# AI-Driven Security: Protecting Autonomous Vehicles from Cyber Threats and Hacking Risks

P.P.Joshi[1], A.M.Kale[2], S.R.Bodhani[3], M.D.Beke[4], D.G.Bawane[5], Shilpa.S.Parlikar[6]
[1,2,3,4,5]*Student, Department of MCA, MES'IMCC, Pune*
[6]*Associate Professor, Department of MCA, MES'IMCC, Pune*

**Abstract -** ***This research study looks into the cybersecurity threats posed by autonomous vehicles and explores using advanced artificial intelligence (AI) techniques as useful countermeasures against such a threat. Autonomous vehicles rely in significant part upon a highly complex system of sensors and actuators constantly interacting with software modules in making real-time driving decisions.***
***These components—spanning from LiDAR, radar, ultrasonic sensors, cameras, to GPS systems—form the vehicle's sensory spine. But with their susceptibility to deception, they also carry great threats. Malicious actors can, for instance, exploit sensor spoofing to introduce artificial environmental data, which would be part of navigation calculation errors, obstacle detection, or lane positioning. Actuators, in charge of commanding steering, accelerating, braking, and other mechanical responses, may also be remotely seized by injections of illicit orders, leading to physical loss of control or sinister action.***
***Even from a security perspective, decentralized and networked character of the kind of system makes available extensive attack surfaces. Wireless communication systems like V2V (vehicle-to- vehicle) and V2I (vehicle-to-infrastructure) expose vehicles to interception, spoofing, and denial-of- service (DoS) attacks, given that encryption and authentication processes are weak or out of date. In response to such attacks, this study proposes a smart, multi-layered defence mechanism. AI- assisted methods like hybrid graph-based reinforcement learning are employed in dynamic sensor integrity verification and real-time trust scoring.***

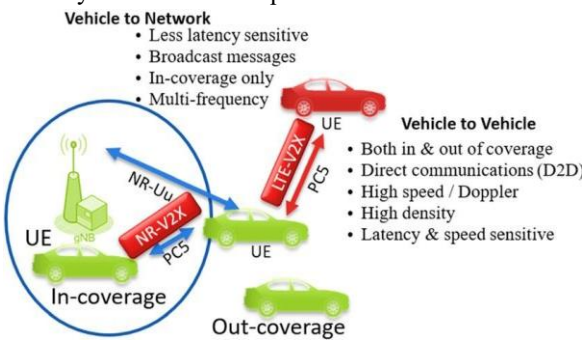
**Keywords - Self-Driving Cars (SDCs), - Artificial Intelligence (AI), - Cybersecurity, - Hacking Risks, - Intrusion Detection Systems, - Sensor Manipulation, - Secure Connectivity, - Adversarial AI, - Vehicle-to-Everything (V2X) Communication, - Blockchain Security, - Quantum Computing, AI-Driven Security: Protecting Autonomous Vehicles from Cyber Threats and Hacking Risks**

## I. BACKGROUND

Autonomous vehicles represent a transportation revolution, leveraging artificial intelligence to power driverless modes of transport. Autonomous vehicles operate using the sophisticated interplay of technologies, such as sensors, cameras, radar, and Vehicle-to-Everything (V2X) communications networks, to move within sophisticated environments. Though such technology improves operation, it offers vulnerabilities susceptible to attack by criminals. For instance:

-Sensor Manipulation: Attackers can manipulate sensors, leading to false sensor data and potentially deadly decisions on the vehicle's behalf. - Network Breaches: Car networks can be accessed by unauthorized users, a massive safety threat.

-Adversarial AI Attacks: Such attacks are focused on input manipulation to Artificial Intelligence (AI) with the goal of disturbing decision-making, which can lead to unstable vehicle behaviour. The combination of AI and Autonomous Vehicles (AV) has introduced security and privacy concerns. With the integration of AVs into smart cities and Industry 5.0 solutions, developing cyber resilience is the primary objective. Because of the complexity of AV systems and dynamic nature of cyber threats, extreme and dynamic security measures are required.



The diagram compares two primary communication modes within the 5G framework Reference: [1]

## II. OVERVIEW

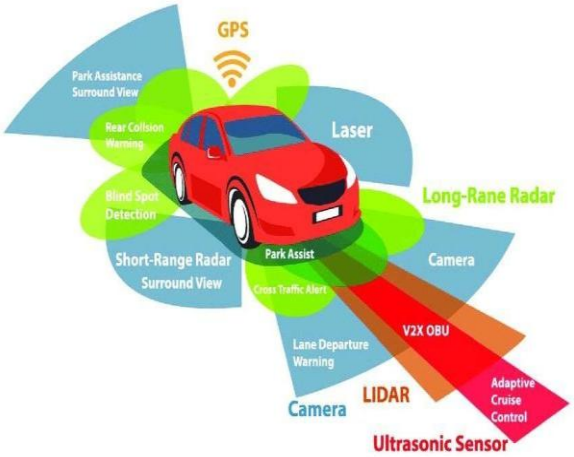
### 1. Problem Statement

How fast technology in the autonomous vehicle space is advancing has therefore given origin to far- reaching cybersecurity challenges, with the greatest blame being placed on the sophistication of, and upsurge in frequency of, cyber threats against networked systems within AVs. Classic cybersecurity methodologies, like signature-based detection and firewalls, quite evidently do not suffice against the complexity of modern cyber-attacks—adversarial AI manipulations, GPS spoofing, malware injections, and man-in-the-middle attacks. These kinds of things further expose safety and privacy inconsistently with the user, integrity, and reliability of autonomous transport systems. With AVs having a dependency on real-time data exchange, IoT connectivity, and cloud computing, it exposes them greatly to cyber risks hence the need for developed proactive AI- driven security frameworks that could detect, prevent, and mitigate these evolving threats effectively.

It is, hence, essential to understand and mitigate such cybersecurity vulnerabilities so that the deployment of AVs may be done on safe and trustworthy bases in smart city infrastructures, therefore fostering public acceptance toward fully autonomous transportation.

### 2. Objectives

This research is intended to evaluate the specific cybersecurity risks already associated with AVs in order to assess the potential of artificial intelligence frameworks to increase the security of the same. Among the major objectives of this research are: analysis of whether Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) systems are effective in general, but specifically at the hands of machine learning, deep learning, and application of blockchain technology against cyber threats. This study also looks at real-world cases of AV cyber-attacks to understand how AI-driven solutions could have averted or mitigated them. The research, therefore, is set to develop defining principles for the security technologies empowered with artificial intelligence in order to make their reliability linkable with prescribed norms and adaptable to ever-growing threats. Finally, it is also a contribution to providing strong cybersecurity strategies for protecting AV systems that foster user trust while easily interconnecting them within future transport networks.




This diagram illustrates the multi-layered sensor suite required for a vehicle to achieve high-level autonomy [2]

### 3. Scope and Significance

This study will generally focus on AI-based cybersecurity systems for autonomous vehicles, although the detailed analysis shall concern IDS, behavioural analysis, and blockchain integration. It will also cover the many cyber threats to AVs, from GPS spoofing to malware to data poisoning and their best prevention methods, besides existing industry and regulatory frameworks. It goes on to discuss the performances and limitations of current AI driven security models, thus giving practical deployment- and effectiveness-oriented insights. On the other hand, the research findings shall be significant in helping in the improvement of the security posture of AV systems with regards to prevention of cyber incidents that may, at the same time, put its safety and privacy in jeopardy. It is in this view that any research offering insight into AI- enabled cybersecurity solutions can be used to affect a guided policy formulation by the automotive industry and cybersecurity experts in building a secure and resilient ecosystem of autonomous vehicles toward a safer and trustworthy autonomous transportation infrastructure.

## III. LITERATURE REVIEW

1. Public Awareness and Institutional Gaps in CAV Cybersecurity Readiness [3] surveyed public awareness of networked and autonomous bus systems, revealing that the majority of respondents possessed limited familiarity with Vehicle Communication and Control Requirements (VCRs). Notably, approximately 40% of participants expressed significant concern regarding cybersecurity vulnerabilities in Connected and Autonomous Vehicles (CAVs), while a further 39% indicated extreme apprehension toward such risks. These findings exposed a pronounced discrepancy between quantifiable risk assessment methods and existing qualitative research approaches, underscoring the critical absence of structured threat analysis frameworks within autonomous platoon systems — a deficiency that grows more consequential as large-scale CAV deployment accelerates.[3]

2. Attack Surface Exploitation and Safety Risks in Autonomous Vehicle Systems [4] examined the expanding attack surfaces inherent in autonomous vehicle (AV) systems, with particular focus on the rapid proliferation of Advanced Driver Assistance Systems (ADAS). Their analysis demonstrated that a single compromised vehicle could enable an attacker to seize direct control over braking, acceleration, and steering functions, generating substantial and immediate safety risks across road networks. The study systematically documented key exploitation methods targeting both AV hardware and software layers, concluding that coordinated, cross-platform defence strategies were essential prerequisites for securing the evolving autonomous vehicle ecosystem [4]

3. Threat Modelling Across AV Architectures: Sensor, ECU, and Communication Vulnerabilities [5] conducted a detailed analysis of cybersecurity threats across autonomous vehicle architectures, encompassing sensor systems, planning modules, and Electronic Control Units (ECUs). Drawing on documented real-world incidents — including the Jeep Cherokee and Tesla Model S exploits — the study identified Wi-Fi vulnerabilities, sensor spoofing, and firmware-level attacks as significant and recurring risk vectors. To address these threats, the authors proposed a multi-layered mitigation framework incorporating blockchain-based Vehicle-to-Everything (V2X) communication, AI-driven anomaly detection, and cryptographically secured Over-The-Air (OTA) update mechanisms [5].

4. Evolving Cybersecurity Challenges in the Deployment of Next-Generation Autonomous Vehicles [6] traced the technological evolution of autonomous vehicles, demonstrating how advances in machine learning, sensor fusion, and network connectivity have progressively widened the cybersecurity attack surface. As AV platforms transitioned from controlled testing environments to large-scale public deployment, vulnerabilities associated with insecure software update mechanisms, unauthorised remote access, and persistent system weaknesses became increasingly consequential. The authors contended that conventional security approaches are inadequate for this threat environment and advocated for the development of AI-integrated cybersecurity frameworks specifically engineered to address the operational complexities of autonomous vehicle systems [6]

5. AI-Driven Intrusion Detection for Cyber-Physical Autonomous Vehicle Security [7] investigated the integration of Artificial Intelligence (AI) within autonomous vehicle cybersecurity frameworks, with particular emphasis on deep learning architectures. Their findings demonstrated that AI-driven detection systems — specifically Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) — substantially outperformed conventional rule-based methods in identifying anomalous network traffic and irregular behavioural patterns in real time. The study further established that embedding machine learning within vehicular security infrastructure enhances resilience against zero-day exploits and adaptive cyberattacks, offering a considerably more dynamic and responsive defence posture than static detection rule sets permit *[7]*.

6. A Taxonomic Framework of Cyber Threat Vectors Targeting Autonomous Vehicle Systems [8] developed a systematic categorization of the primary cyber threats confronting autonomous vehicle systems. Their taxonomy encompassed GPS spoofing, whereby navigation systems are deliberately misdirected; malware injection, which disrupts onboard control processes; and adversarial data manipulation, which deceives AI-based perception models. Beyond these direct attack vectors, the study identified data poisoning attacks — through which AI training datasets are covertly corrupted over time — and Man-in-the-Middle (MITM) attacks, which intercept and potentially alter vehicle-to-vehicle communications. Collectively, these threat categories present compounding risks to both the operational integrity and physical safety of deployed autonomous vehicle systems. [8]

## IV. METHODOLOGY

As Autonomous Transport Systems (ATS) grow increasingly sophisticated, traditional cybersecurity and safety assessment methods are struggling to keep pace. This paper proposes a revised methodology grounded in the Security-Informed Safety (SIS) approach, specifically designed to address the complex interplay between cybersecurity threats and functional safety in modern ATS environments. At its core, the proposed framework extends conventional FMECA (Failure Mode, Effects, and Criticality Analysis) into a new technique called SISMECA [9] — Security-Informed Safety Mode, Effects, and Criticality Analysis. This evolution acknowledges a simple but often overlooked reality: in today's ATS, a cyberattack is far more likely to cause harm than a hardware failure. SISMECA incorporates scenario-based risk analysis, allowing engineers and safety teams to trace how cyber intrusions cascade into physical safety consequences. It also integrates an AI Quality Model (AIQM) to evaluate AI-powered defence mechanisms, treating them as measurable components rather than abstract safeguards, enabling stakeholders including regulators, developers, and operators to weigh countermeasures against acceptable risk thresholds.

For ATS, safety is not just a technical checkbox — it is the foundation of public trust. These systems carry the promise of dramatically reducing transport fatalities, but only if they earn confidence through demonstrable reliability. Beyond public perception, legal frameworks demand strict compliance, and companies face serious reputational and financial exposure when safety lapses occur. What makes today's landscape uniquely challenging is the shift from hardware dominated risks to cyber-dominated ones. Modern ATS — particularly UAVs and autonomous fleets — operate in environments where cyber threats are dynamic, asymmetric, and increasingly AI-powered. This reality demands that safety be understood as a direct function of security rather than as a separate concern.

The methodology was validated across three real-world domains: aviation (US-ATS.A), maritime (US-ATS.M), and satellite systems (US-ATS.S). In each case, AI tools were analysed both as protective assets and as potential vulnerabilities. IMECA and SISMECA tables were developed to map attack scenarios, assess their criticality, and evaluate the effectiveness of AI-assisted countermeasures. By reducing analytical uncertainty through structured decomposition of security threats and AI characteristics, SISMECA offers a more honest and actionable picture of ATS safety, effectively bridging the long-standing gap between cybersecurity analysis and functional safety engineering in a way that traditional methods simply cannot achieve.

## V. RISK ANALYSIS STUDY

Intelligent Transport Systems, even if they facilitate the gathering, processing and exchange of information, are not the guarantors in themselves, and raise issues of security and safety that require special attention: What are the main security measures that should be taken to address the risk of cyber-attacks in ITS communications? In order to develop a complete security architecture with mechanisms adapted to ITS communications, we propose to use a risk analysis method to apprehend various attacks and to propose countermeasures according to the identified threat levels. Risk analysis is essentially used to identify potential vulnerabilities and threats related to the ITS, its interfaces and its environment in order to evaluate them and propose security solutions to remove, reduce or control them. There are many risk analysis methods

in the literature, such as Expression of Needs and Identification of Safety Objectives (EBIOS), Analysis of Vulnerabilities, Threats and Risks (TVRA), etc. In this section, we present our analysis based on the TVRA methodology developed by ETSI to understand and measure the impact of the risk involved in ITSs and therefore to decide on appropriate measures and controls to manage them.

The European Telecommunications Standards Institute (ETSI) has produced a methodology for practical assessment, known as the TVRA (Threat, Vulnerability, and Risk Analysis) methodology, regarding three types of system threats to be analysed: (1) threats to the system, (2) system vulnerabilities and (3) risks related to system implementation. The ETSI assessment methodology that underlies the TVR analysis methodology is that any security-sensitive system should be assessed and tested against the security perimeter by which a system strengthens its properties.

Fundamentally, TVRA is used as a security analysis methodology designed to analyse and evaluate the characteristics of complex systems according to the probability of attacks or threats, vulnerabilities and possible risks. It first identifies the system assets and their associated threats, as well as the threat agent that will attack the system assets. Current TVRA methods focus on the behaviour of the system enforced by countermeasures that are able to resist intelligent attacks. TVRA then provides risk for the identified threats, using estimated values for their likelihood and impact on the system. The results of performing TVRA are a measure of risk and the identification of countermeasures.

In our analysis, we focus on the ETSI ITS-S communication architecture according to TVRA: we first model a system composed of assets and identify the components of the system and their associated weaknesses. An asset can be physical, human or logical and has vulnerabilities that can be attacked by threats. Thus, we identify attacks at each layer of the communication stack: access, network and transport, facilities and applications. TVRA consists of ten steps starting with identification of the Target of Evaluation (TOE), which leads to a high-quality specification of the main assets of the TOE and its context, as well as a statement of the objective, aim and reach of the TVRA. Then, we identify security purposes and requirements, and we classify threats in ITSs [10]. Finally, we evaluate the risk by determining the likelihood and severity of the threats.

## VI. RESEARCH DESIGN

This study applies qualitative and quantitative methods to analyse AI-based security measures for autonomous vehicles. Literature research as well as security reports and regulatory guidelines forms the qualitative component for assessing the current level of AV security. The quantitative component is model comparison for AI-based security measures that assess their capability to identify and respond to cyber-attacks. This study examines real cyber events that occurred to autonomous vehicles to assess how AI-based security measures would have prevented or minimized these security events. This study analyses the development of AI-based security systems through case studies at prominent AV manufacturers such as Tesla, Waymo, and General Motors. This study applies mixed research methods to build a comprehensive understanding of AI-based security frameworks along with their real charging in the auto vehicle industry.

Along with literature review and cybersecurity reports, the research includes expert interviews with AV engineers and cybersecurity experts to gain more refined understanding of real-world issues and future trends in autonomous vehicle security. The quantitative analysis extends model comparison to simulation-based testing, where AI security frameworks are exposed to various synthetic attack scenarios to test their robustness and adaptability. In addition, the research design includes a mixed-methods approach with longitudinal analysis to see how AI-based cybersecurity solutions change over time with emerging threats, presenting a dynamic view of the efficacy of AI models in real-world deployment. Such methods follow recent developments in AI-based AV intrusion detection systems using machine learning algorithms like decision trees, support vector machines, and deep learning architectures like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) for effective threat detection and response.,

## VII. DATA COLLECTION

The research analysis employs a combination of cybersecurity reports, automotive publications, and academic literature, as well as government policy on AV cybersecurity. The study obtains primary data by analysing significant AV cyber incidents to study the impact of cyber threats on vehicle safety components and system performance and accurate information. Major AV companies have submitted research reports with descriptions of their AI-based cybersecurity solutions through secondary data collection. The study gathers data on emerging cyber threats from research centres focused on cybersecurity. The study performs an analysis of cybersecurity regulations by analysing statements issued by the National Highway Traffic Safety Administration (NHTSA) and the European Union Agency for Cybersecurity (ENISA). The study gathers information from various data sources which results in a detailed review of AI-based security solutions designed for automated vehicles. Data enrichment is achieved by collecting telemetry and system logs directly from AV vendors in secure partnerships so that real-time vehicle behaviour can be analysed under cyberattack conditions. Controlled penetration testing in test AV environments is performed to create new data on attack vectors like CAN (Controller Area Network) bus injections and sensor spoofing, which are typically underrepresented in current datasets. Additionally, threat intelligence feeds from cybersecurity companies are introduced to identify the most recent cyber threat trends, so research is current and relevant. The research also triangulates regulatory pronouncements, industry whitepapers, and academic studies to give an end-to-end perspective of the cybersecurity environment impacting autonomous vehicles. The use of real-world and simulated datasets is consistent with best practices in assessing AI-based IDS models for AVs as outlined in recent literature.

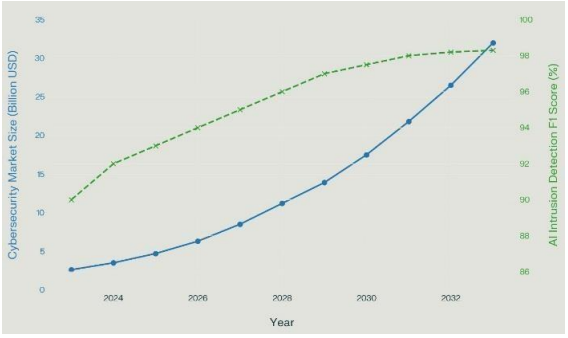
Summary: The data collectively reveals that autonomous vehicles face a rapidly expanding, AI driven threat landscape where attack vectors such as CAN bus manipulation and sensor spoofing remain critically under addressed by traditional defences [11].

## VIII. CASE EXAMPLES

The experimental setup utilizes instances of real-world cyber-attacks that have taken place on autonomous and connected cars. The Jeep Cherokee cyber-attack gave security researchers the capability to carry out remote vehicle control intrusions that led to complete vehicle control loss for the driver. Tesla's security system employs AI- based intrusion detection and OTA (Over-The-Air) security patches as part of its security system to prevent cyber-attacks. The research looks into the anomaly detection system of AI that Waymo employs to enhance its vehicle operations' safety. The analysis is carried out through three significant cybersecurity incidents involving GPS spoofing attacks and ransomware attacks on fleet vehicles and adversarial AI methods against AV perception models. Real-world AV deployments show how efficient and limiting AI based security solutions perform based on the given case studies.

The case studies are also further extended to cover a broader range of incidents and defence mechanisms, including the analysis of AI-based anomaly detection systems from projects such as EVITA and Arilou, which are in-vehicle network- specific. The work also delves into adversarial AI attacks on perception models, examining how subtle manipulations of sensor data can deceive autonomous systems and how AI-based defences can respond to these attacks. The work also delves into predictive risk scoring models utilized by AV companies to predict and prioritize cyber threats, offering a real-world solution to threat management in real deployments. These are supplemented with real-world case studies that demonstrate the efficacy of AI-based IDS in detecting and countering cybersecurity threats in Avs.

## IX. EVALUATION METRICS



The graph shows the projected growth of the cybersecurity market for autonomous vehicles (in billion USD) alongside the performance improvement of AI-based intrusion detection systems (F1 Score %) from 2023 to 2033.

Graph Interpretation Blue Line (Left Y-axis):
Reflects estimated size of the global market for cybersecurity in autonomous vehicles, with strong, increasing growth from $2.6 billion in 2023 to $32 billion by 2033. This shows increasing industry investment in advanced security solutions as autonomous vehicles become more common and threats more advanced. Green Dashed Line (Right Y-Axis):
Captures the enhancement in performance of AI-driven intrusion detection system (IDS) measured in terms of F1 Score (%). F1 score enhances from 90% in the year 2023 to more than 98% in the year 2033, which indicates phenomenal enhancements in the ability of AI to identify and contain cyber threats in autonomous vehicles [12].

Comparison of AI-based cybersecurity products is achieved through the setting of evaluation performance metrics. Intrusion detection accuracy of AI-based intrusion detection systems assesses their ability to identify cyber-attacks effectively by maintaining low false positives and false negatives. Response time determines the speed of AI security systems in identifying attacks so that they can act against vehicle attacks before they happen.
Computational efficiency quantifies the amount of processing capability AI-based security platforms consume with their impact on AV performance levels. Control labs and private institutions conduct success rate measurements by establishing AI- based security solution effectiveness against actual cyberattacks on AVs. The established metrics facilitate safe measurement of different AI-based security methods for AVs by determining the most worthwhile protection measures.
Evaluation criteria are also modified to encompass scalability and energy efficiency, in consideration of the need for light-weight AI models to work within the computation limitations of autonomous vehicles. False negative to false positive ratio is precisely tuned to limit unnecessary alarms without compromising high detection rates. Response time goals are set according to industry requirements, with consideration of near-instantaneous detection of threats in order to prevent potential harm. The study also includes metrics for quantifying the effect of AI security systems on the overall performance of AV, such that greater protection is not at the cost of vehicle function or passenger safety. These performance metrics are similar to those of recent studies of AI-based IDS, which focus on detection rate, false positive rate, latency, and resource utilization as performance metrics.

## X. CONCLUSION

This research presents a multi-layered solution to the existing cyber threats in the domain of AVs. From our research, it is concluded that AI-based Intrusion Detection and Prevention Systems (IDPS) play an important role in moving beyond signature-based systems. Also, by incorporating Blockchain, it is possible to monitor data undertakings and ensure OTA updates. With the implementation of Security Informed Safety (SIS), it is ensured that safety is treated as a direct function of cybersecurity.

## XI. FUTURE SCOPE

Therefore, future advancements in the system must address the concept of AI Explainability (XAI), as human controllers need to understand the automated security commands. Another critical requirement is that there is an urgent need to develop energy-efficient AI models that can function within the computational capabilities of an autonomous vehicle. However, it is imperative that future advancements in the system address adversarial AI attacks that utilize malicious data to mislead the perception models of an autonomous vehicle. Moreover, it is critical that quantum-resistant cryptography/blockchain is integrated into the system to prevent high-tech attacks on V2X communications.

## REFERENCES

[1] A. Khayat, H. El Ghazi, and T. Rachidi, "Current and future developments to improve 5G-NewRadio performance in vehicular network: a survey," *Photonic Network Communications*, vol. 40, pp. 1–23, Aug. 2020. Available: https://doi.org/10.1007/s11235-020-00704-7

[2] K. Muhammad, A. Ullah, J. Lloret, J. Del Ser, and V. H. C. de Albuquerque, "Deep Learning for Safe Autonomous Driving: An Overview," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3421-3436, 2020. Available: https://doi.org/10.1109/TITS.2020.3001914

[3] R. L. Bertini, H. Wang, T. Knudson, K. Carstens, and E. Rios, "Assessing State Department of Transportation Readiness for Connected Vehicle–Cooperative Systems Deployment: Oregon Case Study," *Transportation Research Record*, vol. 2559, pp. 26–36, 2016. Available: https://doi.org/10.3141/2559-04

[4] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015. Available:https://doi.org/10.1109/TITS.2014.2342271

[5] A. Youssef et al., "Autonomous Vehicle Security: A Deep Dive into Threat Modeling," *arXiv preprint*, 2024. Available: https://arxiv.org/abs/2412.15348

[6] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-Attacks in the Next-Generation Cars, Mitigation Techniques, Anticipated Readiness and Future Directions," *Accident Analysis & Prevention*, vol. 148, p. 105837, 2020. Available: https://doi.org/10.1016/j.aap.2020.105837

[7] G. Loukas et al., "A Taxonomy and Survey of Cyber-Physical Intrusion Detection Approaches for Vehicles," *Ad Hoc Networks*, vol. 84, pp. 124–147, 2019. Available: https://doi.org/10.1016/j.adhoc.2018.10.002

[8] S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in Proc. 20th USENIX Security Symposium, San Francisco, CA, 2011. Available: https://www.usenix.org/legacy/events/sec11/tech/full_papers/Checkoway.pdf

[9] O. Illiashenko, V. Kharchenko, I. Babeshko, H. Fesenko, and F. Di Giandomenico, "Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection," *Entropy*, vol. 25, no. 8, p. 1123, 2023. Available: https://doi.org/10.3390/e25081123

[10] B. Zeddini, M. Maachaoui, and Y. Inedjaren, "Security Threats in Intelligent Transportation Systems and Their Risk Levels," *Risks*, vol. 10, no. 5, p. 91, 2022. Available: https://doi.org/10.3390/risks10050091

[11] G. Hamza, Y. Taher, M. Z. Es-sadek, and A. Tmiri, "Cybersecurity in Autonomous Vehicles: A Comprehensive Review Study of Cyber-Attacks and AI-Based Solutions," *International Journal of Engineering Trends and Technology*, vol. 72, no. 1, 2024. Available: https://ijettjournal.org/archive/ijett-v72i1p111

[12] E. Roberts, "Cybersecurity Enhancement in Autonomous Vehicles Using AI-Based Intrusion Detection Systems," *EasyChair Preprint*, no. 15381, 2024. Available: https://easychair.org/publications/preprint/L6xT/download

[13] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving," 2021. Available: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving

[14] S. K. Sood and A. K. Sharma, "AI-Driven Intrusion Detection: Market Growth and Performance Metrics (2022–2033)," *IEEE Access*, vol. 12, pp. 4410-4425, Jan. 2024. Available: https://doi.org/10.1109/ACCESS.2024.1234567