World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Modern vehicle security: Analyzing software vulnerabilities and protection mechanisms in connected cars

Mayank Rai *

General Motors LLC, USA.

World Journal of Advanced Research and Reviews, 2025, 26(01), 414-422

Publication history: Received on 25 February 2025; revised on 03 April 2025; accepted on 05 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1078

Abstract

The rapid digitalization of modern vehicles has introduced significant cybersecurity challenges for the automotive industry. As vehicles evolve into sophisticated cyber-physical systems, the integration of multiple electronic control units and communication networks has created extensive attack surfaces requiring robust protection mechanisms. This technical document examines the landscape of automotive cybersecurity, focusing on vulnerabilities in-vehicle networks, emerging attack vectors, and defensive measures implemented by manufacturers. The findings highlight critical areas, including Controller Area Network security, firmware protection, secure over-the-air updates, and intrusion detection systems. Additionally, the document explores emerging technologies such as AI-based anomaly detection, blockchain implementations, and quantum-resistant cryptography, providing recommendations for enhancing automotive security posture through standardized protocols and comprehensive incident response mechanisms.

Keywords: Automotive Cybersecurity; Vehicle Network Protection; Electronic Control Units; Connected Car Security; Intrusion Detection Systems

1. Introduction

The automotive industry has undergone a revolutionary transformation with the integration of sophisticated software systems and electronic components. Modern vehicles have evolved into complex cyber-physical systems, with premium vehicles containing upwards of 150 Electronic Control Units (ECUs) interconnected through various communication protocols. According to comprehensive research in the field of electric vehicle security, these vehicles now typically process between 500MB to 1TB of data per day during normal operation, highlighting the massive scale of digital integration in modern automobiles [1].

The integration depth of software systems spans across multiple vehicle domains, creating an intricate network of interconnected components. The Controller Area Network (CAN), operating at data rates of up to 1 Mbps to 8 Mbps, serves as the primary communication backbone for critical vehicle functions. This is supplemented by the Local Interconnect Network (LIN) operating at 20kbps for less critical functions, and FlexRay protocols achieving speeds of up to 10Mbps for safety-critical applications, and automotive Ethernet that operates up to 1Gbps. Recent studies have shown that modern vehicles implement up to 70 different CAN messages per second during normal operation, creating a complex web of real-time communications that must be secured against potential threats [1].

Vehicle architecture has evolved to incorporate multiple layers of connectivity, from internal vehicle networks to external communication interfaces. Research has documented that contemporary vehicles maintain connections across an average of 5 different wireless protocols simultaneously, including Wi-Fi, Bluetooth, cellular networks, dedicated

* Corresponding author: Mayank Rai

short-range communications (DSRC), and GPS. This extensive connectivity framework has led to the identification of 364 potential attack surfaces in modern vehicles, as documented in recent security assessments [2].

1.1. Scope

The scope of this analysis encompasses the multifaceted nature of automotive cybersecurity. The examination begins with current software architecture implementations, where research has shown that modern vehicles employ a hierarchical network structure with an average of 4 distinct domains: powertrain, chassis, body, and infotainment. Each domain controller manages multiple ECUs, with communication latencies ranging from 10ms for critical functions to 100ms for non-critical operations [2].

Security measures and protocols form a crucial component of this analysis, focusing on both preventive and detective controls. The analysis draws from several authoritative data sources, including the National Vulnerability Database (NVD), which provides standardized vulnerability metrics for automotive systems, and comprehensive academic research documenting security assessments of vehicle platforms. The Common Vulnerability Scoring System (CVSS) framework has been instrumental in providing standardized vulnerability scoring data for the analysis [2].

The methodology employed a systematic approach to vulnerability assessment using the CVSS v3.0 framework. Performance analysis focused on several key areas of automotive security, including the evaluation of Hardware Security Module (HSM) requirements for real-time processing and the assessment of secure boot implementation impacts. Particular attention was paid to the analysis of CAN bus message processing requirements, where research has verified a critical 0.5ms processing time constraint for effective security measures [2].

The research findings have established important baseline requirements for automotive security implementations. Studies have demonstrated that intrusion detection systems must maintain strict processing parameters, specifically the ability to analyze CAN bus messages within 0.5ms to effectively prevent potential attacks. Additionally, the research has established fundamental requirements for Hardware Security Modules and secure boot processes, highlighting their crucial role in maintaining effective security levels in automotive implementations [1]

The study concludes by examining future trends and recommendations, particularly focusing on the integration of artificial intelligence and machine learning in automotive security. Current implementations have demonstrated the capability to detect anomalous behavior with 96.5% accuracy and a false positive rate of less than 0.1%, suggesting promising directions for future security enhancements [1].

Table 1 Comprehensive Automotive Network and Security Metrics [1, 2, 6]

Metric Category	Parameter	Value	Unit
Network Protocols	CAN Data Rate	1	Mbps
	LIN Data Rate	20	Kbps
	FlexRay Data Rate	10	Mbps
	Automotive Ethernet (100BASE-T1)	100	Mbps
	Automotive Ethernet (1000BASE-T1)	1000	Mbps
Network Performance	CAN Messages	70	Messages/Second
	Ethernet Frame Rate	1000	Frames/Second
Security	Critical/High Severity Vulnerabilities	43	Percentage
Response Times	CAN Bus Message Processing	0.5	Milliseconds
	Ethernet Packet Processing	0.1	Milliseconds
	Domain Controller (Critical)	10	Milliseconds
	Domain Controller (Non-Critical)	100	Milliseconds

2. Methodology

2.1. Data Sources

The methodology for this analysis incorporates a systematic approach to data collection and evaluation of automotive security vulnerabilities. The National Vulnerability Database (NVD) has been instrumental in providing standardized vulnerability metrics, particularly in analyzing Controller Area Network (CAN) vulnerabilities that represent approximately 60% of all reported automotive security incidents [3].

Multiple databases and reporting systems complement the NVD for tracking vulnerabilities across different automotive network protocols. According to Jing et al. [3], modern vehicle networks employ various protocols, including Automotive Ethernet, FlexRay, and LIN, each requiring specific security monitoring approaches. The Common Vulnerability Scoring System (CVSS) provides standardized scoring for these vulnerabilities across different protocols, as documented in recent automotive security assessments by Brighente et al. [1].

The Auto-ISAC (Automotive Information Sharing and Analysis Center) serves as a central hub for sharing threat intelligence and vulnerability information across the automotive industry. Research by Mwanje et al. [6] demonstrates how this collaborative approach has enhanced the industry's ability to track and respond to vulnerabilities across multiple network protocols.

This comprehensive approach to vulnerability tracking has enabled researchers to monitor security issues across different vehicle systems, with particular emphasis on the increasing complexity of modern vehicle networks that typically contain 70-100 Electronic Control Units (ECUs) [3].

The Automotive Information Sharing and Analysis Center (Auto-ISAC) reports have been fundamental in understanding threat landscapes, providing data that indicates a 32% annual increase in reported security incidents between 2020 and 2023. SAE International standards documentation, specifically focusing on cybersecurity guidelines for connected vehicles, has established baseline security requirements that address 85% of known attack vectors in modern automotive systems [3].

Academic research contributions have played a vital role in understanding emerging security challenges. Analysis of recent studies reveals that modern vehicles are exposed to approximately 55 different types of cyber attacks, with 15 classified as severe threats requiring immediate mitigation. The research data demonstrates that 68% of these attacks target communication systems, while 32% focus on hardware vulnerabilities. These findings have been instrumental in developing comprehensive security frameworks for next-generation vehicles [4].

Manufacturer security bulletins have provided critical insights into real-world security challenges, documenting that 47% of identified vulnerabilities require hardware updates for complete mitigation, while 53% can be addressed through software patches. This data has been essential in understanding the practical implications of security measures and their effectiveness in real-world scenarios [4].

2.2. Analysis Framework

The analytical framework employs the Common Vulnerability Scoring System (CVSS) v3.0 for standardized vulnerability assessment. Recent analysis shows that among documented automotive vulnerabilities, 25% received high severity scores (7.0-8.9), particularly in systems related to vehicle communication networks and remote access capabilities. The scoring distribution reveals that CAN bus vulnerabilities consistently receive higher severity ratings, with an average CVSS score of 7.8 across documented incidents [3].

Risk assessment methodologies incorporate detailed analysis of attack vectors and their potential impact on vehicle systems. Research indicates that 42% of successful attacks exploit vulnerabilities in wireless communication systems, while 28% target diagnostic interfaces. The remaining 30% of attacks leverage various other entry points, including physical access and social engineering techniques. This distribution has been crucial in developing targeted security measures for specific vulnerability types [4].

Statistical analysis of incident reports utilizes advanced correlation techniques to identify patterns in security breaches. The framework has revealed that 73% of successful attacks follow predictable patterns, with initial compromise occurring through wireless interfaces in 45% of cases. The data shows that vehicles with integrated telematics systems face 2.3 times more attempted security breaches compared to vehicles without these systems [3].

The evaluation of mitigation effectiveness employs a structured assessment methodology examining both preventive and detective controls. Analysis shows that implementing secure boot mechanisms reduces the risk of unauthorized system modifications by 89%, while encrypted communication protocols demonstrate 94% effectiveness in preventing man-in-the-middle attacks. Hardware security modules have proven 99% effective in protecting critical system components, though their implementation increases system cost by an average of 12% [4].

Table 2 Key Automotive Security Metrics [3, 4]

Security Category	Type	Percentage
Attack Distribution	Communication Systems	68
	Hardware Systems	32
Protection Effectiveness	Hardware Security Modules	99
	Encrypted Protocols	94
	Secure Boot	89
Mitigation Approach	Software Patches	53
	Hardware Updates	47
Attack Vectors	Wireless Systems	42
	Diagnostic Interfaces	28
	Physical/Social Access	30

3. Current Landscape

3.1. Software Architecture

The software architecture in modern vehicles represents an intricate network of interconnected systems that control critical vehicle functions. The Controller Area Network (CAN) serves as the primary communication protocol, with research demonstrating that modern vehicles typically contain 2-5 separate CAN buses operating at different speeds. These networks collectively process between 60-100 distinct messages per second during normal vehicle operation, while performance-critical applications such as engine control can generate up to 500 messages per second under high-load conditions [5].

The Local Interconnect Network (LIN) provides supplementary communication capabilities for less time-critical functions, operating at speeds suitable for body electronics and comfort features. Experimental analysis has shown that compromising a single ECU can potentially provide access to up to 60% of the vehicle's network traffic, highlighting significant security concerns in current architectural implementations. The research demonstrates that attacks on these networks can be executed within 250ms, faster than a human driver's typical reaction time of 750ms [5].

FlexRay technology has emerged as a crucial component for safety-critical systems, particularly in applications requiring deterministic timing. Security analysis has revealed that these networks can be susceptible to targeted attacks, with researchers successfully demonstrating the ability to inject malicious messages into the FlexRay bus within 128ms of gaining access to the network. The implications of such vulnerabilities are particularly concerning given that FlexRay typically controls safety-critical systems such as brake-by-wire and steer-by-wire implementations [6].

Automotive Ethernet implementations have introduced new security challenges while providing essential high-bandwidth capabilities. Recent security assessments have identified that modern connected vehicles process an average of 25GB of data per day through various Ethernet-connected systems. Analysis shows that approximately 40% of this traffic relates to safety-critical functions, while 35% involves infotainment and connectivity features, with the remaining 25% dedicated to diagnostic and maintenance data [6].

3.2. Attack Surface Analysis

The attack surface of modern vehicles has expanded significantly with the integration of complex software systems. Experimental security analysis has revealed that attackers can gain access to ECUs by exploiting vulnerabilities in the

CAN protocol, with successful attacks demonstrated on 14 out of 16 ECUs tested in laboratory conditions. These vulnerabilities enabled researchers to inject malicious messages capable of affecting critical vehicle functions, including engine performance, braking systems, and instrument cluster displays [5].

Over-the-air (OTA) update mechanisms present substantial security challenges in contemporary vehicle architectures. Security assessments have shown that vehicles receiving regular OTA updates maintain active wireless connections for an average of 45 minutes per day, creating potential attack windows. Research has documented that compromised update processes can potentially affect up to 80% of a vehicle's ECUs, with critical systems becoming vulnerable during the update process [6].

Vehicle-to-everything (V2X) communication systems significantly expand the potential attack surface. Recent analysis indicates that V2X-enabled vehicles process an average of 150 external messages per minute in urban environments, with each message requiring verification within 100ms to maintain real-time operation. Security testing has demonstrated that approximately 15% of these messages could potentially be manipulated without detection by current security measures [6].

Third-party applications have introduced additional complexity to the security landscape. Experimental analysis has shown that compromising a single third-party application can potentially provide access to up to 40% of the vehicle's internal network traffic. The research demonstrated successful attacks against multiple vehicle systems through compromised applications, with attack execution times ranging from 500ms to 3 seconds depending on the targeted system [5].

Diagnostic interfaces continue to present significant security concerns in modern vehicles. Research has shown that standard diagnostic protocols can be exploited to gain access to critical vehicle systems, with successful attacks demonstrated against both CAN and Ethernet-based diagnostic interfaces. Experimental results indicate that an attacker with access to the diagnostic port can potentially compromise up to 75% of vehicle systems within 5 minutes of initial access [6].

4. Vulnerability Analysis

4.1. Common Attack Vectors

Modern vehicles present an extensive attack surface spanning multiple electronic systems and communication protocols. Analysis of CAN bus injection attacks has revealed significant vulnerabilities in vehicle networks, with research demonstrating that a typical vehicle contains between 6-and 12 separate CAN buses operating at different speeds. These networks handle an average of 40-100 messages per second during normal operation, with each message being broadcast to all nodes on the network. The study identified that vehicles with remote connectivity features expose additional attack surfaces through cellular connections (telematics), Bluetooth wireless access, and WiFi connectivity, each presenting unique security challenges [7].

ECU firmware manipulation represents a critical vulnerability in modern vehicles. Research has shown that a typical vehicle contains between 50 to 100 ECUs, each running proprietary firmware that could potentially be compromised. The study identified that many ECUs lack robust authentication mechanisms, with only 30% implementing secure boot procedures. Analysis of remote attack surfaces revealed that telematics control units in particular present significant risks, as they often have direct CAN access and cellular connectivity, potentially allowing remote exploitation [7].

Key fob systems have evolved to incorporate various wireless technologies, introducing new security challenges. Testing conducted across multiple vehicle models revealed that keyless entry systems typically operate at frequencies between 315 MHz and 433 MHz, with transmission ranges of 5-20 meters under normal conditions. The research demonstrated that these systems are susceptible to various forms of attack, including signal amplification and replay attacks, particularly when operating in the 433 MHz band commonly used in modern vehicles [8].

Mobile applications associated with connected vehicles introduce additional vulnerability points. Security assessment of automotive mobile applications revealed that they commonly interface with vehicle systems through cellular networks, processing between 50-100 MB of data monthly. The applications typically maintain persistent connections to vehicle telematics systems, with connection intervals ranging from 30 seconds to 5 minutes, depending on the implementation [8].

Cellular network interfaces in modern vehicles have expanded significantly, with telematics control units handling various forms of remote communication. Research has shown that these systems typically process between 10-50 MB of data daily during normal operation, maintaining persistent cellular connections for remote monitoring and control functions. The study identified that cellular-based attacks could potentially affect multiple vehicles simultaneously within a single cellular network cell, particularly in urban environments where vehicle density is high [7].

4.2. Statistical Findings

Analysis of automotive cybersecurity incidents has revealed concerning trends in vulnerability exploitation. Research conducted across multiple vehicle platforms showed that approximately 20% of identified attack vectors could potentially be exploited remotely, without requiring physical access to the vehicle. The study documented that vehicles with advanced telematics systems exposed an average of 20 potential remote attack surfaces, compared to 5 or fewer in vehicles without such systems [7].

Remote attack capabilities have demonstrated significant evolution, with modern vehicles exposing multiple wireless interfaces. The research identified that telematics systems, in particular, present elevated risk levels, as they typically combine cellular connectivity with direct CAN bus access. Analysis of vehicle networks showed that CAN messages related to physical vehicle functions (such as steering and braking) represent approximately 60% of all network traffic, while diagnostic and status messages account for the remaining 40% [8].

Security assessment of connected vehicle systems revealed that communications between vehicles and charging infrastructure present additional vulnerability points. The study documented that charging stations typically exchange between 2-5 MB of data per charging session, with communication intervals ranging from 100ms to 1 second during active charging. Analysis of these interactions identified potential vulnerabilities in authentication mechanisms and data exchange protocols, particularly in systems implementing ISO 15118 for vehicle-to-grid communication [8].

Table 3 Core Automotive Security Vulnerabilities [7,8]

Attack Vector	Component Affected	Risk Level
CAN Bus Injection	Network Systems	Critical
ECU Firmware	Control Systems	Critical
Key Fob Systems	Access Control	High
Mobile Applications	Remote Access	Moderate
Cellular Networks	Remote Communication	High

5. Protection Mechanisms

5.1. Current Security Measures

Modern automotive security architectures have evolved to address the complex threat landscape facing connected vehicles. Hardware Security Modules (HSMs) form a fundamental component of vehicle security, with research showing implementation rates of 68% across new vehicle models. Current generation HSMs in automotive applications demonstrate the capability to execute cryptographic operations with latencies under 1 millisecond while maintaining power consumption within the 100-300mW range. Studies indicate that HSM implementation has resulted in a 92% reduction in successful firmware tampering attempts across tested vehicle platforms [9].

Secure Boot mechanisms serve as a critical defense against unauthorized software modifications. Research has demonstrated that modern secure boot implementations can verify firmware integrity across an average of 15 ECUs within a 2-second window during vehicle startup. Analysis of secure boot effectiveness shows successful detection rates of 95% for unauthorized firmware modifications, with false positive rates maintained below 0.1% across tested platforms [10].

Message authentication for CAN communications represents a significant advancement in in-vehicle network security. Studies have shown that authenticated messaging systems can effectively process CAN frames at the standard 500 kbit/s rate while adding a security overhead of approximately 8-16 bytes per message. Implementation analysis reveals

that these systems have successfully prevented 96% of attempted message injection attacks in controlled testing environments, particularly when combined with timing-based intrusion detection mechanisms [9].

Intrusion Detection Systems (IDS) have demonstrated significant effectiveness in identifying anomalous behavior within vehicle networks. According to Scalas and Giacinto [2], modern automotive IDS implementations can monitor up to 2,500 CAN messages per second while maintaining detection accuracy rates of 94%. The systems have shown particular effectiveness in identifying message injection attacks, with detection rates reaching 97% for high-risk anomalies within 100ms of occurrence [10].

Security-oriented gateway architectures provide essential network segmentation and access control. Studies show that modern automotive gateways can effectively manage communication between an average of 6-8 different network domains while performing security checks on cross-domain traffic. Performance analysis indicates that security filtering adds approximately 2-5ms of latency to inter-domain communications while maintaining effectiveness rates above 90% in preventing unauthorized access attempts [9].

5.2. Standardization Efforts

The ISO/SAE 21434 standard has established comprehensive requirements for automotive cybersecurity engineering. Implementation studies indicate that organizations typically require 18-24 months to achieve basic compliance across their development processes. Analysis shows that companies implementing ISO/SAE 21434 experience a 45% reduction in security-related design issues during the development phase, with particularly strong improvements in threat modeling and risk assessment activities [10].

UNECE WP.29 regulations have fundamentally altered the automotive security landscape. Research indicates that manufacturers require an average of 24 months to fully implement the required Cybersecurity Management System (CSMS), with testing procedures covering approximately 50 distinct security controls. Organizations that have achieved compliance demonstrate a 55% improvement in their ability to detect and respond to security incidents compared to non-compliant entities [9].

AutoSAR Secure Onboard Communication specifications have standardized security implementations across vehicle platforms. Studies show that implementations following these specifications achieve interoperability rates of 89% while maintaining security effectiveness. The standardized approach has resulted in a 40% reduction in development time for secure communication implementations across different vehicle platforms [10].

NIST Cybersecurity Framework adaptations for automotive applications have shown a significant impact on security posture. Research indicates that organizations implementing the framework achieve maturity level improvements of 60% within the first year of adoption. The framework's adaptation to automotive requirements has led to standardized security controls across supply chains, with 75% of surveyed organizations reporting improved vulnerability management processes [9].

Table 4 Key Automotive Security Protection Metrics [9, 10]

Protection Measure	Effectiveness Rate (%)
HSM Tamper Prevention	92
Secure Boot Detection	95
Message Authentication	96
Intrusion Detection	97
Gateway Security	90
NIST Framework Implementation	75

6. Future Trends

6.1. Emerging Technologies

The landscape of automotive security continues to evolve with the integration of advanced technologies. AI-based anomaly detection systems have emerged as a crucial component in modern vehicle security architectures. According

to Scalas and Giacinto [2], advanced detection systems in modern vehicles can effectively monitor CAN networks with a throughput of up to 500 CAN messages per second during normal operation, with detection algorithms capable of identifying suspicious patterns within 50ms of occurrence. Implementation studies show that machine learning models can effectively process data from multiple vehicle subsystems while maintaining false positive rates below 1% during normal operation [11].

Blockchain technology for secure Over-The-Air (OTA) updates represents a significant advancement in automotive security. Studies indicate that blockchain implementations can provide tamper-evident update distribution while maintaining complete transaction records across vehicle fleets. The technology has demonstrated particular effectiveness in securing the software supply chain, with implementations showing the capability to verify and validate updates across multiple ECUs within a 5-second window. Research shows that distributed ledger systems can effectively manage update processes while ensuring integrity verification for all software components [12].

Zero-trust architecture adoption in automotive systems has shown promising results in enhancing security posture. Current implementations demonstrate the ability to enforce strict access controls across vehicle networks, with authentication processes completing within 100ms for critical systems. Studies indicate that zero-trust frameworks can effectively manage authentication and authorization for up to 100 ECUs in modern vehicles while maintaining system performance within operational parameters. The architecture has proven particularly effective in preventing unauthorized access attempts, with success rates exceeding 95% in controlled testing environments [11].

Quantum-resistant cryptography development addresses emerging security challenges in automotive systems. Research shows that post-quantum cryptographic implementations can operate effectively within the computational constraints of automotive ECUs, with encryption operations completing within acceptable timeframes for real-time vehicle applications. These advanced cryptographic systems demonstrate resilience against both traditional and quantum-based attack vectors while maintaining compatibility with existing vehicle network architectures [12].

Recommendations

Enhanced supply chain security represents a critical focus area for automotive manufacturers. Studies show that comprehensive security programs can effectively monitor and validate components throughout the manufacturing process, with automated systems capable of tracking thousands of individual parts across the supply chain. Implementation of secure supply chain practices has demonstrated significant improvement in component validation, with verification processes completed within standardized timeframes while maintaining accuracy rates above 95% [11].

Standardized security testing protocols have become essential for maintaining consistent security levels across vehicle platforms. Research indicates that automated testing frameworks can complete comprehensive security assessments covering all critical vehicle systems within 48 hours. These testing protocols demonstrate particular effectiveness in identifying potential vulnerabilities across multiple vehicle subsystems while maintaining test coverage above 90% for critical components [12].

Regular security audits have proven crucial for maintaining robust security postures in modern vehicles. Implementation studies show that continuous monitoring systems can effectively track security metrics across all vehicle subsystems, generating alerts for potential security violations within seconds of detection. These audit mechanisms demonstrate the capability to monitor hundreds of security controls simultaneously while maintaining accurate compliance reporting across vehicle fleets [11].

Incident response capabilities continue to evolve with the increasing sophistication of security threats. Research demonstrates that modern response systems can effectively contain and mitigate security incidents within the first 15 minutes of detection, significantly reducing potential impact on vehicle operations. Studies show that automated response mechanisms can effectively handle multiple concurrent security events while maintaining system stability and preventing cascade failures across vehicle networks [12]

7. Conclusion

The automotive industry faces unprecedented security challenges as vehicles become increasingly connected and software-dependent. The evolution of attack vectors and the expanding complexity of vehicle networks necessitate continuous advancement in protection mechanisms. While current security measures, such as Hardware Security Modules, secure boot implementations, and intrusion detection systems provide fundamental protection, emerging

technologies offer promising solutions for future security challenges. The adoption of artificial intelligence, blockchain technology, and quantum-resistant cryptography, combined with enhanced supply chain security and standardized testing protocols, will be crucial in maintaining robust security postures. The successful implementation of these measures, supported by industry standards and regular security assessments, will be essential in safeguarding the next generation of connected vehicles against evolving cyber threats.

References

[1] Alessandro Brighente et al., "Electric Vehicles Security and Privacy: Challenges, Solutions and Future Needs," ResearchGate, Jan. 2023. [Online]. Available: https://www.researchgate.net/publication/367050012_Electric_Vehicles_Security_and_Privacy_Challenges_Solutions_and_Future_Needs

[2] Michele Scalas, Giorgio Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," IEEE 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8923077

[3] Pengfei Jing et al., "Revisiting Automotive Attack Surfaces: a Practitioners' Perspective ," IEEE 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10646688

[4] Asha .K et al., "Analysis of Automotive Security Risk using Cyber Security," Research Gate. 2023. [Online]. Available: https://www.researchgate.net/publication/374792444_Analysis_of_Automotive_Security_Risk_using_Cyber_Security

[5] Karl Koscher et al., "Experimental Security Analysis of a Modern Automobile," ResearchGate, 2010. [Online]. Available: https://www.researchgate.net/publication/220713691_Experimental_Security_Analysis_of_a_Modern_Automobile

[6] Maria Drolence Mwanje et al., "Cyber Security Analysis of Connected Vehicles," ResearchGate 2024. [Online]. Available: https://www.researchgate.net/publication/379782725_Cyber_security_analysis_of_connected_vehicles

[7] Chris Valasek and Charlie Miller, "A Survey of Remote Automotive Attack Surfaces," IOActive, 2014. [Online]. Available: https://ioactive.com/wp-content/uploads/pdfs/IOActive_Remote_Attack_Surfaces.pdf

[8] Cabell Hodge et al., "Vehicle Cybersecurity Threats and Mitigation Approaches," National Renewable Energy Laboratory, NREL, 2019. [Online]. Available: https://www.nrel.gov/docs/fy19osti/74247.pdf

[9] Ignacio Fernandez de Arroyabe et al., "Cybersecurity Maintenance in the Automotive Industry Challenges and Solutions: A Technology Adoption Approach," Future Internet. 2024. [Online]. Available: https://www.mdpi.com/1999-5903/16/11/395

[10] Andrew Roberts et al., "A Global Survey of Standardization and Industry Practices of Automotive Cybersecurity Validation and Verification Testing Processes and Tools," ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/375699820_A_Global_Survey_of_Standardization_and_Industry_Practices_of_Automotive_Cybersecurity_Validation_and_Verification_Testing_Processes_and_Tools

[11] Stefan Hansen, "Cybersecurity for Connected Vehicles," Cryptomathic, Jan. 2023. [Online]. Available: https://www.cryptomathic.com/blog/cybersecurity-for-connected-vehicles

[12] Klaus Kainrath et al., "Advancing Automotive Connectivity: New Technologies and Security Considerations," IEEE, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10631203