An Overview of Cybersecurity in Connected and Autonomous Vehicles (CAVs)

Vaishali Kailas Shinde
Joshi S.G
Corresponding Author: vaishalishinde.gurukul@gmail.com

Abstract

Connected and Autonomous Vehicles (CAVs) are revolutionizing transportation by integrating advanced communication systems, sensors, and artificial intelligence. While these technologies enhance safety and efficiency, they also introduce significant cybersecurity challenges. This paper provides a comprehensive overview of the cybersecurity landscape in CAVs, discussing potential threats, vulnerabilities, defense mechanisms, regulatory frameworks, and future research directions.

Keywords: Intrusion Detection Systems (IDS), secure Over-the-Air (OTA)

---

1. Introduction

1.1 Background: Overview of CAVs and their role in modern transportation.

Connected and Autonomous Vehicles (CAVs) represent a transformative shift in modern transportation, combining advanced connectivity technologies with artificial intelligence to enable vehicles that can communicate with each other, infrastructure, and the cloud, while also navigating and operating without human intervention. These vehicles leverage a range of sensors, such as LiDAR, radar, and cameras, alongside vehicle-to-everything (V2X) communication protocols to perceive their environment and make real-time driving decisions. The integration of connectivity and autonomy promises numerous benefits, including enhanced road safety, reduced traffic congestion, lower emissions, and increased mobility for individuals who are unable to drive. As part of intelligent transportation systems, CAVs are expected to play a critical role in the development of smart cities and sustainable urban mobility solutions, making them a cornerstone of future transportation infrastructure.[1]

1.2 Importance of Cybersecurity: The critical need for robust cybersecurity measures in CAVs.

Cybersecurity is a critical component in the development and deployment of Connected and Autonomous Vehicles (CAVs) due to the high level of digital connectivity and automation involved. These vehicles rely on complex networks of software, sensors, and communication systems to operate safely and efficiently. However, this reliance also introduces a wide array of potential vulnerabilities that malicious actors can exploit. Cyberattacks on CAVs can lead to serious consequences, such as unauthorized control of vehicle functions, manipulation of sensor data, theft of sensitive user information, or even large-scale disruptions to traffic systems. Furthermore, because CAVs often interact with external systems like traffic infrastructure and cloud services, a breach in one vehicle or component can potentially compromise broader transportation networks. As a result, implementing robust cybersecurity measures is essential not only to protect individual vehicles and passengers but also to ensure the safety, reliability, and public trust in autonomous and connected transportation systems.[2]

2. Threat Landscape in CAVs

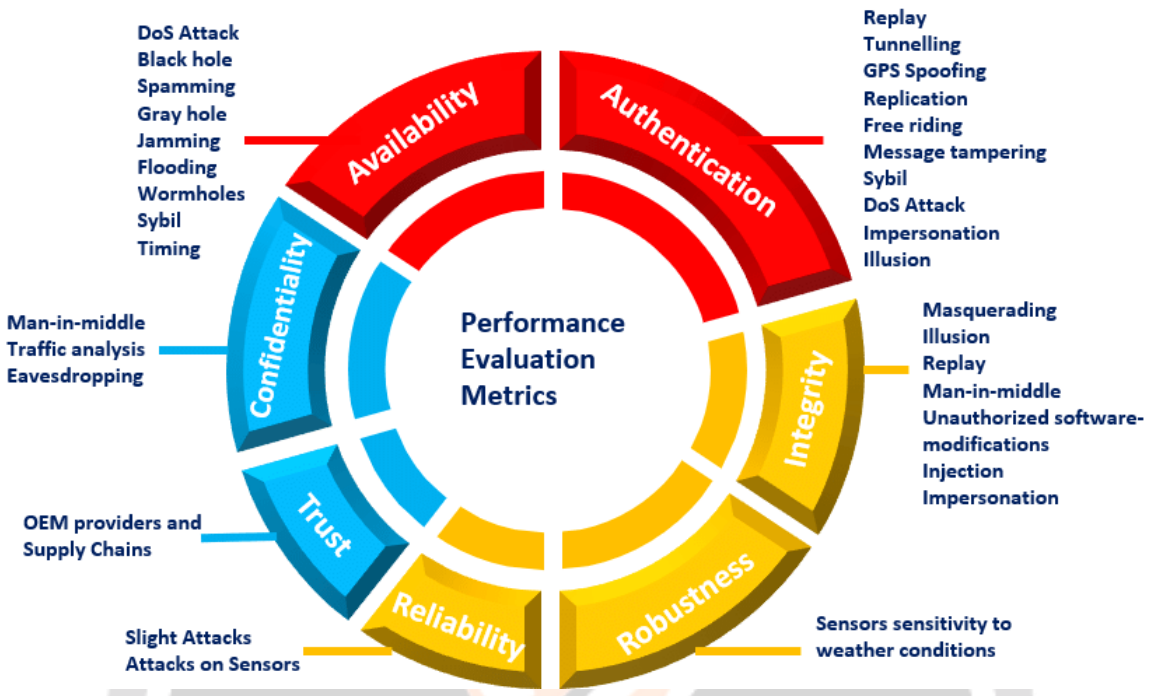

Fig 1: CAVs cyber-attacks classification under security performance evaluation metrics

2.1 Remote Hacking: Examination of remote attacks, such as the 2015 Jeep Cherokee incident:

Remote hacking poses a significant threat to Connected and Autonomous Vehicles (CAVs), as demonstrated by the widely publicized 2015 Jeep Cherokee incident. In this case, cybersecurity researchers Charlie Miller and Chris Valasek exploited vulnerabilities in the vehicle's infotainment system, which was connected to the internet via the cellular network. By remotely accessing the system, they were able to take control of critical vehicle functions—including steering, braking, and acceleration—while the car was being driven on a highway. This attack highlighted how external connectivity, while essential for many advanced features, can also open doors to potentially dangerous intrusions if not properly secured. The Jeep incident served as a wake-up call for the automotive industry, underscoring the urgent need for rigorous security testing, secure software architectures, and ongoing updates to protect vehicles from similar remote threats in the future.[3]

2.2 Sensor Manipulation: How attackers can deceive sensors like LiDAR and cameras :

Sensor manipulation is a growing cybersecurity concern for Connected and Autonomous Vehicles (CAVs), as these vehicles rely heavily on sensors such as LiDAR, cameras, radar, and ultrasonic devices to perceive their environment and make driving decisions. Attackers can exploit these dependencies by feeding false or misleading data to the sensors, effectively deceiving the vehicle's perception systems. For example, adversarial attacks can use carefully crafted images or signals—such as placing altered road signs, using laser beams to confuse LiDAR, or projecting fake obstacles—to cause the vehicle to misinterpret its surroundings. This can lead to unsafe behaviors, including unnecessary braking, swerving, or failing to stop at traffic signs. Such manipulations are particularly dangerous because they can be subtle and hard to detect, both by the vehicle's onboard systems and human observers. As sensor spoofing techniques become more sophisticated, ensuring sensor data integrity and developing robust sensor fusion and validation algorithms have become critical areas of research in autonomous vehicle cybersecurity.[4]

2.3 Data Breaches: Risks associated with unauthorized access to sensitive data:

Data breaches in Connected and Autonomous Vehicles (CAVs) pose serious risks due to the vast amount of sensitive data these vehicles generate and process. This data includes real-time location tracking, biometric identifiers, user preferences, driving habits, and even personal communications. Unauthorized access to such information can lead to privacy violations, identity theft, financial fraud, and surveillance. Moreover, attackers gaining access to backend servers or cloud platforms used for vehicle communication and data storage can compromise not just individual vehicles but entire fleets. In some cases, breached data can be used to plan targeted attacks or sold on the black market. The interconnectivity of CAVs with external systems such as mobile apps, roadside infrastructure, and manufacturer services increases the attack surface and the potential for exploitation. Therefore, securing data both at rest and in transit, enforcing strict access controls, and employing end-to-end encryption are essential measures to protect against data breaches and maintain user trust in CAV technologies.[5]

2.4 Denial-of-Service (DoS) Attacks: Impact of overwhelming vehicle systems or networks:

Denial-of-Service (DoS) attacks represent a significant cybersecurity threat to Connected and Autonomous Vehicles (CAVs) by overwhelming their systems or communication networks, thereby rendering them unresponsive or inoperative. In a typical DoS attack, an adversary floods a vehicle's onboard or external network—such as Vehicle-to-Everything (V2X) channels or the Controller Area Network (CAN) bus—with an excessive volume of data packets or commands. This can overload the processing capabilities or communication bandwidth, causing delays, system crashes, or the disabling of critical functions like braking, steering, or navigation. In more advanced Distributed Denial-of-Service (DDoS) scenarios, multiple compromised devices may coordinate attacks simultaneously, amplifying the disruption. The consequences of such attacks are particularly severe in autonomous vehicles, where uninterrupted operation and real-time decision-making are crucial for safety. A successful DoS attack could stall a vehicle in traffic, cause it to misinterpret its environment, or even lead to collisions. To mitigate these risks, CAVs must be equipped with resilient network architectures, traffic filtering mechanisms, and real-time anomaly detection systems capable of identifying and neutralizing DoS attempts before they impact operations.[6]

3. Vulnerabilities in Vehicle Communication Systems

3.1 Controller Area Network (CAN) Bus: Lack of inherent security features and susceptibility to attacks:

The Controller Area Network (CAN) bus is a critical communication protocol used in most modern vehicles, including Connected and Autonomous Vehicles (CAVs), to enable various electronic control units (ECUs) to communicate with one another. While the CAN bus is efficient and reliable for real-time communication, it was originally designed without cybersecurity in mind, and thus lacks fundamental security features such as encryption, authentication, or access control. This makes it particularly susceptible to cyberattacks. Once an attacker gains physical or remote access to the CAN bus—often through vulnerabilities in infotainment systems, diagnostic ports, or wireless interfaces—they can inject malicious messages, spoof sensor data, or override legitimate commands. Since the CAN protocol trusts all nodes equally, there is no built-in mechanism to verify the authenticity or integrity of the data being transmitted. As a result, attackers can manipulate vehicle behavior by impersonating ECUs or flooding the network with false messages. This inherent insecurity highlights the urgent need for supplemental security mechanisms, such as intrusion detection systems (IDS), message authentication codes (MACs), and network segmentation to protect against CAN-based attacks in CAVs.[7]

4. Defense Mechanisms and Best Practices

4.1 Intrusion Detection Systems (IDS): Monitoring network traffic for anomalies:

Intrusion Detection Systems (IDS) play a crucial role in safeguarding the cybersecurity of Connected and Autonomous Vehicles (CAVs) by monitoring network traffic for signs of malicious activity or anomalies. IDS are designed to detect

unauthorized access, suspicious behavior, or potential security breaches within the vehicle's communication networks, such as the Controller Area Network (CAN) bus or Vehicle-to-Everything (V2X) channels. By analyzing network traffic patterns in real-time, IDS can identify irregularities—such as unusual data flows, unexpected command sequences, or unauthorized attempts to communicate with critical vehicle systems—that may indicate an ongoing cyberattack or security vulnerability.[8]

There are two primary types of IDS:

1. **Signature-based IDS**: This type relies on predefined patterns or signatures of known threats. While effective at detecting attacks with known signatures, it can struggle to identify new, previously unseen threats.
2. **Anomaly-based IDS**: This system establishes a baseline of normal vehicle network behavior and flags deviations from this norm as potential threats. This approach is more flexible and can detect unknown attacks, but it may result in false positives if the baseline is not properly calibrated.

For CAVs, IDS can monitor both internal vehicle networks (e.g., CAN bus) and external communication channels (e.g., V2X), alerting operators or triggering automated responses to mitigate any detected threats. IDS systems are crucial for maintaining the integrity and safety of autonomous driving functions, as they enable real-time detection and rapid response to emerging cyber threats.[9]

4.2 Encryption and Authentication: Ensuring data confidentiality and authenticity:

Encryption

Encryption is the process of transforming data into a format that is unreadable to unauthorized users, ensuring that sensitive information—such as location data, driving patterns, and personal details—remains private. For CAVs, encryption is essential for securing communication both within the vehicle (e.g., between various electronic control units or ECUs) and externally (e.g., between the vehicle and cloud services, infrastructure, or other vehicles). By using encryption algorithms, CAVs can protect data during transmission over potentially vulnerable channels, such as Vehicle-to-Everything (V2X) communications, which can be targeted by cyber attackers. The use of strong encryption methods, such as AES (Advanced Encryption Standard), prevents data from being intercepted and read by malicious actors, ensuring that even if data is compromised, it remains unintelligible without the proper decryption key.[10]

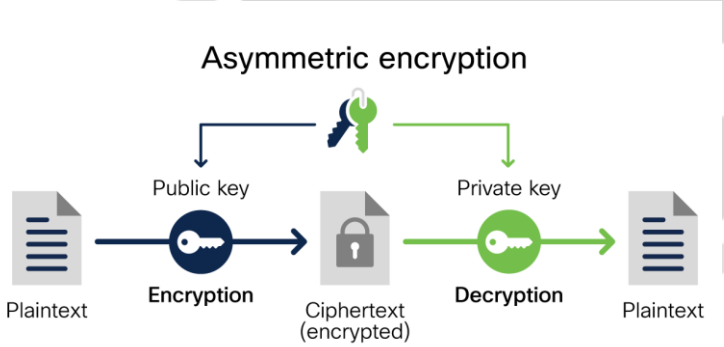

Fig 2: Asymmetric encryption

Authentication

Authentication verifies the identity of the entities involved in communication, ensuring that data is only exchanged with trusted parties. In CAVs, authentication is critical for preventing unauthorized access to vehicle systems, both internal (e.g., ECU communications) and external (e.g., interactions with V2X infrastructure or mobile apps). By

implementing secure authentication protocols such as Public Key Infrastructure (PKI), digital certificates, or multi-factor authentication (MFA), CAVs can verify the legitimacy of external connections and prevent impersonation attacks. For instance, in the case of V2X communications, each vehicle and infrastructure component must authenticate itself to ensure that they are authorized to exchange critical safety information, such as traffic signals or collision warnings.

Together, encryption and authentication work to safeguard the vehicle's data integrity, ensuring that sensitive information remains secure and that the vehicle's interactions with other entities are legitimate and trustworthy. These mechanisms are vital in maintaining the security, privacy, and overall safety of CAV systems.[11]

4.3 Secure Over-the-Air (OTA) Updates: Safely updating vehicle software:

Secure Over-the-Air (OTA) updates are a critical cybersecurity feature for Connected and Autonomous Vehicles (CAVs), enabling manufacturers to remotely and safely deliver software updates, security patches, and new features to vehicles after they have been sold and deployed. OTA updates provide a convenient way to address vulnerabilities, enhance performance, and ensure vehicles remain up to date with the latest security protocols without requiring physical visits to service centers.

However, the process of delivering OTA updates also introduces potential security risks, as malicious actors could attempt to intercept, alter, or inject malicious code into the update files. To mitigate these risks, several key security measures must be implemented:

1. **Encryption**: The update files must be encrypted during transmission to prevent interception and tampering. This ensures that only authorized recipients (i.e., the vehicle receiving the update) can decrypt and apply the update.[12]
2. **Digital Signatures**: Each update must be digitally signed to verify its authenticity and integrity. By using a private key to sign the update, manufacturers can ensure that the update comes from a trusted source and has not been altered in transit.
3. **Secure Communication Channels**: The OTA process should utilize secure communication channels, such as Transport Layer Security (TLS), to protect data while it is being transmitted from the manufacturer's servers to the vehicle. This helps prevent man-in-the-middle attacks.
4. **Authentication and Authorization**: Before an update is applied, the vehicle's system must authenticate the source and verify the integrity of the update. Additionally, authorization protocols should ensure that only authorized systems (e.g., the vehicle's onboard computer) can initiate or approve the update.
5. **Rollback Mechanism**: In case an update causes problems or introduces new vulnerabilities, a secure rollback mechanism should be in place to allow the vehicle to revert to the previous software version. This ensures that the vehicle can continue to operate safely even if an update fails.
6. **Monitoring and Validation**: Manufacturers should monitor the update process to detect any anomalies or failed attempts to tamper with the update. This includes validating the successful installation of the update and confirming that no issues have emerged post-installation.

By implementing these measures, manufacturers can ensure that OTA updates for CAVs are both secure and reliable, reducing the risk of cyberattacks while enabling ongoing improvements to vehicle systems. Secure OTA updates are essential for maintaining the integrity of CAV software and ensuring the safety and longevity of autonomous transportation systems.

4.4 Hardware Security Modules (HSMs): Enhancing system security through secure key storage .(WIRED):

Hardware Security Modules (HSMs) are specialized physical devices designed to securely store cryptographic keys and perform encryption and decryption operations. In the context of Connected and Autonomous Vehicles (CAVs),

HSMs play a crucial role in enhancing system security by providing a secure environment for sensitive operations, particularly those involving encryption keys, digital certificates, and authentication credentials.

Role of HSMs in CAV Security

CAVs are heavily reliant on cryptography for secure communication, data integrity, and user authentication. HSMs ensure that the cryptographic keys used in these processes are stored and handled in a tamper-resistant hardware device, making it significantly harder for attackers to extract or manipulate these keys. This is especially critical in the following areas:

1. **Secure Key Storage**: HSMs provide a secure and isolated space for storing cryptographic keys, such as those used for encrypting vehicle-to-everything (V2X) communication or securing data within the vehicle. By protecting keys from unauthorized access, HSMs ensure that even if a vehicle's internal systems are compromised, the encryption keys remain secure.
2. **Protection Against Physical Attacks**: HSMs are designed to be resistant to physical tampering. They use advanced techniques such as intrusion detection, self-destruction of keys upon unauthorized access attempts, and secure boot processes to prevent attackers from extracting sensitive information by physically accessing the device.
3. **Authentication and Digital Signatures**: HSMs can be used to generate and verify digital signatures, ensuring the authenticity of software updates, communications, and data exchanged between the vehicle and external systems (e.g., infrastructure or other vehicles). This is particularly important for preventing man-in-the-middle attacks, where an attacker impersonates a legitimate source.
4. **Secure Communication**: For CAVs, V2X communication is a critical function that enables vehicles to exchange information with each other and with traffic infrastructure. HSMs facilitate secure V2X communication by securely managing the keys used in encryption and authentication processes, ensuring that only trusted entities can participate in the network.
5. **Support for Secure Software Updates**: HSMs can play a pivotal role in ensuring the integrity of Over-the-Air (OTA) updates by securely storing keys used to sign and verify updates. This ensures that only authorized, unaltered updates are applied to the vehicle's systems, reducing the risk of malicious software injections during the update process.

WIRED and HSMs in Vehicle Security

WIRED, a leading technology and security publication, often highlights the importance of hardware-based security solutions like HSMs in the protection of critical systems, including CAVs. In its coverage of cybersecurity in the automotive industry, WIRED has emphasized how manufacturers are increasingly adopting HSMs as part of a layered security approach. As CAVs become more connected and autonomous, the potential attack surface grows, making it imperative to secure cryptographic processes with hardware-based solutions that provide both performance and protection.

HSMs help safeguard the integrity of CAVs by ensuring that sensitive cryptographic operations, such as key management, digital signatures, and encryption, are conducted in a secure, tamper-resistant environment. With the increasing sophistication of cyberattacks on the automotive industry, HSMs are becoming an indispensable tool for enhancing vehicle cybersecurity and protecting both drivers and manufacturers from emerging threats.

By integrating HSMs into CAV architecture, manufacturers can significantly improve the resilience of their systems against both remote and physical attacks, ensuring the long-term security of autonomous and connected transportation systems.

5. Conclusion

Summarization of key findings, emphasizing the importance of a multi-layered defense approach and the need for ongoing research and collaboration to ensure the cybersecurity of CAVs.

In conclusion, the cybersecurity of Connected and Autonomous Vehicles (CAVs) is of paramount importance as these technologies become increasingly integrated into modern transportation systems. The potential for cyberattacks, ranging from remote hacking to sensor manipulation, data breaches, and denial-of-service disruptions, highlights the critical need for robust security measures. By implementing a multi-layered approach—incorporating encryption, authentication, Intrusion Detection Systems (IDS), secure Over-the-Air (OTA) updates, and Hardware Security Modules (HSMs)—the automotive industry can safeguard CAVs against these evolving threats.

As CAVs rely on advanced connectivity, data-sharing, and automation, securing these systems is not only essential for protecting individual vehicles and passengers but also for maintaining the overall safety and trust in autonomous transportation. The ongoing development and integration of cutting-edge security technologies will be crucial in addressing vulnerabilities and ensuring that CAVs remain resilient in the face of increasingly sophisticated cyber threats. By prioritizing cybersecurity, manufacturers can help foster a secure, reliable, and trustworthy ecosystem for the next generation of transportation, driving forward the promise of safer, more efficient, and more sustainable mobility solutions.

References

1. N. V. A. Ravikumar, R. S. S. Nuvvula, P. P. Kumar, N. H. Haroon, U. D. Butkar and A. Siddiqui, "Integration of Electric Vehicles, Renewable Energy Sources, and IoT for Sustainable Transportation and Energy Management: A Comprehensive Review and Future Prospects," 2023 12th International Conference on Renewable Energy Research and Applications (ICRERA), Oshawa, ON, Canada, 2023, pp. 505-511, doi: 10.1109/ICRERA59003.2023.10269421.
2. K. Bhaga, G. Sudhamsu, S. Sharma, I. S. Abdulrahman, R. Nittala and U. D. Butkar, "Internet Traffic Dynamics in Wireless Sensor Networks," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 1081-1087, doi: 10.1109/ICACITE57410.2023.10182866.
3. Butkar, U. (2015). User Controlling System Using LAN. Asian Journal of Convergence in Technology, 2(1).
4. Butkar, U., Pokale, N.B., Thosar, D.S. and Potdar, S.R. 2024. THE JOURNEY TO SUSTAINABLE DEVELOPMENT VIA SOLAR ENERGY: A RECAP. ShodhKosh: Journal of Visual and Performing Arts. 5, 2 (Feb. 2024), 505–512. DOI:https://doi.org/10.29121/shodhkosh.v5.i2.2024.2544.
5. Butkar, U., Mahajan, R., Thosar, D. S., & Mahajan, S. (2024). APPLICATION OF INTERNET OF THINGS AND MACHINE LEARNING IN SMART FARMING FOR EFFICIENT RESOURCE MANAGEMENT . ShodhKosh: Journal of Visual and Performing Arts, 5(1), 573–578. https://doi.org/10.29121/shodhkosh.v5.i1.2024.1910
6. Vaishali Rajput. (2024). "Quantum Machine Learning Algorithms for Complex Optimization Problems". International Journal of Intelligent Systems and Applications in Engineering, 12(4), 2435 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6663
7. Butkar, U. D., Sabale, R. P., & Patil, P. C. (2024). THE FUTURE OF TRANSPORTATION: A COMPREHENSIVE ANALYSIS OF ELECTRIC VEHICLES AND THEIR IMPACT ON SUSTAINABILITY, ECONOMY, AND SOCIETY. ShodhKosh: Journal of Visual and Performing Arts, 5(3), 900–907. https://doi.org/10.29121/shodhkosh.v5.i3.2024.3431
8. D. S. Thosar, R. D. Thosar, P. B. Dhamdhere, S. B. Ananda, U. D. Butkar and D. S. Dabhade, "Optical Flow Self-Teaching in Multi-Frame with Full-Image Warping via Unsupervised Recurrent All-Pairs Field Transform," 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI), Wardha, India, 2024, pp. 1-4, doi: 10.1109/IDICAIEI61867.2024.10842718.
9. P. B. Dhamdhere, D. S. Thosar, S. B. Ananda, R. D. Thosar, D. S. Dabhade and U. D. Butkar, "A Semantic Retrieval System Using Imager Histogram Computation to reduce Trademark infringement based on the conceptual similarity of text," 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI), Wardha, India, 2024, pp. 1-6, doi: 10.1109/IDICAIEI61867.2024.10842701.

10. SNS Swati Satyajit Ghadage, Umakant Dinkar Butkar, Rajesh Autee, "Revolutionizing Intelligence: Synergizing Human and Artificial Intelligence",Journal of Information Systems Engineering and Management 10 (37S), 10
11. "Real Time Monitoring System for Women's Privacy Protection in Gender Sensitive Zones", Int Res J Adv Engg Hub, vol. 3, no. 03, pp. 829–833, Mar. 2025, doi: 10.47392/IRJAEH.2025.0117.
12. Accident Prevention Using IoT for Car Safety. (2025). International Research Journal on Advanced Engineering Hub (IRJAEH), 3(03), 777-781. https://doi.org/10.47392/IRJAEH.2025.0108