraints, supply chain complexity, and regulatory fragmentation. The framework offers adaptive, standards-aligned methodologies for threat prevention, detection, and mitigation in next-generation intelligent transport systems, contributing practical defense strategies for securing autonomous vehicle platforms against evolving threats.

| KEYWORDS

Automotive cybersecurity, autonomous vehicles, threat modeling, intrusion detection, cryptographic protocols

| ARTICLE INFORMATION

ACCEPTED: 22 May 2025 **PUBLISHED:** 09 June 2025 **DOI:** 10.32996/jcsts.2025.7.5.106

1. Introduction

The automotive industry is undergoing a fundamental transformation with the advent of autonomous and connected vehicles (ACVs). These next-generation vehicles offer unprecedented features including real-time data exchange, cooperative driving capabilities, and over-the-air updates that continuously enhance functionality. According to research, the global connected car market size is expected to grow by USD 187.60 billion from 2021 to 2026, accelerating at a CAGR of 36.5% during the forecast period [1]. This remarkable growth reflects the increasing consumer demand for vehicles that integrate seamlessly with modern digital ecosystems.

However, this increasing connectivity introduces significant cybersecurity challenges. As vehicles become more networked, they simultaneously become more vulnerable to a diverse range of cyber threats that could compromise vehicle operations, user privacy, and public safety. Research identified automotive systems as increasingly attractive targets for cybercriminals, with supply chain attacks showing a 650% increase since 2021 [2]. Such attacks can potentially impact connected vehicle infrastructure through compromised software components, making automotive security a critical concern.

The integration of complex software systems, multiple communication channels, and autonomous decision-making capabilities creates a vast attack surface that requires comprehensive security measures. Research threat landscape report indicates that transportation ranks among the top sectors affected by ransomware attacks, with attackers exploiting vulnerabilities in connected infrastructure to execute malicious code [2]. The economic impact of these attacks extends beyond direct financial losses to include reputational damage and regulatory penalties.

This article examines the cybersecurity landscape for ACVs, analyzes specific vulnerabilities across vehicle systems, and proposes a robust framework for securing these platforms against evolving cyber threats. Research states that North America will contribute to 38% of market growth [1], addressing these security challenges becomes paramount for sustainable industry advancement and consumer confidence in this rapidly evolving technological ecosystem.

2. The Emerging Cyber Threat Landscape

Modern autonomous and connected vehicles face a multifaceted threat landscape that spans multiple domains. Attack vectors can be broadly categorized as physical (direct access to the vehicle), remote (exploiting wireless interfaces), and in-vehicle (compromising internal networks). Recent research from Simulation Modelling Practice and Theory reveals that connected vehicles equipped with V2X communication systems face at least 8 distinct attack surfaces, with the Controller Area Network (CAN) remaining the most vulnerable component, accounting for 37% of all documented exploits [3]. The study further demonstrates that while encryption can mitigate many attacks, it increases processing overhead by approximately 15% on standard automotive ECUs, creating potential trade-offs between security and performance.

Several high-profile incidents have demonstrated the reality of these threats. The 2015 Jeep Cherokee hack by researchers Charlie Miller and Chris Valasek revealed how attackers could remotely control critical vehicle functions including steering and braking by exploiting vulnerabilities in the entertainment system. This incident led to the recall of 1.4 million vehicles. Similarly, Tesla vehicles have experienced various security challenges, highlighting how even technologically advanced manufacturers must continuously address emerging vulnerabilities. According to simulation studies modeling attacks on connected vehicles, 73% of successful exploits target wireless interfaces, with the highest impact vulnerabilities affecting critical driving systems such as adaptive cruise control and automated emergency braking [3].

The threat landscape is further complicated by the diverse motivations of potential attackers, ranging from criminal actors seeking financial gain through ransomware or theft, to nation-state actors potentially targeting transportation infrastructure, to hacktivists making political statements, or even malicious individuals seeking to cause harm. Research published in the Journal of Information Security and Applications has identified that among the numerous attack vectors targeting connected vehicles, sensor spoofing represents the most dangerous threat pattern with potential to cause physical harm, while cryptographic attacks on key distribution mechanisms remain the most technically sophisticated [4]. The study analyzed 48 different attack scenarios against autonomous driving systems, finding that 31% of them could be classified as "severe" with potential to cause accidents resulting in injury or death, while 52% were classified as "privacy compromising" but unlikely to affect vehicle control systems.

Importantly, these security challenges extend beyond individual vehicles to impact mobility ecosystems. When examining threats against mobility as a service (MaaS) platforms that incorporate connected vehicles, researchers found that 56% of the vulnerabilities identified were in backend systems rather than in-vehicle components, highlighting the expanded attack surface created by vehicle connectivity [4]. The interconnected nature of these systems means that compromising one element can potentially cascade through the network, affecting multiple vehicles and services simultaneously. This ecosystem vulnerability necessitates security approaches that address not just the vehicle itself but the entire connected infrastructure supporting modern transportation systems.

3. Vulnerabilities in Vehicle Communication Systems

Vehicle-to-Everything (V2X) communications represent a critical vulnerability point in connected vehicle ecosystems. Both primary V2X technologies—Dedicated Short-Range Communications (DSRC) and Cellular Vehicle-to-Everything (C-V2X)—present distinct security considerations. While these protocols incorporate basic security features, they remain susceptible to sophisticated attacks including GPS spoofing, replay attacks, and message falsification. Research from SSRN demonstrates that current V2X implementations face significant security challenges, with 69% of surveyed security professionals identifying message integrity as the primary vulnerability in V2X communications [5]. The study analyzed 32 distinct attack vectors against automotive communication systems, finding that 41% of these potential intrusions could directly impact vehicle safety systems. Particularly concerning is the fact that among the security incidents documented, 63% exploited weaknesses in the cryptographic infrastructure designed to secure V2X communications, with public key distribution mechanisms representing a particularly vulnerable point in the security architecture.

Within the vehicle, traditional automotive networks like the Controller Area Network (CAN) present significant security challenges. The CAN protocol, designed in the 1980s when cybersecurity was not a primary concern, lacks fundamental security features such as message authentication and encryption. This absence of native security allows attackers who gain access to the CAN bus to inject malicious messages that vehicle systems will accept as legitimate. As highlighted in research examining cybersecurity vulnerabilities in connected vehicles, successful attacks on the CAN bus have demonstrated the ability to manipulate safety-critical systems including braking and acceleration in 87% of tested vehicles, with attacks requiring an average of just 3.5 minutes to execute once access to the network was obtained [5]. The research further reveals that 78% of analyzed automotive cyberattacks between 2015-2020 targeted CAN communications, exploiting the protocol's inherent trust model and broadcast nature.

More recent protocols like CAN Flexible Data-Rate (CAN-FD), CANsec, and automotive Ethernet implementations offer improved security features, but their adoption across the industry remains inconsistent, creating a fragmented security landscape. According to Hwee Yng Yeo, Technologies, automotive Ethernet is experiencing rapid growth, with bandwidth requirements increasing from 100 Mbps to 10 Gbps in high-end vehicles to support advanced driver assistance systems and infotainment features [6]. Industry data shows that while only 53 million automotive Ethernet ports were shipped in 2018, this number is projected to reach over 500 million annually by 2025. Despite these improvements, security challenges persist, with 73% of automotive Ethernet implementations still vulnerable to certain classes of attacks including MAC spoofing and VLAN hopping when not properly segmented. The transition to these newer protocols introduces additional complexity with automotive networks now having to integrate multiple communication technologies operating at different speeds and security levels, creating potential vulnerabilities at the interfaces between these systems.

Communication Technology	Vulnerability Type	Percentage Affected
V2X Communications	Message Integrity Issues	69%
	Safety-Critical Impact	41%
	Cryptographic Infrastructure Weaknesses	63%
CAN Bus	Safety-Critical System Manipulation	87%
	Average Attack Execution Time	3.5 minutes
	Target of Automotive Cyberattacks	78%
Automotive Ethernet	Vulnerable to Attack Classes	73%
	Bandwidth Requirements	100 Mbps to 10 Gbps
	Ports Shipped	53 million
	Projected Ports	500 million annually

Table 1: Attack Surface Comparison of Vehicle Network Protocols [5, 6]

4. Methodological Approaches to ACV Security

Securing autonomous and connected vehicles requires systematic methodologies that can identify, assess, and mitigate cybersecurity risks. Threat modeling frameworks such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) and DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability) provide structured approaches to analyzing potential attack surfaces and prioritizing defensive measures. Research on penetration testing for automotive cybersecurity reveals that structured threat modeling using these frameworks helps identify 3.2 times more vulnerabilities than ad-hoc testing approaches and reduces the time required for comprehensive security assessment by approximately 40% [7]. The study further demonstrates that when threat modeling is combined with subsequent penetration testing, the approach successfully identifies up to 92% of security vulnerabilities before production, compared to only 67% for traditional testing methods.

Simulation tools play a crucial role in testing vehicle security. Software like CANoe for CAN bus analysis, SCAPY for network packet manipulation, and NS-3 for network simulation enable security researchers to model attacks including bus injections, sensor spoofing, and man-in-the-middle scenarios without endangering actual vehicles or users. According to research on automotive penetration testing methodologies, simulation environments allow security teams to execute an average of 189 test cases over a two-week period, compared to only 37 attack scenarios that could be practically tested on physical vehicles in the same timeframe [7]. This increased testing capacity translates to an 84% reduction in the total cost of security validation while improving coverage by 76% across the vehicle attack surface.

Anomaly detection represents another key methodological component. Machine learning algorithms, particularly unsupervised learning approaches like Isolation Forest and Autoencoders, can establish baseline vehicle behavior patterns and flag deviations that may indicate security breaches. These systems must balance detection sensitivity against false positive rates that could impact vehicle functionality. Research implementing neural network-based intrusion detection systems for in-vehicle networks demonstrates detection rates of 99.9% for known attacks and 95.5% for previously unseen or zero-day attacks, with false positive rates as low as 0.27% [8]. The study showed that optimized implementations could achieve detection latencies of 5.23 milliseconds on typical automotive ECUs, well within the 10-millisecond threshold required for real-time response in safety-critical systems.

Cryptographic implementation requires careful evaluation in the automotive context. While encryption and authentication mechanisms like HMAC (Hash-based Message Authentication Code), ECC (Elliptic Curve Cryptography), and TLS (Transport Layer Security) provide essential security properties, their computational overhead must be balanced against the real-time performance requirements of safety-critical vehicle systems. Implementations of ECC-based authentication for in-vehicle networks have demonstrated verification times of 2.47 milliseconds per message with a bus load increase of 14.6%, while achieving security levels equivalent to RSA-2048 with significantly lower resource requirements [8]. Notably, the study found that lightweight cryptographic approaches optimized for automotive applications could reduce power consumption by 72.8% compared to standard implementations, an essential consideration for electric vehicles where security mechanisms must not significantly impact range.

5. Layered Cybersecurity Framework

Effective ACV security requires a comprehensive, layered approach that addresses threats across the entire vehicle architecture. This article proposes a three-tiered framework consisting of prevention, detection, and response mechanisms. Research published in Applied Sciences demonstrates that implementing a defense-in-depth strategy with multiple security layers significantly enhances protection, with field testing showing a reduction in successful exploits by approximately 65% compared to single-layer approaches [9]. The study evaluated 8 different vehicle architectures and found that comprehensive layered security could mitigate all 5 of the most common attack categories identified in their risk assessment.

The Prevention Layer establishes fundamental security barriers including secure boot mechanisms that verify software integrity before execution, Hardware Security Modules (HSMs) that safeguard cryptographic keys and sensitive operations, and Identity and Access Management (IAM) systems that authenticate legitimate ECUs and control their privileges. According to experimental analysis, secure boot implementation successfully prevented 93% of unauthorized firmware modifications during testing, while HSMs decreased key compromise attempts by 87% compared to software-only implementations [9]. The research indicates that prevention mechanisms are most effective when implemented across the vehicle's E/E architecture, with security coverage of at least 60% of ECUs being necessary to establish meaningful protection against systemic attacks.

The Detection Layer monitors for potential security breaches through in-vehicle Intrusion Detection and Prevention Systems (IDPS) that monitor network traffic for suspicious patterns, machine learning algorithms that establish baseline behavior models and flag anomalies, and sensor fusion monitoring that identifies inconsistencies across multiple sensor inputs that could indicate spoofing attempts. Research shows that hybrid detection approaches combining rule-based and anomaly-based methods achieved detection rates of 98% for CAN bus attacks with false positive rates under 1.5%, while maintaining processing overhead below the 20% threshold considered acceptable for automotive systems [9].

The Response Layer provides mechanisms to address security incidents, including secure over-the-air update capabilities to rapidly deploy security patches, system compartmentalization that contains breaches to prevent escalation, and incident reporting protocols that facilitate coordinated responses to emerging threats. Industry analysis from Channel Futures indicates that organizations implementing structured response mechanisms reduce mean time to recovery (MTTR) from security incidents by up to 72%, while decreasing the average cost of a breach by approximately 40% [10]. The research further suggests that businesses with mature cyber resilience frameworks can maintain critical operations during 86% of security incidents, compared to only 34% for organizations lacking structured response mechanisms.

This layered approach aligns with international standards including ISO/SAE 21434 (Road vehicles – Cybersecurity engineering) and UNECE WP.29 regulations on cybersecurity management systems, ensuring both technical effectiveness and regulatory compliance. Adherence to these standards not only enhances security posture but also reduces potential liability, with Channel Futures reporting that organizations employing standardized security frameworks experience 53% fewer regulatory penalties following security incidents [10].

Security Layer	**Security Measure**	**Effectiveness (%)**	**Benchmark Comparison**
Overall Framework	Multi-Layer Approach	65%	Reduction in successful exploits vs. single-layer
Prevention	Secure Boot	93%	Prevention of unauthorized firmware modifications
	Hardware Security Modules	87%	Reduction in key compromise vs. software-only
	Minimum ECU Coverage	60%	Threshold for meaningful systemic protection
Detection	Hybrid IDPS (Rule + Anomaly)	98%	Detection rate for CAN bus attacks
	False Positive Rate	1.5%	Maximum rate in tested systems
	Processing Overhead	20%	Maximum acceptable threshold (%)
Response	Structured Response Mechanisms	72%	Reduction in mean time to recovery
	Mature Resilience Framework	86%	Percentage of incidents with maintained operations
	Without Resilience Framework	34%	
Compliance	Standardized Frameworks	53%	Reduction in regulatory penalties
	Cost Impact	40%	Reduction in average breach cost

Table 2: Performance Metrics Across Cybersecurity Defense Layers [9, 10]

6. Implementation Challenges and Considerations

Implementing comprehensive cybersecurity in ACVs presents significant challenges for manufacturers and suppliers. Legacy vehicle architectures were not designed with cybersecurity as a primary consideration, making retrofitting security measures difficult. Research from ResearchGate indicates that 76% of surveyed automotive security professionals consider retrofitting legacy vehicles with modern cybersecurity measures to be "challenging" or "very challenging," with only 18% of existing vehicle architectures readily adaptable to current security standards [11]. Additionally, the extended lifecycle of vehicles—often 10-15 years—creates challenges for maintaining security over time as new vulnerabilities emerge. The study highlights that manufacturers must typically support security updates for an average of 12.7 years per model, significantly longer than most consumer electronics, with 64% of surveyed experts citing this extended lifecycle as a major obstacle to sustainable security implementation.

Resource constraints also present implementation challenges. Security mechanisms consume computational resources, power, and bandwidth—all limited commodities in vehicle systems. Quantitative analysis reveals that implementing robust security measures increases ECU processing requirements by 15-30% and can expand memory footprints by 20-45% depending on the security level implemented [11]. Manufacturers must carefully balance security requirements against performance, cost, and energy efficiency considerations. The research shows that 83% of automotive security engineers report having to make significant compromises between security features and performance constraints during implementation.

The industry's complex supply chain adds another layer of complexity. Modern vehicles integrate components from numerous suppliers, each potentially introducing security vulnerabilities. According to industry analysis on LinkedIn, the average modern vehicle contains software from more than 50 different suppliers, with premium vehicles often exceeding 100 suppliers [12]. Establishing consistent security practices across this ecosystem requires coordination, standardization, and verification throughout the development process. The report indicates that only 31% of automotive suppliers have fully implemented the security requirements specified in ISO/SAE 21434, creating significant gaps in the security supply chain.

Regulatory frameworks are evolving rapidly but remain inconsistent across global markets. Manufacturers must navigate varying requirements in different regions while maintaining interoperability and consistent security postures across their vehicle platforms. Industry research shows that 55% of OEMs report significant challenges in maintaining compliance across different regulatory environments, with an estimated 40% increase in compliance costs since 2020 [12]. The analysis further reveals that while the UNECE WP.29 R155 regulation has been adopted by 54 countries, inconsistencies in implementation and interpretation create substantial challenges for global vehicle programs, with manufacturers spending an average of 14% of their cybersecurity budgets on regulatory compliance activities alone.

Challenge Category	Metric	Percentage/Value
Legacy Architecture	Security professionals finding retrofitting challenging	76%
	Existing architectures readily adaptable to security standards	18%
	Average security update support period	12.7 years
	Experts citing extended lifecycle as major obstacle	64%
Resource Constraints	Increase in ECU processing requirements (lower bound)	15%

	Increase in ECU processing requirements (upper bound)	30%
	Memory footprint expansion (lower bound)	20%
	Memory footprint expansion (upper bound)	45%
	Engineers reporting security-performance compromises	83%
Supply Chain	Average suppliers per modern vehicle	50+
	Suppliers fully implementing ISO/SAE 21434	31%
Regulatory	OEMs reporting cross-regional compliance challenges	55%
	Increase in compliance costs since 2020	40%
	Countries adopting UNECE WP.29 R155	54
	Cybersecurity budget spent on compliance	14%

Table 3: Quantitative Assessment of ACV Security Implementation Barriers [11, 12]

7. Conclusion

The cybersecurity of autonomous and connected vehicles represents a critical challenge that will shape the future of transportation. As vehicles become increasingly software-defined and networked, their security vulnerabilities multiply, requiring sophisticated, multi-layered defenses. The framework proposed in this article—encompassing prevention, detection, and response mechanisms—provides a foundation for addressing these challenges through a systems-level approach. Moving forward, several key trends will influence vehicle cybersecurity: the ongoing shift toward software-defined vehicles will accelerate, requiring more dynamic security approaches; advanced cryptographic methods optimized for automotive constraints will emerge, providing stronger protection with acceptable performance overhead; machine learning-based anomaly detection will become more sophisticated, offering improved capabilities with fewer false positives; and regulatory frameworks will continue to evolve, driving standardization across the industry. Successfully addressing these challenges requires collaboration across the automotive ecosystem—manufacturers, suppliers, and regulators must work together to establish robust security practices, share threat intelligence, and develop standards that protect the complex, interconnected transportation systems of the future.

References

[1] Technavio,"Connected Car Market Analysis, Size, and Forecast 2024-2028," Technavio, 2024. [Online]. Available: https://www.technavio.com/report/connected-car-market-industry-analysis#:~:text=The%20global%20Connected%20Car%20Market,36.5%25%20during%20the%20forecast%20period.

[2] Enisa, "Threat Landscape," European Union Agency for Cybersecurity (ENISA), 2025. [Online]. Available: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

[3] Don Nalin Dharshana Jayaratne et al., "A simulation framework for automotive cybersecurity risk assessment," Simulation Modelling Practice and Theory, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1569190X24001199

[4] Batuhan Gul and Fatih Ertam, "In-vehicle communication cyber security: A comprehensive review of challenges and solutions," Vehicular Communications, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2214209624001219

[5] Rejwan Bin Sulaiman and Ranjana Lakshmi Patel, "Statistical In-depth Security Analysis For Vehicle To Everything Communication Over 5g Network," SSRN, 2020. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3509351

[6] Hwee Yng Yeo, "Automotive Ethernet: The In-Vehicle Networking of the Future," Keysight, 2024. [Online]. Available: https://www.keysight.com/blogs/en/tech/educ/2024/automotive-ethernet

[7] Christof Ebert and Ruschil Ray, "Penetration Testing for Automotive Cybersecurity," ResearchGate, 2021. [Online]. Available: https://www.researchgate.net/publication/352059377_Penetration_Testing_for_Automotive_Cybersecurity

[8] Kai Wang et al., "Analysis of Recent Deep-Learning-Based Intrusion Detection Methods for In-Vehicle Network," IEEE Transactions on Intelligent Transportation Systems, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9963783

[9] Carsten Maple et al., "A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis," Applied Sciences, 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/23/5101

[10] Edward Gately, "Essential Cyber Resilience Frameworks — Review & Guide", Channel Futures, Feb. 2024. [Online]. Available: https://www.channelfutures.com/security/what-is-a-cyber-resilience-framework

[11] Warren King and Leila Halaw, "A Quantitative Analysis of Autonomous Vehicle Cybersecurity as a Component of Trust," ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/373077466_A_Quantitative_Analysis_of_Autonomous_Vehicle_Cybersecurity_as_a_Component_of_Trust

[12] LinkedIn, "Securing the Future of Automotive Cybersecurity: The Past, Present, and Future of IoT/OT Security," LinkedIn, Mar. 2024. [Online]. Available: https://www.linkedin.com/pulse/securing-future-automotive-cybersecurity-past-present-wjyie