Autonomous Vehicles and Cloud Systems
A Review of Emerging Threats and Challenges

Shubham Bhosale
Department of Computer Applications
D. Y. Patil Institute of Masters of Computer Application and Management
Pune, India
shubhabhosale2017@gmail.com

Rupesh Patil
Department of Computer Applications
D. Y. Patil Institute of Masters of Computer Application and Management
Pune, India
rupeshpatil1572005@gmail.com

Devesh Vispute
Department of Computer Applications
D. Y. Patil Institute of Masters of Computer Application and Management
Pune, India
deveshvispute16@gmail.com

Akhilesh Bodwade
Department of Computer Applications
D. Y. Patil Institute of Masters of Computer Application and Management
Pune, India
akhileshbodwade528@gmail.com

Bhagyashree Patil
Department of Computer Applications
D. Y. Patil Institute of Masters of Computer Application and Management
Pune, India

Abstract - Autonomous vehicles are an emerging technology that combines Artificial Intelligence (AI), cloud computing, sensors, and communication networks to support intelligent transportation. Cloud systems play an important role in data storage, processing, monitoring, and software updates. However, the increasing connectivity of autonomous vehicles also introduces several cybersecurity risks.

This research presents a review of security threats and challenges associated with autonomous vehicles and cloud systems. It examines threats such as sensor spoofing, denial-of-service attacks, vehicle network manipulation, AI-based attacks, cloud vulnerabilities, and communication security issues. The study also reviews risk assessment techniques, including STRIDE, DREAD, and CVSS, along with security measures such as encryption, authentication, intrusion detection, and secure software updates.

The review highlights the importance of protecting vehicle systems, communication networks, and cloud infrastructure through a layered security approach. It also identifies areas requiring further research to improve the safety, reliability, and cybersecurity of autonomous transportation.

Keywords: Autonomous Vehicles, Cloud Computing, Cybersecurity, Artificial Intelligence, Security Threats, Risk Assessment.

Introduction

Autonomous vehicles use sensors such as cameras, LiDAR, radar and GPS, along with artificial intelligence, to understand their surroundings and make driving decisions. Cloud computing supports these vehicles by providing data storage, analytics, machine-learning services and remote software updates. Vehicles also communicate with other vehicles and infrastructure through Vehicle-to-Everything (V2X) networks.

However, connectivity creates cybersecurity risks. Threats include sensor spoofing, denial-of-service attacks, Controller Area Network (CAN) bus manipulation, adversarial machine-learning attacks and insecure cloud APIs. Security techniques such as encryption, authentication, intrusion detection, threat modelling and secure over-the-air updates can help protect these systems.

The main objective of this research is to study cloud security challenges in autonomous vehicles and review approaches for improving the security and reliability of cloud-integrated vehicle systems.

The specific objectives are:

To explain the role of cloud computing, IoT, AI and V2X communication in autonomous vehicle ecosystems.

To identify and describe major cybersecurity threats, including sensor spoofing, denial-of-service attacks, CAN bus manipulation, adversarial machine-learning attacks and cloud API vulnerabilities.

To examine how these threats may affect vehicle safety, data integrity, service availability and operational reliability.

To review threat-modelling and risk-assessment approaches, particularly STRIDE, DREAD and CVSS.

To study mitigation techniques such as secure communication, encryption, authentication, intrusion detection, blockchain-based verification and secure OTA updates.

To highlight security gaps and potential directions for future research in cloud-integrated autonomous vehicle systems Zero

This study helps explain why cybersecurity is important for cloud-connected vehicles. It summarizes key threats and review techniques such as secure connection, authentication, intrusion detection and secure software updates.

Literature Review

A. Relevance of Sources

The sources reviewed in the reference paper are relevant to the study because they examine cybersecurity challenges in autonomous vehicles and connected transportation systems. These vehicles depend on cloud computing, Internet of Things (IoT) technologies, artificial intelligence and communication networks. As a result, research on these technologies helps explain the security risks that may affect autonomous vehicle operations.

Biswas and Wang (2023) discuss the integration of IoT, edge intelligence, 5G and blockchain in autonomous vehicles, highlighting the importance of secure Vehicle-to-Everything (V2X) communication. Durlik et al. (2024) examine vulnerabilities across sensors, onboard computing, communication modules and cloud infrastructure. Sheik et al. (2023) discuss cloud-assisted monitoring for detecting abnormal behavior in connected networks. These sources are directly related to the research topic because they consider different parts of the vehicle-cloud ecosystem.

B. Coverage of Literature

The literature covers several important areas: V2X communication security, sensor spoofing, denial of service attack, CAN but attacks, adversarial machine learning and cloud API vulnerabilities. It also reviews threat-assessment methods such as STRIDE, DREAD and CVSS, along with mitigation techniques including secure communication, intrusion detection system, blockchain-based verification and secure over-the-aur updates.

C. Critical Analysis

The reviewed studies show that cybersecurity is an important concern throughout the autonomous vehicle ecosystem. Research on V2X communication emphasizes the need to protect messages exchanged between vehicles and infrastructure. Work on sensor security highlights that manipulated inputs can lead to incorrect environmental perception. Studies of cloud-assisted monitoring suggest that cloud resources can help analyze communication patterns and identify possible attacks.

The literature also indicates that threat-modelling frameworks can help organize security analysis and prioritize vulnerabilities. However, the threats described in the paper affect different system components, so one protective method is unlikely to address every possible attack. For example, securing communication alone does not necessarily prevent sensor spoofing or weaknesses in machine-learning models. Similarly, an intrusion detection system may identify suspicious activity, but other controls are still needed to protect data and software updates.

Overall, the source paper supports a layered approach in which several security measures complement one another. At the same time, the reviewed work does not establish that one specific combination of measures is universally best. Further evaluation is needed to understand how different controls work together under the performance and reliability requirements of autonomous vehicles.

D. Organization and Clarity

The reference paper presents the topic in a logical sequence. It begins with an introduction to autonomous vehicles and their dependence on cloud computing, IoT and V2X communication. It then reviews existing research before describing the main cybersecurity threats, threat-modelling frameworks, mitigation strategies and system security architecture.

This organization helps readers move from the background of the problem to the threats and possible responses. The comparison table in the literature review summarizes selected studies according to their focus and contributions, including IoT integration, autonomous-vehicle security, cloud monitoring, threat modelling, sensor security and data security. The later sections connect these themes with protective measures such as secure communication, intrusion detection and secure OTA updates.

Although the paper covers several technical areas, its section-based structure makes the subject easier to follow. For this proposal, the literature is organized around source relevance, coverage, critical analysis and the research gap so that the relationship between prior work and the present study is clear.

Research Gap

The reviewed literature identifies a variety of threats and discusses several methods for protecting autonomous vehicle systems. However, the source paper's conclusion calls for integrated security frameworks that combine AI-driven intrusion detection, blockchain authentication and secure communication protocols. This indicates that security should be considered across the complete vehicle-cloud environment rather than within individual components alone.

A research gap is the need to better understand how multiple security mechanisms can be combined to address threats across sensors, onboard networks, communication channels and cloud services. Another related issue is how to identify and prioritize vulnerabilities while maintaining the reliable operation required by autonomous vehicles. The reference paper reviews these issues but does not present an experimental evaluation of a new integrated security solution.

Therefore, this study will review existing literature to organize the main threats, compare the security approaches described by previous researchers and identify areas where further investigation may be useful. Particular attention will be given to layered security, threat modelling, intrusion detection, authentication and secure software updates

Problem Statement

The increasing use of autonomous vehicles has created new cybersecurity challenges due to their dependence on Artificial Intelligence, cloud computing, sensors, and connected communication networks. These technologies exchange and process large amounts of data, making autonomous vehicle systems vulnerable to various cyber threats. Attacks such as sensor spoofing, denial-of-service, unauthorized access, vehicle network manipulation, and cloud security breaches may affect the safety, reliability, and performance of these vehicles.

Existing security measures may not be sufficient to address all the risks arising from the integration of vehicle systems with cloud infrastructure. Therefore, it is important to identify the major security threats, understand their possible impact, and examine the available risk assessment and protection techniques.

This research aims to review the emerging cybersecurity threats and challenges in autonomous vehicles and cloud systems and explore possible security approaches to improve their safety, reliability, and protection against cyberattacks.

Research Methodology

The research follows a design-oriented and conceptual methodology made up of six steps.

1. Problem Identification

Autonomous vehicles depend on sensors, Artificial Intelligence, onboard networks, and cloud platforms to perform their operations. The connection between these technologies creates several cybersecurity risks. Threats such as sensor spoofing, denial-of-service attacks, CAN bus manipulation, and cloud security vulnerabilities may affect vehicle safety, data privacy, and system reliability. The main problem addressed in this research is understanding these security weaknesses and identifying suitable methods to reduce the associated risks.

.

2. Literature Review

Existing research on autonomous vehicles highlights the importance of cybersecurity in connected transportation systems. Previous studies have discussed attacks on vehicle sensors, communication networks, AI-based systems, and cloud infrastructure. The reviewed literature also explains security techniques such as encryption, authentication, intrusion detection, and secure software updates. This research brings these topics together to understand the overall security challenges in autonomous vehicle and cloud environments.

3. Security Requirement Identification

The study examines different cybersecurity threats and their possible effects on autonomous vehicle systems. Sensor spoofing may lead to incorrect environmental detection, while denial-of-service attacks can interrupt communication. CAN bus attacks may affect internal vehicle messages, and cloud vulnerabilities can expose sensitive information. Techniques such as STRIDE, DREAD, and CVSS are reviewed for understanding and assessing these risks. Suitable mitigation approaches include encryption, authentication, monitoring, and secure communication.

4. Framework Design

The proposed framework uses a layered cybersecurity approach to protect autonomous vehicles and cloud systems. It includes sensor, vehicle network, AI software, communication, cloud, and OTA update layers. Each layer uses security measures such as encryption, authentication, and intrusion detection. These measures help prevent cyberattacks, protect data, and ensure secure communication. The framework aims to improve the overall security and reliability of autonomous vehicles.Scenario-Based Evaluation

Different hypothetical situations are considered to understand how cybersecurity threats may affect autonomous vehicles.

Scenario 1 – Sensor Spoofing: Manipulated sensor information may cause an autonomous vehicle to incorrectly identify objects or road conditions.

Scenario 2 – Denial-of-Service Attack: Excessive malicious requests may interrupt communication between a vehicle and cloud services.

Scenario 3 – Cloud Security Attack: Unauthorized access to cloud APIs or storage may expose vehicle-related information.

Scenario 4 – CAN Bus Manipulation: Malicious messages within the vehicle network may affect communication between electronic components.

These scenarios are illustrative examples based on the threats discussed in existing literature. They were not tested on a real vehicle.

5. Evaluation

The identified threats and security techniques are examined through qualitative comparison of the available literature. STRIDE, DREAD, and CVSS are considered for understanding threat categories and risk severity. The review indicates that individual security measures cannot address every type of attack. A combination of authentication, encryption, intrusion detection, secure communication, and software verification is therefore important for improving overall system protection.

6. Proposed Zero Trust Framework

The study highlights the importance of a layered cybersecurity approach for autonomous vehicles and cloud systems. The framework considers different protection levels:

Sensor Layer: Sensor validation and data verification to reduce manipulation risks.

Vehicle Network Layer: Secure communication and monitoring to protect internal networks.

AI and Software Layer: Protection of AI models and application components against malicious inputs.

Communication Layer: Encryption and authentication for secure V2X communication.

Cloud Layer: Access control, secure APIs, data encryption, and continuous monitoring.

Update Layer: Digital verification and authentication of over-the-air software updates.

7. Expected Outcomes

The research is expected to provide a clear understanding of major cybersecurity threats affecting autonomous vehicles and cloud systems. It aims to:

Identify important security vulnerabilities in connected vehicle systems.

Explain the possible effects of cyberattacks on vehicle operations.

Understand the role of STRIDE, DREAD, and CVSS in risk assessment.

Review existing techniques for protecting vehicle and cloud infrastructure.

Highlight the importance of layered security mechanisms.

Identify areas that require further research and development.

8. Conclusion

This research reviews the emerging cybersecurity threats associated with autonomous vehicles and cloud computing. The study identifies vulnerabilities affecting sensors, onboard networks, AI systems, communication channels, and cloud infrastructure. It also examines different risk assessment methods and available security techniques. The findings suggest that protecting autonomous vehicles requires a coordinated approach involving multiple security layers. Strong authentication, encryption, intrusion detection, and secure software updates can contribute to improved system safety and reliability. Further research is needed to evaluate integrated security approaches under practical operating conditions.

Acknowledgment

S. Bhosale, R. Patil, D. Vispute, A. Bodwade thank their research guide, Asst. Prof. Bhagyashree Patil, for her valuable guidance, constructive feedback, and continuous encouragement throughout this research work. The authors also thank the Head and the faculty members of Dr. D. Y. Patil Institute of Master of Computer Applications and Management, Akurdi, Pune, for providing the academic environment and resources needed to complete this study.

References

[1] A. Cardenas and B. Thuraisingham, “Cybersecurity for Next-Generation Road Transportation: A Review,” *ACM Journal on Autonomous Transportation Systems*, vol. 3, no. 2, Art. no. 9, 2025. Available: https://doi.org/10.1145/3744352
[2] “Cybersecurity on Connected and Automated Transportation Systems: A Survey,” *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 1, pp. 1382–1401, 2024. Available: https://doi.org/10.1109/TIV.2023.3326736
[3] “A Survey of Cybersecurity Challenges and Mitigation Techniques for Connected and Autonomous Vehicles,” *IEEE Transactions on Intelligent Vehicles*, vol. 10, no. 10, pp. 4742–4757, 2025. Available: https://doi.org/10.1109/TIV.2024.3493938
[4] “Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense,” *Computers & Security*, vol. 103, Art. no. 102150, 2021. Available: https://doi.org/10.1016/j.cose.2020.102150
[5] “A Survey on Security Attacks and Defense Techniques for

Connected and Autonomous Vehicles," *Computers & Security*, vol. 109, Art. no. 102269, 2021. Available: https://doi.org/10.1016/j.cose.2021.102269
[6] "A Survey of Security and Privacy Issues in V2X Communication Systems," *ACM Computing Surveys*, vol. 55, no. 9, 2023. Available: https://doi.org/10.1145/3567474
[7] "Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies," *PMC*, 2024. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC11435732/
[8] [Reference details not provided.]
[9] "Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art," *IEEE Access*, vol. 10, pp. 108979–108996, 2022. Available: https://doi.org/10.1109/ACCESS.2022.3213843
[10] "Autonomous Driving Security: State of the Art and Challenges," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7572–7595, 2022. Available: https://doi.org/10.1109/JIOT.2021.3130054
[11] "A Systematic Survey of Attack Detection and Prevention in Connected and Autonomous Vehicles," *Vehicular Communications*, vol. 37, Art. no. 100515, 2022. Available: https://doi.org/10.1016/j.vehcom.2022.100515
[12] M. S. Sheikh, J. Liang, and W. Wang, "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey," *Wireless Communications and Mobile Computing*, vol. 2020, Art. no. 5129620, 2020. Available: https://doi.org/10.1155/2020/5129620
[13] "A Taxonomy and Survey of Edge Cloud Computing for Intelligent Transportation Systems and Connected Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 6206–6221, 2022. Available: https://doi.org/10.1109/TITS.2021.3084396
[14] R. Meneguette, "Vehicular Edge Computing: Architecture, Resource Management, Security, and Challenges," *ACM Computing Surveys*, vol. 55, no. 1, Art. no. 4, 2022. Available: https://doi.org/10.1145/3485129
[15] T. Yang, R. Sun, R. S. Rathore, and I. Baig, "Enhancing Cybersecurity and Privacy Protection for Cloud Computing-Assisted Vehicular Network of Autonomous Electric Vehicles: Applications of Machine Learning," *World Electric Vehicle Journal*, vol. 16, no. 1, Art. no. 14, 2025. Available: https://doi.org/10.3390/wevj16010014
[16] A. T. Sheik, C. Maple, G. Epiphaniou, and M. Dianati, "A Comprehensive Survey of Threats in Platooning—A Cloud-Assisted Connected and Autonomous Vehicle Application," *Information*, vol. 15, no. 1, Art. no. 14, 2024. Available: https://doi.org/10.3390/info15010014
[17] A. D. M. Ibrahum, M. Hussain, and J.-E. Hong, "Deep Learning Adversarial Attacks and Defenses in Autonomous Vehicles: A Systematic Literature Review from a Safety Perspective," *Artificial Intelligence Review*, 2024. Available: https://doi.org/10.1007/s10462-024-11014-8
[18] "Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models," *IEEE Open Journal of Vehicular Technology*, 2023. Available: https://doi.org/10.1109/OJVT.2023.3265363
[19] B. Badjie, J. Cecílio, and A. Casimiro, "Adversarial Attacks and Countermeasures on Image Classification-Based Deep Learning Models in Autonomous Driving Systems: A Systematic Review," *ACM Computing Surveys*, vol. 57, no. 1, Art. no. 20, 2024. Available: https://doi.org/10.1145/3691625
[20] "LiDAR in Connected and Autonomous Vehicles: Perception, Threat Model, and Defense," *IEEE Transactions on Intelligent Vehicles*, vol. 10, no. 11, pp. 5023–5041, 2025. Available: https://doi.org/10.1109/TIV.2024.3510787
[21] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A Survey on Vehicular Cloud Computing," *Journal of Network and Computer Applications*, 2013. Available: https://doi.org/10.1016/j.jnca.2013.08.004
[22] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, National Institute of Standards and Technology, 2011. Available: https://doi.org/10.6028/NIST.SP.800-145
[23] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," NIST Special Publication 800-144, National Institute of Standards and Technology, 2011. Available: https://doi.org/10.6028/NIST.SP.800-144
[24] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper 29, National Institute of Standards and Technology, 2024. Available: https://doi.org/10.6028/NIST.CSWP.29
[25] International Organization for Standardization and SAE International, *ISO/SAE 21434:2021—Road Vehicles: Cybersecurity Engineering*, 2021. Available: https://www.iso.org/standard/70918.html
[26] SAE International, *J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, 2016. Available: https://doi.org/10.4271/J3061_201601