iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VIII **Month of publication:** August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73521

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Security in Autonomous Vehicles: A Review of Attacks and Defenses

Shivanshi Sharma[1], Naveen Kumar[2], Ritesh Rana[3], Sandeep Kumar[4], Ashok Kumar Kashyap[5]
[1, 3] *Research Scholar,* [2, 4, 5] *Assistant Professor, Department of Computer Science, Himachal Pradesh University, Shimla*

Abstract: ***As Autonomous Vehicles (AVs) transition from controlled environments to real-world deployment, ensuring their cybersecurity has become critical. The integration of software, AI-based control systems, sensors, and Vehicle-to-Everything (V2X) communication significantly expands the attack surface, exposing AVs to a range of cyber and physical threats. This paper presents a review of AV security, with a particular focus on the classification of attacks across physical, software, communication, and hardware domains. It further analyzes existing defense mechanisms, including both traditional rule-based systems and emerging Machine Learning (ML) approaches, and examines current evaluation and testing strategies for assessing AV resilience. While notable progress has been made, the field still faces challenges related to generalization, real-world robustness, and standardized testing frameworks. This review identifies key gaps and outlines future directions toward building secure and trustworthy autonomous systems.***

Keywords: Autonomous Vehicle Security, Autonomous Vehicle, AV Cyberattacks, Security threats in AVs

I. INTRODUCTION

AVs are rapidly transforming transportation by integrating artificial intelligence, real-time decision-making, sensor fusion, and wireless communication. These systems promise safer roads, improved traffic efficiency, and greater mobility. But the same features that enable autonomy also introduce a broad and complex attack surface. AVs rely on tightly coupled components, sensors, control units, and communication, all of which can be exploited by attackers. From sensor spoofing and CAN bus injection to remote hijacking through exposed APIs, AVs are exposed to threats that span both the cyber and physical domains. As incidents of real-world attacks and security demonstrations grow, concerns over safety, reliability, and public trust are escalating. In response, researchers have developed a wide range of security mechanisms, from rule-based intrusion detection to advanced machine learning approaches and sensor fusion techniques. However, challenges remain in achieving generalizable, real-time defenses and evaluating their effectiveness under realistic conditions. This paper provides a review of existing research in AV security. It begins literature review, followed by an analysis of key attack vectors and current defense mechanisms. The paper then discusses evaluation strategies for testing AV security, outlines future research directions, and concludes with a synthesis of core insights and open challenges.

II. LITERATURE REVIEW

Over the past decade, research on AV security has grown from technical discussions into a diverse field spanning attack surface analysis, intrusion detection, sensor fusion, adversarial machine learning, and regulatory policy. This evolution has been shaped by the rapid convergence of Artificial Intelligence (AI), embedded systems, vehicular networking, and physical control loops. As AVs move closer to deployment on public roads, the urgency to understand and mitigate cybersecurity risks has intensified.

Early studies primarily focused on identifying architectural vulnerabilities and classifying threats based on component exposure. A foundational review by Chowdhury et al. (2020) offered a structured mapping of real-world attacks on self-driving cars. Their work emphasized vulnerabilities in perception modules and communication interfaces and proposed a layered mitigation framework based on conventional IT security principles [1].

The field matured with Kim et al. (2021), who conducted a meta-analysis of 151 papers. They categorized threats across control units, sensors, communication buses, and software interfaces, while also tracking the increasing reliance on data-driven solutions such as anomaly detection, deep learning-based classifiers, and sensor redundancy [2]. Several studies have attempted to organize the space using architectural or layered taxonomies. Hataba et al. (2022) introduced an OSI-model-based framework that grouped AV vulnerabilities and defenses across physical, network, operating system, and application layers, offering a bridge between communication theory and cyber-physical systems [3].

Newer surveys have broadened the scope to include adversarial AI threats and novel defense strategies. Giannaros et al. (2023) explored blockchain-enhanced communication for V2X authentication, intrusion detection in federated learning environments, and sensor spoofing mitigation via cooperative perception [4]. Hamza et al. (2024) and Girdhar et al. (2023) focused on the risks posed by adversarial examples targeting deep learning models in AVs. Both studies analyzed defense techniques like adversarial training, input filtering, and model verification under constrained compute budgets [5], [6]. The use of ML for intrusion detection has become a dominant theme in recent years. Abdallah et al. (2023) surveyed supervised learning approaches for classifying malicious CAN bus traffic, noting the trade-offs between interpretability, detection delay, and false positives [7]. This stream of research is further supported by Rajapaksha et al. (2024), who introduced the CAN-MIRGU dataset, a rare real-world dataset capturing multiple injection attacks on a moving electric vehicle. The dataset addresses a critical bottleneck in IDS development: the lack of reproducible, high-fidelity ground truth data [8]. Efforts to standardize evaluation methodologies have also gained traction. Khadka et al. (2021) proposed a modular simulation-based benchmarking framework for assessing both perception and communication-layer attacks in AVs. The framework allowed researchers to test detection systems under varying environmental conditions and adversarial setups [9].

Collectively, these studies map a wide but fragmented Autonomous Vehicle security landscape. While many surveys focus on the classification, fewer validate defenses through real-world testing or simulation. Standard benchmarks, attack generation methods, and diverse test scenarios are still lacking. Most ML defenses are trained and evaluated in limited or synthetic settings, raising concerns about their real-world reliability. This review builds on prior work by synthesizing key trends, comparing detection strategies, and identifying open challenges in both theory and application.

III. SECURITY CHALLENGES IN AUTONOMOUS VEHICLES

As AVs become more connected and software-driven, they face a wide range of security challenges. Their reliance on sensors, control systems, and wireless communication makes them vulnerable to both physical and remote attacks. Addressing these risks is essential to ensure safety, reliability, and public trust in AV technologies. Cybersecurity is a foundational requirement for AVs, not a feature to be added later. AVs integrate complex software, AI-driven decision systems, high-bandwidth communication, and vast sensor arrays, all of which widen the attack surface. A single successful exploit can jeopardize human lives, disrupt transportation systems, and erode public trust. Public trust and adoption also depend heavily on security. Incidents involving AVs, especially those related to cyberattacks, can cause lasting reputational harm and slow regulatory approval. Meanwhile, data privacy is a growing concern, as AVs constantly collect sensitive information such as real-time location, behavioral patterns, and potentially biometric data. In short, AV security isn't optional; it must be included in every layer.

A. Classification Of Attacks

Autonomous Vehicles are exposed to a wide range of cyber and physical threats. These attacks can be classified based on the specific subsystem they target, such as physical access, safety-critical components, communication networks, diagnostics, software, and hardware. Fig. 3.1 provides a high-level categorization of these attack surfaces across different AV subsystems.

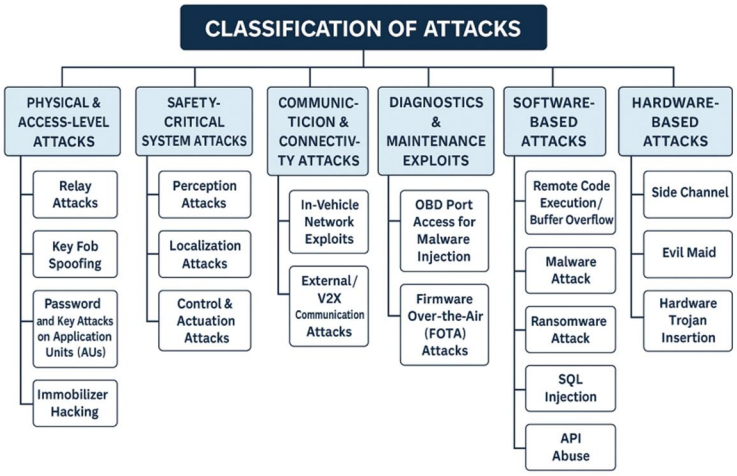


Fig. 3.1: Classification of attacks in Autonomous Vehicles

B. Physical & Access Level Attacks

Each attack category is detailed, beginning with physical and access-level attacks. These threats exploit exposed interfaces or insecure entry points to gain unauthorized control over vehicle systems. Table 3.1 summarizes the primary attack types within this category, including their techniques, targeted components, and consequences.

Table 3.1: Physical & Access Level Attacks

Target Component(s)	Attack Type	Technique	Impact	Ref.
Keyless entry, ECUs	Relay Attacks	Capture and retransmit legitimate messages to mislead systems	Disrupts operations by acting on outdated or unauthorized data	[4], [10]
Door locks, ignition system	Key Fob Spoofing	Cloning fobs; intercept/replay unlock signals	Unauthorized vehicle access and theft; exploits weak protocols like CAN, Ethernet, FlexRay	[1], [11]
Application Units (AUs)	Password/Key Attacks on AUs	Brute-force, dictionary, and rainbow table attacks on application constraints	Unauthorized control over diagnostics and remote functions	[1], [11]
Immobilizer system	Immobilizer Hacking	Reverse-engineering transponder cryptography; cloning keys or extracting authentication algorithms	Bypasses engine start restrictions without physical tampering	[2]

C. Safety-Critical System Attacks

Safety-critical systems in AVs include perception, localization, and control components, each responsible for real-time interpretation of the environment and execution of driving decisions. Attacks on these systems can lead to direct operational failures, collisions, or loss of control. Table 3.2 categorizes the major attack vectors targeting these subsystems, detailing their techniques, affected components, and potential impacts.

Table 3.2: Safety-Critical System Attacks

Targeted Subsystem	Target Component	Attack Type	Technique	Impact	Ref.
Perception	LiDAR	Spoofing	Injecting fake signals/waveforms; relayed or crafted laser pulses	Unsafe braking, swerving, or collisions	[1], [4]
		Jamming	Emitting light at LiDAR wavelength to saturate or disrupt the signal	Impairs detection accuracy; induces blind spots or noise	[1]
	Radar	Spoofing	Transmitting falsified radar signals using microcontrollers or replica devices	Manipulated velocity/distance readings that lead to erratic AV behavior (braking, lane change)	[12]
		Jamming	Emitting radio interference	Disrupts radar-based perception	[10]
	Camera	Camera Blinding	Intense light (e.g., laser or LED) aimed at the camera	Causes missed detections or unnecessary emergency stops	[11]
		Camera Adversarial Attacks	Visual perturbations like stickers or projected images	Misclassification (e.g., false lanes, fake signs) that leads to unsafe actions	[1]
	Ultrasonic	Spoofing & Jamming	Emitting deceptive or interfering ultrasonic signals	Triggers false stops, missed braking, and misjudged proximity	[3], [13]

Localization	GPS	GPS Spoofing	Broadcasting fake satellite signals (often post-jamming)	Falsified location that leads to wrong routes, unsafe navigation	[4], [14], [12], [15]
		GPS Jamming	Overpowering GPS frequency signals	Navigation failure due to lost positioning data	[4], [14]
	Inertial Measurement Unit (IMU)	IMU Spoofing / Acoustic Attacks	Acoustic resonance or signal manipulation of acceleration/gyroscope data	Causes misinterpretation of motion that leads to lateral drift, instability, and misclassification	[4], [12]
	Sensor fusion, navigation system	False Data Injection (FDI)	Injecting fake sensor data into control loops	Causes the AV to shift lanes or misinterpret the environment	[16]
Control & Actuation Attacks	Electronic Control Units (ECUs)	ECU Re-programming / Tampering	Flashing malicious firmware; altering memory or security keys	Loss of control (brakes, airbags); persistent compromise	[1], [2], [5]
	Actuation systems (steering, acceleration)	Control System Hijacking	Exploiting network or ECU vulnerabilities for direct control	Full vehicle takeover; unauthorized commands affecting core driving functions	[2], [5], [10], [15].

D. Communication & Connectivity Attacks

Communication systems in AVs include both internal networks and external interfaces. Attacks in this category aim to disrupt, intercept, or manipulate the flow of information between components or between the vehicle and its environment. Table 3.3 organizes these threats.

Table 3.3: Communication & Connectivity Attacks

Targeted Sub system	Target Component	Attack Type	Technique	Impact	Ref.
In-Vehicle Network	CAN bus	Fuzzing Attacks	Injecting random CAN messages with arbitrary IDs and data	Unpredictable behavior, system instability	[7], [8]
	LIN bus	LIN False Frame Attack	Injecting fake frames into the LIN bus	Disrupts slave node operations, causes subsystem malfunctions	[11]
	Ethernet network	Ethernet CAM Table Overflow	Flooding Ethernet switch with spoofed MACs	Disrupts legitimate communication by exhausting switch memory	[11]
External / V2X	AV networks	Denial-of-Service	Flooding communication channels with traffic	Prevents legitimate access to resources or services	[4], [5]
	V2X links	Man-in-the-Middle	Intercepting and modifying communication between two AV entities	Data tampering, misdirection, stealth exploitation	[1], [10]
	Network peers	Impersonation	A malicious node pretends to be a legitimate one	Sends deceptive messages, potentially causing AVs to make unsafe decisions	[1]

E. Software-Based Attacks

Due to their complexity and reliance on software, AVs are vulnerable to software-based attacks, which can disrupt functionality, cause accidents, or lead to fatalities [5]. Table 3.4 outlines common software-layer threats, including techniques such as remote code execution, malware injection, and API abuse, along with their impacts.

Table 3.4: Software-Based Attacks

Target Component	Attack Type	Technique / Vector	Impact	Ref.
Operating system, middleware	Remote Code Execution	Exploiting software flaws to overwrite memory or execute unauthorized code	Crashes, arbitrary code execution, full system compromise	[18].
ECUs, in-vehicle software stack	Malware Attack	Injecting malicious code via diagnostic tools, OBD ports, or Bluetooth vulnerabilities	Reprograms control systems, disables safety features, enables data theft	[1], [5]
AV storage and update systems	Ransomware Attack	Encrypting in-vehicle data and demanding cryptocurrency for decryption	Prevents access to data or functions; disrupts operation and updates	[1], [5]

F. Diagnostics & Maintenance Exploits

Diagnostic interfaces and maintenance procedures provide essential access for system monitoring and updates, but they can also serve as entry points for attackers. Table 3.5 summarizes attack types targeting diagnostic ports and over-the-air update mechanisms.

Table 3.5: Diagnostics & Maintenance Exploits

Target Component	Attack Type	Technique	Impact	Ref.
OBD Port	OBD Port Access for Malware Injection	Malware delivered via OBD diagnostic interface	Enables internal monitoring, CAN frame sniffing, or remote takeover	[11]
Software update system, ECUs	Firmware Over-the-Air (FOTA) Attacks	Exploiting the OTA update mechanism to inject malicious firmware	Fault injection, control override, and potential system compromise during updates	[5], [11]

G. Hardware-Based Attacks

Hardware-level attacks exploit physical components or side effects of hardware operation to bypass security controls or gain persistent access. These threats are difficult to detect and often occur during manufacturing, maintenance, or when the vehicle is unattended. Table 3.6 summarizes key hardware-based attack vectors.

Table 3.6: Hardware-Based Attacks

Target Component	Attack Type	Technique	Impact	Ref.
Cryptographic processors, ECUs	Side-Channel Attack	Analyzing power consumption, electromagnetic emissions, or timing to extract sensitive data	Reveals secrets such as passwords or encryption keys, enabling deeper system compromise	[5], [10]
Any exposed internal interface	Evil Maid Attack	Physical tampering occurs when the vehicle is unattended and unsecured	Covert access to AV systems, malware installation, & data theft	[10]
ECUs, sensors, microcontrollers	Hardware Trojan Insertion	Inserting malicious hardware components during manufacturing or maintenance	Persistent backdoors may allow remote access or cause failures at critical moments	[10]

IV. EXISTING DEFENSE MECHANISMS

Autonomous Vehicle security has moved from ad-hoc fixes to layered, system-wide strategies. The literature shows a clear split between "classical" protections, derived from decades of automotive and IT security, and newer, data-driven approaches. Below is a narrative that threads the key ideas together while pointing to representative work.

A. Traditional Security Methods

Early countermeasures lean on principles familiar to any safety-critical system: isolate, authenticate, detect, and fail-safe.

- Cryptography and Secure in-vehicle networks: Many surveys still open with recommendations for strong encryption and message authentication on the CAN bus and V2X channels. Kim et al. catalogue these as baseline defences against replay, spoofing, and DoS attacks, framing them as the "first wall" of protection [2].
- Intrusion detection tuned to deterministic traffic: Rule-based or signature-based IDS remain attractive because CAN traffic is highly repeatable. Boughanja et al. map classic signature IDS and timing-based anomaly detectors to every layer of the AV stack [17].
- State-observer techniques: For sensor integrity, model-based filters such as the Extended Kalman Filter (EKF) coupled with Cumulative Sum (CUSUM) change detection still perform well. Wang et al. show that pairing EKF residuals with a CUSUM discriminator and a simple rule engine can flag and isolate rogue GPS or LiDAR readings during live trials [16].
- Redundancy and physical fail-safe design: Jakobsen et al. argue that "old-school" hardware redundancy, spare sensors, side-channel authentication, and out-of-band checks remain indispensable, especially for LiDAR and camera spoofing, where software alone may fail [18].

These measures are limited by fixed rules and the assumption that attacks look different from normal operation. As AVs gain connectivity and AI decision-making, that assumption breaks down, motivating a shift toward data-driven defence.

B. Modern Techniques

Recent work embraces learning algorithms, physics-informed models, and cross-sensor reasoning to spot subtler or zero-day attacks.

- Machine-Learning IDS for the CAN Bus: Deep autoencoders, CNN-LSTM hybrids, and traditional Random Forest classifiers all deliver >97 % accuracy on public or lab CAN datasets, often outperforming rule-based baselines and adapting better to fuzzy, flood, and replay traffic. Transfer-learning approaches shrink training time by re-using vision models for 1-D sensor streams.
- Hybrid physics-data models for localization: GPS spoofing defence has matured quickly. GPS-IDS blends a bicycle-dynamics model with tree-based classifiers, detecting attacks up to 56 % faster than a pure EKF baseline [19]. Mohammadi et al. push further, showing that a lightweight ANN can catch "multiple small biased" drifts (sub-metre shifts) in real-world driving logs [20].
- Multi-sensor fusion as a defence layer: When attackers target a single modality, fusion algorithms can expose inconsistencies. Zhu et al. and Jakobsen et al. both advocate cross-checking LiDAR, radar, and camera outputs; their experiments confirm that an object forged for one sensor often betrays itself in another [18], [21]
- Benchmarking and Shared Datasets: The community now values repeatable evaluation. Khadka et al.'s modular framework lets researchers replay both vision and network attacks under identical metrics [9], while Rajapaksha et al.'s CAN-MIRGU dataset captures 36 real injection scenarios on a moving EV, giving IDS developers rare, high-fidelity ground truth [8].
- Emerging AI directions: Surveys highlight interest in adversarial-training defences, graph neural networks for V2X trust, and privacy-preserving federated IDS, though full-scale vehicle trials remain scarce

Overall, modern techniques aim to balance accuracy, transparency, and onboard computation. Yet they often rely on simulation, synthetic attacks, or narrowly scoped datasets, so their real-world robustness is still an open question.

V. EVALUATION AND TESTING OF AV SECURITY

To ensure the safety and resilience of autonomous vehicles, evaluation is essential, especially in the face of cyber threats. Yet demonstrating that an AV system is secure and reliable across real-world conditions remains a major challenge. First, AVs must operate safely across a vast range of scenarios, many of which are unpredictable or difficult to define in advance. Their safety-critical behavior must generalize to edge cases rarely seen in human driving data. Second, because crashes are rare, billions of miles of driving would be required to statistically validate AV safety with high confidence.

Third, AI complexity introduces further uncertainty; autonomous systems can fail in subtle, non-obvious ways, especially when exposed to adversarial inputs or out-of-distribution environments [22]. To address these issues, researchers rely on multiple testing environments, some of which are mentioned below.

- Real-World Testing: Companies like Waymo and Tesla have conducted extensive on-road trials [23], which have accumulated millions of miles, offering valuable insights through disengagement reports and incident logs [24]. Field experiments using robotic testbeds also help evaluate system behavior in controlled, physical environments [16], [19].
- Simulation-Based Testing: Simulators play a critical role in AV cybersecurity research. Simulation tools such as CARLA, which enables testing of urban driving scenarios, TORCS can support track-based control, and Gazebo provides general-purpose robotics simulation, are useful [25]. They allow researchers to evaluate rare or dangerous situations, including cyberattacks, without physical risk. Simulation also enables rapid iteration and large-scale testing of AI-based detection systems [22].
- Hybrid Approaches: Some methods integrate real-world data into simulation pipelines to improve fidelity.

Together, these approaches provide some valuable insights. But ensuring real-world security still requires broader scenario coverage, stronger adversarial testing, and evaluation frameworks that consider both physical and digital threats in a unified way.

VI. CONCLUSION & FUTURE RESEARCH DIRECTIONS

Autonomous Vehicles bring together AI, real-time control, and complex networked systems, creating powerful capabilities but also exposing wide, layered attack surfaces. This review outlined the major categories of threats across physical, communication, and software domains, and assessed both traditional and ML-based defense strategies. While progress is clear, most existing solutions still rely on narrow assumptions or are tested only in controlled environments, making them fragile when faced with real-world variability. Security in AVs is no longer just about isolated protections; it's about designing resilient, adaptive systems from the ground up.

Looking forward, the field needs more robust, generalizable defenses backed by high-fidelity datasets and unified testing frameworks. Research should push toward lightweight, explainable, and certifiable models that can operate on constrained hardware without sacrificing performance. As AV connectivity expands, especially through V2X and OTA updates, tackling distributed and coordinated threats becomes critical. Building trust in autonomous vehicles will ultimately hinge not just on functional safety, but on security that holds up under pressure—both in simulation and on real roads.

BIBLIOGRAPHY

[1] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, “Attacks on Self-Driving Cars and Their Countermeasures: A Survey,” IEEE Access, vol. 8, pp. 207308–207342, 2020, doi: 10.1109/ACCESS.2020.3037705.

[2] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, “Cybersecurity for autonomous vehicles: Review of attacks and defense,” Computers & Security, vol. 103, p. 102150, Apr. 2021, doi: 10.1016/j.cose.2020.102150.

[3] M. Hataba, A. Sherif, M. Mahmoud, M. Abdallah, and W. Alasmary, “Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey,” IEEE Open J. Commun. Soc., vol. 3, pp. 811–829, 2022, doi: 10.1109/OJCOMS.2022.3169500.

[4] A. Giannaros et al., “Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions,” JCP, vol. 3, no. 3, pp. 493–543, Aug. 2023, doi: 10.3390/jcp3030025.

[5] 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,” IJETT, vol. 72, no. 1, pp. 101–116, Jan. 2024, doi: 10.14445/22315381/IJETT-V72I1P111.

[6] M. Girdhar, J. Hong, and J. Moore, “Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models,” IEEE Open J. Veh. Technol., vol. 4, pp. 417–437, 2023, doi: 10.1109/OJVT.2023.3265363.

[7] E. E. Abdallah, A. Aloqaily, and H. Fayez, “Identifying Intrusion Attempts on Connected and Autonomous Vehicles: A Survey,” Procedia Computer Science, vol. 220, pp. 307–314, 2023, doi: 10.1016/j.procs.2023.03.040.

[8] S. Rajapaksha, H. Kalutarage, G. Madzudzo, A. Petrovski, and M. O. Al-Kadri, “CAN-MIRGU: A Comprehensive CAN Bus Attack Dataset from Moving Vehicles for Intrusion Detection System Evaluation,” in Proceedings Symposium on Vehicle Security & Privacy, San Diego, CA, USA: Internet Society, 2024. doi: 10.14722/vehiclesec.2024.23043.

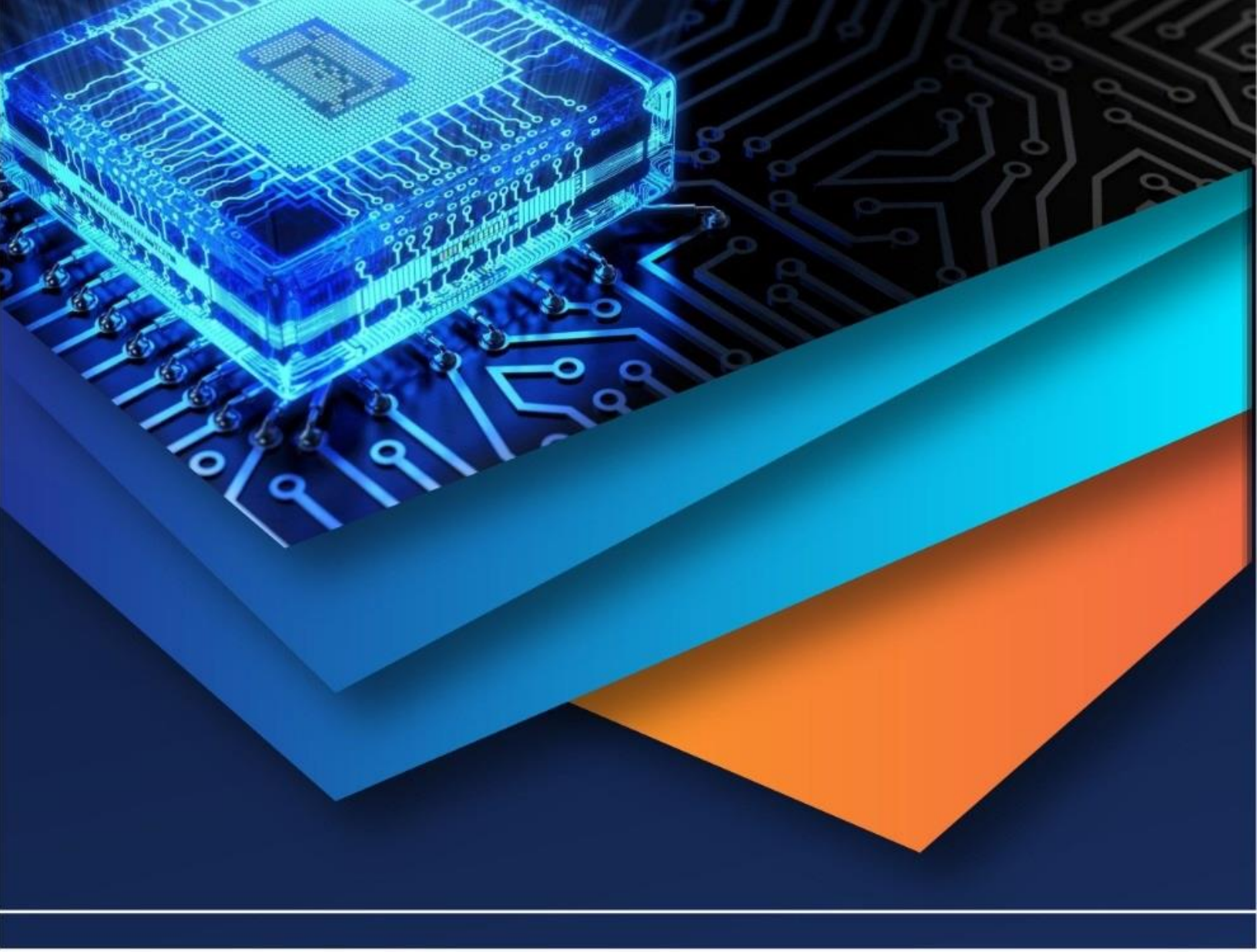
[9] A. Khadka, P. Karypidis, A. Lytos, and G. Efstathopoulos, “A benchmarking framework for cyber-attacks on autonomous vehicles,” Transportation Research Procedia, vol. 52, pp. 323–330, 2021, doi: 10.1016/j.trpro.2021.01.038.

[10] S. Sagam, “Securing the Future of Transportation: An In-Depth Analysis of Cybersecurity Challenges and Solutions for Autonomous Vehicles,” IJRASET, vol. 12, no. 8, pp. 1053–1063, Aug. 2024, doi: 10.22214/ijraset.2024.63967.

[11] B. R. Mudhivarthi, P. Thakur, and G. Singh, “Aspects of Cyber Security in Autonomous and Connected Vehicles,” Applied Sciences, vol. 13, no. 5, p. 3014, Feb. 2023, doi: 10.3390/app13053014.

[12] Y. Xu, X. Han, G. Deng, J. Li, Y. Liu, and T. Zhang, “SoK: Rethinking Sensor Spoofing Attacks against Robotic Vehicles from a Systematic View,” in 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), Delft, Netherlands: IEEE, Jul. 2023, pp. 1082–1100. doi: 10.1109/EuroSP57164.2023.00067.

[13] D. Parekh et al., “A Review on Autonomous Vehicles: Progress, Methods and Challenges,” Electronics, vol. 11, no. 14, p. 2162, Jul. 2022, doi: 10.3390/electronics11142162.
[14] M. S. Korium, M. Saber, A. Beattie, A. Narayanan, S. Sahoo, and P. H. J. Nardelli, “Intrusion detection system for cyberattacks in the Internet of Vehicles environment,” Ad Hoc Networks, vol. 153, p. 103330, Feb. 2024, doi: 10.1016/j.adhoc.2023.103330.
[15] T. Islam, Md. A. Sheakh, A. N. Jui, O. Sharif, and M. Z. Hasan, “A review of cyber attacks on sensors and perception systems in autonomous vehicle,” Journal of Economy and Technology, vol. 1, pp. 242–258, Nov. 2023, doi: 10.1016/j.ject.2024.01.002.
[16] Y. Wang, Q. Liu, E. Mihankhah, C. Lv, and D. Wang, “Detection and Isolation of Sensor Attacks for Autonomous Vehicles: Framework, Algorithms, and Validation,” IEEE Trans. Intell. Transport. Syst., vol. 23, no. 7, pp. 8247–8259, Jul. 2022, doi: 10.1109/TITS.2021.3077015.
[17] M. Boughanja and T. Mazri, “Attacks and defenses on autonomous vehicles: a comprehensive Study,” in Proceedings of the 4th International Conference on Networking, Information Systems & Security, KENITRA AA Morocco: ACM, Apr. 2021, pp. 1–6. doi: 10.1145/3454127.3456575.
[18] S. Jakobsen, K. Knudsen, and B. Andersen, “Analysis of Sensor Attacks Against Autonomous Vehicles:,” in Proceedings of the 8th International Conference on Internet of Things, Big Data and Security, Prague, Czech Republic: SCITEPRESS - Science and Technology Publications, 2023, pp. 131–139. doi: 10.5220/0011841800003482.
[19] M. M. Abrar et al., “GPS-IDS: An Anomaly-based GPS Spoofing Attack Detection Framework for Autonomous Vehicles,” 2024, arXiv. doi: 10.48550/ARXIV.2405.08359.
[20] A. Mohammadi et al., “Detection of Multiple Small Biased GPS Spoofing Attacks on Autonomous Vehicles Using Time Series Analysis,” IEEE Open J. Veh. Technol., vol. 6, pp. 1152–1163, 2025, doi: 10.1109/OJVT.2025.3559461.
[21] Y. Zhu, C. Miao, H. Xue, Y. Yu, L. Su, and C. Qiao, “Malicious Attacks against Multi-Sensor Fusion in Autonomous Driving,” in Proceedings of the 30th Annual International Conference on Mobile Computing and Networking, Washington D.C. DC USA: ACM, May 2024, pp. 436–451. doi: 10.1145/3636534.3649372.
[22] Dr. N. Katiyar, Dr. A. Shukla, and Dr. N. Chawla, “AI in Autonomous Vehicles: Opportunities, Challenges, and Regulatory Implications,” eatp, Apr. 2024, doi: 10.53555/kuey.v30i4.2373.
[23] T. H. H. Aldhyani and H. Alkahtani, “Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity,” Sensors, vol. 22, no. 1, p. 360, Jan. 2022, doi: 10.3390/s22010360.
[24] J. Wang, L. Zhang, Y. Huang, J. Zhao, and F. Bella, “Safety of Autonomous Vehicles,” Journal of Advanced Transportation, vol. 2020, pp. 1–13, Sep. 2020, doi: 10.1155/2020/8867757.
[25] E. Yurtsever, J. Lambert, A. Carballo, and K. Takeda, “A Survey of Autonomous Driving: Common Practices and Emerging Technologies,” IEEE Access, vol. 8, pp. 58443–58469, 2020, doi: 10.1109/ACCESS.2020.2983149.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY