International Journal of Multidisciplinary Engineering in Current Research - IJMEC

Volume 11, Issue 7, July-2026, http://ijmec.com/, ISSN: 2456-4265

Vehicle security and car hacking detection using wired and wireless communication

Dr J Madhavan[1], R. Anjali[2], G. Bhuvana kruthi[3], V. Navya[4]

[1]Professor: Department of Electronics and Communication Engineering, Bhoj Reddy Engineering College for Women Hyderabad, India

[2,3,4]B. Tech Students: Department of Electronics and Communication Engineering, Bhoj Reddy Engineering College for Women Hyderabad, India

Mail Id's: ravulaanjali26@gmail.com , gundalabhuvanakruthi045@gmail.com , vankudothnavya3002@gmail.com

Accepted 4 July 2026

Abstract

Modern vehicles rely heavily on Electronic Control Units (ECUs) and in-vehicle communication networks such as the Controller Area Network (CAN) bus, making them increasingly vulnerable to cyberattacks. This project presents a secure and efficient vehicle security system that detects and prevents malicious activities on the CAN bus using an Intrusion Detection System (IDS) integrated with cloud and blockchain technologies. The proposed system continuously monitors CAN messages using an ESP32 microcontroller interfaced with a CAN module. The collected data is analyzed in real time to identify abnormal patterns or unauthorized message injections. Upon detecting a potential attack, the system immediately triggers alerts through visual or audio indicators such as LEDs or buzzers. Additionally, the alert information is transmitted wirelessly using Wi-Fi or GSM to a cloud server for remote monitoring. To ensure data integrity and security, the detected attack logs are stored in a blockchain ledger, making them tamper-proof and reliable. The incident response center receives notifications and can take further actions based on the classified reports. A prototype model using a toy car is developed to demonstrate the practical implementation of the system. This setup effectively simulates real vehicle communication and attack scenarios in a controlled environment. The combination of wired (CAN bus) and wireless (Wi-Fi/GSM) communication enhances the flexibility and scalability of the system. The proposed solution provides a low-cost, real-time, and reliable approach to vehicle cybersecurity. It not only detects intrusions but also ensures secure data storage and remote accessibility.

Keywords: *Vehicle Cybersecurity, Controller Area Network (CAN) Bus, Intrusion Detection System (IDS), Electronic Control Unit (ECU), ESP32, Blockchain, Cloud Computing, Wi-Fi, GSM Communication, Real-Time Monitoring.*

Introduction

The rapid evolution of intelligent transportation systems has significantly increased the dependence of modern vehicles on electronic control units (ECUs) and in-vehicle communication networks. Among these networks, the Controller Area Network (CAN) bus has become the de facto communication standard because of its simplicity, reliability, and real-time performance. Multiple ECUs, including engine control, braking, steering, transmission, and infotainment systems, exchange critical information through the CAN bus to ensure coordinated vehicle operation. Despite its widespread adoption, the CAN protocol was originally designed with a primary focus on communication efficiency rather than cybersecurity. As a result, it lacks essential security mechanisms such as authentication, encryption, and message integrity verification, making it susceptible to various cyber threats.

The increasing integration of wireless communication technologies, including Wi-Fi, Bluetooth, GSM, and Internet of Things (IoT) connectivity, has further expanded the attack surface of connected vehicles. Cybercriminals can exploit these communication channels to inject malicious CAN messages, perform replay attacks, spoof legitimate ECUs, or gain unauthorized access to safety-critical vehicle functions. Such attacks may compromise vehicle performance, threaten passenger safety, and result in significant financial losses for vehicle manufacturers and owners. Consequently, ensuring the security of in-vehicle communication has become a critical research area in modern automotive engineering.

Intrusion Detection Systems (IDSs) have emerged as one of the most promising approaches for protecting automotive networks against cyberattacks. Unlike conventional preventive security mechanisms, an IDS continuously monitors network traffic, identifies abnormal communication patterns, and generates alerts whenever suspicious activities are detected. The effectiveness of an IDS can be further enhanced by integrating cloud computing technologies, which enable remote monitoring, centralized data analysis, and rapid incident reporting. In addition, blockchain

technology offers a secure and decentralized mechanism for storing security logs in an immutable ledger, ensuring that intrusion records remain tamper-resistant and can be trusted during forensic investigations.

This research proposes a secure Vehicle CAN Security System that combines CAN bus monitoring, intrusion detection, cloud connectivity, and blockchain technology into a unified cybersecurity framework. The proposed system employs an ESP32 microcontroller interfaced with a CAN communication module to continuously monitor CAN messages generated by vehicle ECUs. The collected data is analyzed in real time to identify unauthorized message injections, abnormal communication patterns, and other indicators of cyberattacks. Whenever suspicious activity is detected, the system immediately activates visual and audio alerts using LEDs and buzzers while simultaneously transmitting notification messages to a cloud platform through Wi-Fi or GSM communication. The detected attack information is securely recorded in a blockchain ledger, ensuring data integrity, transparency, and resistance to unauthorized modifications. Furthermore, an incident response center can remotely monitor security events and initiate appropriate countermeasures based on the reported alerts.

To validate the proposed approach, a prototype system is implemented using a toy vehicle integrated with an ESP32 controller, CAN communication module, cloud platform, and blockchain-enabled storage. The prototype provides a practical environment for simulating vehicle communication and evaluating the system under different attack scenarios, including unauthorized CAN message injection and abnormal traffic generation. Experimental implementation demonstrates that the proposed framework is capable of detecting malicious activities in real time while maintaining secure event logging and remote accessibility. The solution offers a cost-effective, scalable, and practical approach for strengthening cybersecurity in modern connected vehicles.

The overall architecture of the proposed system consists of four major functional modules: **(i)** Vehicle ECU Data Acquisition, **(ii)** CAN Bus Communication, **(iii)** Intrusion Detection System (IDS), and **(iv)** Cloud and Blockchain-Based Monitoring through Wi-Fi/GSM communication. Each module performs an independent function while maintaining seamless integration with the remaining components, thereby enabling modular deployment, easy maintenance, and future scalability. This modular architecture also provides flexibility for incorporating advanced machine learning-based intrusion detection algorithms, secure over-the-air updates, edge intelligence, and predictive threat analysis in future developments.

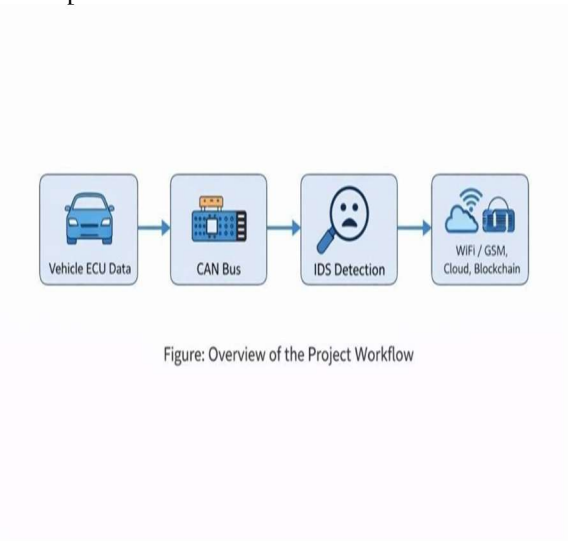

Figure: Overview of the Project Workflow

Figure 1: Overview of the Project Workflow

Literature Survey

The increasing adoption of connected vehicles has made automotive cybersecurity an important research area. Modern vehicles use the Controller Area Network (CAN) bus to enable communication among Electronic Control Units (ECUs). Although the CAN protocol provides reliable and real-time communication, it lacks built-in security features such as authentication and encryption, making it vulnerable to attacks including message spoofing, replay attacks, and unauthorized message injection. These security concerns have encouraged researchers to develop effective intrusion detection mechanisms for vehicle networks.

The CAN protocol was introduced by **Robert Bosch GmbH** for efficient in-vehicle communication. Later, **Charlie Miller** and **Chris Valasek** demonstrated real-world cyberattacks on connected vehicles, highlighting the need for stronger automotive security. Their work motivated extensive research on Intrusion Detection Systems (IDSs) for detecting malicious CAN messages.

Researchers have proposed both signature-based and anomaly-based IDS techniques to identify cyber threats in CAN networks. Recent studies have also incorporated machine learning and deep learning methods, inspired by the work of **Geoffrey Hinton**, to improve the detection of unknown attacks with higher accuracy. Cloud computing enables remote monitoring and centralized analysis of CAN data, while blockchain technology, introduced by **Satoshi Nakamoto**, provides secure and tamper-proof storage of intrusion logs. Wireless technologies such as Wi-Fi

and GSM further support real-time alert transmission to users and monitoring centers.

Despite these developments, challenges such as limited processing capability of embedded devices, communication latency, and real-time analysis of high-speed CAN traffic still exist. This project addresses these issues by integrating CAN bus monitoring, IDS, ESP32, Wi-Fi/GSM communication, cloud computing, and blockchain into a unified vehicle security framework. The proposed system offers a scalable, low-cost, and reliable solution for detecting cyberattacks, securely storing intrusion records, and enabling remote monitoring for modern connected vehicles.

System Analysis

Existing System

Modern vehicles use the **Controller Area Network (CAN) bus** for communication between Electronic Control Units (ECUs). Although the CAN bus provides reliable and real-time communication, it does not include security features such as authentication or encryption. As a result, the network is vulnerable to cyberattacks including message spoofing, replay attacks, and Denial-of-Service (DoS) attacks.

Existing vehicle security solutions mainly rely on signature-based Intrusion Detection Systems (IDS), which are capable of detecting only known attacks. These systems generally lack real-time monitoring, remote alert mechanisms, and centralized storage for security events. In addition, they do not utilize cloud computing or blockchain technologies for secure data management, making it difficult to perform large-scale monitoring and forensic analysis.

Proposed System

The proposed system provides a secure and real-time vehicle security solution by continuously monitoring CAN bus messages using an **ESP32-based Intrusion Detection System (IDS)**. The system analyzes CAN traffic to detect abnormal activities such as spoofing, replay attacks, and unauthorized message injection. When an intrusion is detected, an alert is generated through LEDs or a buzzer, and the incident is transmitted to a cloud server using **Wi-Fi or GSM** communication. The detected attack logs are securely stored using **blockchain technology**, ensuring data integrity and preventing unauthorized modifications.

Real-Time Vehicle Intrusion Detection

The proposed IDS continuously monitors CAN messages exchanged between vehicle ECUs and analyzes them in real time. It detects abnormal communication patterns and identifies malicious activities such as message spoofing, replay attacks, and unauthorized message injection. This enables early detection of cyber threats and improves the overall security of the vehicle network.

Wired and Wireless Communication Integration

The proposed system combines both wired and wireless communication technologies for efficient data transfer. The **CAN bus** serves as the wired communication network between ECUs, while **Wi-Fi and GSM** provide wireless connectivity for transmitting alerts and vehicle data to the cloud. This hybrid communication approach enables remote monitoring, faster incident reporting, and secure management of vehicle security information.

Block Diagram

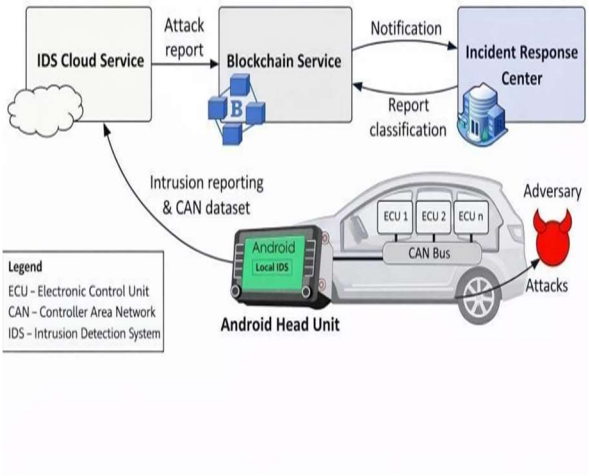

Figure 2 : Block Diagram of Vehicle security and car hacking detection

Methodology

The proposed **Vehicle Security and Car Hacking Detection System** follows a systematic approach to detect, analyze, and respond to cyberattacks on the Controller Area Network (CAN) bus. Initially, CAN messages transmitted between Electronic Control Units (ECUs) are continuously monitored using an ESP32-based Intrusion Detection System (IDS). The IDS analyzes the incoming CAN frames in real time to identify abnormal communication patterns such as message spoofing, replay attacks, and unauthorized message injection. Whenever malicious activity is detected, the system immediately generates alerts through LEDs or a buzzer and transmits the intrusion information to a cloud server via Wi-Fi or GSM. The detected attack logs are securely stored in a blockchain ledger to ensure data integrity and prevent tampering. Finally, the incident information can be accessed remotely for monitoring and further analysis, while the

collected data can be used to improve future detection performance.

System Overview

The proposed system consists of five major components: the **In-Vehicle Network (ECUs and CAN Bus)**, **ESP32-based Intrusion Detection System (IDS)**, **Cloud Server**, **Blockchain Storage**, and **Wireless Communication Module (Wi-Fi/GSM)**. These components work together to provide continuous monitoring, real-time intrusion detection, secure data storage, and remote access to vehicle security information.

The major functions of the system include:

- Continuous monitoring of CAN bus messages.
- Real-time detection of malicious CAN traffic.
- Instant alert generation using LED or buzzer.
- Wireless transmission of attack information through Wi-Fi/GSM.
- Secure storage of attack logs using blockchain.
- Remote monitoring through a cloud platform.

In-Vehicle Network (ECUs and CAN Bus)

The vehicle contains several Electronic Control Units (ECUs) that communicate through the Controller Area Network (CAN) bus. These ECUs control important vehicle functions such as engine operation, braking, steering, and sensors. Since the CAN protocol does not provide authentication or encryption, it remains vulnerable to cyberattacks.

System Workflow Summary

The overall workflow begins with monitoring CAN bus communication between vehicle ECUs. The ESP32-based IDS analyzes each CAN message in real time and detects abnormal activities. If an attack is identified, the system immediately generates an alert, transmits the event to the cloud through Wi-Fi or GSM, and securely stores the attack information in blockchain. This architecture provides continuous monitoring, secure data management, and remote accessibility.

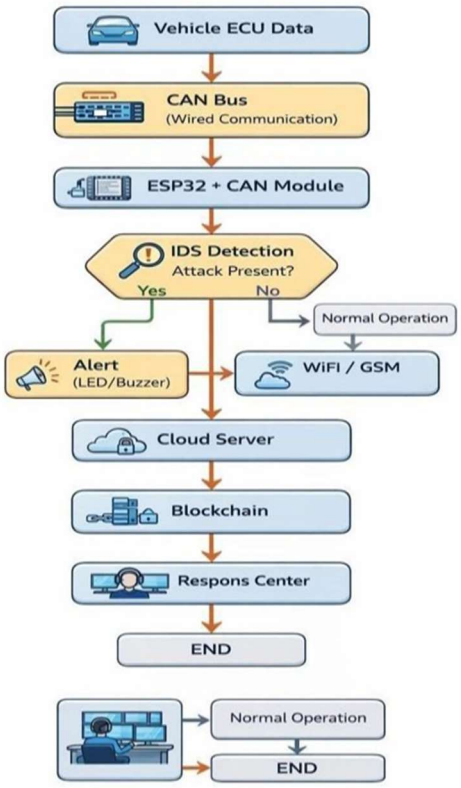

Figure 3; presents the overall workflow of the proposed Vehicle Security and Car Hacking Detection System.

Working

The proposed Vehicle Security and Car Hacking Detection System continuously monitors the vehicle communication network using both wired and wireless communication technologies to detect unauthorized access and suspicious activities.

1. **System Initialization:** When the vehicle is powered on, the ESP32 microcontroller initializes the CAN module, communication interfaces, sensors, and other hardware components to begin system monitoring.
2. **Data Monitoring:** The system continuously reads CAN bus messages exchanged between Electronic Control Units (ECUs). These messages are analyzed in real time to identify abnormal communication patterns that may indicate hacking attempts.
3. **Threat Detection:** If unusual activities such as unauthorized CAN messages, spoofing, replay attacks, or unexpected data transmission are detected, the system classifies them as potential security threats.

4. **Alert Generation:** Once a threat is identified, the system immediately activates warning indicators such as an LED and buzzer while simultaneously generating wireless notifications to inform the vehicle owner or administrator.
5. **Wireless Communication:** The detected intrusion information is transmitted through Wi-Fi or GSM communication to a cloud platform, enabling remote monitoring and timely response.
6. **Data Logging:** All detected security events and communication data are securely stored for future analysis, performance evaluation, and system improvement.

Results and Discussion

The implementation of the proposed Vehicle Security and Car Hacking Detection System successfully demonstrated real-time monitoring of vehicle communication and effective detection of potential cyber threats. The system continuously monitored CAN bus messages and accurately identified abnormal communication patterns that could indicate hacking attempts.

Whenever suspicious activity was detected, the system immediately generated alerts through LED and buzzer indicators, enabling quick notification to the user. The detected intrusion information was successfully transmitted using wireless communication for remote monitoring through the cloud platform.

The developed system operated reliably in both online and offline modes, ensuring continuous protection even during temporary network interruptions. The integration of wired (CAN bus) and wireless (Wi-Fi/GSM) communication technologies provided efficient monitoring, rapid threat detection, and secure transmission of security information. Overall, the experimental results demonstrate that the proposed system is effective in improving vehicle security by providing continuous intrusion detection, real-time alert generation, and reliable communication.

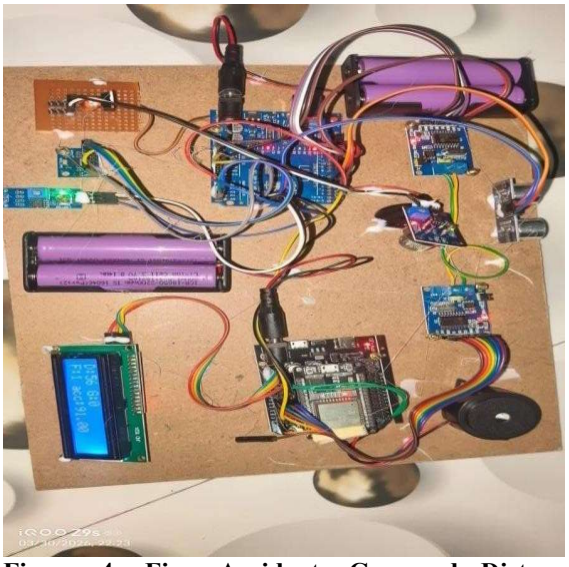

Figure 4: Fire, Accident, Gas and Distance Detection Displayed on LCD

Figure 5.3.1 shows the LCD output of the developed hardware prototype displaying the status of fire detection, accident detection, gas leakage detection, and distance measurement. The output confirms that the ESP32 microcontroller, CAN communication module, sensors, and display unit are functioning correctly. The successful integration of these hardware components demonstrates the system's capability to monitor multiple vehicle parameters in real time while providing reliable detection and alert generation. The recorded information can also be stored for future analysis, thereby improving the overall safety and reliability of the vehicle.

Figure 5: Output of Vehicle Security and Car Hacking Detection

Figure 5.3.2 illustrates the output of the proposed Vehicle Security and Car Hacking Detection System during intrusion monitoring. The system continuously

analyzes CAN bus communication and identifies abnormal or unauthorized messages. When suspicious activity is detected, alerts are generated immediately and transmitted through wireless communication to the cloud platform for remote monitoring. The successful execution of these functions demonstrates the effectiveness of the proposed system in detecting vehicle cyberattacks in real time.

Conclusion and Future Scope

Conclusion

The proposed Vehicle Security and Car Hacking Detection Using Wired and Wireless Communication system successfully demonstrates a reliable and cost-effective approach for enhancing vehicle cybersecurity. The system continuously monitors Controller Area Network (CAN) bus communication using an ESP32-based Intrusion Detection System (IDS) to detect unauthorized access, message spoofing, replay attacks, and other malicious activities in real time. Upon detecting suspicious behavior, the system immediately generates alerts through an LED and buzzer while transmitting intrusion information to the cloud using Wi-Fi or GSM communication. Furthermore, blockchain technology ensures secure and tamper-proof storage of attack logs, improving data integrity and reliability.

The developed prototype validates the effectiveness of integrating CAN bus monitoring, wired and wireless communication, cloud connectivity, and blockchain technology into a unified vehicle security framework. The system operates efficiently in both online and offline modes, providing continuous monitoring and reliable intrusion detection. Overall, the proposed solution offers a scalable, low-cost, and practical approach for protecting modern connected vehicles against evolving cyber threats while improving vehicle safety and security.

Future Scope

The proposed Vehicle Security and Car Hacking Detection system can be further enhanced by incorporating advanced technologies to improve detection accuracy and overall system performance. Artificial Intelligence (AI) and Machine Learning (ML) algorithms can be integrated to identify sophisticated and zero-day cyberattacks with higher precision. A dedicated mobile application can be developed to provide real-time notifications, remote monitoring, and security management for vehicle owners.

Future enhancements may also include GPS-based vehicle tracking for theft prevention, secure over-the-air (OTA) software updates, and support for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. The use of edge computing can reduce response time by performing intrusion detection closer to the vehicle, while enhanced cloud services can provide predictive threat analysis and centralized fleet monitoring. These improvements will make the proposed system more intelligent, scalable, and suitable for next-generation connected and autonomous vehicles.

References

[1] B. S. Bari, K. Yelamarthi, and S. Ghafoor, “Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study,” *Sensors*, vol. 23, no. 18, pp. 1–25, 2023.

[2] V. Tanksale, “Intrusion Detection System for Controller Area Network,” *International Journal of Information Security and Cybersecurity*, 2024.

[3] T. Andreica, A. Popescu, M. Ionescu, and C. Dobre, “Blockchain Integration for In-Vehicle CAN Bus Intrusion Detection Systems,” *Scientific Reports*, vol. 14, 2024.

[4] R. Rai, J. Grover, and P. Sharma, “Securing the CAN Bus Using Deep Learning for Intrusion Detection in Vehicles,” *Scientific Reports*, vol. 15, 2025.

[5] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, “LSTM-Based Intrusion Detection System for In-Vehicle CAN Bus Communications,” *IEEE Access*, vol. 8, pp. 182487–182502, 2020.

[6] A. Taylor, S. Leblanc, and N. Japkowicz, “IDS for CAN: A Practical Intrusion Detection System for CAN Bus Security,” in *Proc. IEEE International Conference on Communications (ICC)*, 2016, pp. 1–6.

[7] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” Black Hat USA, Las Vegas, NV, USA, Aug. 2015.

[8] R. Bosch GmbH, **CAN Specification Version 2.0**, Stuttgart, Germany, 1991.

[9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] G. E. Hinton, S. Osindero, and Y. W. Teh, “A Fast Learning Algorithm for Deep Belief Nets,” *Neural Computation*, vol. 18, no. 7, pp. 1527–1554, 2006.