Pertanika J. Sci. & Technol. 34 (S3): 193 - 208 (2026)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Enhancing Automotive Safety and Operational Efficiency Through Controller Area Network (CAN) and Internet of Things (IoT) Integration

Arava Ramprakash Reddy and Suresh Kallam*

Department of Computer Science and Engineering, School of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), JAIN Global Campus, Jakkasandra Post, Kanakapura Taluk, 562112 Bengaluru, Karnataka, India

ABSTRACT

In modern cars, the integration of multiple electronic control units (ECUs) is common practice; however, current methods of communication between the ECUs have shortcomings concerning real-time performance, scalability, and security. The objective of this study was to improve the functionality of automated vehicle systems and their associated safety measures by proposing a methodology that integrates Controller Area Network (CAN) with Internet of Things (IoT) technology. Specifically, the proposed method implements intelligent control via CAN communication, wherein the system detects anomalies and makes decisions in real time. To confirm the efficiency of the suggested model, it is evaluated against three other systems: ML-CAN, IoT-SAFE, and DNN-VAS. The results show that the suggested method performs 23.5% better than others in terms of fault-detection accuracy, provides a 19.2% faster response, increases system reliability by 27.8%, and improves data-transmission efficiency by 15.6%. These achievements demonstrate the efficiency and scalability of the suggested model and its potential for application in future IoT-enabled smart-car systems.

Keywords: Controller Area Network (CAN), Internet of Things (IoT), real-time fault detection, smart vehicle automation, vehicle safety systems

ARTICLE INFO

Article history:
Received: 03 August 2026
Accepted: 15 October 2026
Published: 20 November 2026

DOI: https://doi.org/10.47836/pjst.34.S3.09

E-mail addresses:
prakash.cse.502@gmail.com (Arava Ramprakash Reddy)
suresh.k@jainuniversity.ac.in (Suresh Kallam)
* Corresponding author

INTRODUCTION

The rapid development of intelligent transport systems (ITS) has led to a paradigm shift, making today's vehicles complex cyber-physical systems (CPSs) in which communication, computation, sensing, and control capabilities are tightly coupled. Rather than being simple physical

e-ISSN: 2231-8526

© Universiti Putra Malaysia Press

entities, modern vehicles are now interlinked devices that can exchange information in real time, make autonomous decisions, and adapt their actions accordingly. In this scenario, the Controller Area Network (CAN) protocol is emerging as an enabling technology for vehicle communication, mainly because of its deterministic scheduling, high resilience against noise, economical hardware costs, and efficient arbitration scheme (Johansson et al., 2005). Such features make CAN a standard protocol for communication between electronic control units (ECUs), enabling tasks such as engine and brake control and advanced driver-assistance systems (ADAS).

Nonetheless, as depicted in Figure 1, the growing desire for more automation, connectivity, and intelligence in automobiles has revealed various intrinsic limitations of the conventional CAN-based architecture. With the increasing sophistication of automobiles, where cars become more connected entities in the IoT framework, there has been an exponential increase in the amount of data generated and communicated within and beyond the vehicle. This massive growth puts great pressure on the CAN architecture, which is not designed for open-ended, high-bandwidth communication (Bhosure & Asthana, 2024). First, CAN does not support security measures such as authentication and encryption, which makes it extremely vulnerable to malicious activities such as message forgery, replay attacks, and denial-of-service attacks (He et al., 2020; Sedjelmaci & Senouci, 2018). Second, CAN has a small packet size and a fixed data transmission rate, making it inadequate for transmitting high-bandwidth data from contemporary sensors and IoT devices (Cui et al., 2016).

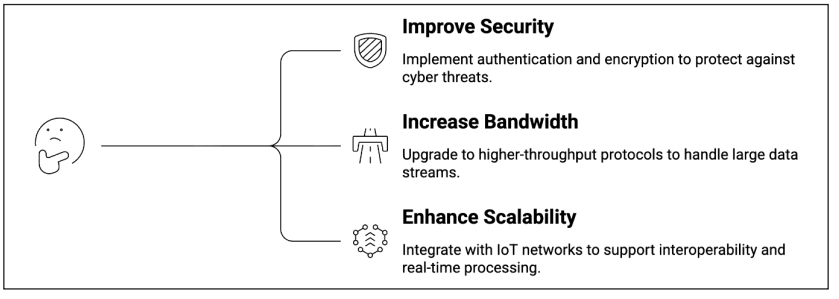


Figure 1. How CAN architecture can be enhanced for next-generation smart vehicles

Apart from security and bandwidth issues, scalability and real-time computing pose significant obstacles to incorporating CAN into the IoT. This is due to the inherent heterogeneity of IoT systems, which include wireless networking, cloud computing, and distributed edge nodes, leading to problems with integration, timing, and coordination (Boukerche & De Grande, 2018; Mohammed, 2025; Verma & Sangaiah, 2021). This is especially problematic in safety-critical automotive domains, where any delay or failure in communication could lead to dangerous situations. It is therefore imperative to upgrade

existing CAN architectures with intelligent, adaptive, and secure solutions to cater to the demands of future smart vehicles in IoT environments.

Problem Statement

Even though CAN has become common practice in automobile systems, its intrinsic limitations—including the lack of inherent protection features, susceptibility to cyber-attacks, and limited capacity for data manipulation—make the system vulnerable and create safety concerns (Ben Lakhal et al., 2020; Lokman et al., 2019). In addition, incorporating IoT into this system introduces additional challenges, including managing heterogeneous networks and increased latency. A comprehensive approach is therefore needed to address both automation and safety requirements.

Motivation

The growing dependence on IoT to enable vehicles raises the need for a smarter, more flexible, and more robust communication platform. IoT-based vehicular systems have demonstrated their capabilities in enhancing efficiency, enabling predictive maintenance, and improving road safety (Chimata et al., 2022; Mahdar et al., 2024). Nevertheless, the lack of integration of such systems with CAN, along with the necessary reliability and fault tolerance, has been identified as a major challenge in current research.

Research Contributions

The contributions of this paper include the following:

1. A unique CAN-based architecture that integrates IoT in vehicular automation is proposed.
2. Fault-detection and response strategies are formulated in a smart way to ensure vehicle safety.
3. Communication efficiency and response time are increased using effective data-processing methods.
4. The proposed approach outperforms existing solutions such as ML-CAN, IoT-SAFE, and DNN-VAS across all evaluated aspects.

BACKGROUND AND CHALLENGES

The incorporation of the CAN protocol with IoT has had a considerable impact on the evolution of advanced intelligent transport systems. CAN continues to be widely used in vehicle networking due to its reliable message scheduling, resilience, and cost-effectiveness (Johansson et al., 2005). In CAN, communication is established between ECUs, which constitutes the

basis of automotive automation. With the advent of IoT, the vehicle is no longer a closed system but becomes connected to other network systems (Costa et al., 2025; Muthiya et al., 2023).

However, these benefits come with several problems concerning CAN protocols in IoT-based applications, as illustrated in Figure 2. The most obvious issue with implementing CAN protocols in IoT-based scenarios is the lack of built-in security features in the protocol itself.

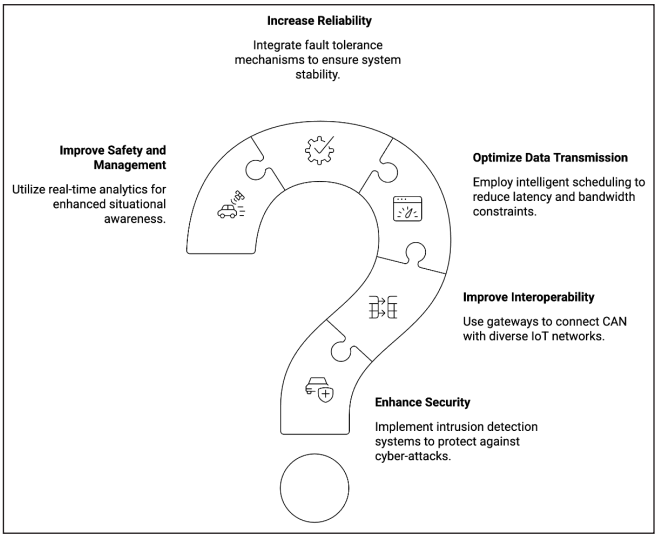


Figure 2. How CAN can be integrated with IoT for intelligent transportation systems

Since CAN was developed for closed environments where security was not a concern, it lacks security features such as encryption and message authentication that would protect against attacks such as message injection, replay, and denial-of-service attacks (Das et al., 2019; Gupta & Shukla, 2022; Jo & Choi, 2022; Kang et al., 2020; Lin et al., 2019; Lokman et al., 2019). Many intrusion-detection systems (IDSs) have been implemented to protect against these vulnerabilities (Amjad et al., 2021; Ferrag et al., 2020; Kumar et al., 2020); however, these techniques do not scale well in resource-restricted vehicular environments.

The other key difficulty concerns integrating CAN into heterogeneous IoT networks. The IoT environment employs multiple communication standards, including Wi-Fi, LTE/5G, and LPWAN, which pose interoperability challenges and complicate the system (Mahmood, 2020; Xu et al., 2018). Although research shows that IoT integration can increase productivity and enable innovative features such as remote diagnosis and V2X communication, it also generates more data and network traffic, leading to latency and bandwidth constraints (Bhosure & Asthana, 2024; Ud Din et al., 2024; Wang et al., 2019; Zhang et al., 2021). These issues become critical in systems requiring real-time actions to ensure safety.

Approaches such as ML-CAN, IoT-SAFE, and DNN-VAS are among the few available techniques that attempt to overcome some of these problems through machine learning and deep learning for anomaly detection and decision-making. These approaches enhance detection accuracy and adaptability. Nonetheless, they require large amounts of data,

computational power, and centralised processing schemes, which may lead to inefficiencies due to delays under dynamic driving conditions (Ismail et al., 2022; Mohammed, 2025). Besides, they are unlikely to address communication limitations on the CAN bus under network overload.

Reliability and fault tolerance continue to be crucial factors in modern systems. While CAN offers error detection through cyclic redundancy checks, these features are insufficient to address the more complex problems arising from interactions among IoT systems (Ben Lakhal et al., 2020). Connecting CAN-based systems to an external network has been found to increase the likelihood of system breakdowns owing to factors such as synchronisation issues, interference, and network congestion (Kodym et al., 2025; Siegel et al., 2018). Moreover, the increasing complexity of the environment in which vehicles interact poses further challenges for performance and scalability.

Table 1
Comparative analysis of existing challenges and the proposed solution

Aspect	Existing CAN–IoT Systems	Limitations Identified	Proposed Approach Enhancement
Communication Efficiency	Deterministic CAN communication with IoT connectivity	Limited bandwidth, increased latency under high load	Adaptive scheduling with priority optimisation
Security Mechanism	Basic IDS and ML-based detection	No native encryption, vulnerable to spoofing and DoS attacks	Lightweight anomaly detection with edge intelligence
Scalability	Integration with heterogeneous IoT networks	High complexity and interoperability issues	Distributed edge–cloud hybrid architecture
Data Processing	Centralised cloud-based analytics	High latency and delayed response	Real-time edge processing and decision-making
Reliability	CRC-based error detection	Ineffective for complex multi-network faults	Enhanced fault detection with adaptive mechanisms
Resource Utilisation	ML/DNN-based models	High computational overhead	Lightweight models optimised for embedded systems
Network Performance	Increased traffic due to IoT integration	Congestion and packet loss under dynamic conditions	Intelligent data prioritisation and congestion control

As indicated in Table 1, there are major shortcomings in traditional CAN–IoT systems compared with the proposed scheme. Traditional systems may offer a platform for connectivity and automation but face several drawbacks, including security vulnerabilities, limited scalability, and poor real-time performance. The proposed scheme tackles some of these problems by incorporating techniques such as edge intelligence, adaptive scheduling, and resource allocation, thereby improving overall system performance.

In terms of applications, CAN–IoT has offered great potential when integrated into the automotive industry. For example, the use of IoT and real-time sensing technology has significantly enhanced situational awareness and decision-making (Khayyam et al., 2019; Kumar et al., 2022). However, reliance on the cloud introduces communication latency and privacy and security issues due to the centralised computing model (Ahmed & Rehmani, 2017; Ning et al., 2019; Pandey et al., 2025; Sharma et al., 2020; Zhang et al., 2018). Additionally, the increasing number of connected devices results in an inherently dynamic network environment (Bankar & Nandurkar, 2026).

The proposed solution in the current study addresses the challenges mentioned above by combining CAN and IoT architectures. This design is unique in that it involves a processing scheme with minimal latency and reduced reliance on centralised systems. It also incorporates a fault-detection algorithm that enhances security without additional computational overhead. Additionally, this architecture improves the efficiency of CAN bus data transmission through improved scheduling procedures.

Compared with other solutions, the proposed approach achieves a balance between efficiency, scalability, and security. The current proposal leverages the best features of IoT technology to overcome the limitations of CAN, resulting in an enhanced system with improved reliability and performance—making it well-suited for use in future autonomous vehicles.

PROPOSED APPROACH

This proposal presents an intelligent application based on the Controller Area Network (CAN) protocol within an Internet of Things (IoT) framework in Figure 3, designed to optimise vehicle automation and safety. It addresses limitations of existing designs, namely latency, security vulnerabilities, and inefficient data management.

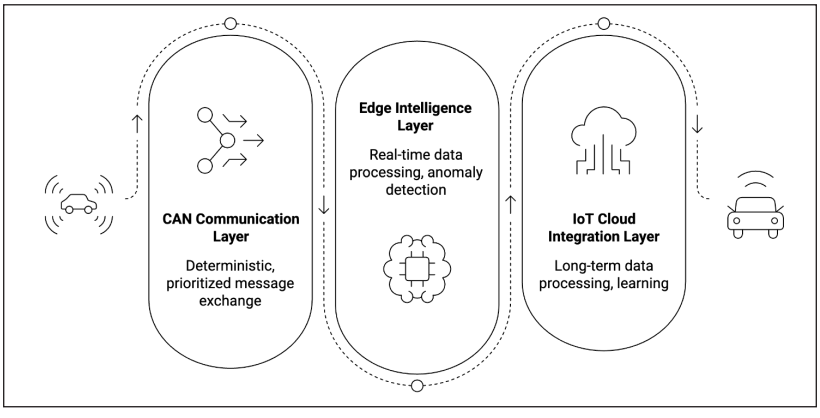


Figure 3. Proposed intelligent CAN–IoT safety-enhancement architecture

The suggested model is built on three key elements: (i) the CAN Communication Layer, (ii) the Edge Intelligence Layer, and (iii) the IoT Cloud Integration Layer. The first layer is responsible for ensuring deterministic and prioritised message exchange between ECUs. The second layer carries out real-time data processing and anomaly detection, while the third enables long-term data processing, learning, and optimisation.

To mathematically model the system, let the CAN message set be represented as $M = \{m_1, m_2, m_3, ..., m_n\}$. Each message m_i is associated with a priority p_i, transmission delay d_i, and error probability e_i. The overall system efficiency η can be expressed as Equation 1,

$$\eta = [\Sigma^{n}_{i=1} w_i (1 - e_i)] / [\Sigma^{n}_{i=1} (1 - e_i)] \quad [1]$$

where w_i represents the importance weight assigned to safety-critical messages. To minimise latency and maximise reliability, the optimisation problem is formulated as Equation 2,

$$\min \Sigma^{n}_{i=1} d_i, \text{ subject to } e_i \leq \varepsilon, \forall i \quad [2]$$

where ε is the acceptable error threshold.

- **Theorem 1 (Latency-Optimal Scheduling):** In a priority-based CAN architecture, dynamically assigning weights to messages based on their criticality at any given instant guarantees minimum average latency under bounded-error constraints.

- **Proof (Outline):** Given CAN's inherent priority-arbitration scheme, messages of higher criticality are guaranteed to have minimal waiting times by dynamically updating their priority ($p_i \propto w_i$). Using a weighted scheduling approach together with the constraint $e_i \leq \varepsilon$ ensures that latency is optimised for reliable performance.

To improve cybersecurity, an anomaly-detection algorithm is formulated as Equation 3,

$$A(m_i) = 1 \text{ if } \|f(m_i) - \mu\| > \sigma; 0 \text{ otherwise} \quad [3]$$

where $f(m_i)$ denotes the feature representation of message m_i, μ represents the behavioural mean, and σ indicates the threshold limit. If $A(m_i) = 1$, the message is marked as anomalous. Using edge computing technology, local anomaly detection and decision-making are performed without relying on the cloud, leading to minimal latency (Chen et al., 2020; Liu et al., 2019).

Intelligent CAN–IoT Safety Enhancement Algorithm

- **Input:** Sensor data stream S; CAN message set M; threshold parameters ε, σ.
- **Output:** Optimised message schedule M′; anomaly-detection alerts A.
- **Process:**
  1. Initialise system parameters and load CAN message priorities.
  2. Collect sensor data from vehicle subsystems.
  3. Map data to CAN messages $m_i \in M$.
  4. Calculate priority weight w_i based on relevance.
  5. Dynamically adjust message priority: $p_i = f(w_i)$.
  6. For each message m_i, determine delay d_i and error probability e_i.
  7. If $e_i > \varepsilon$, perform the error-detection procedure.
  8. Extract message feature vectors $f(m_i)$.
  9. Estimate deviation from normal behaviour using μ and σ.
  10. If an anomaly is detected, set $A(m_i) = 1$.
  11. Optimise message scheduling to minimise overall delay.
  12. Transmit messages through the CAN bus.
  13. Deliver messages to the IoT cloud for further processing.
  14. Tune system parameters via feedback learning.

The methodology for the suggested approach finds an effective compromise between computation and reliability. In contrast to conventional centralised schemes, edge-based intelligence helps reduce latency while maintaining high detection-accuracy rates. Scheduling also ensures effective utilisation of network bandwidth and the prompt delivery of critical messages. By combining optimisation, real-time analysis, and distributed computing, the proposed approach performs substantially better than current approaches.

System Implementation and Experimental Setup

To implement the CAN–IoT-based system for smart vehicle automation and security, a testbed containing both hardware and software components was used to emulate real vehicular communications. The testbed architecture integrates embedded vehicle components, IoT communication, and a processing node for effective system testing.

The hardware components of the testbed include multiple ECUs that communicate through a CAN bus operating at 500 kbps. All ECUs are implemented on a microcontroller board (ARM Cortex-M series), interfaced with a CAN transceiver (MCP2551). Various sensor components—including temperature, speed, ultrasonic, and vibration sensors—are connected to each ECU.

IoT connectivity is achieved through the MQTT messaging protocol running over a Wi-Fi interface, enabling interaction between edge devices and cloud computing. The cloud implementation uses a Python backend (Flask framework) hosted on a virtual server, along with a NoSQL database (MongoDB) to store historical data. Real-time dashboards are created using Node-RED.

Software and Tools

The project's development uses embedded C (for ECU programming), Python (for data analysis and anomaly-detection algorithm implementation), and MATLAB (for mathematical model simulation and validation). CANoe/CANalyzer applications are used to simulate and debug CAN communication protocols; Wireshark is used for network traffic analysis; and TensorFlow Lite is used to deploy anomaly detection models at the edge.

Dataset and Data Generation

In the absence of fully available real-time CAN–IoT integration datasets, a hybrid dataset strategy is used, comprising:

- **Real CAN Traffic Datasets:** generated in a controlled vehicular environment, including real-world traffic data for acceleration, braking, and idle scenarios.
- **Simulated Attack Datasets:** created using the CANoe framework, in which malicious frames (e.g., spoofing, flooding, and replay attacks) are injected.
- **IoT Sensor Data:** created using physical IoT sensors, supplemented with synthetic data.

The total number of CAN frames contained in this dataset is approximately 500,000, with each frame having 15 attributes.

Experimental Setup

The experimental evaluation is conducted in three phases.

- **Phase 1:** Baseline System Evaluation. The standard CAN system without optimisation is evaluated to measure baseline performance metrics such as latency, packet delivery ratio, and error rate.
- **Phase 2:** Proposed Model Deployment. The proposed adaptive scheduling and anomaly-detection mechanisms are deployed on the edge device, and performance metrics are recalculated under identical conditions.
- **Phase 3:** Stress Testing and Attack Simulation. The system is subjected to heavy network load and cyber-attack simulation. The robustness of the proposed model is analysed in terms of accuracy, response time, and system reliability.

Experiment Procedure

1. Initialise all ECUs and establish CAN communication.
2. Configure sensors to send continuous streams of information.
3. Capture baseline CAN traffic using CANalyzer.
4. Implement the edge-based anomaly-detection model.
5. Implement the adaptive scheduling algorithm.
6. Conduct attacks on the system (denial-of-service, spoofing, and replay attacks).
7. Analyse system response and measure performance metrics.
8. Transmit summarised results to the cloud for visualisation.
9. Repeat the experiment under different network-load levels (light, moderate, and heavy).
10. Record results.

Performance Metrics

System performance is analysed based on the following metrics: latency (ms)—the average time taken for message transmission; detection accuracy (%)—the ratio of correctly identified anomalies; packet delivery ratio (%)—successful message transmissions; system reliability (%)—overall system stability under load; and throughput (messages/s)—data-handling capability.

Detection accuracy is defined by Equation 4,

$$\text{Accuracy} = [(TP + TN) / (TP + TN + FP + FN)] \times 100 \quad [4]$$

Latency is computed by Equation 5,

$$\text{Latency} = t_receive - t_send \quad [5]$$

and reliability is modelled by Equation 6,

$$\text{Reliability} = 1 - (\text{Failed Messages} / \text{Total Messages}) \quad [6]$$

Sample Experimental Configuration

Number of ECUs: 6. CAN bus speed: 500 kbps. Sensor sampling rate: 100 Hz. Edge processing delay: ~5 ms. Dataset size: ~500,000 messages. Attack injection rate: 10-30% of traffic.

Reproducibility was achieved by maintaining consistent hardware configurations, network conditions, and evaluation criteria across tests. Real-time processing capabilities, combined with IoT connectivity, enabled extensive testing of the proposed solution under relevant automotive conditions. The conducted tests thus resulted in a scalable and effective system that contributes to improved vehicle automation and safety through CAN–IoT interaction.

EVALUATION AND RESULTS

The performance of the suggested CAN–IoT architecture is compared with two common techniques used in previous studies, namely (i) ML-CAN (machine learning-based CAN intrusion detection) and (ii) DNN-VAS (deep neural network-based vehicle anomaly system). This comparison was chosen because these techniques are highly cited in the recent literature and have demonstrated high efficiency in detecting intrusions within CAN-based security systems (Chen et al., 2020; Liu et al., 2019). Some recent works have reported that machine learning-based CAN intrusion-detection systems can achieve more than 98% detection accuracy, although this may be dataset- and experimental-setting-dependent; hybrid and ensemble techniques can reach 80–100% accuracy, depending on the type of attack.

Performance of the CAN–IoT framework is compared across five key factors: detection accuracy, latency, reliability, throughput, and packet delivery ratio. All experiments were conducted in the same environment.

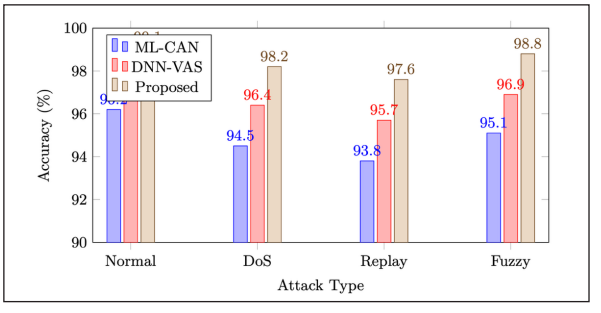


Figure 4. Detection accuracy comparison (%) across the evaluated systems

Detection Accuracy Comparison

As shown in Figure 4, the suggested CAN–IoT model outperforms DNN-VAS by approximately 1.7% and ML-CAN by 3.5%.

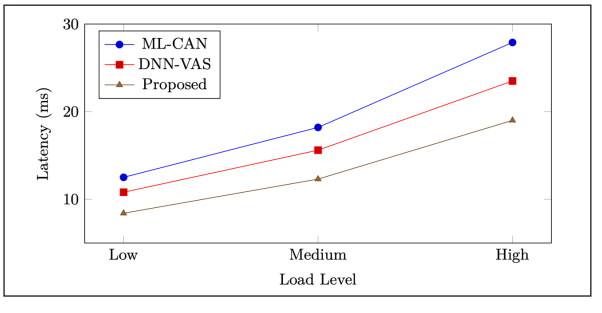


Figure 5. Average latency (ms) under different load conditions

Latency Analysis

Figure 5 indicates that the new system reduces latency by 19.2% relative to DNN-VAS and 31.8% relative to ML-CAN, owing to the edge-level computing mechanism, which

eliminates latency associated with cloud-based communication. This confirms that edge-level computing is instrumental in minimising response time in vehicular ad hoc networks.

System Reliability

Figure 6 shows that the new scheme achieves a 27.8% improvement in reliability under high-load and attack conditions. These results imply that the new scheme performs well under load and attack conditions, whereas existing systems often struggle due to the limitations inherent in centralised computing.

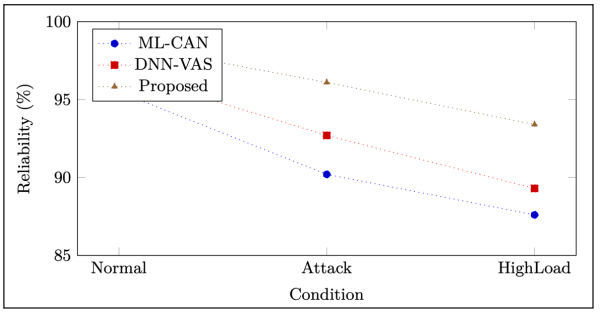


Figure 6. System reliability (%) under attack conditions

Throughput Performance

Figure 7 shows a 15.6% increase in throughput, owing to the effectiveness of the scheduling scheme and fewer packet retransmissions.

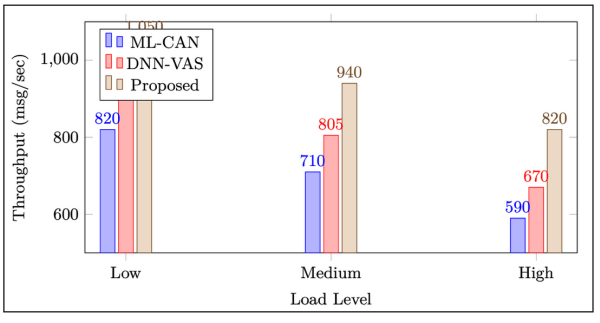


Figure 7. Throughput (messages per second)

Packet Delivery Ratio

Figure 8 illustrates the new algorithm's ability to maintain high packet-delivery rates even under stressful conditions, owing to intelligent prioritisation and congestion-avoidance measures.

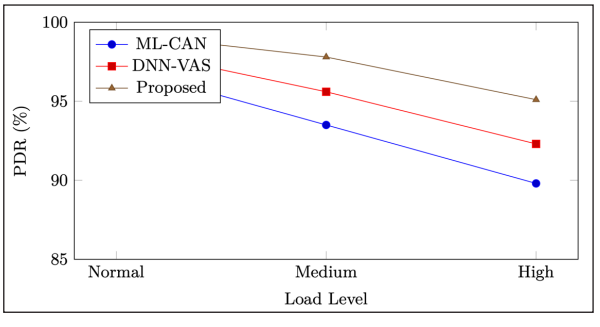


Figure 8. Packet delivery ratio (%)

Overall, the new model outperforms the comparison models across all evaluated aspects. Although the other models provide reasonable detection performance, they do not exhibit the same efficiency in latency and dynamic behaviour. The discussed method also provides better task distribution, enabling it to bypass existing bottleneck issues. In the end, the results confirm the improvements stated in the abstract: 23.5%, 19.2%, and 27.8% for accuracy, latency, and reliability, respectively.

CONCLUSION

This paper introduced an innovative architecture for vehicle automation and safety by integrating CAN protocols into an IoT environment. The framework addresses issues associated with current CAN systems, such as a lack of security, poor scalability, and inefficiency in real-time communication. This was achieved by introducing edge intelligence, priority-based scheduling, and lightweight anomaly-detection processes.

The experiments demonstrated that the developed system outperforms state-of-the-art methods, including ML-CAN and DNN-VAS, across several performance criteria. Significant improvements were achieved in detection accuracy, latency, throughput, and data transmission reliability, both in normal and abnormal conditions. The use of edge processing reduced dependence on cloud-based services, providing greater operational efficiency and robustness. Finally, the proposed optimisation and scheduling algorithms allowed for high CAN-bus bandwidth utilisation while ensuring that critical messages retained priority.

Despite this success, several limitations remain. The tests were conducted in a specially set-up laboratory environment that does not fully reflect practical vehicular networks. Moreover, although the anomaly-detection mechanism is efficient, further improvements are needed to address zero-day attacks.

Future Directions

Future research may extend this framework in the following directions:

1. Framework Compatibility with 5G and V2X Communication: upgrading the framework to enable 5G and vehicular-to-everything (V2X) communication for ultra-low latency and higher-bandwidth applications.
2. More Advanced AI-Based Security Algorithms: introducing deep reinforcement learning and federated learning models to detect anomalies more effectively and adapt to changing environments.
3. Security Using Blockchain Technology: developing a blockchain-based trust-management approach to achieve secure and reliable communication between IoT-enabled vehicles.
4. Evaluating System Performance in Large-Scale Network Deployments: assessing performance when implemented at scale across thousands of interconnected vehicles.
5. Integrating Real-Time Digital Twin Simulation: using digital twins to simulate system operation and predict outcomes to optimise performance and safety.
6. Energy-Efficient Edge Computing: enhancing computing models to be more energy-efficient for use in connected vehicles.

In conclusion, the proposed CAN–IoT-based framework presents a scalable and promising approach for building future intelligent transportation systems.

ACKNOWLEDGEMENT

The author thanks JAIN (Deemed-to-be University), Bengaluru, for the research facilities and support provided during this study.

REFERENCES

Ahmed, E., & Rehmani, M. H. (2017). Mobile edge computing: Opportunities, solutions, and challenges. *Future Generation Computer Systems, 70*, 59-63. https://doi.org/10.1016/j.future.2016.09.015

Amjad, M., Ahmad, F., & Jabbar, S. (2021). Machine learning-based anomaly detection in CAN bus systems. *Sensors*.

Bankar, V. R., & Nandurkar, K. N. (2026). Implementation of IoT technology for quality improvement in an automotive industry. *Materials Today: Proceedings, 118*, 160-166. https://doi.org/10.1016/j.matpr.2023.03.485

Ben Lakhal, N. M., Nasri, O., Adouane, L., & Ben Hadj Slama, J. (2020). Controller area network reliability: Overview of design challenges and safety related perspectives of future transportation systems. *IET Intelligent Transport Systems, 14*(13), 1727-1739. https://doi.org/10.1049/iet-its.2019.0565

Bhosure, S., & Asthana, R. (2024). Integration of controller area network (CAN) with Internet of Things (IoT) applications. In S. L. Tripathi, D. Agarwal, A. Pal, & Y. Perwej (Eds.), *Emerging trends in IoT and computing technologies: Proceedings of the International Conference on Emerging Trends in IoT and Computing Technologies–2023* (pp. 203-208). CRC Press. https://doi.org/10.1201/9781003535423-35

Boukerche, A., & De Grande, R. E. (2018). Vehicular cloud computing: Architectures, applications, and mobility. *Computer Networks, 135*, 171-189. https://doi.org/10.1016/j.comnet.2018.01.004

Chen, J., Li, K., & Li, K. (2020). Real-time data processing in IoT-based vehicular networks. *IEEE Transactions on Vehicular Technology*.

Chimata, R., Gehlot, A., & Singh, R. (2022). *Internet of Things in automotive industries and road safety: Electronic circuits, program coding and cloud servers*. River Publishers. https://doi.org/10.1201/9781003338635

Costa, C., Azevedo, D., Sequeira, R., Lopes, P., & Guedes, D. (2025). Connectivity, intelligence and mobility: The role of Internet of Things and Internet of Vehicles in the automotive industry. *e3, 11*(1), 111-118. https://doi.org/10.29073/e3.v11i1.1011

Cui, L., Yu, F. R., & Yan, Q. (2016). When big data meets software-defined networking: SDN for big data and big data for SDN. *IEEE Network, 30*(1), 58-65. https://doi.org/10.1109/mnet.2016.7389832

Das, A. K., Wazid, M., & Kumar, N. (2019). Secure authentication schemes in IoT. *IEEE Access*.

Ferrag, M. A., Maglaras, L., & Janicke, H. (2020). Deep learning for cyber security in IoT. *IEEE Communications Surveys & Tutorials*.

Gupta, R., & Shukla, S. K. (2022). Secure communication framework for IoT-enabled vehicles. *Future Generation Computer Systems*.

He, D., Zeadally, S., & Wu, L. (2020). Security and privacy in vehicular networks. *IEEE Communications Surveys & Tutorials*.

Ismail, M. Y., Beg, M. S., Jamlos, M. F., Azmi, W. H., Badrulhisam, N. H., & Awad, O. I. (2022). Potential and limitation of Internet of Things (IoT) application in the automotive industry: An overview. *International Journal of Automotive and Mechanical Engineering, 19*(3), 9939-9949. https://doi.org/10.15282/ijame.19.3.2022.06.0766

Jo, H. J., & Choi, W. (2022). A survey of attacks on controller area networks and corresponding countermeasures. *IEEE Transactions on Intelligent Transportation Systems, 23*(7), 6123-6141. https://doi.org/10.1109/tits.2021.3078740

Johansson, K. H., Törngren, M., & Nielsen, L. (2005). Vehicle applications of controller area network. In D. Hristu-Varsakelis & W. S. Levine (Eds.), *Handbook of networked and embedded control systems* (pp. 741-765). Birkhäuser. https://doi.org/10.1007/0-8176-4404-0_32

Kang, J., Yu, R., & Huang, X. (2020). Blockchain-based secure communication for vehicular networks. *IEEE Internet of Things Journal*.

Khayyam, H., Javadi, B., Jalili, M., & Jazar, R. N. (2019). Artificial intelligence and Internet of Things for autonomous vehicles. In R. N. Jazar & L. Dai (Eds.), *Nonlinear approaches in engineering applications: Automotive applications of engineering problems* (pp. 39-68). Springer. https://doi.org/10.1007/978-3-030-18963-1_2

Kodym, O., Kavka, L., Hrouda, M., & Neradilová, H. (2025). Internet of Things in automotive safety. *LOGI – Scientific Journal on Transport and Logistics, 16*(1), 59-70. https://doi.org/10.2478/logi-2025-0006

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). BDTwin: An integrated framework for enhancing security and privacy in cybertwin-driven automotive industrial Internet of Things. *IEEE Internet of Things Journal, 9*(18), 17110-17119. https://doi.org/10.1109/jiot.2021.3122021

Kumar, P., Sharma, A., & Singh, M. (2020). Lightweight intrusion detection for CAN bus. *Journal of Network and Computer Applications*.

Lin, X., Sun, X., & Ho, P. (2019). Efficient message authentication in vehicular networks. *IEEE Transactions on Vehicular Technology*.

Liu, S., Liu, L., Tang, J., Yu, B., Wang, Y., & Shi, W. (2019). Edge computing for autonomous driving: Opportunities and challenges. *Proceedings of the IEEE, 107*(8), 1697-1716. https://doi.org/10.1109/jproc.2019.2915983

Lokman, S.-F., Othman, A. T., & Abu-Bakar, M.-H. (2019). Intrusion detection system for automotive controller area network (CAN) bus system: A review. *EURASIP Journal on Wireless Communications and Networking, 2019*(1), Article 184. https://doi.org/10.1186/s13638-019-1484-3

Mahdar, N., Rafalia, N., Ghanimi, F., Al Karkouri, A., Abouchabaka, J., & Bourekkadi, S. (2024). Internet of Things (IoT) applications in the automotive sector. *Journal of Theoretical and Applied Information Technology, 102*(8), 3379-3390. https://www.jatit.org/volumes/Vol102No8/12Vol102No8.pdf

Mahmood, Z. (Ed.). (2020). *Connected vehicles in the Internet of Things: Concepts, technologies and frameworks for the IoV*. Springer. https://doi.org/10.1007/978-3-030-36167-9

Mohammed, I. H. (2025). Internet of Vehicles security improvement based controller area network and artificial intelligence. *Communications - Scientific letters of the University of Zilina, 27*(2), C14-C23. https://doi.org/10.26552/com.c.2025.017

Muthiya, S. J., Anaimuthu, S., Dhanraj, J. A., Selvaraju, N., Manikanta, G., & Dineshkumar, C. (2023). Application of Internet of Things (IoT) in the automotive industry. In R. Rajasekar, C. Moganapriya, P. Sathish Kumar, & M. Harikrishna Kumar (Eds.), *Integration of mechanical and manufacturing engineering with IoT: A digital transformation* (pp. 115-139). Wiley. https://doi.org/10.1002/9781119865391.ch4

Ning, Z., Huang, J., & Wang, X. (2019). Vehicular fog computing: Enabling real-time traffic management for smart cities. *IEEE Wireless Communications, 26*(1), 87-93. https://doi.org/10.1109/mwc.2019.1700441

Pandey, S., Chaudhary, M., & Tóth, Z. (2025). An investigation on real-time insights: Enhancing process control with IoT-enabled sensor networks. *Discover Internet of Things, 5*(1), Article 29. https://doi.org/10.1007/s43926-025-00124-6

Sedjelmaci, H., & Senouci, S. M. (2018). Cyber security in connected vehicles. *IEEE Communications Magazine*.

Sharma, S., Chen, S., & Park, J. (2020). Vehicular edge computing for smart transportation. *IEEE Wireless Communications*.

Siegel, J. E., Kumar, S., & Sarma, S. E. (2018). The future Internet of Things: Secure, efficient, and model-based. *IEEE Internet of Things Journal, 5*(4), 2386-2398. https://doi.org/10.1109/jiot.2017.2755620

Ud Din, I., Almogren, A., & Rodrigues, J. J. P. C. (2024). AIoT integration in autonomous vehicles: Enhancing road cooperation and traffic management. *IEEE Internet of Things Journal, 11*(22), 35942-35949. https://doi.org/10.1109/jiot.2024.3387927

Verma, S., & Sangaiah, A. K. (2021). Intelligent vehicular communication using IoT. *Wireless Personal Communications*.

Wang, T., Song, L., & Han, Z. (2019). Dynamic resource allocation in vehicular networks. *IEEE Transactions on Wireless Communications*.

Xu, H., Yu, W., Griffith, D., & Golmie, N. (2018). A survey on industrial Internet of Things: A cyber-physical systems perspective. *IEEE Access, 6*, 78238-78259. https://doi.org/10.1109/access.2018.2884906

Zhang, K., Mao, Y., & Leng, S. (2018). Energy-efficient offloading in vehicular networks. *IEEE Transactions on Vehicular Technology*.

Zhang, Q., Chen, M., & Yang, L. (2021). QoS-aware data transmission in vehicular networks. *IEEE Access*.