International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246/ICRTCSIT-127
Eureka Vision Publication | ICRTCSIT'25-Conference Proceeding

Original Article

Securing the Next Generation of Vehicles: Threats and Countermeasures in SDVs

Suresh Sureddi
Senior Technical Program Manager, Harman International.

Abstract - As vehicles evolve into software-defined platforms, the cybersecurity landscape of modern transportation systems is undergoing rapid transformation. This paper examines the heightened risks associated with increased connectivity, complex software architectures, and cloud integration in Software-Defined Vehicles (SDVs). We analyze core threat vectors such as insecure communication protocols, OTA vulnerabilities, and AI-based attacks. Furthermore, we outline a layered cybersecurity framework, practical mitigation strategies, and the role of artificial intelligence in threat detection and prevention. This comprehensive study combines insights from real-world deployments and scholarly research to propose a future-proof approach to automotive cybersecurity.

Keywords- SDV, cybersecurity, connected vehicles, V2X, OTA updates, AI in automotive, vehicle networks, intrusion detection, cloud security.

1. Introduction

The rapid digital transformation of the automotive industry is reshaping vehicles into highly connected, software-centric platforms. Software-Defined Vehicles (SDVs) leverage centralized computing, over-the-air updates, and cloud ecosystems to deliver personalized and intelligent driving experiences. However, this evolution introduces significant cybersecurity challenges due to increased attack surfaces, third-party integrations, and the exchange of real-time data.

2. SDV Architecture and Emerging Cyber Threats

Unlike traditional vehicles with isolated ECUs, SDVs operate on centralized compute platforms integrated with cloud APIs and virtualized environments. This dependence on external communication channels, sensors, and remote access protocols increases vulnerability to cyberattacks. Threat vectors include legacy protocol exploitation (e.g., CAN, LIN), OTA update tampering, API abuse, AI spoofing, and misconfigured cloud interfaces [1][2].

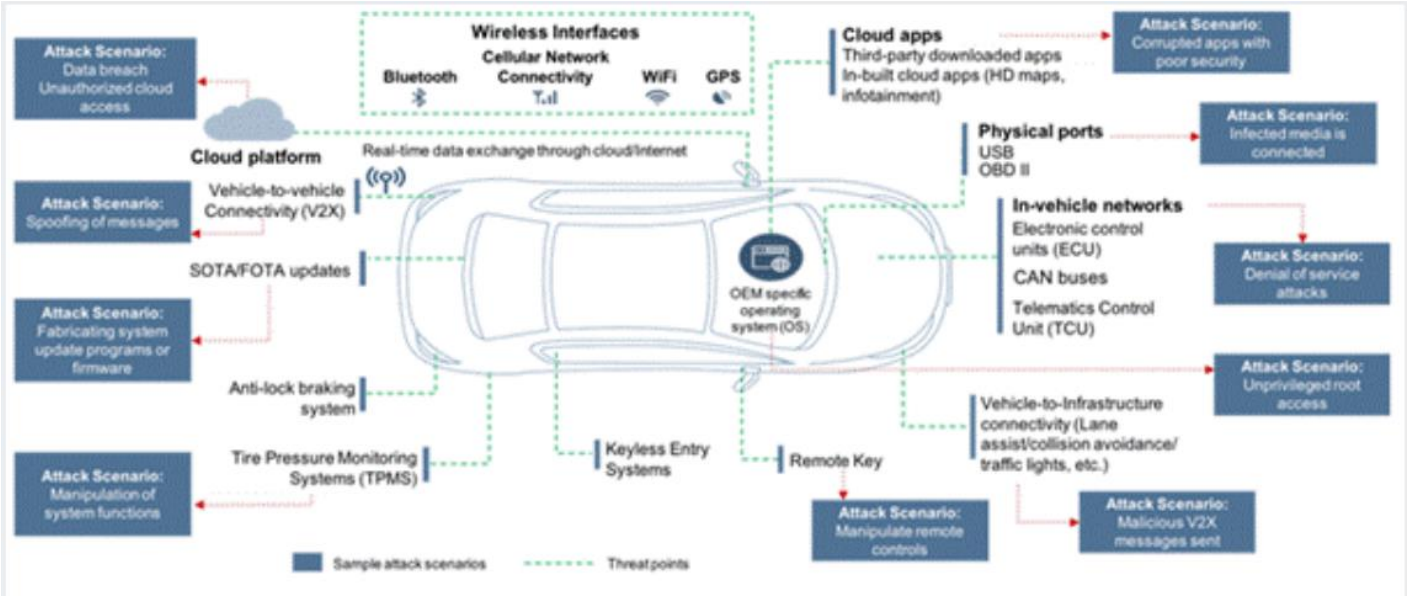

Figure1. Key Attack Surfaces in SDVs

3. Cybersecurity Countermeasures in SDVs

As SDVs evolve to become more connected and software-intensive, securing their digital ecosystem requires a layered approach encompassing both proactive and reactive mechanisms. Cybersecurity strategies must be integrated at all levels of the vehicle system from in-vehicle networks and ECUs to cloud platforms and V2X infrastructure. The countermeasures below are aligned with international best practices and real-world deployments.

3.1. Security-by-Design Principles

Modern vehicle platforms are adopting Security-by-Design (SbD) to embed protection mechanisms from the earliest stages of architecture definition. This includes secure boot processes, trusted execution environments (TEEs), and enforcing the principle of least privilege across embedded modules. Secure Boot & Firmware Validation ensures that only authenticated software runs on ECUs, utilizing cryptographic signatures. Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs) protect cryptographic keys and secure execution. SbD frameworks emphasize threat modeling using standards like ISO/SAE 21434 [1][3].

3.2. Intrusion Detection and Prevention Systems (IDPS)

Given the dynamic nature of threats in connected vehicles, real-time detection is crucial. Automotive IDPS architectures include signature-based detection for known attacks, and anomaly-based detection using AI/ML models to identify deviations (e.g., CAN message anomalies). Host and network-based sensors gather telemetry. Federated learning enables fleet-wide detection without sharing raw data [2][5].

3.3. Secure Over-the-Air (OTA) Updates

OTA mechanisms ensure ongoing protection. These use encrypted channels (TLS), digital signatures for firmware, fail-safe recovery for interruptions, access control, and audit logging. Redundant memory and dual partitioning enable rollback in the event of failed or compromised updates [4][6].

3.4. Secure Vehicle-to-Everything (V2X) Communication

V2X introduces unique risks. SCMS (in U.S.) and ETSI ITS (Europe) define frameworks for authenticated, pseudonymized messages. Short-lived certificates, frequent key rotation, and authentication protocols like TESLA mitigate spoofing and tracking [7][8].

3.5. Cloud and Edge Security

SDV services rely on cloud backends for navigation, analytics, and personalization. These adopt Zero Trust principles, API gateways, cloud-native firewalls, SIEM tools, and techniques like differential privacy and homomorphic encryption. Distributed data centers ensure resilience [2][4].

3.6. AI-driven Predictive Defense

AI techniques are utilized to model ECU communications, detect sensor spoofing, and simulate the behavior of attackers. Graph-based models, GANs, and time-series analysis identify unknown threats. Federated and online learning models enhance detection [5][10].

3.7. Regulatory Compliance and Risk Governance

OEMs now comply with regulations like UNECE WP.29 (R155, R156) and ISO/SAE 21434. Governance practices include risk classification, penetration testing, incident response, supplier management, and deployment of AutoCSOCs. CPSOs are being appointed across OEMs to oversee security [3][9].

4. Future Research Directions

Despite advances in automotive cybersecurity, SDVs still face emerging challenges that demand further exploration. The following areas are critical for future research:

4.1. Quantum-Resistant Cryptography

As quantum computing evolves, traditional cryptographic algorithms like RSA and ECC could become vulnerable. Post-quantum cryptographic schemes (e.g., lattice-based, code-based cryptography) are being explored for automotive use, but need optimization for low-power, embedded ECUs [1][2].

4.2. Secure Federated Learning for Vehicle Fleets

Federated learning allows training of AI models across distributed fleets without sharing raw data. However, model poisoning and performance degradation due to heterogeneous data remain challenges. Robust aggregation algorithms and cross-OEM collaboration are essential [5][10].

4.3. Integration of Digital Twin-Based Security Testing

Digital twins simulate real vehicle systems to test and validate security. Future implementations must combine real-time telemetry, behavioral modeling, and attack simulation for a complete lifecycle security assessment [4][6].

4.4. Securing AI-Driven Vehicle Functions

Adversarial machine learning introduces threats to perception and control systems. Data poisoning, evasion attacks, and model inversion must be mitigated via certifiable AI, explainability (XAI), and runtime attestation [5][9].

4.5. Cross-Domain Standardization and Cybersecurity Metrics

While ISO/SAE 21434 provides a foundational structure, quantitative metrics and cross-domain taxonomies are required. Integration with 5G, IT, and IoT standards is key for interoperable SDV ecosystems [3][9].

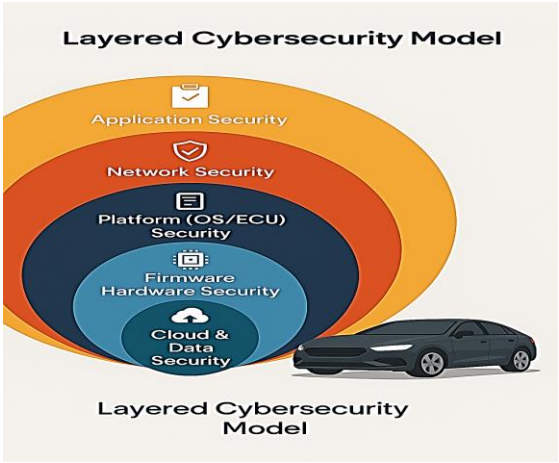

Figure 2. Layered Cybersecurity Model for SDVs

5. Conclusion

Software-Defined Vehicles mark a paradigm shift in mobility, where digital intelligence and connectivity are central to vehicle value. However, with this transformation comes an expanded threat landscape. This paper has outlined the evolution of threats in SDVs from traditional in-vehicle exploits to sophisticated cloud and V2X-based attacks and presented a comprehensive set of countermeasures aligned with state-of-the-art practices and standards.Building secure SDVs requires a multi-layered approach: embedding security at design-time, leveraging real-time detection, ensuring resilient communication, and preparing for future risks through AI, quantum threats, and evolving architectures. Continued research, standardization, and cross-industry collaboration will be critical to building trust in next-generation vehicle platforms.

References

[1] R. S. Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, “In-Vehicle Communication Cyber Security: Challenges and Solutions,” Sensors, vol. 22, 2022.
[2] T. Guan, Y. Han, N. Kang, et al., “An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles,” Sustainability, vol. 14, no. 21, 2022.
[3] M. D. Mwanje, O. Kaiwartya, et al., “Cybersecurity Analysis of Connected Vehicles,” IET Intelligent Transport Systems, vol. 18, no. 1, pp. 10–22, 2024.
[4] VicOne Automotive Threat Intelligence Team, “The State of SDV Cybersecurity,” Whitepaper, 2024.
[5] S. Sureddi, “The Use and Impact of AI in Enhancing Automotive Cyber Protection,” J. Artif Intell Mach Learn & Data Sci, Nov. 2024.
[6] S. Sureddi, “Mitigating Escalating Cybersecurity Threats in Advanced Automotive Systems,” Automotive IQ, Sept. 2024.
[7] S. Sureddi, “Enhancing Cybersecurity in Vehicle Networks,” Automotive IQ, Nov. 2022.

[8] S. Sureddi, “Advancements in V2X Security,” Automotive IQ, Oct. 2023.
[9] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-Physical Systems Security—A Survey,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, Dec. 2017
[10] K. Mahbub, et al., “A Survey of Machine Learning for Secure SDVs,” IEEE Access, vol. 10, pp. 6523–6540, 2022.
[11] K. R. Kotte, L. Thammareddi, D. Kodi, V. R. Anumolu, A. K. K and S. Joshi, "Integration of Process Optimization and Automation: A Way to AI Powered Digital Transformation," *2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT)*, Bhimtal, Nainital, India, 2025, pp. 1133-1138, doi: 10.1109/CE2CT64011.2025.10939966.
[12] B. C. C. Marella, G. C. Vegineni, S. Addanki, E. Ellahi, A. K. K and R. Mandal, "A Comparative Analysis of Artificial Intelligence and Business Intelligence Using Big Data Analytics," *2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT)*, Bhimtal, Nainital, India, 2025, pp. 1139-1144, doi: 10.1109/CE2CT64011.2025.10939850.
[13] Thirunagalingam, A. (2024). Transforming real-time data processing: the impact of AutoML on dynamic data pipelines. Available at SSRN 5047601.
[14] V. M. Aragani and P. K. Maroju, "Future of blue-green cities emerging trends and innovations in iCloud infrastructure," in Advances in Public Policy and Administration, pp. 223–244, IGI Global, USA, 2024.
[15] Settibathini, V. S., Kothuru, S. K., Vadlamudi, A. K., Thammreddi, L., & Rangineni, S. (2023). Strategic analysis review of data analytics with the help of artificial intelligence. International Journal of Advances in Engineering Research, 26, 1-10.
[16] Sehrawat, S. K. (2023). The role of artificial intelligence in ERP automation: state-of-the-art and future directions. *Trans Latest Trends Artif Intell*, *4*(4).
[17] B. C. C. Marella, “Data Synergy: Architecting Solutions for Growth and Innovation,” International Journal of Innovative Research in Computer and Communication Engineering, vol. 11, no. 9, pp. 10551–10560, Sep. 2023.
[18] Kommineni, M. "Explore Knowledge Representation, Reasoning, and Planning Techniques for Building Robust and Efficient Intelligent Systems." International Journal of Inventions in Engineering & Science Technology 7.2 (2021): 105- 114.
[19] Naga Surya Teja Thallam, 2024/12/30, AI-Powered Cybersecurity: How Machine Learning is Redefining Threat Detection and Prevention, International Journal of Scientific research in Engineering and Management, 8(12).
[20] Reddy, R. R. P. (2024). Enhancing Endpoint Security through Collaborative Zero-Trust Integration: A Multi-Agent Approach. *International Journal of Computer Trends and Technology*, *72*(8), 86-90.
[21] Varinder Kumar Sharma - Zero Trust Architecture for 5G Networks - International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences (IJIRMPS) Volume 12, Issue 6, November-December 2024. DOI: https://doi.org/10.37082/IJIRMPS.v12.i6.232707
[22] Amrish Solanki1, ShrikaaJadiga, AI Applications for Improving Transportation and Logistics Operations, International Journal ofINTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING, International Journal of Intelligent Systems and Applications in EngineeringIJISAE, 2024, 12(3), 2607–2617.