IJCRT.ORG ISSN : 2320-2882
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Cybersecurity In Automative Vehicals

1th Prof. Sagar Dhanake
Dept. of Computer Engineering
Pune, India

2nd Ruturaj A. Wakchaure
Dept. of Computer Engineering
Pune, India

3st Vedanti G. Shende
Dept. of Computer Engineering
Pune, India

4rd Siddhanth R. Ghungarde
Dept. of Computer Engineering
Pune, India

5th Linesh S. Sonawane
Dept. of Computer Engineering
Pune, India

***Abstract*—Automated vehicles (AVs) are transforming the transportation industry with the integration of advanced sensors, communication systems, and artificial intelligence (AI). These technologies make travel safer, smarter, and more efficient. However, the high level of connectivity in modern vehicles also exposes them to various cybersecurity threats that can jeopardize data integrity, privacy, and passenger safety. This study explores the major cybersecurity challenges faced by automated vehicles, the potential attack pathways, and the defense frameworks currently used to counter these threats. It also highlights methods such as secure vehicle-to-everything (V2X) communication and AI-powered intrusion detection systems as effective approaches to strengthen vehicular cybersecurity. Modern vehicles depend heavily on interconnected sensors for operations like speed regulation, braking, navigation, and safety control. These sensors communicate mainly through in-vehicle networks such as the Controller Area Network (CAN) bus, which unfortunately lacks built-in security mechanisms like encryption and authentication. As a result, if a sensor is compromised or hacked, it could feed false information into the system, disrupting other sensors and interfering with crucial vehicle functions. Overall, cybersecurity remains one of the most critical concerns in autonomous vehicles, given their vulnerabilities across software, hardware, wireless communication, and external interfaces.**

Keywords:- Autonomous vehicles, cyber security, security, integrity, Cybersecurity, Intrusion Detection System, Vehicle-to-Everything (V2X), Artificial Intelligence, Threat Mitigation

I. INTRODUCTION

Automated cars also known as self-driving or autonomous vehicles are designed to operate without human intervention by using a complex network of sensors, control systems, and communication technologies. These vehicles rely on tools such as LiDAR, GPS, cameras, and artificial intelligence (AI) to perceive and interpret their surroundings. However, as automa-tion increases, so does the risk of cyberattacks. Such attacks can manipulate sensor data, disrupt communication networks, or gain unauthorized control over vehicle systems. Therefore, ensuring strong cybersecurity measures in autonomous vehi-cles is essential to maintain user trust and public safety. The development of autonomous driving technology began in 1984, when the Carnegie Mellon University (CMU) Navigation Lab-oratory known as the Navlab group conducted pioneering research on computer-controlled vehicles for automated and assisted driving. Since then, the field has gained significant momentum, becoming a central focus in modern automotive research. With rapid advancements in artificial intelligence (AI) and machine learning (ML), autonomous vehicles have evolved to incorporate semi-autonomous and fully autonomous driving capabilities, reshaping traditional driving practices and marking a major technological milestone for the automotive industry. Despite these advances, cybersecurity remains a major concern. The Controller Area Network (CAN) bus, a widely used communication protocol in vehicles, lacks built-in encryption and authentication mechanisms, leaving it vulnerable to attacks such as spoofing, denial-of-service, and false data injection. Although current technologies like in-trusion detection systems (IDS), message authentication codes (MACs), and anomaly detection methods have improved the identification of malicious activities, they often fall short in isolating compromised sensors. This limitation highlights an important research gap: the need for a system that not only detects cyberattacks but also isolates the affected components and provides a secure fallback mechanism to ensure continu-ous and safe vehicle operation.

II. DESIGN AND IMPLEMENTATION

A. *Raspberry Pi 3*

The Raspberry Pi 3, developed by the Raspberry Pi Foun-dation, is a compact and affordable single-board computer designed to make computing more accessible. It is widely used by students, developers, and researchers to explore computer science concepts and build innovative projects across domains such as cybersecurity, automation, and the Internet of Things (IoT). Powered by a 1.2 GHz 64-bit quad-core ARM Cortex-A53 processor and equipped with 1 GB of RAM, the Rasp-berry Pi 3 provides ample processing power for embedded

Fig. 1. Raspberry-pi-3

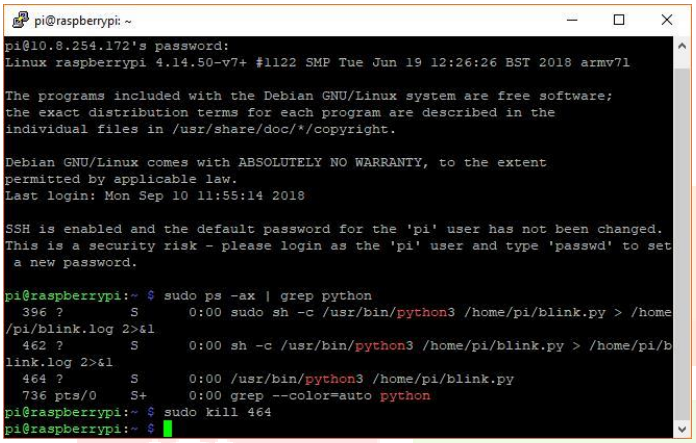

Fig. 2. Terminal Window of Raspberry Pi

applications and lightweight computing tasks. Its built-in Blue-tooth and Wi-Fi capabilities make it especially suitable for IoT-based security systems and wireless communication projects. The board is equipped with 40 General Purpose Input/Output (GPIO) pins, multiple USB ports, an HDMI output, and a microSD card slot for storage, enabling easy integration with sensors, cameras, and other hardware components. It supports various operating systems, including the Linux-based Raspberry Pi OS (formerly Raspbian), offering great flexibility and low power consumption. Because of these features, the Raspberry Pi 3 has become a popular choice for cyberse-curity projects such as network monitoring, intrusion detec-tion, penetration testing, and secure communication setups. In the automotive sector, it serves as a powerful platform for developing and testing cybersecurity applications, including CAN bus attack detection, vehicle network traffic analysis, and the deployment of secure IoT modules in connected and autonomous vehicles.

III. Objectives

The goal of this research is to design a secure communica-tion architecture for automobiles that can independently isolate and authenticate data flow from each sensor. This approach ensures that if one sensor is compromised or hacked, the false data it generates will not affect or disrupt the functioning of other sensors connected to the vehicle's network. Along with cryptographic validation techniques to maintain data integrity and authenticity, the proposed system will also include a fail-safe backup mechanism to ensure that the vehicle continues to operate safely and reliably even in the event of a cyber-attack. The primary objective of this study is to analyze and understand the cybersecurity challenges faced by automated vehicles, with a particular focus on vulnerabilities within the Controller Area Network (CAN) protocol. The research aims to identify the key weaknesses in CAN communication that could be exploited by attackers to compromise vehicle safety and control. Additionally, it seeks to evaluate existing defense mechanisms such as intrusion detection systems (IDS) and cryptographic techniques while examining different types of cyber threats affecting automotive networks. Ultimately, this study aims to propose practical strategies to strengthen the security of CAN-based systems, raise awareness of vehicular cybersecurity risks, and encourage the automotive industry to implement stronger protection measures for developing safer and more reliable autonomous vehicles.

IV. Ease of Use

Automated vehicles are designed to simplify driving by reducing the need for human intervention and providing in-telligent assistance through advanced electronic systems. The Controller Area Network (CAN) plays a key role in enabling seamless communication between various vehicle components, including the infotainment system, engine control, steering, and braking systems. Its reliable and real-time data exchange ensures quick response, smooth performance, and enhanced user experience. These vehicles are also equipped with user-friendly interfaces, automated alerts, and built-in safety fea-tures, making them accessible even to non-technical drivers. However, as vehicles become increasingly connected, main-taining strong cybersecurity measures becomes essential. A secure CAN network not only prevents unauthorized access or data manipulation but also helps build user confidence in the safety and reliability of automated driving systems.

V. Problem Statement

The advent of automated and connected vehicles has trans-formed the transportation industry by enhancing convenience, safety, and efficiency. At the core of these vehicles are com-plex electronic systems that communicate through in-vehicle networks, with the Controller Area Network (CAN) serving as the primary communication backbone. The CAN protocol connects multiple Electronic Control Units (ECUs) respon-sible for critical vehicle functions such as braking, steering, acceleration, engine management, and infotainment. Although the CAN protocol is widely used and highly reliable in

terms of real-time performance, it was not originally designed with cybersecurity in mind. This lack of built-in security mechanisms such as encryption, sender authentication, and message verification makes it highly susceptible to various cyber threats. As a result, addressing these vulnerabilities has become a key priority in ensuring the safety and security of modern connected and autonomous vehicles.

A. *Abbreviations*

This study report uses several abbreviations to simplify the understanding of technical terms. Some of the key acronyms include: Electronic Control Unit (ECU), Controller Area Network (CAN), Intrusion Detection System (IDS), Denial of Ser-vice (DoS), Vehicle-to-Everything (V2X), Message Authenti-cation Code (MAC), Over-The-Air (OTA) updates, Recurrent Neural Network (RNN), Cyclic Redundancy Check (CRC), and Controller Area Network Flexible Data-rate (CAN-FD). These abbreviations are used consistently throughout the report to maintain clarity, readability, and uniformity in technical discussions.

VI. Literature Review

Over the past decade, the increasing complexity and interconnectivity of in-vehicle networks have made cybersecurity a major focus in autonomous vehicle research. Early studies revealed that modern vehicles are vulnerable to cyberattacks targeting the Controller Area Network (CAN) bus, which connects critical systems such as braking, steering, and acceleration. One of the most influential works in this area was conducted by Koscher et al. (2010), who demonstrated that attackers could exploit the CAN bus to gain unauthorized control over essential vehicle functions. This study highlighted a significant design flaw the CAN protocol was originally developed for reliability and real-time communication rather than protection against malicious access. A few years later, Miller and Valasek (2015) provided further evidence of these risks by successfully executing a remote cyberattack on a Jeep Cherokee. By infiltrating the vehicle's infotainment system, they were able to send falsified messages to the car's control units, effectively manipulating its operation from a distance. This landmark experiment demonstrated that vehicle cyberat-tacks are not merely theoretical but can occur in real-world scenarios, raising serious concerns about driver safety and system integrity. In response to these findings, researchers have proposed several methods to enhance the security of CAN networks. One widely explored approach involves Intrusion Detection Systems (IDS), which monitor network traffic to detect unusual or unauthorized messages. Some advanced IDS implementations use machine learning algorithms to automat-ically recognize suspicious patterns and potential threats. An-other strategy is the integration of cryptographic mechanisms, such as Message Authentication Codes (MACs), to verify message authenticity and prevent data tampering. However, implementing these security measures poses challenges due to the limited bandwidth and real-time performance requirements of CAN-based systems. Balancing security with system efficiency remains an ongoing challenge in the development of safer, more resilient automotive communication networks.

VII. Controller Area Network (CAN) Overview

The Controller Area Network (CAN) in a vehicle function much like the human nervous system, enabling seamless communication between different electronic components known as Electronic Control Units (ECUs). These ECUs manage and coordinate a variety of vehicle systems, including the engine, steering, braking, and infotainment systems, ensuring that all parts of the vehicle work together efficiently and in real time.

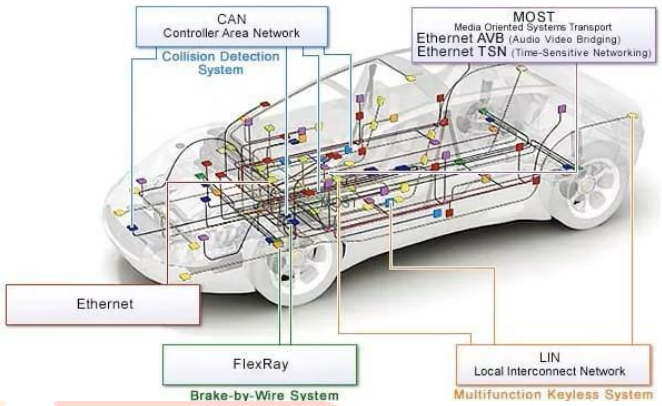

Fig. 3. CAN Architecture

In automated vehicles, the Controller Area Network (CAN) plays an even more crucial role, as these cars depend heavily on sensors, cameras, and artificial intelligence (AI) systems that continuously exchange information. The CAN network enables the vehicle to make rapid decisions, such as automatically adjusting speed, steering, and braking to ensure safe and efficient operation. However, because the CAN protocol lacks built-in security features, it remains vulnerable to cyberattacks making its protection a vital aspect of automotive cybersecurity.

VIII. Cybersecurity Threats in Automated Vehicles

Automated vehicles face many types of cybersecurity threats because they are connected and rely on electronic networks. Some of the main attack types are:

1. Spoofing: Hackers send fake messages on the CAN bus pretending to be a legitimate ECU. Example: Sending a false braking message to the car, which can confuse the system.

2. Denial of Service (DoS): The attacker floods the CAN network with fake messages. This slows down or stops real messages from being delivered, which can prevent critical systems from working properly.

3. Remote Attacks: Hackers exploit wireless connections like Wi-Fi, Bluetooth, or cellular networks to access the car's systems remotely. Example: Controlling the infotainment system or even sending commands to ECUs from far away.

4. Firmware Hacks: Attackers modify the software inside ECUs, which can give them permanent control of certain functions. Example: Changing engine or braking software to behave incorrectly.

5. Sensor and Actuator Manipulation: Automated vehicles use sensors (like radar, LiDAR, cameras) to detect the environment and make decisions. Hackers can spoof sensor data or send incorrect signals to ECUs. Example: Faking distance readings from a radar sensor could make the car accelerate into traffic or ignore obstacles. Manipulating sensors can bypass normal CAN security because the system trusts the sensor inputs.

6. Physical Access Attacks: If a hacker gains direct access to the CAN bus (e.g., via the OBD-II port), they can send malicious messages or reprogram ECUs.Physical access attacks are less common but extremely dangerous because they bypass all wireless security measures.

IX. Security Solutions and Techniques for Automated Vehicles

Researchers and engineers have developed several techsniques to protect automated vehicles from cyberattacks targeting the Controller Area Network (CAN). The most commonly implemented security measures include Intrusion Detection Systems (IDS), network segmentation, cryptographic methods, and secure Over-The-Air (OTA) update mechanisms, all designed to enhance the resilience and safety of vehicular communication systems.

1. Intrusion Detection Systems (IDS): An Intrusion Detection System (IDS) acts as a security guard for the Controller Area Network (CAN), continuously monitoring message traffic for any unusual or suspicious activity. By analyzing factors such as message frequency, timing, and content, IDS can detect attacks like replay, denial-of-service (DoS), and message spoofing. Some advanced IDS implementations use machine learning algorithms to automatically recognize new or previously unseen attack patterns. While IDS cannot directly prevent attacks, it plays a crucial role in alerting the system and enabling the vehicle to respond proactively before significant damage occurs.

2. Cryptographic Methods: Cryptographic techniques help ensure that messages transmitted over the Controller Area Network (CAN) are authentic and have not been tampered with. Security can be enhanced through methods such as lightweight encryption and Message Authentication Codes (MACs), which verify the integrity and origin of each message. In this process, a unique code is generated for every message using a secret key, allowing the receiving Electronic Control Unit (ECU) to confirm its authenticity. By preventing attackers from replaying old messages or injecting false ones, cryptog-raphy plays a vital role in securing vehicle communications. However, these mechanisms must be efficient and lightweight to avoid affecting the real-time performance of the vehicle's systems.

3. Network Segmentation and Gateways: Network segmentation enhances vehicle cybersecurity by dividing the Controller Area Network (CAN) into separate sections, isolating safety-critical systems such as steering and braking from non-critical systems like infotainment. This separation mini- mizes the potential impact of an attack, as it becomes more difficult for a compromised non-essential Electronic Control Unit (ECU) to affect critical vehicle functions. Gateways play a key role in this process by regulating and filtering communication between different network segments, ensuring that only legitimate messages are transmitted. As a result, network segmentation significantly reduces the likelihood of cyberattacks spreading across the entire vehicle network.

4. Secure Over-The-Air (OTA) Updates: Modern vehicles commonly use Over-The-Air (OTA) technology to update their software remotely, allowing manufacturers to deliver improvements and security patches without physical intervention. Secure OTA updates ensure that Electronic Control Units (ECUs) receive only verified and authorized firmware. By incorporating digital signatures and encryption, these updates prevent attackers from installing malicious or unauthorized software. This process is essential not only for fixing security vulnerabilities but also for enhancing vehicle performance and maintaining cybersecurity throughout the vehicle's lifecycle.

X. Challenges in Securing CAN Networks in Automated Vehicles

While several methods have been developed to improve cybersecurity in autonomous vehicles, achieving complete security for Controller Area Network (CAN) systems remains a significant challenge. The primary obstacles include the inherent limitations of the CAN protocol, the continued use of legacy systems, and the absence of standardized security frameworks across the automotive industry. These factors collectively make it difficult to fully protect in-vehicle networks from evolving cyber threats.

1. Constraints of CAN: The Controller Area Network (CAN) protocol was originally designed to provide fast and reliable communication between vehicle components, not to address cybersecurity concerns. One of its key limitations is the small data payload typically limited to just 8 bytes per message which makes it difficult to incorporate cryptographic protections or additional authentication codes. Since vehicles require real-time responsiveness, any added security measures must not delay message transmission. However, stronger security mechanisms often increase processing time or message size, creating a difficult balance between ensuring robust protection and maintaining the system's real-time performance.

2. Legacy System Limitations: Many automobiles continue to operate with outdated CAN systems that were never intended to withstand contemporary cybersecurity threats. Adding en-cryption, authentication, or intrusion detection system capabil-ity to these systems can be costly and technically challenging. Older cars become more susceptible to attacks as a result of the gap this creates between them and more recent, secure models.

3. Standardization Issues: At the moment, there isn't a single, industry-wide standard for automobile cybersecurity. Update

techniques, security protocols, and CAN implementations vary among automakers. It is challenging to apply uniform and efficient security measures for all vehicles due to a lack of standardization. Additionally, this makes it more difficult for vehicles in linked systems, such as Vehicle-to-Everything (V2X) networks, to communicate with one another.

XI. Applications

1. Protects vehicle communication and control systems.
2. Prevents unauthorized access and hacking.
3. Secures software and OTA (Over-the-Air) updates.
4. Protects driver and passenger data privacy.
5. Ensures safety of connected and self-driving cars.
6. Detects and blocks suspicious network activities.
7. Secures mobile app and infotainment connections.
8. Improves passenger safety and system reliability.

References

Cybersecurity has emerged as a critical concern in the automotive industry as modern vehicles become increasingly autonomous and interconnected. These vehicles rely heavily on in-vehicle communication networks such as the Controller Area Network (CAN) to exchange data between various electronic components. However, this growing connectivity has also introduced new vulnerabilities, making vehicles susceptible to cyberattacks such as infotainment system breaches, keyless entry exploits, and unauthorized access to critical Electronic Control Units (ECUs). [1], [2], [4]. To mitigate these cybersecurity threats, Intrusion Detection Systems (IDS) leveraging machine learning and hybrid deep learning techniques have been developed to enhance the security of in-vehicle networks. These systems analyze network traffic patterns to identify abnormal or malicious activities, providing an additional layer of protection against potential cyberattacks within the vehicle's communication infrastructure. [1], [5]. In-vehicle communications are further protected by secure communication frameworks and lightweight cryptographic protocols that use devices such as Arduino and Raspberry Pi [2], [6]. According to various studies and reviews, adaptive defense mechanisms, secure software updates, and continuous monitoring are essential to addressing the ongoing challenges in vehicle cybersecurity. These measures help ensure that vehicles remain resilient against evolving threats by enabling real-time threat detection, timely patching of vulnerabilities, and dynamic response strategies to prevent potential cyber intrusions. [3].

References

[1] Seo, J., Kim, H., Lee, Y. (2021). Machine Learning-Based Intrusion Detection System for In-Vehicle Networks. IEEE Access.
[2] Patel, M., Gupta, S. (2022). Lightweight Cryptographic Protocol for Secure CAN Communication. Journal of Information Security and Applications.
[3] Singh, R., Sharma, P. (2022). A Review of Automotive Cybersecurity: Challenges and Solutions. International Journal of Emerging Technologies.
[4] Verma, N., Raj, T. (2023). Development of CAN Intrusion Detection Using Raspberry Pi. International Conference on Smart Systems and IoT.
[5] Zhang, L., Chen, W. (2023). Hybrid IDS for Vehicle Networks using Deep Learning. Elsevier – Vehicular Communications Journal.
[6] Mehta, S., Rao, D. (2024). Secure Vehicle Communication Using Arduino and Raspberry Pi. IEEE International Symposium on Connected Vehicles.