ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue II, February 2025

Challenges of Securing Artificial Intelligence-Powered Systems from Cyber Threats: Case Study of Autonomous Vehicles

[1]Oluwatosin Ogunlade [2]Abimbola Ogunlade* [3]Mobolaji Tenibiaje.

[1]University of East London, UK

[2]Engineering Institute of Technology, Australia

[3]Bamidele Olumilua University of Education, Science and Technology Ikere Ekiti.

***Corresponding Author**

DOI : https://doi.org/10.51583/IJLTEMAS.2025.1402007

Received: 18 February 2025; Accepted: 22 February 2025; Published: 07 March 2025

Abstract: The integration of Artificial intelligence (AI) into various sectors, including transportation, has a significant impact on human endeavors, in addition to eco-friendly advantages. One of the most promising areas of AI-powered systems is the manufacture of Autonomous Vehicles (AVs). These self-driving cars, also known as driverless, are intelligent vehicles that can operate without human aid or support. AVs are equipped with sophisticated AI-powered technologies such as sensors, radars, Global Positioning System (GPS), and advanced algorithms that can transmit information and navigate the environment using analyzed data. These driverless cars have the potential of revolutionizing the transport sector by improving efficiency, reducing road accidents, improving flexibility, and decreasing congestion. However, AI in AV applications poses some risks and challenges associated with securing systems from cybersecurity threats and attacks. This paper explores the dangers and difficulties of securing AI systems from cyber threats, highlighting various detection and prevention mechanisms. The ethical and legal implications, including strategies to address these challenges proactively, are also discussed. It is believed that the challenges in the automotive industry can be mitigated through collaboration among stakeholders, manufacturers, researchers, IT professionals, and policymakers by implementing robust security measures, conducting regular vulnerability assessments, and leveraging the expertise of software security specialists. Collaboration between industry and cybersecurity professionals is essential to safeguarding public safety.

Keywords: Autonomous Vehicles, Artificial Intelligence, Transportation, Cyber Threats.

I. Introduction

The integration of Artificial Intelligence (AI) into various sectors, including transportation, has had a profound impact on human activities, offering efficiency, automation, and sustainability benefits. One of the most significant applications of AI is in Autonomous Vehicles (AVs), also known as self-driving or driverless cars. These vehicles operate without direct human assistance; these systems leverage sensors, radars, cameras, Global Positioning Systems (GPS), and advanced AI-driven algorithms to perceive and navigate their environment effortlessly (Scalas & Giacinto, 2019).

Autonomous vehicles have revolutionized the transportation industry by reducing road accidents, easing traffic congestion, which is considered human-induced, improving mobility, and enhancing energy efficiency (Kojchev et al., 2022; Wang et al., 2021). However, despite these benefits, AVs present serious cybersecurity concerns that could impact their functionality, safety, and public acceptance. As AI-powered transportation systems become increasingly connected, they also become more vulnerable to cyber threats, including remote hacking, data breaches, and system manipulation (Boddupalli et al., 2022; Khattak et al., 2021). A successful cyber-attack on an AV could compromise its control system, leading to severe accidents, privacy violations, and operational failures.

This research aims to analyze the risks and challenges of securing AI-powered autonomous vehicle systems from cyber threats and attacks. It explores various cybersecurity vulnerabilities, risk mitigation strategies, and best practices for enhancing the security of these intelligent transportation systems. Furthermore, the study highlights detection and prevention mechanisms and discusses the ethical and legal implications of securing AVs. It is believed that effective collaboration among stakeholders, manufacturers, researchers, IT professionals, and policymakers is crucial for addressing these challenges. By implementing robust security frameworks, regular vulnerability assessments, and adopting advanced AI security models, AVs can be safeguarded against evolving cyber threats, ensuring their safe and reliable integration into modern transportation ecosystems.

II. Background

The concept of Artificial Intelligence (AI) was first introduced in 1956 at a Dartmouth College conference, where researchers such as John McCarthy, Allen Newell, Herbert Simon, and Marvin Minsky explored the possibility of creating "thinking machines" capable of simulating human intelligence. AI is a branch of computer science that focuses on developing intelligent systems capable of performing tasks that typically require human cognition, such as decision-making, language processing, and pattern recognition.

Over the decades, AI has evolved into a powerful technology integrated into various aspects of daily life, including virtual assistants, social media algorithms, facial recognition, speech recognition, and autonomous systems. Its impact spans multiple industries, such as healthcare, finance, retail, and transportation. One of the most promising applications of AI is in Autonomous Vehicles (AVs), where AI-driven systems allow self-driving cars to perceive their surroundings, analyze data, and make real-time navigation decisions.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue II, February 2025

AI-powered AVs utilize a combination of machine learning, deep learning, and neural networks to process large amounts of data from sensors and cameras. This enables them to detect obstacles, recognize road signs, and predict the movement of pedestrians and other vehicles. These capabilities enhance driving safety, efficiency, and the overall road experience. However, the increasing dependence on AI in AVs also raises concerns regarding security, as cybercriminals can exploit vulnerabilities in AI-driven systems to manipulate vehicle controls, steal sensitive data, or disrupt operations.

The rapid development of AI-powered technologies underscores the need for robust security measures, ethical considerations, and regulatory frameworks to ensure their safe and reliable deployment. As AI continues to advance, ongoing research is essential to address cybersecurity threats and optimize its applications across various sectors, particularly in transportation.

Definition and Components of AI-Powered Autonomous Vehicles

Autonomous vehicles, or self-driving cars, are defined by their ability to function without human interference, utilizing AI procedures and sensors to observe the environment, make decisions, and navigate (Alrubaian et al., 2019). These vehicles rely on a combination of hardware and software components, including proximity sensors, cameras, GPS, radar, advanced automation systems, actuators, processors, algorithms, and communication systems. The integration of these technologies enables AVs to detect objects, navigate through traffic, and safely reach their destinations. Augmented reality further enhances the driving experience by displaying vital information to drivers in innovative ways.

Overview of AI-Powered Autonomous Vehicles

Autonomous Vehicles (AVs), also known as self-driving cars, have become a significant focus in the transportation sector due to advancements in Artificial Intelligence (AI). These vehicles integrate sophisticated technologies such as sensors, cameras, radars, and the Global Positioning System (GPS) to perceive and navigate their surroundings without human intervention (Alrubaian et al., 2019). Companies like Tesla, Google, and Mercedes-Benz are leading the charge in developing AVs, aiming to enhance road safety, reduce traffic congestion, and improve mobility for individuals with disabilities (Zamindar, 2022).

Potential Benefits and Challenges

The deployment of AVs presents numerous advantages, including enhanced road safety, reduced environmental impact, and optimized traffic flow. According to Sadiku et al. (2021), AI in AVs improves efficiency by automating driving decisions, thereby minimizing human errors related to fatigue, distraction, and impaired judgment. AVs can also predict mechanical failures and schedule proactive maintenance, reducing the likelihood of breakdowns (Atakishiyev et al., 2023).

Despite these benefits, AVs face substantial challenges, particularly in cybersecurity. The reliance on wireless networks and interconnected systems makes them vulnerable to cyber threats such as hacking, data breaches, and system manipulation (Aurangzeb et al., 2023). The lack of universal safety standards and regulatory frameworks further complicates the widespread adoption of AVs. Additionally, the high development and maintenance costs remain a barrier to large-scale implementation (Algarni & Thayananthan, 2022).

Overview of Existing Research on Cyber Threats to AVs

Cybersecurity threats in AVs have been well-documented, with researchers identifying multiple vulnerabilities in autonomous driving systems. One of the most notable incidents was the remote hacking of a Jeep Cherokee in 2015, where attackers exploited weaknesses in the vehicle's infotainment system to gain full control (Henze et al., 2018). Similarly, Greenberg (2018) documented the NotPetya cyberattack, which affected critical infrastructure, highlighting the potential risks to AV networks.

A study by Meissner (2019) identified key cyber threats to AVs, including GPS spoofing, malware injections, denial-of-service (DoS) attacks, and unauthorized remote access. These threats can compromise vehicle functionality, endanger passenger safety, and disrupt transportation systems. Radoglou-Grammatikis et al. (2018) emphasized that AVs' continuous reliance on over-the-air software updates (SOTA and FOTA) increases their exposure to cyber risks. Attackers can exploit these updates to introduce malicious code into AV systems.

Autonomous Vehicle Cybersecurity Risks and Challenges

The cybersecurity landscape for AVs is rapidly evolving, with new attack vectors emerging as technology advances. One major concern is data privacy, as AVs collect and process vast amounts of sensitive user information, including travel patterns, personal preferences, and biometric data (Savitha & Madhu, 2023). Unauthorized access to this data can lead to identity theft, financial fraud, and surveillance risks.

Another significant risk is sensor manipulation, where attackers interfere with AV sensors to distort environmental perception. Alrajeh & Prenosil (2019) demonstrated that hackers could alter LiDAR and camera readings, causing AVs to misinterpret road conditions and make hazardous driving decisions. Additionally, supply chain vulnerabilities pose a critical threat, as compromised hardware or software components from third-party vendors can introduce backdoors into AV systems (Kukkala et al., 2020).

Attack vector	Impact	Consequences
Vehicle's entertainment system	Hijack and locking of the in-vehicle entertainment.	The vehicle occupant was unable to turn on the entertainment system.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue II, February 2025

Control System	Hijack and misuse of the vehicle features such as the in-vehicle audio system and arbitrarily increasing the volume.	The distraction of the driver
Car locking system	Locking vehicle resulting in jack ware	Denial of access into the vehicle.
Externally connected devices	The unauthorized modification of vehicle files and access to connected devices.	Compromise of integrity of the car files and denial of service of user-brought-in devices connected to the car
Computational resources of the vehicle	Arbitrary consumption of computational resources (such as memory and CPU cycles)	Disruption of vehicle operations
Sensitive and private data compromise	Unauthorized access to personal and sensitive data of car users.	Theft of users' confidential data
Vehicle safety system	Disabling vehicle safety functions	Compromise of passenger safety
Compromised Connected Autonomous Vehicle (CAV)	Using a compromised vehicle to send misleading, false, and bogus data to other CAVs	Impersonation of AV, thereby leading to the exchange of compromised information.

Recommendations for Securing Autonomous Vehicle Systems

To mitigate cybersecurity risks, researchers and industry professionals have proposed several defensive strategies. McKeever et al. (2020) advocate for multi-layered security architectures that incorporate encryption, intrusion detection systems (IDS), and AI-based anomaly detection. The adoption of zero-trust security models, where every system interaction requires continuous authentication, is also recommended (Miettinen & Gasser, 2017).

Furthermore, regulatory bodies such as the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) have introduced standards like ISO/SAE 21434, which outlines cybersecurity requirements for AVs (Kshetri, 2018). Regular penetration testing, security audits, and collaboration between automotive manufacturers and cybersecurity experts are essential for strengthening AV defenses (Antonini et al., 2020).

The increasing reliance on Artificial Intelligence (AI) in Autonomous Vehicles (AVs) has introduced significant cybersecurity challenges, making it essential to develop robust security measures. A comprehensive security framework must incorporate multi-layered defenses, encryption technologies, regulatory compliance, and continuous monitoring to mitigate cyber threats effectively. Researchers and industry professionals have proposed various strategies to strengthen AV security and protect them from malicious actors.

1. Implement Cybersecurity-Conscious Design Techniques

One of the critical shortcomings in AV security is that cybersecurity is often treated as an afterthought rather than an integral part of the design process (Horowitz & Lucero, 2017; Khan et al., 2020) (Antonini et al., 2020). To address this issue, the security-by-design approach must be adopted, integrating security measures into the Software Development Lifecycle (SDL) from the early stages. A defense-in-depth model is also essential, ensuring that multiple layers of security mechanisms protect vehicle systems (Ansari et al., 2018; Kukkala et al., 2022).

2. Secure the Software and Hardware Stack

Modern AVs rely on Electronic Control Units (ECUs) to manage key functions such as steering, acceleration, and braking. These ECUs are attractive targets for cybercriminals, making it crucial to implement robust security measures (Ayres et al., 2021; Yousseef et al., 2024). One way to protect ECUs is through the use of Hardware Security Modules (HSMs) and Trusted Platform Modules (TPMs), which provide secure key storage and cryptographic capabilities (Henze et al., 2018).

Additionally, software-over-the-air (SOTA) and firmware-over-the-air (FOTA) updates should be implemented to ensure that AVs receive security patches regularly. While many manufacturers have adopted SOTA updates, FOTA is still underutilized, exposing AVs to vulnerabilities (Ayres et al., 2021; Catuogno & Galdi, 2023; Radoglou-Grammatikis et al., 2018). Ensuring that these updates are digitally signed and verified before installation will help prevent cybercriminals from injecting malicious code into AV systems (Kukkala et al., 2020).

3. Strengthen Communication Security

AVs rely heavily on wireless communication for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) interactions. However, these communication channels can be exploited by cybercriminals to intercept or manipulate data (Boddupalli et al., 2022). Researchers suggest using end-to-end encryption and authentication protocols such as Transport Layer Security (TLS) and Public Key Infrastructure (PKI) to secure AV communications (Miettinen & Gasser, 2017).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue II, February 2025

Another effective technique is intrusion detection and prevention systems (IDPS), which monitor network traffic and detect anomalies that could indicate a cyberattack (Meissner, 2019). Additionally, anomaly-based AI detection systems can identify and respond to unusual behavior in real time, minimizing the risk of AV hijacking (Savitha & Madhu, 2023).

4. Develop Industry-Wide Security Standards and Regulations

A significant challenge in AV cybersecurity is the lack of universal security regulations. Although ISO and SAE have introduced ISO/SAE 21434, which provides cybersecurity guidelines for AV manufacturers, there is still a need for globally standardized policies (Kshetri, 2018).

Governments and regulatory bodies must enforce strict compliance measures, including:

- Regular security audits and penetration testing for AV software (Alrajeh & Prenosil, 2019).
- Implementing real-time cybersecurity monitoring centers to track and respond to cyber threats targeting AV fleets (Algarni & Thayananthan, 2022).
- Establishing legal accountability for cybersecurity breaches to ensure manufacturers prioritize security investments (Atakishiyev et al., 2023).

5. Enhance Supply Chain Security

AVs are complex systems with components sourced from multiple third-party vendors. This supply chain dependency introduces significant cybersecurity risks, as attackers can exploit vulnerabilities in software or hardware supplied by external manufacturers (Greenberg, 2018). To mitigate these risks, companies should:

- Conduct rigorous security assessments of all suppliers.
- Require third-party vendors to comply with secure coding practices and software verification standards (Aurangzeb et al., 2023).
- Use blockchain technology for tracking the authenticity of AV components and preventing counterfeit parts from being introduced into the supply chain (Kukkala et al., 2020).

6. Leverage Artificial Intelligence for Threat Detection

AI-based security mechanisms can significantly improve AV cybersecurity by identifying suspicious behavior and potential cyberattacks in real-time. Machine learning algorithms can analyze large volumes of data and detect patterns indicative of an attack before it occurs (Meissner, 2019).

Deep learning-based security models can also help distinguish between legitimate and fraudulent firmware updates, ensuring that AVs do not install malicious software disguised as system patches (Radoglou-Grammatikis et al., 2018).

7. Conduct Regular Cybersecurity Training and Awareness Programs

Human error remains one of the most significant vulnerabilities in cybersecurity. Even with robust technical defenses, AV systems remain at risk if stakeholders—including manufacturers, software engineers, fleet operators, and end-users—are not adequately trained in cybersecurity best practices (McKeever et al., 2020).

Organizations should implement mandatory cybersecurity training for all personnel involved in AV development and maintenance. Awareness programs should also educate vehicle owners on best practices, such as using strong authentication measures and regularly updating their vehicle's software (Savitha & Madhu, 2023).

8. Establish Cybersecurity Incident Response Plans

Despite the best preventive measures, cyberattacks on AVs are inevitable. Therefore, manufacturers and regulatory agencies must develop incident response plans to minimize damage and ensure quick recovery from cyber incidents (Kshetri, 2018).

A robust incident response strategy should include:

- Real-time monitoring to detect cyber threats as they emerge.
- Automated rollback features that restore compromised AV software to its last secure state (Henze et al., 2018).
- Collaboration with law enforcement and cybersecurity agencies to track and neutralize cybercriminal activities (Aurangzeb et al., 2023).

Roadmap elements	Components
Cybersecurity-aware design practices	Defense-in-depth / multi-layered security
	Zero-trust security approach

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue II, February 2025

	Security requirements
Secure the software and hardware stack.	HSMs/TPMs
	SDLs
	SOTA/FOTA updates
New Standards and Regulations for	ISO/SAE 21434
Automotive Security and AI.	Rules and regulations
Intelligence on advanced threats	Penetrations tests
	Vulnerability assessments

Key elements in the cybersecurity roadmap for autonomous vehicles.

III. Research Methodology, Methods, and Ethical Considerations

Research Approach and Design

The research employs a case study approach to examine the risks and challenges of securing AI-powered Autonomous Vehicles (AVs) from cyber threats. A case study methodology provides an in-depth investigation of real-world cybersecurity incidents, vulnerabilities, and countermeasures in AV systems. This approach enables a comprehensive analysis of the problem while considering multiple perspectives from industry reports, academic literature, and existing security frameworks (McKeever et al., 2020).

The study is qualitative in nature, utilizing secondary data sources such as peer-reviewed journal articles, conference papers, technical reports, and cybersecurity threat analyses. These sources offer rich contextual insights into AV cybersecurity challenges and best practices for mitigating risks. (Meissner, 2019).

A structured content analysis method is applied to identify recurring cybersecurity themes, trends, and vulnerabilities in AV systems. This involves systematically reviewing academic and industry sources to extract relevant data on security risks, attack vectors, and proposed solutions (Kukkala et al., 2020).

Additionally, comparative analysis is used to evaluate different cybersecurity frameworks and regulations, such as ISO/SAE 21434, which outlines cybersecurity risk management for AVs (Kshetri, 2018). The study also references historical case studies of cyberattacks on AVs, such as the Jeep Cherokee hack (2015) and Tesla's system vulnerabilities, to highlight real-world security breaches and their implications (Greenberg, 2018).

Data Collection and Analysis

Since the study is non-experimental, data is obtained exclusively from secondary sources. The data collection process involves gathering cybersecurity reports, regulatory guidelines, research papers, and industry case studies (Alrajeh & Prenosil, 2019).

The data analysis phase follows a thematic approach, where relevant cybersecurity threats, countermeasures, and industry trends are identified and categorized (Radoglou-Grammatikis et al., 2018). Content from multiple sources is synthesized to highlight commonalities in AV cybersecurity risks and identify gaps in existing security solutions.

The key steps in the data analysis process include:

1. Identification of recurring cybersecurity threats (e.g., GPS spoofing, malware, sensor manipulation).
2. Categorization of cyber threats by severity and impact on AV operations (Savitha & Madhu, 2023).
3. Comparative evaluation of cybersecurity solutions (e.g., encryption, intrusion detection, AI-based anomaly detection) (Aurangzeb et al., 2023).
4. Analysis of regulatory compliance and security best practices across different AV manufacturers (Algarni & Thayananthan, 2022).

Limitations of the Adopted Research Approach

While the case study method provides valuable insights into AV cybersecurity risks, it has certain limitations. One major challenge is the lack of direct empirical data since the study relies on secondary sources. Unlike experimental research, this approach does not involve hands-on testing of AV security vulnerabilities (Meissner, 2019).

Another limitation is potential data bias in the sources used. Cybersecurity research is often influenced by industry perspectives, which may overemphasize certain risks while downplaying others (McKeever et al., 2020). To mitigate this issue, the study incorporates a diverse range of sources, including independent academic research, cybersecurity white papers, and regulatory reports.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue II, February 2025

Additionally, the rapidly evolving nature of AV cybersecurity threats means that findings may become outdated as new attack techniques emerge. Continuous monitoring and adaptation of cybersecurity frameworks are necessary to address these evolving challenges (Kukkala et al., 2020).

Ethical Considerations Relevant to the Research

Since this study involves secondary data analysis, ethical considerations focus on data integrity, source credibility, and responsible use of information (Kshetri, 2018). Key ethical principles guiding the research include:

1. Citation and Avoidance of Plagiarism

Proper attribution is given to all academic sources, industry reports, and regulatory guidelines referenced in the study (Alrajeh & Prenosil, 2019). This ensures compliance with academic integrity standards and prevents the misrepresentation of research findings.

2. Selection of Credible and Reliable Sources

The study prioritizes peer-reviewed journal articles, government reports, and cybersecurity standards over non-verified online sources. The credibility of data is assessed based on author qualifications, publication source, and citation frequency (Radoglou-Grammatikis et al., 2018).

3. Ethical Use of Findings

The research findings are used solely for academic purposes, with no intent to exploit or misrepresent data. Ethical handling of cybersecurity-related information is crucial to prevent misuse by malicious actors (Savitha & Madhu, 2023).

4. Data Privacy and Confidentiality

Although no personally identifiable information (PII) is used, the study adheres to data privacy standards, ensuring that all referenced materials comply with General Data Protection Regulation (GDPR) and other data protection laws (Algarni & Thayananthan, 2022).

5. Research Validity and Reliability

To ensure research validity, the study employs triangulation, where findings from multiple sources are cross-verified to enhance accuracy (Meissner, 2019). The study also maintains transparency in data collection by documenting the selection criteria for research materials (Kukkala et al., 2020).

Reliability is ensured by using standardized analysis methods, such as content analysis and comparative evaluation of cybersecurity frameworks (Aurangzeb et al., 2023). The findings are structured to allow replicability, enabling future researchers to build upon the study's insights.

IV. Conclusion

Artificial intelligence is advancing rapidly in the automotive industry as the backbone of self-driving vehicles. Securing AI-powered systems, particularly autonomous vehicles, from cyber threats is a complex and evolving challenge. This report highlights the risks associated with cybersecurity in autonomous vehicles and the various detection and prevention mechanisms researchers propose. Ethical and legal implications, industry initiatives, and best practices are also discussed. Further research and collaboration among academia, industry, and policymakers are crucial to address the evolving cybersecurity landscape and ensure the safe deployment of AI-powered systems in the transportation sector.

It is equally essential for stakeholders in the automotive industry, including manufacturers, researchers, policymakers, and cybersecurity professionals, to address these risks proactively. Implementing robust security measures, conducting regular vulnerability assessments, promoting secure software development practices, and fostering collaboration between industry and cybersecurity experts are crucial steps to mitigate these risks and ensure the safe and secure adoption of autonomous vehicles. Examples of how cybercriminals have already demonstrated their intent by exploiting several vulnerabilities in the automotive ecosystem's intelligent transport systems can be found with the development of technology and the use of innovative connected vehicles. We are going to see a massive increase in cyber attacks on them. In contrast to malware that may be present on people's computers and mobile devices, the vulnerabilities of AV software could pose far more danger.

References

1. Algarni, A., & Thayananthan, V. (2022). Autonomous vehicles: The cybersecurity vulnerabilities and countermeasures for big data communication (pp. 2–19).
2. Alrajeh, D., & Prenosil, V. (2019). Cybersecurity in autonomous vehicles: Trends and challenges. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES)* (pp. 1–10). IEEE.
3. Alrubaian, M., Abolhasan, M., & Ni, W. (2019). Securing connected autonomous vehicles: A survey. *IEEE Communications Surveys & Tutorials, 21*(1), 616–646.
4. Ansari, M. T. J., Pandey, D., & Alenezi, M. (2018). STORE: Security Threat Oriented Requirements Engineering Methodology. *Journal of King Saud University - Computer and Information Sciences, 34*(2), 191. https://doi.org/10.1016/j.jksuci.2018.12.005

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue II, February 2025

5. Antonini, M., Barenghi, A., & Pelosi, G. (2020). Security issues in autonomous driving: Threats and a survey of solutions. *ACM Transactions on Cyber-Physical Systems, 4*(1), 1–34.
6. Atakishiyev, S., Salameh, M., Yaoa, H., & Goebel, R. (2023). Explainable Artificial Intelligence for Autonomous Driving: A Comprehensive Overview and Field Guide for Future Research Directions (pp. 1–19).
7. Aurangzeb, S., Aleem, M., Khan, M. T., Anwar, H., & Siddique, M. S. (Year). Cybersecurity for autonomous vehicles against malware attacks in smart-cities (pp. 2–12).
8. Ayres, N., Deka, L., & Paluszczyszyn, D. (2021). Continuous automotive software updates through container image layers. *Electronics, 10*(6), 739. https://doi.org/10.3390/electronics10060739
9. Boddupalli, S., Rao, A. K., & Ray, S. (2022). Resilient cooperative adaptive cruise control for autonomous vehicles using machine learning. *IEEE Transactions on Intelligent Transportation Systems, 23*(9), 15655. https://doi.org/10.1109/tits.2022.3144599
10. Catuogno, L., & Galdi, C. (2023). Secure firmware update: Challenges and solutions. *Cryptography, 7*(2), 30. https://doi.org/10.3390/cryptography7020030
11. Greenberg, A. (2018, March 15). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
12. Henze, M., Popper, C., & Shabtai, A. (2018). Autonomous vehicles security: An overview. *IEEE Security & Privacy, 16*(1), 14–20. https://doi.org/10.1109/MSP.2018.2701161
13. Horowitz, B., & Lucero, D. S. (2017). System-aware cyber security: A systems engineering approach for enhancing cyber security. *Insight, 20*(3), 66. https://doi.org/10.1002/inst.12165
14. Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention, 148*, 105837. https://doi.org/10.1016/j.aap.2020.105837
15. Khattak, Z. H., Smith, B. L., & Fontaine, M. D. (2021). Impact of cyberattacks on safety and stability of connected and automated vehicle platoons under lane changes. *Accident Analysis & Prevention, 150*, 105861. https://doi.org/10.1016/j.aap.2020.105861
16. Kojchev, S., Hult, R., & Fredriksson, J. (2022). Optimization based coordination of autonomous vehicles in confined areas. In *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)* (p. 1957). https://doi.org/10.1109/itsc55140.2022.9922180
17. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.007
18. Kucuk, Y., & Yilmaz, E. (2019). A survey of cybersecurity challenges in intelligent transportation systems. *Computers & Electrical Engineering, 74*, 444–462.
19. Kukkala, V. K., Thiruloga, S. V., & Pasricha, S. (2020). Roadmap for cybersecurity in autonomous vehicles. *Colorado State University* (pp. 1–8).
20. Kukkala, V. K., Thiruloga, S. V., & Pasricha, S. (2022). Roadmap for cybersecurity in autonomous vehicles. *arXiv (Cornell University)*. https://doi.org/10.48550/arXiv.2201
21. McKeever, S., Kozlowski, D., & Venkateswaran, N. (2020). Cybersecurity in autonomous vehicles: A systematic review. *ACM Computing Surveys, 53*(6), 1–34.
22. Meissner, M. (2019). The future of autonomous vehicles and cybersecurity. *Journal of Cybersecurity, 5*(1), tyz002. https://doi.org/10.1093/cybsec/tyz002
23. Miettinen, M., & Gasser, L. (2017). Security and privacy challenges in industrial Internet of Things. *ACM Transactions on Internet Technology, 17*(3), 1–24.
24. Radoglou-Grammatikis, P., Sarigiannidis, P., Moscholios, I., & Obaidat, M. S. (2018). Cybersecurity for connected autonomous vehicles: Adversarial machine learning, threats, and countermeasures. *IEEE Communications Magazine, 56*(12), 95–101.
25. Sadiku, M. N. O., Musa, S. M., & Ajayi-Majebi, A. (2021). Artificial intelligence in autonomous vehicles. *International Journal of Trend in Scientific Research and Development (IJTSRD), 5*(2), 715–720.
26. Savitha, P. B., & Madhu, S. (2023). Cyber security issues in connected autonomous vehicle. *International Journal of Research Publication and Reviews, 4*(3), 929–936.
27. Scalas, M., & Giacinto, G. (2019). Automotive cybersecurity: Foundations for next-generation vehicles (p. 1). https://doi.org/10.1109/ictcs.2019.8923077
28. Wang, X., Lin, X., & Li, M. (2021). Aggregate modeling and equilibrium analysis of the crowdsourcing market for autonomous vehicles. *arXiv (Cornell University)*. https://doi.org/10.48550/arXiv.2102
29. Youssef, A., Satam, S., Latibari, B. S., Pacheco, J., Salehi, S., Hariri, S., & Satam, P. (2024). Autonomous vehicle security: A deep dive into threat modeling. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2412.15348
30. Zamindar, A. (2022). Artificial intelligence in self-driving cars research and innovation. *International Research Journal of Modernization in Engineering Technology and Science, 4*(3), 895–890.