ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(4):1-9

REVIEW ARTICLE

A Review on Security Threats and Vulnerabilities in Connected and Autonomous Vehicles

Sumeet Mathur*

Department of Computer Science, University of Waikato NZ - Joint Institute, Zhejiang University, Hangzhou, China

Received on: 12-10-2025; Revised on: 18-11-2025; Accepted on: 05-12-2025

ABSTRACT

Connected and autonomous vehicles (CAVs) are transforming modern transportation by integrating advanced sensing, communication, and intelligent control technologies. However, the increasing connectivity of these vehicles also expands their exposure to cyber threats, raising significant concerns regarding safety, privacy, and system reliability. This paper provides a comprehensive review of the security threats, vulnerabilities, and defense mechanisms associated with CAV ecosystems. It examines passive and active attacks targeting perception systems, communication protocols, control layers, and cloud-based infrastructures, emphasizing how compromised components can endanger vehicle operation and passenger safety. A detailed analysis of key vulnerability parameters – including software flaws, sensor manipulation, protocol weaknesses, supply chain issues, and regulatory gaps – highlights the multidimensional nature of CAV cybersecurity risks. The paper further reviews state-of-the-art defense strategies such as encryption-based methods, intrusion detection systems, authentication frameworks, and blockchain-supported architectures. By consolidating current research and identifying existing gaps, this study underscores the need for resilient, scalable, and adaptive cybersecurity frameworks to ensure the safe deployment of CAVs in future intelligent transportation systems.

Key words: Blockchain, connected and autonomous vehicles, cybersecurity, encryption, intrusion detection systems

INTRODUCTION

According to the World Health Organization (WHO), annual traffic accidents account for 1.3 million, and it is considered the first cause of death among young people aged 5–29 years old. According to the WHO statistics, every 24 s, a fatal accident occurs. Even with the presence of many preventive safety measures such as airbags, antilock brakes, and other built-in technologies that can help many people involved in accidents to survive, the number of traffic accidents continues to rise.[1] The impact of traffic accidents is not only restricted to increasing the number of road fatalities and injuries but is considered a prime factor in holding back economic growth.[2] The economic losses and monetary burden associated with traffic accidents have an adverse and significant impact on society. Consequently, innovative and industrial automotive networking solutions have emerged out of necessity to address many safety and non-safety issues. These solutions included the introduction of connectivity into vehicles named connected vehicles (CVs) and autonomous vehicles (AV), which, as a result, has been reshaping the transportation industry. AVs are also known as self-driving cars that require little of driver's assistance.[3] It is important to understand the difference between the terms AV, "connected vehicle (CV)," and "connected autonomous vehicle (CAV)."[4]

To automatically operate a vehicle on its own, the AV relies on the sensors installed in the vehicle that helps in inspecting the surrounding environment. Sensors such as the global positioning system and high-definition cameras record the position of the car and review other elements of traffic around the AV. With the built-in software functionality and smart algorithms, AVs can then identify the obstacles on the road such as road markings, preceding and following vehicles, vehicle on adjacent lanes, traffic signals, presence

Address for correspondence:
Sumeet Mathur
E-mail: sumeet.mathur@hotmail.com

of pedestrians, cyclists, and other infrastructure installations. The proper data acquisition, processing, and communication, on an AV is very important to ensure the driving safety.

The advent of autonomous connected vehicle (ACVs) poses a significant threat to future data security and mobility, providing hackers with novel avenues to carry out destructive assaults. Integrating federated reinforcement learning (FRL) with blockchain (BC) can protect ACVs from dangerous threats.[5] Although FRL and BC have distinct characteristics, they can be used together to tackle many privacy and security issues related to ACVs.[6] FRL can enhance BC's design by enhancing its safety, efficiency, and effectiveness. The unchangeability of data and the trust mechanism offered by BC enhance FRL-driven solutions' transparency, dependability, and comprehensibility. Figure 1 shows ACVs' basic data privacy and security models in smart city environments. The ACVs can gather personal data in many scenarios.

Modern cars consist of many interconnected subsystems and computers which control every aspect of the car's functionality. A software malfunction in a car could in a worst case scenario not only lead to substantial brand damage and loss of revenue for the manufacturer but also risk the lives of the users and pose a risk to their environment.[7] These robust systems must, however, also be durable in other ways than merely physical. Just like computers, cars are now also at risk of malicious attacks. Vulnerabilities can be exploited which can lead to software or hardware malfunction, data leaks or a variety of other results, the worst case being life-threatening situations.[8]

Structure of the Paper

The paper is structured as follows: Section II describes the architecture of CAVs, covering perception, communication, and control layers. Section III outlines major security threats, including passive and active attacks. Section IV details key vulnerabilities across vehicle systems. Section V presents the comparative literature review. Finally, Section VI provides the conclusion and future research directions.

CONNECTED AND AV (CAV) ARCHITECTURE

CAVs consist of three main layers. The perception layer uses sensors such as cameras, LiDAR, radar, and ultrasonic sensors to detect objects, lanes, and surroundings. The network and communication layer enables data exchange through vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle to everything (V2X) for real-time awareness. The application and control layer acts as the vehicle's "brain," integrating data to perform path planning, control, decision-making, and advanced driver assistance system (ADAS) functions, ensuring safe and efficient autonomous driving.

Perception Layer

The perception layer is responsible for enabling the vehicle to "see" and understand its environment. It

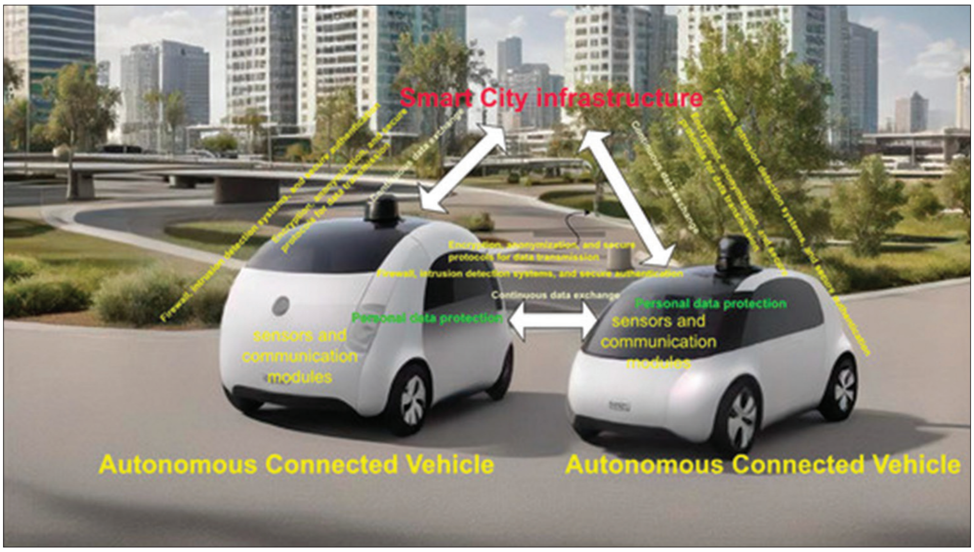
Smart City infrastructure
Firewall, intrusion detection systems, and secure authentication
Encryption, anonymization, and secure protocols for data transmission
Continuous data exchange
Continuous data exchange
Encryption, anonymization, and secure protocols for data transmission
Firewall, intrusion detection systems, and secure authentication
Encryption, anonymization, and secure protocols for data transmission
Firewall, intrusion detection systems, and secure authentication
Continuous data exchange
Personal data protection
sensors and communication modules
Personal data protection
sensors and communication modules
Autonomous Connected Vehicle
Autonomous Connected Vehicle

Figure 1: Basic model of data privacy and security in autonomous connected vehicles in smart city environments

uses a combination of sensors to detect objects, pedestrians, vehicles, road signs, lane markings, and other environmental features, as shown in Figure 2.

Key components include:

- Cameras: Capture[9] visual information for lane detection, traffic signs, and object recognition
- Light detection and ranging (LiDAR): Uses laser pulses to create 3D maps of the surroundings, providing precise distance measurements
- Radar: Detects objects and their speed, especially in adverse weather conditions where cameras and LiDAR may be less effective
- Ultrasonic sensors: Used for short-range detection, such as parking assistance or collision avoidance in low-speed scenarios.

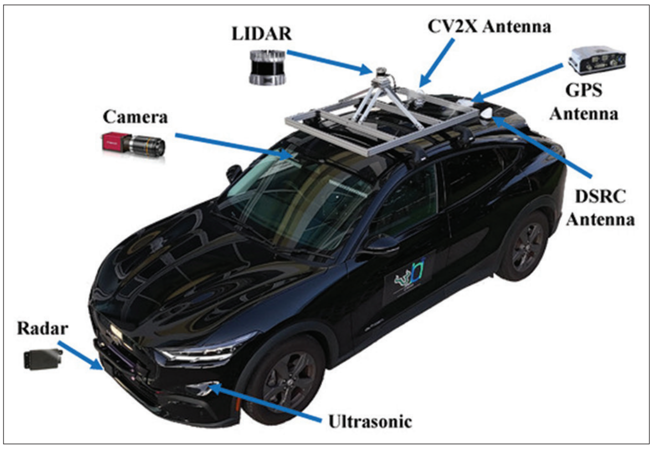

Figure 2: Sensors in connected and autonomous vehicle's enabling perception

The Network and Communication Layer

The network and communication layer enables vehicles to exchange data with each other and with infrastructure to enhance safety and efficiency, as shown in Figure 3.

V2X communication enables cooperative perception in intelligent transportation systems, allowing vehicles to exchange messages with other agents such as the infrastructures and pedestrians. V2X communication framework has four layers. The cloud layer serves as the central data hub, while the edge computing layer focuses on regional data processing with local gateway and multi-access edge computing host.[11] The infrastructure layer handles collaborative communications, and the client layer brings forth intelligent connected vehicle applications.

The following are introductions to different types of collaborative communications:

- V2V: Allows the exchange of real-time information between several vehicles, enhancing safety and efficiency on the road.
- V2I: Connects vehicles to traffic signals, road signs, and smart infrastructure for optimized routing and traffic management.
- Vehicle-to-network: Includes the interaction with central servers or cloud-based services, allowing the access and exchange of data with remote servers or services for various purposes.

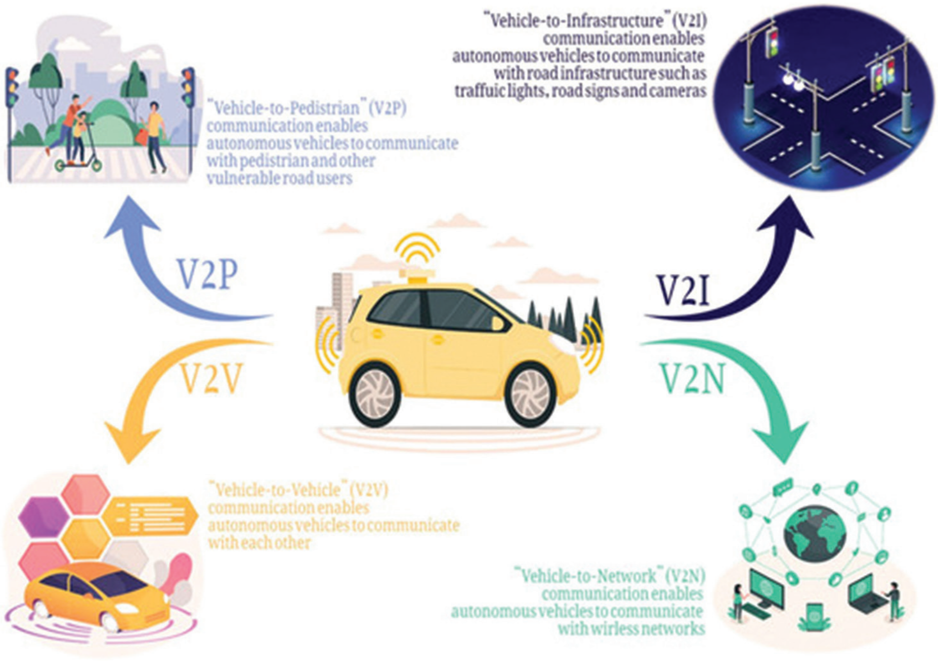
"Vehicle-to-Infrastructure" (V2I) communication enables autonomous vehicles to communicate with road infrastructure such as traffuic lights, road signs and cameras
"Vehicle-to-Pedistrian" (V2P) communication enables autonomous vehicles to communicate with pedistrian and other vulnerable road users
V2P
V2I
V2V
V2N
"Vehicle-to-Vehicle" (V2V) communication enables autonomous vehicles to communicate with each other
"Vehicle-to-Network" (V2N) communication enables autonomous vehicles to communicate with wirless networks

Figure 3: Autonomous vehicle communication scenarios[10]

- Vehicle-to-pedestrian: Involves the exchange of information with pedestrians and other vulnerable road users, which aims to help prevent accidents and improve overall pedestrian safety on the road.

Application and Control Layer (Decision-Making Algorithms)

The application and control layer is the "brain" of a CAV, responsible for decision-making, planning, and control of vehicle actions. It integrates perception and communication data to execute safe and efficient driving behaviors:

- Path planning algorithms: Determine optimal routes and trajectories based on sensor input and traffic conditions
- Control systems: Manage acceleration, braking, and steering to follow planned paths safely
- Decision-making algorithms: Handle complex driving scenarios such as lane changes, obstacle avoidance, and intersection management using artificial intelligence/machine learning (AI/ML) techniques.
- ADAS integration:[12] Supports ADASs such as adaptive cruise control, lane-keeping assist, and automated emergency braking, as shown in Figure 4.

SECURITY THREAT LANDSCAPE IN CAVS

CAV connectivity with the outside world is imperative, but this exposes the vehicle to experiencing hazardous cyberattacks. If fail to provide a shield against such attacks, hackers may initiate commands to electronic control units to misguide the vehicle, track its location, and steal passengers' private data from a remote location. This section explores the active and passive attacks on CAVs.

Passive Attacks

Identifying passive attacks is a challenging task as attackers cannot alter the contents of transmitted data. Both sender and receiver are unacquainted with the man in the middle of their activities. Such attacks monitor the traffic flow and do not interact with a third party.[14] The following passive attacks may be faced by CAVs:

- Eavesdropping: In such attacks, attackers passively steal the communication messages on the V2X communication channel. The CAN bus' potential vulnerability to cyber threats offers attackers the opportunity to gain access to the in-vehicle network and eavesdrop on the

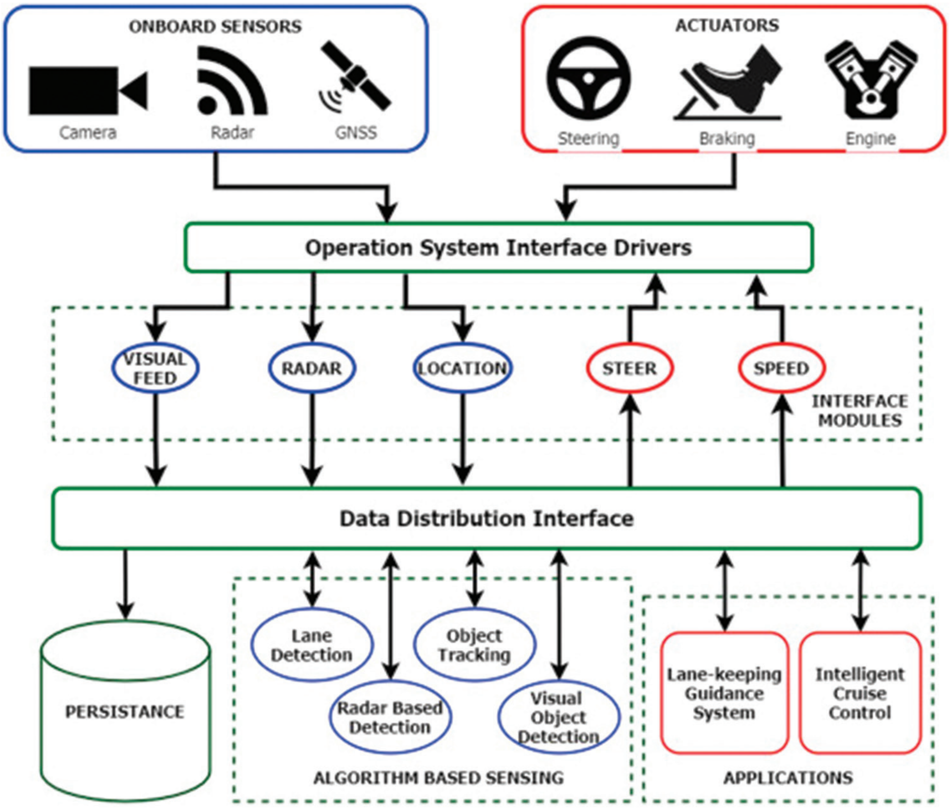

Figure 4: Advanced driver assistance systems enhancing driving safety and efficiency[13]

CAN transmission. The connectivity of CAVs with pedestrians, infrastructure, and vehicles gives more significance to eavesdropping attacks, as more private information may be listened to or monitored by hackers without permission

- Traffic analysis: Eavesdropping attacks may be prevented by using cryptography. However, attackers may use traffic analysis techniques to deduce information by observing traffic flow, that is, the length and time of the message, how many times (frequency) the vehicle communicated with X-person, the amount of data, and the presence or absence of the peculiar driver. Based on these properties, attackers may infer the user's working time and daily habits.

Active Attacks

In active attacks, the attackers intrude on the communication network, alter the contents of data, or generate new packets to damage the messages. Active attacks are much more dangerous than passive attacks, especially in a CAV environment, because alteration of messages can cause physical damage to drivers as well as the vehicle itself. The following active attacks may be faced by CAVs:

- Spoofing: In spoofing attacks, an unauthorized person intrudes into the network and poses as an authorized person. Based on false messages transmitted by the attacker, CAV may take the wrong decision. For instance, a serious accident could be caused if the vehicle believes that there is no obstacle in front. Similarly, attackers may direct all cars toward the wrong path, which ultimately causes traffic jams.
- Replay attacks: Replay attacks happen when a malicious user "sniffs" out data on the communication channel, captures it, and rebroadcasts it. In a replay attack, both the sender and receiver are verified, but they are unaware of the node in the middle intercepting the messages.
- Masquerade: In a masquerade attack, an unauthorized person impersonates a legitimate node and an authorized entity to gain access to information resources. The unavailability of encryption and lack of message authentication in CAN frames are two factors that facilitate the masquerade attacks.
- Denial-of-service (DOS): A DoS attack is a high-level security threat extensively used for many years to interrupt network operations by sending a vast number of high-priority messages toward hosts to overload them, and so, the host fails to provide service to legitimate users. In short, dummy messages are introduced to jam the network.[15] Thus, the efficiency and performance of the host will be reduced.

Vulnerabilities in Connected and Automated Vehicles

Table 1 summarizes the major vulnerability parameters affecting AVs and maps them to their corresponding application areas. It highlights weaknesses across software, communication protocols, sensors, AI systems, supply chains, and regulatory frameworks, emphasizing where security risks most commonly emerge within AV ecosystems.[16]

CYBER DEFENCE IN CAVS

In this section, the different cyber defense mechanisms for CAVs are discussed which can be broadly classified into three categories:[18] (A) Encryption based methods, (B) intrusion detection, and (C) authentication-based defense.[19]

Encryption-Based Methods

- Cryptography: Cryptography is a method of secure communication between authorized entities that creates cipher text from plain text.

Table 1: Key vulnerability parameters and application areas in autonomous vehicles[17]

Vulnerability parameter	Application area
Software and firmware flaws	Vehicle control systems, engine management, and infotainment systems
Communication protocols (V2V, V2I, V2X)	Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) communications
Sensor systems (LiDAR, GPS, cameras)	Navigation, object detection, collision avoidance, and environmental perception
Artificial intelligence and machine learning	Decision-making systems, autonomous driving algorithms, and real-time data analysis
Supply chain dependencies	Component sourcing, software updates, hardware integrity, and third-party vendors
Regulatory and legal gaps	Compliance with cybersecurity standards, data privacy laws, and liability in cyberattacks

Modern cryptography applies mathematical theories and models, computer science, electrical, and communication technology to enhance security mechanisms. Cryptographic hash functions create a short, bit-string digest for a long message, which can be helpful for creating a digital signature for the sender and quick verification by the receiver.

Intrusion detection system (IDS)

Intrusion is an illegitimate entry into a network without the authorized user's knowledge.[20] IDS acts as a defensive measure to prevent the same.[21] The IDS in cyber-physical system is used to detect compromised devices through scanning the sensors, control nodes, and actuators at optimal intervals.[22] Machine learning models are prevalently used to develop IDSs, which can be broadly classified into two categories:[23] anomaly-based detection and signature-based detection.[24]

- Machine learning techniques for IDS: Different ML techniques such as supervised, unsupervised, and reinforcement learning are used to detect cyber-attack on AVs. Deep reinforcement learning-based defense techniques are also gaining prominence, in real-time detection of black-hole, traffic control, jamming, and spoofing attacks on CAVs.
- Anomaly-based detection: In anomaly detection, the normal behavior is first identified and compared with the actual behavior of the vehicles. This includes movement of vehicles as well as network traffic, sensors data, and operating characteristics.
- Signature-based detection: Signature detection IDSs operate by matching the activities of participating nodes with known attack scenarios (signatures) stored in the database. Although signature-based IDSs have high detection accuracy for known attacks, they are ineffective for zero-day exploits and are easy to evade with minor changes in the attack signature.

Authentication-based defense

- User authentication: Strong authentication protocols are essential for securing AVs against unauthorized access and cyber threats. By implementing multi-factor authentication, digital certificates, and secure key management practices, the integrity and security of the vehicle's systems and data are maintained. These measures are crucial for ensuring the safe and reliable operation of AVs in an increasingly connected and complex digital environment.
- Firewall: A firewall is a network security technique that filters and controls incoming and outgoing network traffic having malicious features. Using rule-based techniques, firewalls can distinguish between legitimate and malicious networks in V2V/V2I communications.
- BC and trust-based defense mechanism: BC is a type of distributed ledger technology in which a digital ledger of the transactions are recorded with an immutable cryptographic signature (hash) that makes vehicle BC systems impossible to falsify. VANET BC-based systems ensure secure data sharing with additional features such as decentralization, distribution, immutability, flexibility, and transparency.

LITERATURE OF REVIEW

The reviewed literature collectively highlights the multifaceted security challenges faced by CAVs. Studies emphasize proactive approaches such as ethical hacking, anomaly detection, and firmware scanning to identify vulnerabilities across hardware, software, sensors, and communication systems. In addition, frameworks such as BC-based over-the-air (OTA) security and lifecycle-based cybersecurity demonstrate practical methods for mitigating risks, enhancing system resilience, and guiding automakers toward safe. A comparative summary of the various machine learning–based security approaches, datasets, and performance outcomes discussed in these studies is presented in Table 2.

Morić *et al*., analyzed these vulnerabilities from an ethical hacking perspective, emphasizing the importance of proactive testing and system resilience. It explores how ethical hackers can identify weaknesses before they are exploited and how advanced security mechanisms, such as IDSs, secure communication protocols, and adaptive architectures, can mitigate risks. In addition, the work highlights future challenges related to data privacy, regulatory inconsistencies, supply chain integrity,

Table 2: Based on the comparative literature review table, various machine learning approaches

Reference	Focus area	Key findings	Challenges	Key contribution	Limitations/gap
Morić *et al*., (2025)	Ethical hacking–based security assessment in CAVs	Ethical hacking proactively identifies vulnerabilities; advanced mechanisms (IDS, secure protocols, adaptive architectures) strengthen resilience	Data privacy concerns, regulatory inconsistencies, supply chain integrity issues, user trust	Lifecycle-based cybersecurity framework integrating ethical hacking	Requires validation across large-scale and diverse CAV deployments
Memon and Saini (2025)	Blockchain-based security enhancement for OTA updates	Blockchain verification significantly improves OTA update security with minimal system overhead	Integration with existing infrastructures; large-scale deployment in real fleets	Cost-effective, low-overhead, scalable OTA security architecture	Proof-of-concept only; lacks real-world implementation and long-term testing
Kumar *et al*., (2025)	Comprehensive review of AV cybersecurity threats and solutions	Highlights cybersecurity risks, equipment vulnerabilities, and emerging solutions (blockchain, ML, encryption)	Need for improvement in current cybersecurity protocols; evolving threat landscape	Holistic evaluation of AV cybersecurity measures and potential enhancement strategies	Broad review; lacks experimental validation or implementation-level insights
Sun *et al*. (2024)	Hardware security analysis of in-vehicle terminals	Vulnerability mining validates hardware risks; provides mitigation guidelines to strengthen terminal security	Hardware design flaws; lack of proactive verification methods in industry	Practical recommendations for improving hardware security and managing vulnerabilities	Focused only on hardware; does not address software, network, or system-level threats
Niroumand *et al*., (2024)	CAV vulnerability modeling and attack detection from control-system perspective	Proposes generalized attack model; analyzes vulnerabilities and detection/mitigation strategies for CAV control systems	Limited research treating CAVs as control systems; complexity of multi-vector attacks	Multi-vector mitigation strategy to strengthen CAV security and safety	Requires real-world validation; limited integration with full CAV ecosystem
Shiwen *et al*. (2023)	Firmware vulnerability scanning in intelligent connected vehicles	Firmware scanning framework improves understanding of component-level security risks	Real-time firmware updates and patch management	Enhances theoretical and practical understanding of firmware-level vulnerabilities	Does not integrate network, sensor, or communication-layer vulnerabilities

CAVs: Connected and autonomous vehicles, IDS: Intrusion detection system, OTA: over-the-air, AV: autonomous vehicle, ML: Machine learning

and the need for user trust. The findings highlight the necessity of a lifecycle-based approach to CAV cybersecurity that incorporates ethical hacking as a central strategy. Through this framework, the paper aims to contribute to developing safer, more trustworthy AV ecosystems.[25]

Memon and Saini outlines the context and motivation for this research, reviews current BC-based secure mechanisms for OTA updates, details the proposed method, and presents the implementation and evaluation results from our proof of concept. The results demonstrate that the proposed BC-based verification system significantly enhances the security of OTA updates against common cyber attacks, with minimal overhead and low impact on system performance. In addition, the proposed architecture can be easily integrated into existing OTA update infrastructures, making it a cost-effective solution for protecting CAVs against potential cyber threats at a scale.[26]

Kumar *et al*., provided a comprehensive review of various cybersecurity threats associated with AVs and presents potential solutions. In addition, it examines the vulnerabilities of the sophisticated equipment used in AVs. This article aims to enhance the understanding of the safety and security concerns associated with AVs and offers insights into the importance of cybersecurity in this evolving technological field. Furthermore, this article addresses the current state of cybersecurity measures in AVs, evaluating the effectiveness of existing protocols and identifying areas that require improvement. It also explores emerging technologies and strategies that can enhance the security of AVs, such as BC for secure data transactions, machine learning for threat detection, and robust encryption methods.[27]

Sun *et al*., analysed the hardware security of in-vehicle terminals, summarized the hardware security risks existing in intelligent in-vehicle terminals at this stage, verified the security through the method of vulnerability mining, and put forward reasonable suggestions on how to avoid hardware security problems, aiming at guiding automobile enterprises on how to deal with and improve the existing hardware security problems at this stage, and avoiding known risks in advance at the design stage. In addition, the study emphasizes improving and strengthening the hardware security of in-vehicle terminals, helping automobile enterprises master basic security verification methods, and effectively manage and repair identified vulnerabilities.[28]

Niroumand *et al*., aim to propose a generalized attack model, discuss the current vulnerabilities of CAVs, and provide an overview of the previous and current detection and mitigation approaches. A variety of academic and industrial studies have been conducted on categorizing attacks targeting CAVs and their countermeasures. Nonetheless, few have addressed CAVs as a control system. This research focuses on modeling vulnerabilities, detecting cyberattacks, and mitigating them from the perspective of control systems. Furthermore, we suggest utilizing a multi-vector mitigation strategy to enhance the general safety and security of CAVs.[29]

Shiwen *et al*., employed principles of intelligent CV firmware program vulnerability scanning technology, accompanied by a data processing framework. The findings provide valuable insights for improving the security of intelligent CV components. By addressing the research gap, this study contributes to the theoretical understanding and practical mitigation of security risks in the intelligent CV ecosystem. Enhancing the security of component firmware will lead to a safer and more robust intelligent CV infrastructure, with implications for the industry, consumers, and society as a whole.[30]

CONCLUSION AND FUTURE WORK

CAVs represent a pivotal advancement in intelligent transportation, yet their extensive reliance on sensors, communication networks, and embedded software exposes them to a wide range of cybersecurity threats. This review highlights the critical vulnerabilities across perception systems, control algorithms, V2X communication channels, hardware components, and firmware layers. By examining both passive and active cyberattacks, the study demonstrates how malicious interference can compromise vehicle safety, privacy, and operational reliability. The literature further underscores the importance of proactive defense strategies, including ethical hacking methodologies, BC-secured OTA updates, vulnerability modeling, and firmware scanning. These approaches collectively emphasize the need for continuous monitoring, adaptive intrusion detection, and robust authentication frameworks to counter evolving threats. Despite progress in CAV cybersecurity, challenges remain due to rapidly advancing attack techniques, insufficient regulatory standardization, and integration issues across complex vehicle ecosystems. Strengthening cybersecurity requires a coordinated effort among researchers, automakers, policymakers, and technology providers to develop scalable, interoperable, and future-proof security solutions. Ultimately, ensuring the safe and trustworthy deployment of CAVs depends on a holistic, lifecycle-based approach that anticipates vulnerabilities and builds resilience into every layer of vehicle architecture.

Future research should prioritize the development of intelligent, self-adaptive cybersecurity frameworks capable of addressing zero-day vulnerabilities and dynamic attack patterns in real time. Integrating AI-driven intrusion detection, quantum-resistant cryptography, and BC-based trust mechanisms can further enhance end-to-end vehicle security. In addition, large-scale testing environments, digital twin simulations, and unified global cybersecurity standards are essential to validate emerging solutions and support the safe, reliable deployment of CAVs in increasingly complex transportation ecosystems.

REFERENCES

1. Abdelkader G, Elgazzar K, Khamis A. Connected vehicles: Technology review, state of the art, challenges and opportunities. Sensors (Basel) 2021;21:7712.
2. Sagili SR, Kinsman TB. Drive Dash: Vehicle Crash Insights Reporting System. In: 2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA). IEEE; 2024. p. 1-6.
3. Dudhipala A, Karne R, Pativada PK. Mapping Ai failure modes in autonomous vehicles: A structured review of causes and mitigation strategies. Indian J Comput Sci Eng 2025;16:43-53.
4. Ahmed HU, Huang Y, Lu P, Bridgelall R. Technology developments and impacts of connected and autonomous vehicles: An overview. Smart Cities 2022;5:382-404.
5. Alam T. Data privacy and security in autonomous connected vehicles in smart city environment. Big Data Cogn Comput 2024;8:95.
6. Cherukuri BR. AI-driven security solutions: Combating cyber threats with machine learning models. Int J Multidiscip Res 2024;6:1-17.
7. Gülsever M. A Study on Vulnerabilities in Connected Cars. Sweden: KTH Royal Institute of Technology School of Electrical Engineering and Computer Science; 2019.
8. Patel R. Remote troubleshooting techniques for

hardware and control software systems: Challenges and solutions. Int J Res Anal Rev 2024;11:933-9.

9. Ban XJ, Yang D, Wang J, Hamdar S. Editorial: Connected and automated vehicles (CAV) based traffic-vehicle control. Transp Res Part C Emerg Technol 2020;112:116-9.
10. Sadaf M, Iqbal Z, Javed AR, Saba I, Krichen M, Majeed S, *et al*. Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. Technologies 2023;11:117.
11. Zhang X, Li J, Zhou J, Zhang S, Wang J, Yuan Y, *et al*. Vehicle-to-everything communication in intelligent connected vehicles: A survey and taxonomy. Automot Innov 2025;8:13-45.
12. Józefczyk J. Decision-making algorithms in two-level complex operation system. Decis Support Syst 2004;38:171-82.
13. Bhatti G, Mohan H, Singh R. Towards the future of smart electric vehicles: Digital twin technology. Renew Sustain Energy Rev 2021;141:110801.
14. Saeed Z, Masood M, Khan MU. A review: Cybersecurity challenges and their solutions in connected and autonomous vehicles (CAVs). JAREE J Adv Res Electr Eng 2023;7:44-51.
15. Arora S, Khare P, Gupta S. AI-Driven DDoS Mitigation at the Edge: Leveraging Machine Learning for Real-Time Threat Detection and Response. In: 2024 International Conference on Data Science and Network Security (ICDSNS); 2024. p. 1-7.
16. Ande BR. Data processing device for real-time vulnerability detection in large-scale data streams. 2025;2025:6459961.
17. Sarsam SM. Cybersecurity challenges in autonomous vehicles: Threats, vulnerabilities, and mitigation strategies. SHIFRA 2023;2023:34-42.
18. Prajapati V. Enhancing threat intelligence and cyber defense through big data analytics: A review study. J Glob Res Math Arch 2025;12:1-6.
19. Tanaji BA, Roychowdhury S. A survey of cybersecurity challenges and mitigation techniques for connected and autonomous vehicles. IEEE Trans Intell Veh 2025;10:4742-57.
20. Bilipelli AR. AI-driven intrusion detection systems for large- scale cybersecurity networks data analysis: A comparative study. Tijer Int Res J 2024;11:922-8.
21. Patel D. Leveraging blockchain and ai framework for enhancing intrusion prevention and detection in cybersecurity. Tech Int J Eng Res 2023;10:853-8.
22. Narang S, Gogineni A. Zero-trust security in intrusion detection networks: An AI-powered threat detection in cloud environment. Int J Sci Res Mod Technol 2025;4:60-70.
23. Karne PG, Pasham AK. Classification of Intrusion Detection System and its Methodologies. In: International Conference on Research Challenges in Engineering and Technology; 2016.
24. Nutalapati P, Vummadi JR, Dodda S, Kamuni N. Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data. In: 2025 International Conference on Data Science and Its Applications (ICoDSA). IEEE; 2025. p. 880-5.
25. Morić Z, Matahlija D, Kapulica A. Automotive Hacking: Security Risks in Connected and Autonomous Vehicles. In: 2025 15th International Conference on Advanced Computer Information Technologies (ACIT); 2025. p. 584-8.
26. Memon Z, Saini I. Enhancing Security of Over-the-Air Updates in Connected and Autonomous Vehicles using Blockchain: Proof of Concept. In: 2025 International Wireless Communications and Mobile Computing (IWCMC); 2025. p. 349-54.
27. Kumar US, Halder S, Sethi BK. Comprehensive Review of Cybersecurity Vulnerabilities and Safety Concerns in Autonomous Vehicles. In: 2025 IEEE 1st International Conference on Smart and Sustainable Developments in Electrical Engineering (SSDEE), IEEE; 2025. p. 1-6.
28. Sun D, Yu M, Guo Z, Liu T. Hardware Security Vulnerability Mining Techniques for Intelligent Connected Vehicles. In: 2024 3rd International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology (AIoTC); 2024. p. 138-43.
29. Niroumand FJ, Bonab PA, Sargolzaei A. Security of Connected and Autonomous Vehicles: A Review of Attacks and Mitigation Strategies. In: SoutheastCon 2024, IEEE; 2024. p. 1197-204.
30. Shiwen SS, Zhen GZ, Tianling LT, Chenya BC, Yuqiao NY, Yang Y. Research and Analysis of Vulnerabilities in Intelligent Connected Vehicle Components. In: 2023 6th International Conference on Data Science and Information Technology (DSIT); 2023. p. 255-64.