Grenze International Journal of Engineering and Technology, January Issue

Towards Secure Autonomous Mobility: A Survey on CAV Cybersecurity

Mrs. Dakshayani G[1] and Dr. R Vignesh[2]
[1]Dept. of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India
Email: dakshayani@fcrit.ac.in
[2]Dept. of Artificial Intelligence and Machine Learning, Karunya Institute of Technology and Sciences, Coimbatore, India
Email: vignesh@karunya.edu

***Abstract*— Connected autonomous vehicles (CAVs) are receiving notable attention recently as they are trying to replace manual driving with autonomous systems. CAVs are enhancing the modern-day transportation by integrating various sensors, perception, decision making and vehicle-to-everything (V2X) communication technologies. This innovative setting enables improved road safety by minimizing the risk of traffic accidents resulting from human error. The goal of CAV is to improve road safety, enhance the driving experience, increase efficiency and enable future technologies like autonomous driving. The reliance of CAVs on in-vehicle electronic and communication protocols make them highly susceptible to cyberattacks. Cybersecurity breaches in CAVs may lead to serious consequences, including loss of privacy and data manipulation to physical harm and disrupted traffic. This study focuses on the different threats, attacks, and countermeasures related to CAVs. It also examines the motivations behind these attacks and the defense mechanisms available to counter them. By reviewing existing solutions along with emerging technologies and trends, the study aims to contribute toward the safe and secure deployment of autonomous mobility.**

***Keywords*— Connected Autonomous Vehicles (CAVs), Autonomous Vehicles (AVs), Vehicle to Vehicle(V2V), Vehicle to Infrastructure(V2I), Vehicle to Everything(V2X), Intelligent Transportation Systems (ITS), Electronic Control Unit (ECU), Original Equipment Manufacturer (OEM).**

I. INTRODUCTION

Technological advancements have enhanced productivity, safety, and the overall quality of human life, with transportation being one of the most affected domains. The introduction of Intelligent Transportation Systems (ITS) has played a vital role in this transformation. Among these, Connected Autonomous Vehicles (CAVs) mark a major leap in transportation technology, promising greater safety, efficiency, and convenience. These vehicles are designed to optimize traffic flow, ease congestion, improve road safety, minimize environmental impact, and enrich the travel experience. By automating driving tasks, they not only reduce driver stress and the likelihood of accidents but also improve mobility for individuals with physical disabilities

CAVs represent one of the most important innovations within Intelligent Transportation Systems. They integrate multiple sensors for perception, advanced decision-making algorithms, and real-time control systems to achieve high levels of automation [1].

Grenze ID: 01.GIJET.12.1.126

AVs are equipped with advanced sensors like GPS, IMU, LiDAR, RADAR, and cameras, combined with powerful processors and machine learning technology. This allows AVs to interpret the surroundings and operate independently of human intervention. In addition, they take input from V2V, V2I, and V2X communication [2] to exchange vital information about vehicle position, speed, and trajectory with other vehicles and roadside infrastructure.

The increased connectivity and reliance on sensors broaden the potential attack surface of AVs. Modern Connected Autonomous Vehicles gather data from their environment and transmit it to in-vehicle Electronic Control Units (ECUs) and to external entities like other vehicles, roadside units (RSUs), user devices, and Original Equipment Manufacturers (OEMs). These communications, whether occurring within the vehicle's internal networks or across V2X channels, must satisfy most crucial requirements such as low latency, high reliability, scalability, and very important robust security [3]. Without adequate safeguard measures the adversaries could exploit these channels to capture sensitive data such as vehicle location and movement patterns or manipulate control signals, potentially leading to severe safety risks.

In this study, we first present CAVs driving technology overview, covering sensor perception modules, decision-making, control systems, operating systems, hardware platforms, and cloud integration. We then outline the levels of driving automation before discussing the security vulnerabilities, potential attack vectors, and existing defence mechanisms in CAVs.

II. AUTONOMOUS VEHICLE DRIVING TECHNOLOGY OVERVIEW

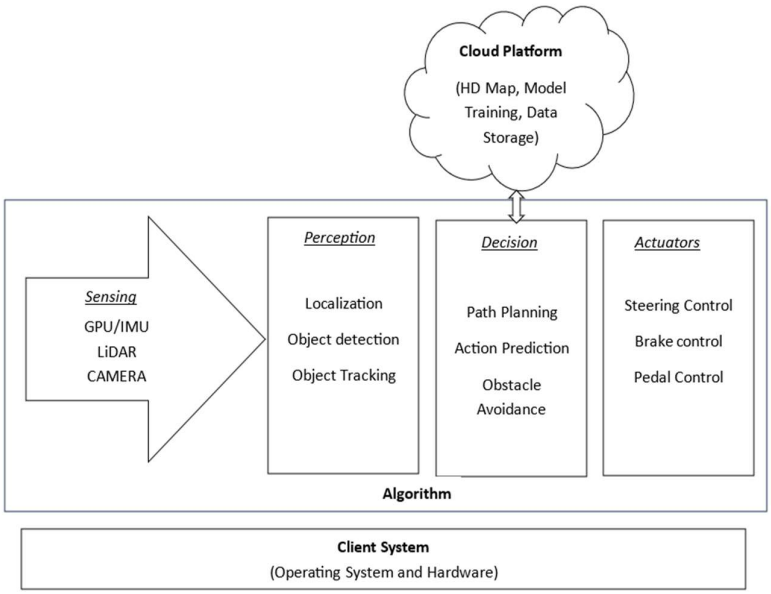

Fig 1: Autonomous Vehicle Driving Architecture

Autonomous driving does not rely on a single technology; rather, it is the result of seamless coordination among multiple subsystems. As shown in Fig. 1, it consists of three key elements such as Algorithms, Client System, and the Cloud Platform.

The algorithmic subsystem includes technology for sensing, perception, and decision-making, that is critical for handling complex driving scenarios. These algorithms analyze the raw data generated by sensor about the surrounding to extract meaningful information, which in turn help vehicle to understand its environment and take appropriate actions. Client System comprises of operating system and hardware platform. It integrates algorithms designed to address the real-time performance and reliability needs, enabling the vehicle to effectively respond to dynamic road conditions.

The cloud platform provides capabilities for high-definition mapping, ML/DL model training, large-scale simulation, and data storage. With the help of its offline computing and storage capabilities, it supports tasks such as testing new algorithms, updating HD maps, and developing improved recognition, tracking, and decision-making models [4].

According to Society of Automotive Engineers (SAE) standards, vehicle automation is classified into six levels, it's the popular framework adopted by organizations such as the International Organization of Motor Vehicle Manufacturers (OICA), the German Federal Highway Research Institute (BASt), and the U.S. National Highway Traffic Safety Administration (NHTSA). These levels range from no automation to full automation refer fig 2:

- Level-0: No automation; the driver does all tasks; car gives only alerts but no actual help.
- Level-1: Driver assistance; limited functions such as Adaptive Cruise Control or Traffic Sign Recognition are automated, but the driver controls acceleration, braking, and monitors the environment.
- Level-2: Partial automation; the vehicle can manage steering task and acceleration task, but the driver will be responsible for safety-critical tasks.
- Level-4: High automation; the vehicle performs all driving functions, with driver intervention needed only in unsafe or exceptional situations.
- Level-5: Full automation; the vehicle operates on its own without any human intervention, making the driver essentially a passenger.

Standard/ Level	LEVEL-0	LEVEL-1	LEVEL-2	LEVEL-3	LEVEL-4	LEVEL-6
SAE	No Automation	Driver Assistance	Partial Automation	Conditional Automation	High Automation	Full Automation
NHTSA	No Automation	Function Specific Automation	Combined Function Specific Automation	Limited Self Driving Automation	Full Self Driving Automation	
BASt	Driver Only	Driver Assistance	Partial Automation	High Automation	Full Automation	
Driver	The driver does everything.	The driver is still in full control.	The driver must stay alert and ready to take over at any moment	The driver doesn't need to watch constantly, but must be ready to step in if asked.	The driver may still need to help in rare or unusual cases.	No human driver is needed — everyone is just a passenger.
Vehicle	The car only gives warnings or alerts, but no actual help.	The car can give a little help, like lane keeping or automatic braking.	The car can handle steering, braking, and acceleration in some cases.	The car can manage most driving tasks in certain conditions.	The car can drive on its own in many situations without driver input.	The car handles everything in all conditions.

Fig 2: Levels of automation

III. Threats in Connected Autonomous Vehicles

The emergence of connected autonomous vehicles signals the transformation of transportation sector with a commitment towards improved safety, operational efficiency, and user convenience through advanced sensors technology, algorithm and communication. In spite of such advancement in technology and communication protocols, there still exist lack of trust on CAVs due to cybersecurity threats. The reliance of CAVs on sensors and V2X communication for automation in autonomous vehicle is introducing significant cybersecurity vulnerabilities with increased attack vector. The automation of autonomous vehicles in intra-vehicle communication is driven entirely by sensor data and interactions with connected vehicles and smart infrastructure.

They completely dependent on data gathered from the vehicle's onboard sensors, along with communication with other CAVs and intelligent infrastructure. On the other hand, inter-vehicle communication is built upon collaboration among CAVs, enabling V2V and V2I communication. Due to the dependency of vehicles on sensors and commination channels there are different attack surfaces through which attacker is hacking the system. For instance, electronic control units (ECUs) which pay a major role in AVs, they are equipped with several critical electronic control units, such as the engine control module, brake control module, vision system, navigation module, door lock receiver, HVAC system, and transmission control module, so on and so forth can potentially be hacked [5], Navigation systems that rely on GPS is cost effective solution for tracking vehicle location, movement, and timing. Aerial vehicles largely rely on GPS receivers which make them more

susceptible to attack such as spoofing [6]. CAVs rely heavily on sensor data, information exchanged with other vehicle and road side unit data. Hence, faulty sensor readings caused by either malicious cyber-attacks or erroneous vehicle sensors can produce hazardous outcomes and potentially lead to fatal accidents [7]. Vehicular communication which includes vehicle to vehicle (V2V) communication, vehicle to infrastructure (V2I) communication and vehicle to everything (V2X) communication. In communication layer, cybersecurity vulnerabilities are sending false messages, using telematics and infotainment systems to gain control of vehicle operations and intercepting on messages sharing among vehicles. The sensor and communication vulnerabilities can impact the control system capability to analyze digital data and handle real-time vehicular tasks like automatic steering control, lane change decision, and brake task. seriousness of attacks estimated according to the scenario and the level of disruption caused by the adversary. For instance, within the range of potential vulnerabilities associated with connected autonomous vehicles, GPS spoofing and camera blindness are classified as high alert threats. In contrast, RADAR and LiDAR confusion, and the manipulation of intra vehicular devices and sensors are categorized as medium range threats. [8].

IV. Attacks Exploiting the Vulnerabilities in Autonomous Vehicle

A. GPS spoofing and jamming

GPS spoofing, often known as GPS jamming, is an attack where hackers send fictitious signals or data. As GPS receivers are configured to receive stronger signals, the unrealistic signal's power grows, and over time, the vehicle's position steadily deviates from the intended target [9].

B. IMU sensor spoofing

The IMU comprises of gyroscope and accelerometer, which provides information about the vehicle orientation, acceleration, and velocity. They also keep an eye on how environmental dynamics, such as the gradient change. It is possible to alter the sensor data in order to identify the road's gradient. On incline roads, it slows down the vehicle's movement, which in turn slows down the cars behind it [9].

C. LiDAR spoofing

LiDAR works by sending laser pulses and measuring the time-of-flight to detect object distance. If a hacker sends fake laser pulses at the same frequency and timing, the LiDAR system may believe there’s an obstacle when there isn’t. This false obstacle detection can cause the autonomous vehicle to slow down or stop unnecessarily.[9]

D. Camera Blinding Attack

Autonomous vehicle cameras rely on CMOS image sensors for tasks like lane detection, traffic sign recognition, and obstacle detection. By shining high-intensity light into the camera, the attacker overexposes the sensor, creating glare or white-out in the captured image. This can cause false detections or missed detections, leading to safety risks.[9]

E. ECU Firmware Tampering Attack

It is a direct access vehicle cyberattack in which an attacker, having physical access to the Engine Control Unit, re-flashes it with malicious or modified firmware to alter its intended functionality. By manipulating the ECU’s memory, security keys, and control logic, the attacker can induce unsafe or unintended actions in vehicle subsystems, such as disabling safety mechanisms, altering sensor outputs, or manipulating actuator behavior. Since the ECU firmware is critical for coordinating sensors and actuators, such tampering can have severe safety implications and persist until the firmware is securely restored. Preventing this attack requires secure boot processes, cryptographic firmware signing, hashing for integrity verification, and authenticated software updates.[10]

F. Communication Network Attack

A V2X network attack exploits vulnerabilities in vehicle-to-everything communication, which connects vehicles with other cars, infrastructure, smartphones, cloud services, and external devices. While enabling features like traffic coordination and real-time updates, V2X relies on channels such as Wi-Fi, Bluetooth, GSM, DSRC, WAVE, and IEEE 802.11p, all of which have known security flaws that attackers can exploit. Compromising these communication links can allow unauthorized access, data interception, or injection of malicious commands, especially when interacting with unfamiliar devices or compromised cloud servers, posing significant safety and privacy risks.[11]

G. Distributed Denial of Service (DDoS) Attack

DDOS attack on connected vehicles involves overwhelming the vehicle's communication or processing resources with excessive traffic from multiple compromised sources, disrupting normal operations. This can block critical V2X communications, hinder sensor or control system responses, and lead to traffic flow disruptions, infrastructure damage, or even vehicle collisions, posing serious safety risks to passengers.[12]

H. Black and Grey Hole Attacks

A vehicle under attack stops sending all data packets (black hole) or certain packets (grey hole) to other AVs. This means that other AVs can't get important safety information, such forward collision warnings.[12]

I. Jamming

An attacker sends out signals to damage the data or stop communication channels from working.[12]
False message injection: A vehicle under attack creates false messages or modifies received messages and disseminates them.[12]

K. Eavesdropping

The compromised car obtains private and sensitive information by using fake identities to obtain unauthorized access to communication packets.[12]

L. Certificate replication

An attacker hides itself from certification authorities by duplicating the certificates of authentic vehicles.[12]

M. Sybil Attack

An adversary generates several fake identities to establish trust with authentic CAVs.[12]

N. Impersonation

Malicious actors impersonate a trusted entity within the network to gain unauthorized access to sensitive information.[12]

O. Adversarial Attacks on Autonomous vehicles:

Adversarial attacks are Intentional alterations of input data that exploit the weaknesses of ML and DL models performance. By adding small perturbations or noise, often unnoticeable to humans, these attacks can mislead models into making incorrect predictions or classifications. Such effects reduce the reliability of AI systems and can have serious consequences in safety-critical applications [13].

V. Attack Motivations on CAVs

- Interrupting Operations: -Attackers aim to disrupt key components of autonomous vehicles, making the self-driving mode unavailable. This is same as traditional network attack which is popularly known as Denial-of-Service attacks.
- Gaining Control: -In this type of attack, adversaries obtain control over the vehicle's core functions. They may alter its route, trigger unnecessary emergency braking, or manipulate its speed. Such actions pose direct safety threats to vehicle occupants and other road users.
- Stealing Information: -Another major threat involves the extraction of sensitive or confidential data from the vehicle. Information such as driving patterns, passenger details, or navigation records can be stolen and later exploited for further malicious activities [14].

VI. Existing Countermeasures

To address the wide range of cybersecurity threats confronting autonomous vehicles (AVs), researchers and industry practitioners have developed several defensive strategies. These countermeasures are designed to safeguard essential systems and data requirements from unauthorized access, alterations, and damages.

A. Intrusion Detection Systems (IDSs)

Intrusion Detection Systems (IDSs) are an essential element of the AV cybersecurity framework. They operate by constant observation of network traffic and system operations to detect malicious activity, thereby protecting critical vehicle functions and sensitive data. IDSs can detect a variety of threats, including unauthorized access, abnormal traffic flows, and malware infections, using two main approaches:

- Signature-based detection: Recognizes previously identified attack patterns.
- Anomaly-based detection: Signals the deviations from normal system behavior that may indicate novel or unknown threats.

In recent years, advanced IDSs have begun to incorporate machine learning and analytics, allowing them to analyse historical data, detect complex attack patterns, and respond to new threats as they emerge.
IDSs are typically divided into two categories:

- Network-based IDSs (NIDSs): Monitor data flow occurring inside the vehicle and across external connections, detecting protocol exploits, denial-of-service attempts, and malicious data exchanges.
- Host-based IDSs (HIDSs): Concentrate on individual devices, such as sensors or control units, to detect suspicious activities like unauthorized file modifications, abnormal processes, or attempts to execute malicious code.

When combined, NIDSs and HIDSs strengthen the overall resilience of AVs by providing real-time alerts and enabling rapid responses to cyber incidents. This layered approach helps maintain safety, reliability, and system integrity [15].

B. Encryption

Encryption serves as a cornerstone of cybersecurity in autonomous vehicles, protecting sensitive data both during transmission and while stored. By converting information into coded formats, encryption prevents unauthorized access and ensures confidentiality and integrity.
The cryptographic methods like RSA and the Advanced Encryption Standard (AES) are frequently employed for its speed and efficiency in protecting vast amount of data. The symmetric algorithm AES is praised for its high speed and effectiveness in protecting vast amounts of data, whereas the asymmetric technique RSA is used for safe key exchanges and building communication partners' trust.
Encryption protects AV systems in multiple ways: it prevents eavesdropping on V2X communications, safeguards data against breaches, and ensures that any unauthorized tampering with navigation or sensor information can be detected.
However, the effectiveness of encryption depends on supporting practices such as strong key management, end-to-end protection, periodic audits, and integration with complementary measures like authentication and intrusion detection. Together, these strategies enhance the trustworthiness, reliability, and resilience of autonomous vehicle ecosystems [16].

C. Authentication and Access Management

Authentication and access management are essential for guaranteeing that only legitimate devices, users, and systems, can communicate with the networks and control units of connected autonomous vehicles. By validating identities and enforcing strict access policies, these mechanisms safeguard both sensitive information and the operational integrity of AV ecosystems.

D. Multi-Factor Authentication (MFA)

MFA enhances security by enforcing several forms of verification. These factors may include something you know such as passwords or PINs, something you have such as tokens or smart cards, and something you are like biometric identifiers such as fingerprints or facial recognition.
In AVs, MFA can be employed for accessing onboard systems and remote maintenance functions, thereby reducing the possibility of unauthorized access [17].

E. Digital Certificates and PKI

Public Key Infrastructure (PKI) provides vehicles and infrastructure components with a cryptographic framework to authenticate each other using digital certificates. This approach builds trust in Vehicle-to-Everything (V2X) communications and in software or firmware updates by preventing impersonation, spoofing, or the injection of malicious data. Certificates ensure that communication endpoints and software packages originate from verified, trusted sources [18].

F. Secure Key Management

Effective key management is crucial in cryptographic operations as they depend heavily on them. This covers secure key generation, sharing, storage and routine rotation of key. Hardware Security Modules (HSMs) are often used to safeguard keys against compromise. In practice, secure key management underpins both MFA and PKI, ensuring that cryptographic credentials remain valid, protected, and inaccessible to attackers.

VII. CONCLUSION

Connected and Autonomous Vehicles (CAVs) hold immense promise for transforming mobility, yet their reliance on sensors, intra vehicle networks, and vehicle to everything communications expose them with wide spectrum of cyber threats. This survey has outlined critical vulnerabilities including sensor spoofing, adversarial machine learning, and communication-based intrusions while also reviewing key defence mechanisms such as Intrusion Detection Systems (IDSs), encryption, and authentication frameworks. Given the evolving nature of attacks, no single solution is sufficient; instead, a layered and adaptive security architecture that integrates prevention, detection, and rapid response is essential. Further the research must focus on intelligent, scalable defence powered by artificial intelligence and real-time threat analysis. The establishment of robust cybersecurity standards and safe implementation of autonomous mobility will require cooperation between researchers, industry, and policymakers.

REFERENCES

[1] Teng, Siyu et al. “Motion Planning for Autonomous Driving: The State of the Art and Future perspectives.” IEEE Transactions on Intelligent Vehicles 8 (2023): 3692-3711.

[2] H. Mun, M. Seo and D. H. Lee, "Secure Privacy-Preserving V2V Communication in 5G-V2X Supporting Network Slicing," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 9, pp. 14439-14455, Sept. 2022, doi: 10.1109/TITS.2021.3129484.

[3] J. Petit and S. E. Shladover, “Potential cyberattacks on automated vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 546–556, Apr. 2015.

[4] Velasco-Hernandez, Gustavo & Yeong, De Jong & Barry, John & Walsh, Joseph. (2020). Autonomous Driving Architectures, Perception and Data Fusion: A Review. 10.1109/ICCP51029.2020.9266268.

[5] N. Sugunaraj and P. Ranganathan, "Electronic Control Unit (ECU) Identification for Controller Area Networks (CAN) using Machine Learning," 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 2022, pp. 1-7, doi: 10.1109/eIT53891.2022.9813928.

[6] Pardhasaradhi, B., Cenkeramaddi, L.R., 2022. GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion. IEEE Sens. J. 22 (11), 11122–11134. https://doi.org/10.1109/JSEN.2022.3168940

[7] Van Wyk, F., Wang, Y., Khojandi, A., Masoud, N., 2020. Real-time sensor anomaly detection and identification in automated vehicles. IEEE Trans. Intell. Transp. Syst. 21 (3), 1264–1276. https://doi.org/10.1109/TITS.2019.2906038

[8] Petit, J., & Shladover, S. E. (2014). Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems, 16,546–556.

[9] Parkinson, Simon & Ward, Paul & Wilson, Kyle & Miller, Jonathan. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Transactions on Intelligent Transportation Systems. 18. 1-18. 10.1109/TITS.2017.2665968.

[10] Eiza, Max & Ni, Qiang. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security. IEEE Vehicular Technology Magazine. 12. 45-51. 10.1109/MVT.2017.2669348.

[11] Bécsi, Tamás & Aradi, Szilárd & Gáspár, Péter. (2015). Security issues and vulnerabilities in connected car systems. 10.1109/MTITS.2015.7223297.

[12] Alnasser A, Sun H, Jiang J. 2019. Cyber security challenges and solutions for V2X communications: A survey. Computer Networks 151:52–67.

[13] Akhtar, Naveed & Mian, Ajmal. (2018). Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey. CoRR abs/1801.00553 URL http://arxiv.org/abs/1801.00553

[14] M. Pham and K. Xiong, “A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles,” Department of Computer Science and Engineering, University of South Florida, Intelligent Computer Networking and Security Laboratory.

[15] Abdallah, Emad & Aloqaily, Ahmad & Fayez, Hiba. (2023). Identifying Intrusion Attempts on Connected and Autonomous Vehicles: A Survey. Procedia Computer Science. 220. 307-314. 10.1016/j.procs.2023.03.040.

[16] Murad, S.; Khan, A.; Shiaeles, S.; Masala, G. Data Encryption and Fragmentation in Autonomous Vehicles Using Raspberry Pi 3. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019; pp. 212–216.

[17] Miao, J.; Wang, Z.; Ning, X.; Xiao, N.; Cai, W.; Liu, R. Practical and Secure Multifactor Authentication Protocol for Autonomous Vehicles in 5G. Softw. Pract. Exp. 2022, 1–18.

[18] Vasudev, H.; Deshpande, V.; Das, D.; Das, S.K. A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles. IEEE Trans. Veh. Technol. 2020, 69, 6709–6717.