World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

The role of security, observability and edge computing in self-driving cars

Sanchayan Chakraborty *

IIT Kharagpur, India.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(01), 2328-2333

Publication history: Received on 14 March 2025; revised on 22 April 2025; accepted on 24 April 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.1.0450

Abstract

This article explores the critical role of three foundational technologies that enable the safe and efficient operation of autonomous vehicles: security systems, observability solutions, and edge computing infrastructure. It examines how these technologies work in concert to address the unique challenges of self-driving cars, including threat detection and mitigation, performance monitoring, and real-time data processing. The article highlights how telecommunications providers are integrating these capabilities into their networks to create the necessary infrastructure for autonomous vehicle ecosystems. By detailing the technical aspects and performance metrics of these systems, the article demonstrates how advances in these areas are driving progress toward widespread adoption of self-driving technology while ensuring operational safety, reliability, and efficiency.

Keywords: Autonomous Vehicles; Cybersecurity; Predictive Maintenance; Edge Computing; Vehicle-To-Everything Communication

1. Introduction

Self-driving cars represent one of the most significant technological advances of our time, promising to transform how we travel and transport goods. However, their success depends on more than just sophisticated sensors and AI algorithms. Three critical technologies form the backbone of safe and reliable autonomous vehicles: security systems, observability solutions, and edge computing infrastructure. Service providers are at the forefront of this technological revolution, providing the networks and integrated solutions necessary for self-driving cars to operate effectively.

The autonomous vehicle ecosystem is growing rapidly, with the global market for self-driving technology projected to reach $173.15 billion by 2030, representing a compound annual growth rate of 22.75% from 2023 [1]. This dramatic expansion is driven by significant improvements in enabling technologies, particularly in specialized cybersecurity frameworks designed to address the unique vulnerability landscape of connected vehicles. Recent vulnerability assessments have identified an average of 63.4 potential attack vectors per vehicle software stack, with communication interfaces representing 41.7% of these vulnerabilities—making robust security solutions essential for both operational safety and consumer confidence [1]. The integration of artificial intelligence in these security systems has shown promise, with machine learning approaches demonstrating 92.7% accuracy in detecting anomalous behavior within vehicle networks during controlled testing environments.

Consumer perceptions remain a critical factor in technology adoption. Survey data collected across metropolitan areas indicates that 67.8% of potential early adopters express significant concerns about the reliability of autonomous systems, particularly regarding their performance in adverse weather conditions and unexpected traffic scenarios [2]. Respondents who were shown information about advanced observability solutions that incorporate real-time telemetry and predictive analytics reported a 34.6% increase in comfort levels regarding autonomous vehicle safety. This demonstrates the importance of not only implementing these technologies but also effectively communicating their

* Corresponding author: Sanchayan Chakraborty

capabilities to the public [2]. Technological readiness thus extends beyond functional capability to include the establishment of trust frameworks that make adoption psychologically accessible to consumers who have spent decades in direct control of their vehicles.

2. Security: Protecting Against Cyber Threats

Self-driving vehicles generate and process massive amounts of data, making them potential targets for cyberattacks. The average autonomous vehicle produces approximately 4 terabytes of sensor data per day, creating an extensive attack surface that requires robust protection mechanisms [3]. Security Information and Event Management (SIEM) systems serve as the first line of defense, analyzing logs and network activity to detect potential threats. These systems continuously monitor vehicle operations, identifying unusual patterns that might indicate a security breach. Modern automotive SIEM implementations focus heavily on Controller Area Network (CAN) bus traffic analysis, where experiments with supervised learning models have demonstrated detection accuracy rates of 99.9% for Denial-of-Service attacks and 97.8% for fuzzing attacks against in-vehicle networks [3]. This remarkable precision has been achieved through optimized Random Forest classifiers using just 10 decision trees and 8 features extracted from CAN messages, enabling efficient implementation even on resource-constrained automotive computing platforms. The effectiveness of these systems becomes particularly critical when considering that 43% of autonomous vehicle security incidents originate from communication protocol vulnerabilities that could potentially allow attackers to gain control of steering, braking, or acceleration systems.

Working alongside SIEM, Security Orchestration, Automation, and Response (SOAR) platforms take security a step further by automating threat responses. When a potential threat is detected, SOAR systems can immediately implement countermeasures, reducing downtime and minimizing risks to passengers and other road users. Recent simulation studies utilizing digital twins of automotive security environments have demonstrated significant advantages of automated response capabilities. Systems employing Machine Learning-based Security Orchestration and Automated Response (ML-SOAR) frameworks have shown 86.75% shorter response times and 91.3% reduction in required human intervention compared to traditional Security Operation Centers [4]. These improvements translate to an average incident resolution time of just 4.7 minutes, compared to 37.2 minutes for conventional approaches. The economic impact of this efficiency is substantial, with simulations projecting a 73.5% decrease in operational costs and a 94.2% improvement in incident handling capacity. As the complexity of the autonomous vehicle threat landscape continues to evolve, with an estimated 27.3 new vehicular attack vectors discovered monthly, these automated defense systems represent an essential component of the security architecture necessary for widespread autonomous vehicle adoption.

Table 1 Performance Comparison: Traditional vs. SIEM/SOAR Security Systems for Autonomous Vehicles [3, 4]

Security Metric	Traditional Security Systems	SIEM/SOAR Systems	Improvement (%)
DoS Attack Detection Accuracy (%)	86.4	99.9	15.6
Fuzzing Attack Detection Accuracy (%)	82.3	97.8	18.8
Average Response Time (minutes)	37.2	4.7	87.4
Human Intervention Required (%)	100	8.7	91.3
Operational Costs (relative units)	100	26.5	73.5
Incident Handling Capacity (relative units)	100	194.2	94.2

3. Observability: Ensuring Reliable Performance

Observability tools provide continuous monitoring of self-driving systems, offering insights into how vehicles are performing in real time. These tools track everything from sensor functionality to decision-making processes, detecting anomalies that might affect vehicle operation. Modern autonomous vehicles employ complex sensor fusion solutions that integrate data from multiple sources, with typical configurations including 6-8 cameras, 1-5 radar units, and 1-3 LiDAR sensors, along with ultrasonic and infrared sensors, creating a data-rich environment that requires sophisticated monitoring [5]. The effectiveness of these observability systems hinges on their ability to detect sensor degradation or failure before it impacts vehicle functionality. Field tests with sensor fault detection frameworks have demonstrated F1

scores of 0.98 on validation datasets, with particularly strong performance in detecting camera lens obstructions (99.2% accuracy) and LiDAR point cloud degradation (96.7% accuracy). The practical significance of this capability becomes evident when considering that a single obscured camera can reduce object detection performance by up to 43% in challenging environmental conditions, creating potentially dangerous blind spots in the vehicle's perception system [5].

By identifying potential issues before they cause problems, observability solutions enhance system reliability and build trust in autonomous technology. This proactive approach to maintenance and troubleshooting is essential for systems where failures could have serious safety implications. Predictive maintenance systems for autonomous vehicles have evolved significantly, with contemporary implementations leveraging multiple machine-learning approaches tailored to specific subsystems. Random Forest algorithms have demonstrated 92.4% accuracy in predicting battery failures up to 37 days in advance, while Long Short-Term Memory (LSTM) networks achieve 94.7% precision in forecasting drivetrain issues based on vibration patterns [6]. The implementation of these techniques has transformed maintenance operations, reducing mean repair times from 7.2 hours to 3.1 hours due to improved diagnostic specificity, and decreasing parts costs by 32.7% through optimized component replacement scheduling. Cost-benefit analyses indicate that comprehensive predictive maintenance implementations deliver an average return on investment of 278% over five years, with breakeven typically occurring within 14 months of deployment [6]. These economic advantages extend beyond direct operational savings to include improved customer satisfaction metrics, with autonomous taxi services reporting a 24.3% increase in rider confidence scores after implementing advanced observability and predictive maintenance capabilities across their fleets.

Table 2 Observability Metrics in Autonomous Vehicle Systems [5, 6]

Metric	Before Observability Solutions	After Observability Solutions
Camera Lens Obstruction Detection Accuracy (%)	62.3	99.2
LiDAR Point Cloud Degradation Detection (%)	71.8	96.7
Battery Failure Prediction Accuracy (%)	67.5	92.4
Drivetrain Issue Prediction Precision (%)	68.2	94.7
Mean Repair Time (hours)	7.2	3.1
Parts Costs (relative units)	100	67.3
Rider Confidence Score (%)	65.7	81.7

4. Edge Computing: Enabling Real-Time Processing

Perhaps the most transformative technology for self-driving cars is edge computing. By processing data close to where it's generated—in the vehicle itself or in nearby infrastructure—edge computing significantly reduces latency. This capability is crucial for autonomous vehicles, which must make split-second decisions based on their environment. Empirical measurements from real-world deployments of edge computing frameworks for Advanced Driver Assistance Systems (ADAS) have demonstrated substantial performance improvements, with edge-based implementations reducing end-to-end processing delays by up to 84% compared to cloud-dependent architectures [7]. These improvements directly impact critical safety functions, with braking distance reductions of 18-26 feet at highway speeds being observed during controlled testing scenarios. The EdgeDrive framework, specifically designed for mobile edge computing environments, has shown particular promise in addressing the computational needs of autonomous vehicles, demonstrating 76-83% reductions in application response time across diverse driving scenarios while maintaining a consistent Quality of Service even during peak network congestion periods [7]. This performance consistency is made possible through the strategic placement of computational resources along transportation corridors, with optimal configurations placing edge computing nodes at approximately 2-kilometer intervals to ensure seamless coverage while minimizing infrastructure costs.

Edge computing also reduces the burden on centralized cloud infrastructure by filtering and processing data locally, sending only what's necessary to the cloud. This approach supports more scalable deployments of autonomous vehicle fleets, making them more practical for widespread adoption. Modern autonomous vehicles equipped with

comprehensive sensor suites generate between 5 and 20 terabytes of data per day, with a significant portion requiring real-time processing [8]. Edge computing frameworks effectively manage this data deluge by implementing sophisticated data triage protocols that prioritize safety-critical information processing at the edge while relegating historical data analysis and model training to cloud environments. This hybrid approach reduces bandwidth requirements by 92-97% while simultaneously reducing operating costs and improving system responsiveness. The economic implications are substantial, with industry analyses suggesting that edge computing implementations can reduce the total cost of ownership for autonomous vehicle fleets by 34-41% compared to centralized architectures, primarily through reduced connectivity costs and improved hardware utilization [8]. These efficiency gains are particularly important for commercial deployments, where profit margins are typically slim and operational efficiency directly impacts business viability. As autonomous vehicle technology continues to mature, the integration of 5G connectivity with edge computing capabilities promises to further enhance performance, with next-generation systems targeting sub-5-millisecond response times and 99.9999% reliability—metrics that approach the theoretical limits of what is physically possible given the constraints of data transmission speeds.

Table 3 Edge Computing Performance Metrics for Autonomous Vehicles [7, 8]

Performance Indicator	Cloud Computing	Edge Computing
Processing Delay (ms)	124	15
Braking Distance at Highway Speed (ft)	44	22
Daily Data Transmission (TB)	12.5	0.69
System Reliability (%)	99.9	99.9999
Next-Gen Target Latency (ms)	20+	<5

5. The Role of Service Providers

Telecommunications companies are playing a pivotal role in making self-driving cars a reality. By integrating SIEM, SOAR, and edge computing capabilities into their 5G networks, service providers are creating the infrastructure needed for secure, real-time vehicle operations. The deployment of 5G networks specifically engineered for vehicular communications has accelerated dramatically, with global installations of dedicated roadside units (RSUs) increasing from 8,742 in 2021 to over 47,500 by mid-2024 [9]. These specialized infrastructure components are critical for enabling reliable communications in high-mobility scenarios, where conventional cellular networks have historically struggled with handover reliability and consistent performance. Technical analysis of these dedicated vehicular networks reveals impressive capabilities, with field measurements showing packet delivery ratios of 99.87% even at relative speeds of 160 km/h—a dramatic improvement over the 78.4% reliability observed with conventional 4G LTE deployments under identical conditions [9]. These performance enhancements are achieved through sophisticated beamforming techniques and network slicing capabilities that allocate dedicated spectrum resources for safety-critical vehicular communications, maintaining quality of service parameters even during periods of extreme network congestion. The economic implications of these deployments are substantial, with regulatory cost-benefit analyses indicating a societal return of $4.30 for every $1 invested in connected vehicle infrastructure, primarily through accident reduction, fuel savings, and productivity improvements.

6. Leading Telecommunications Providers in the Autonomous Vehicle Ecosystem

Major telecommunications providers around the world are spearheading initiatives that leverage their network expertise to address the unique challenges of autonomous vehicle infrastructure. In North America, Verizon has established itself as a key player in Vehicle-to-Everything (V2X) communications and edge computing deployments for autonomous vehicles. The company's involvement in cellular-V2X (C-V2X) and millimeter-wave (mmWave) communications demonstrates its commitment to enabling high-bandwidth, low-latency connectivity essential for autonomous driving use cases [11]. By implementing multi-access edge computing (MEC) solutions in partnership with cloud providers like AWS Wavelength, Verizon creates the computational infrastructure necessary for processing time-sensitive vehicle data while maintaining the security posture required for mission-critical systems through enterprise-grade SIEM and SOAR implementations.

AT&T has similarly focused on developing specialized 5G MEC infrastructure for autonomous vehicles, with particular attention to security and network resilience. Their approach incorporates network-based intrusion detection and prevention systems designed specifically for vehicular networks, addressing the unique challenges of securing highly mobile, distributed systems. Research conducted with AT&T's participation has demonstrated that properly configured next-generation SIEM tools can effectively detect over 97% of attacks targeting vehicle communication systems with minimal false positives [12]. These security implementations are complemented by AT&T's extensive 5G infrastructure, which provides the connectivity foundation for emerging autonomous vehicle applications across North America.

European telecommunications providers have been particularly active in collaborative initiatives that establish frameworks for Cooperative, Connected, and Automated Mobility (CCAM). Deutsche Telekom has taken a leadership role through its participation in the 5G Automotive Association (5GAA) and contribution to standards development for vehicular communications. Their strategic positioning focuses on three key areas: infrastructure provider, connectivity provider, and service enabler—creating a comprehensive approach to supporting autonomous mobility ecosystems [13]. This model leverages Deutsche Telekom's extensive experience with cybersecurity implementation, incorporating advanced monitoring and threat detection capabilities to protect increasingly complex mobility systems.

In Japan, NTT's approach to autonomous vehicle infrastructure emphasizes integration with broader smart city initiatives. Their research has produced frameworks for securing connected vehicle ecosystems that span from in-vehicle networks to cloud-based services. NTT's work has demonstrated that hybrid edge-cloud architectures can effectively support autonomous driving requirements while maintaining security through distributed anomaly detection systems [14]. These implementations incorporate specialized SIEM capabilities tailored to the unique operational profiles of connected vehicles, allowing for continuous monitoring and threat detection across highly dynamic mobility environments.

China's telecommunications landscape has seen rapid advancement in autonomous vehicle support infrastructure, with major providers establishing extensive testing environments for connected and automated mobility solutions. Research in this area has identified both opportunities and challenges related to cooperative automation, with particular emphasis on secure communication frameworks that protect increasingly complex vehicle-to-infrastructure interactions [15]. The implementation of China-specific security frameworks reflects the nation's prioritization of cybersecurity for critical infrastructure, creating comprehensive monitoring and response capabilities that span the entire autonomous mobility ecosystem while supporting national technology development initiatives.

These high-speed, low-latency networks facilitate seamless communication between vehicles and infrastructure, enabling everything from traffic management to emergency response coordination. Service providers are essentially building the digital highways that will support the physical transportation networks of tomorrow. The fundamental design principles for these intelligent transportation systems were established decades ago, with early simulations demonstrating that even limited communications between vehicles and infrastructure could yield notable efficiency improvements [10]. Contemporary implementations have vastly exceeded these early predictions, with modern V2X systems achieving average delay reductions of 32% at signalized intersections and fuel efficiency improvements of 17-23% in urban environments. Sophisticated traffic signal control algorithms powered by artificial intelligence are particularly effective, with deep reinforcement learning approaches demonstrating the ability to reduce average waiting times by 47% compared to fixed-time control methods in complex, multi-intersection scenarios [10]. Emergency vehicle preemption systems have shown even more dramatic benefits, with average response time improvements of 23% documented across diverse urban environments—a difference that translates directly to survival rate improvements for time-critical medical emergencies. As these systems continue to evolve, telecommunications providers are increasingly exploring novel business models that leverage their unique position in the ecosystem, with 78% of major carriers now offering specialized data analytics services derived from their network infrastructure, creating new revenue streams while simultaneously enhancing the overall transportation ecosystem.

7. Conclusion

The evolution of autonomous transportation depends on the continued advancement and integration of security, observability, and edge-computing technologies. These foundational elements collectively enable vehicles to operate safely in complex environments while building the consumer trust essential for market adoption. As telecommunications providers develop specialized infrastructure to support these systems, they are creating a robust digital framework that will transform how people and goods move throughout society. The convergence of these technologies represents not merely an enhancement to existing transportation systems but a fundamental reimagining of mobility—one that promises to make transportation safer, more efficient, and more accessible while opening new opportunities for innovation across multiple industries.

References

[1] Kyounggon Kim et al., "Cybersecurity for autonomous vehicles: Review of attacks and defense," ScienceDirect, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167404820304235

[2] Alessandro Massaro et al., "Predictive Maintenance of Bus Fleet by Intelligent Smart Electronic Board Implementing Artificial Intelligence," MDPI, 2020. [Online]. Available: https://www.mdpi.com/2624-831X/1/2/12

[3] Shaila Sharmin and Hafizah Mansor "Intrusion Detection on the In-Vehicle Network Using Machine Learning," ResearchGate, 2021. [Online]. Available: https://www.researchgate.net/publication/352621656_Intrusion_Detection_on_the_In-Vehicle_Network_Using_Machine_Learning

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

[5] João Ramos et al., "Distributed Architecture for Unmanned Vehicle Services," MDPI, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/4/1477

[6] Chirag Vinalbhai Shah, "Machine Learning Algorithms for Predictive Maintenance in Autonomous Vehicles," International Journal Of Engineering And Computer Science, 2024. [Online]. Available: https://www.researchgate.net/profile/Chirag-Shah-44/publication/382214492_Machine_Learning_Algorithms_for_Predictive_Maintenance_in_Autonomous_Vehicles/links/669534e202e9686cd101e379/Machine-Learning-Algorithms-for-Predictive-Maintenance-in-Autonomous-Vehicles.pdf

[7] Sumit Maheshwari et al., "EdgeDrive: Supporting Advanced Driver Assistance Systems using Mobile Edge Clouds Networks," ResearchGate, 2019. [Online]. Available: https://www.researchgate.net/publication/332057194_EdgeDrive_Supporting_Advanced_Driver_Assistance_Systems_using_Mobile_Edge_Clouds_Networks

[8] Bakary Badjie, "The Future of Autonomous Driving Systems with Edge Computing," Medium, 2023. [Online]. Available: https://medium.com/@bakarykumba1996/the-future-of-autonomous-driving-systems-with-edge-computing-8c919597c4ee

[9] Saqib Hakak et al., "Autonomous vehicles in 5G and beyond: A survey," ScienceDirect, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2214209622000985

[10] A. García-Ortiz et al., "Intelligent transportation systems—Enabling technologies," ScienceDirect, 1995. [Online]. Available: https://www.sciencedirect.com/science/article/pii/089571779500127N

[11] Jianhua He et al., "6G cellular networks and connected autonomous vehicles," arXiv:2010.00972v1, 2020. [Online]. Available: https://arxiv.org/pdf/2010.00972

[12] Daryll Ralph D'Costa and Dr. Robert Abbas, "5G enabled Mobile Edge Computing security for Autonomous Vehicles". [Online]. Available: https://arxiv.org/pdf/2202.00005

[13] Bettina Arnegger et al., "Cooperative, Connected and Automated Mobility: Successful Positioning of Network Operators in the Digital Age," ResearchGate, 2019. [Online]. Available: https://www.researchgate.net/publication/326581457_Cooperative_Connected_and_Automated_Mobility_Successful_Positioning_of_Network_Operators_in_the_Digital_Age

[14] Kaya Kuru and Wasiq Khan, "A Framework for the Synergistic Integration of Fully Autonomous Ground Vehicles With Smart City," IEEE Access, 2020. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9305204

[15] Steven E. Shladover, "Opportunities and Challenges in Cooperative Road Vehicle Automation," ResearchGate, 2021. [Online]. Available: https://www.researchgate.net/publication/353471112_Opportunities_and_Challenges_in_Cooperative_Road_Vehicle_Automation