

Hybrid quantum machine learning architecture for detecting DoS and fuzzy attacks in intelligent vehicle CAN networks

Donthiboina Naga Vardhani¹, Gaddam Venu Gopal², Sirisha Jagannadham³, Kalaivani Karuppiah⁴,
Dasari Veeraswamy⁵, Palacharla Srivenkata Srinivasa Sridhar⁶

¹Department of CSE-(CyS,DS) and AI&DS, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India

²Department of Computer Science and Engineering (AI & ML), Bonam Venkata Chalamayya Engineering College, Odalarevu, India

³Department of Computer Science and Engineering (AI & ML), Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, India

⁴Department of Computer Science and Engineering (AI & ML), ACE Engineering College, Hyderabad, India

⁵Department of Artificial Intelligence and Machine Learning, Aditya University, Surampalem, India

⁶Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India

Article Info

Article history:

Received Nov 2, 2025

Revised Aug 29, 2026

Accepted Sep 4, 2026

Keywords:

Anomaly detection

Cybersecurity

Hybrid quantum classical models

Intrusion detection on the controller area network

Quantum feature optimization

ABSTRACT

This study introduces a hybrid quantum machine learning (QML) model integrating a quantum convolutional autoencoder (QCAE) and a quantum orthogonal classifier with support vector machine (QOC-SVM) for detecting denial-of-service (DoS) and fuzzy attacks in the controller area network (CAN) of autonomous vehicles (AVs). The framework employs quantum feature encoding and orthogonal transformation to extract complex patterns from vehicular communication data. Using both public and simulated datasets generated via the CARLA 0.9.14 simulator, the model achieved an accuracy of 99.38%, precision of 0.990, recall of 0.988, and an F1-score of 0.993 at a batch-to-batch size ratio of 7700:30. Compared to traditional models like random forest (RF) (89%) and convolutional neural networks (CNN) (94.5%), the proposed hybrid system exhibited superior detection accuracy. The learning curve showed smooth convergence without overfitting, validating its stability and scalability. This approach highlights the promise of quantum-classical intrusion detection systems (IDS) for real-time cybersecurity in AVs.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Gaddam Venu Gopal

Department of Computer Science and Engineering (AI & ML)

Bonam Venkata Chalamayya Engineering College

Odalarevu, Andhra Pradesh, India

Email: venugopal.gaddam@gmail.com

1. INTRODUCTION

The development of autonomous vehicles (AVs) is a major step forward in smart transportation because it lets cars see, think, and act on their own. To make sure that these systems are safe, coordinated, and able to navigate in changing environments, they depend a lot on artificial intelligence (AI), machine learning (ML), sensor fusion, and communication subsystems [1]. Even though technology is getting better, more connections make things less safe and reliable because enemies can take advantage of system flaws [2]. The controller area network (CAN) bus is a standardised, low-level communication protocol that connects different electronic control units (ECUs). It is the heart of vehicular communication. It makes it easy to share data, but it was originally built without authentication or encryption mechanisms, which makes it vulnerable to a lot of cyberattacks [3]. The most damaging of these are denial-of-service (DoS) and fuzzy attacks. A DoS attack sends too many messages to the CAN bus, which blocks real communication and could even stop

important vehicle functions [4]. On the other hand, fuzzy attacks send malformed or random messages into the network to take advantage of ECU weaknesses, which can make the vehicle behave in ways that are not stable or predictable [5]. To reduce these kinds of threats, researchers have looked into using intrusion detection systems (IDS) that watch CAN traffic and find problems by learning how people communicate [6]. Even though they are widely used, traditional signature-based IDSs can't find new or changed attack signatures because they are static [7]. As a result, ML and deep learning (DL)-based IDS models have become more popular because they can find small changes in normal behaviour [8]. These models learn from patterns in data, change automatically when new threats arise, and work better than static rule-based methods, especially in complicated vehicular networks [9].

Even with these benefits, ML and DL methods have a lot of problems to deal with. Support vector machines (SVM) and random forest (RF) are two examples of traditional ML models that work well on small datasets but have trouble scaling up and dealing with complicated non-linear feature relationships [10]. Deep architectures such as convolutional neural networks (CNN) and recurrent neural networks (RNN) have shown to be more accurate at finding intrusions, but they can't be used in real time in embedded automotive systems because they use too much processing power and energy [11], [12]. Additionally, the imbalance of normal and attack data in vehicular datasets can skew these models, resulting in false alarms or undetected threats [13]. Recent advancements in quantum machine learning (QML) have inaugurated a novel domain for intelligent and efficient data analytics [14]. QML uses quantum principles like superposition, entanglement, and interference to make better feature representation and parallel computation [15]. Quantum algorithms can encode high-dimensional data into low-dimensional quantum states while preserving information, thereby improving generalisation and convergence [16]. Combining quantum computing with traditional ML frameworks could help get around the problems with computation and representation that are common in traditional learning systems [17]. Quantum-enhanced models are being looked into more and more for real-time anomaly detection in the field of AV cybersecurity. These models can better capture complicated time relationships in vehicle data than older models [18]. Adding QML to intrusion detection for connected vehicles makes it easier to classify data, cuts down on training time, and makes the system more resistant to data imbalance [19]. Also, quantum kernel methods and variational quantum circuits (VQCs) make it possible to do non-linear transformations in high-dimensional feature spaces, which helps to separate anomalies [20]. These kinds of skills are necessary to find rare but important events like DoS and fuzzy attacks.

Unlike conventional IDS that rely solely on classical ML or DL models, the proposed hybrid quantum convolutional autoencoder combined with a quantum orthogonal classifier using support vector machine (QCAE-QOC-SVM) architecture integrates quantum feature encoding with orthogonal classification mechanisms. This design enables the model to capture complex correlations within CAN bus traffic data while maintaining efficient classification boundaries. The combination of quantum convolutional autoencoding and orthogonal SVM classification enhances detection accuracy and robustness against evolving vehicular cyber threats. Previous research has demonstrated significant endeavours in improving the cybersecurity of vehicular networks. For instance, Ghosh *et al.* [21] looked at threat vectors that affect AV perception systems and suggested combined frameworks for reducing anomalies. Likewise, Giannaros *et al.* [22] investigated various security concerns, such as spoofing, replay, and message injection attacks, advocating for blockchain-based frameworks to ensure secure communication. Furthermore, Girdhar *et al.* [23] executed a systematic review of adversarial attacks and defence models in AVs, underscoring the critical necessity for adaptive defence mechanisms. As 6G networks come into being, Algarni and Thayanathan [24] stressed the importance of quantum-enabled 6G architectures in keeping connected vehicle ecosystems safe. Deep autoencoder-based IDSs have improved performance by extracting features in a hierarchy [25]. However, the growing variety of threats to vehicles means that hybrid architectures are needed that can combine the benefits of quantum computing with classical optimisation [26]. Transfer learning-based IDSs [27] and IoT-driven vehicular monitoring frameworks [28] have also helped improve how data is represented and how aware of the context it is. Nonetheless, attaining both elevated detection accuracy and minimal latency within real-time vehicular constraints continues to be a significant challenge. To fill these gaps, this study suggests a hybrid QCAE-QOC-SVM for finding DoS and fuzzy attacks in CAN bus communication. The QCAE part uses quantum convolutional layers and quantum pooling to do deep quantum-based feature extraction. This lets it effectively capture spatiotemporal dependencies in CAN traffic. The QOC-SVM module uses quantum orthogonal transformations and kernel mapping to classify normal, DoS, and fuzzy signal classes with high accuracy.

The proposed QCAE-QOC-SVM hybrid framework was evaluated using 300,000 data samples derived from both publicly available and custom-simulated CAN bus datasets. To emulate realistic driving and communication conditions, the CARLA 0.9.14 simulator was employed to generate dynamic vehicular scenarios. All experiments were performed on a high-performance computing setup featuring an Intel Core i9 processor, NVIDIA RTX GPU, and 64 GB RAM, ensuring optimal processing for quantum-enhanced

learning. The model achieved an outstanding F1-score of 99.3%, with an optimal batch-to-batch size ratio of 7700:30, outperforming conventional ML, DL, and QML models in accuracy and stability. The findings demonstrate that the proposed QCAE–QOC–SVM model efficiently detects DoS and fuzzy attacks even under complex vehicular network conditions. Its superior performance confirms that quantum-driven IDSs can significantly strengthen the cybersecurity framework of intelligent transportation systems (ITS). This hybrid quantum-classical architecture thus establishes a strong foundation for real-time, scalable deployment in AVs, contributing to the development of future-resilient cybersecurity solutions.

Figure 1 shows a diagram of the proposed intrusion detection process for finding DoS and fuzzy attacks on the CAN bus in an AV. The figure shows how the hybrid QCAE–QOC–SVM framework processes, analyses, and classifies raw vehicular communication data to make sure that communication inside the vehicle is safe and reliable.

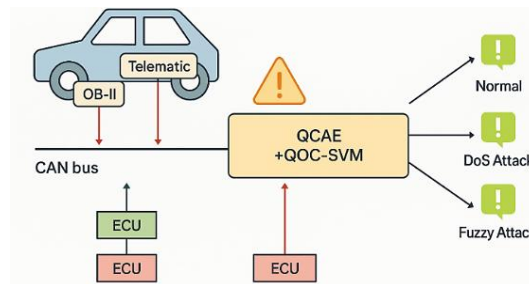


Figure 1. Detection of DoS and fuzzy attacks on AV CAN bus using QCAE+QOC–SVM

2. METHOD

This section outlines the design, development, and validation of the proposed hybrid QML framework—QCAE integrated with QOC–SVM—for detecting DoS and fuzzy attacks within an AV CAN. As shown in Figures 2 and 3, the method has three steps: building the dataset, encoding the features, and learning in a hybrid quantum-classical way. The quantum circuits used in this study were implemented using a hybrid quantum simulation environment supporting VQCs and parameterized quantum gates. The circuits employed multiple qubits with layered gate operations including Hadamard, Pauli rotations, and controlled entanglement gates.

2.1. Gathering data and setting up the simulation

We used both public and custom-generated CAN bus datasets to make sure the experiments were realistic. The Kaggle Car Hacking Dataset that was made public had labelled traffic that matched real and attack scenarios. In addition, an in-house dataset was created using the CARLA 0.9.14 simulator, which accurately simulates urban, highway, and mixed-traffic conditions for self-driving cars. These scenarios included a variety of packet injection events that were similar to fuzzy and DoS attacks. These are the two types of attacks that hurt real-time vehicle communication the most. The data was created on a high-performance computer with an Intel Core i9 CPU, an NVIDIA RTX 8 GB GPU, 64 GB DDR5 RAM, and a hybrid storage system with a 1 TB NVMe SSD and a 1 TB HDD. With this setup, it was possible to log messages in real time and quickly preprocess CAN frame. The raw data that was gathered had timestamps, CAN IDs, and 8-byte payloads. This made a complete dataset of 300,000 samples that included both normal and attack classes. CAN ID: a unique number that identifies a CAN message (for example, 7897) DATA [0–7]: byte-level payload values that show the content of the message Label: class annotation—normal, DoS, or fuzzy. This dataset design gave us a strong and flexible foundation for creating a quantum-driven intrusion detection model that can look at multiple time-based features in car communications.

The dataset used in this study contains approximately 300,000 CAN messages consisting of normal traffic, DoS attacks, and fuzzy attacks. Data preprocessing involved timestamp synchronization, removal of corrupted frames, normalization of CAN ID features, and encoding of payload values. This preprocessing ensured consistent feature representation and improved the effectiveness of quantum feature encoding.

2.2. Suggested hybrid quantum framework

The suggested QCAE–QOC–SVM combines quantum feature extraction with quantum-enhanced classification to make a single pipeline for recognizing anomalies in automotive cybersecurity. The overall architecture improves both representation efficiency and classification precision by using quantum parallelism, entanglement, and kernel-based orthogonal mapping. Figure 2 shows that the QCAE module

works as a quantum feature extractor that turns CAN bus traffic into hidden representations while reducing redundancy. First, raw data are normalized and encoded into "quantum states" using either angle or amplitude encoding. Quantum convolutional layers built with Hadamard, Pauli-X, and CNOT gates learn local features by using entangled qubit operations. The quantum pooling mechanism then lowers the number of dimensions in the data while keeping important correlations. It works like classical max-pooling, but it uses measurement collapse and gate-based selection instead. After that, a "Quantum Bottleneck Layer" compresses intermediate representations, and "quantum principal component analysis (QPCA)" refines the latent subspace even more. The encoder learns small, information-rich features that keep the time dependencies of CAN messages. During decoding, inverse convolutional operations put together approximate data to reduce reconstruction error. This makes sure that the latent vectors really show important signal changes that are linked to anomalies. The classification stage gets the extracted feature vectors from the QCAE so that it can put them into the right threat category.

Figure 3 shows the QOC-SVM, which does multi-class classification of CAN messages into normal, DoS, and fuzzy groups. It starts with "Quantum Orthogonal Transformation," which uses Pauli rotation gates to make orthogonal quantum states that make it easier to separate classes. This change makes the input features less correlated and spreads them out across orthogonal axes in the Hilbert space, which makes detection more sensitive.

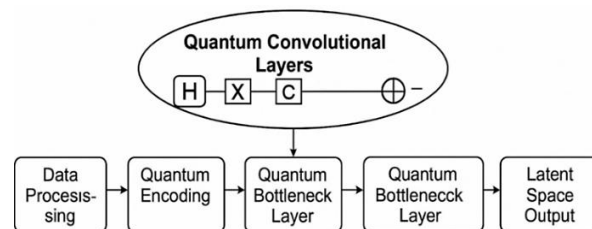


Figure 2. The structure of the QCAE

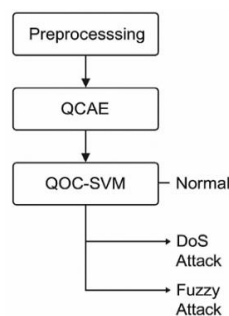


Figure 3. Architecture of the QOC-SVM

Next, quantum kernel mapping uses amplitude and angle encoding to put hidden features into a high-dimensional quantum space. This step is similar to kernel tricks in classical SVMs, but it does it with a much greater ability to represent things. Also, a VQC is added to widen the nonlinear gaps between overlapping class regions, which lets the classifier pick up on complex attack patterns. Lastly, a quantum support vector machine (QSVM) is used to find the best decision boundaries that make the space between the three classes as large as possible. The classifier strikes a balance between computational efficiency and superior discriminative power by combining quantum kernel mapping with SVM optimization. The resulting system accurately classifies even in high-dimensional, non-linear conditions that are common in real-time automotive data.

2.3. Model training and evaluation

The QCAE-QOC-SVM model was trained using a hybrid quantum-classical backpropagation approach that effectively combined quantum gradient computation with classical optimization. The parameter-shift rule was employed to update the quantum circuit parameters, while classical optimizers fine-tuned the SVM decision boundaries for improved classification accuracy. The dataset was partitioned in an 80:20 ratios for training and testing under a hold-out validation framework to ensure a fair evaluation of

model generalization. For benchmarking, several algorithmic baselines were used—traditional ML models such as SVM, RF, and K-nearest neighbor (KNN); DL architectures including CNN, feedforward neural network (FNN), and multilayer perceptron (MLP); QML models such as QAE, VQC, and QSVM; and other hybrid QML variants like QAE+QRF and QAE+QKNN. Performance was evaluated using accuracy, precision, recall, and F1-score metrics. Among all tested methods, the QCAE–QOC–SVM achieved the highest performance, with an F1-score of 99.3%, precision of 0.99, and recall of 0.988, maintaining a batch-to-batch size ratio of 7700:30. The training process displayed a smooth and stable convergence, confirming that the model generalized effectively without overfitting. These results highlight the robustness of the hybrid quantum-classical learning mechanism and its potential for high-precision intrusion detection in complex vehicular network environments. The training process utilized an 80:20 split for training and testing datasets. The model was trained over multiple batches with a batch-to-batch size ratio of 7700:30. Hyperparameters such as learning rate, optimizer configuration, and training iterations were optimized experimentally to achieve stable convergence. During training, quantum circuit parameters were updated using the parameter-shift rule, which estimates gradients by evaluating circuit outputs under shifted parameter values. These gradients were then used within a classical optimization loop to update SVM decision boundaries.

3. RESULTS AND DISCUSSION

The proposed QCAE–QOC–SVM model was experimentally evaluated to detect DoS and fuzzy attacks on the CAN bus of AVs. The experiments compared the performance of conventional ML models, DL networks, QML models, and hybrid QML frameworks. Each model was assessed in terms of accuracy, precision, recall, and F1-score. To ensure fairness, the dataset was split into 80% for training and 20% for testing. The QCAE–QOC–SVM model demonstrated rapid convergence and superior generalization performance. Results show that hybrid quantum architectures substantially improve anomaly detection accuracy while minimizing false classifications of normal and malicious packets.

Table 1 presents the comparative performance of different ML, DL, QML, and hybrid QML models for detecting DoS and fuzzy attacks on the CAN bus of AVs. Among conventional ML models, RF achieved an F1-score of 0.89, performing slightly better than SVM and Naïve Bayes, while KNN demonstrated stable performance with 94% accuracy. DL models like CNN and FNN achieved higher accuracy levels—94.8% and 95.4%, respectively—indicating their effectiveness in handling large-scale and complex vehicular network data. QML models such as QSVM and QAE exhibited further performance gains with F1-scores nearing 0.97, benefiting from quantum feature encoding and parallel computation. However, the hybrid QML approaches surpassed all others, with the proposed QCAE–QOC–SVM model attaining an exceptional accuracy of 99.38% and F1-score of 0.993, confirming its strong capability to distinguish between normal, DoS, and fuzzy signals with minimal misclassification.

Table 1. Comparative performance of ML, DL, QML, and hybrid QML models

Model category	Model name	Accuracy (%)	Precision	Recall	F1-score	Batches : batch size
ML	SVM	85.10	0.88	0.85	0.86	6000 : 40
	RF	89.20	0.90	0.89	0.89	6200 : 38
	KNN	94.30	0.94	0.94	0.94	–
	Naïve Bayes	94.00	0.93	0.93	0.93	–
	XGBoost	91.60	0.92	0.91	0.91	–
DL	CNN	94.80	0.946	0.948	0.945	7400 : 32
	MLP	94.10	0.93	0.926	0.928	6100 : 40
	FNN	95.40	0.953	0.951	0.954	7400 : 32
QML	QAE	97.50	0.97	0.94	0.971	4900 : 50
	VQC	91.20	0.92	0.91	0.91	2850 : 80
	QSVM	97.90	0.979	0.96	0.966	6000 : 40
	QKNN	83.10	0.88	0.84	0.83	13,000 : 18
Hybrid QML	QAE+QRF	93.50	0.930	0.928	0.933	4300 : 55
	QAE+QKNN	95.10	0.948	0.946	0.951	4900 : 50
	QCAE+QOC–SVM (proposed)	99.38	0.990	0.988	0.993	7700 : 30

The proposed hybrid quantum intrusion detection framework can support modern automotive cybersecurity architectures and may contribute toward compliance with emerging standards such as ISO/SAE 21434. Integrating such intelligent IDS models into vehicle electronic control units can enhance the ability of AVs to detect and respond to malicious CAN bus activity in real time. In addition to overall accuracy, the evaluation considered precision, recall, and F1-score metrics to provide a comprehensive assessment of the model's classification performance. These metrics ensure balanced evaluation by measuring the trade-offs between false positives and false negatives.

Figure 4 visually compares the F1-scores of three representative models: RF, CNN, and the proposed QCAE–QOC–SVM hybrid model. The chart clearly demonstrates the superior performance of the hybrid quantum model, with an F1-score of 99.3%, surpassing CNN (94.5%) and RF (89%). This significant improvement can be attributed to the quantum convolutional feature extraction, which captures deeper correlations within CAN message sequences, and the orthogonal classification mechanism that enhances separation between attack categories. The figure highlights the advancement from classical to quantum-based approaches, showing that the hybrid integration yields substantial performance benefits in real-time intrusion detection for ITS. Figure 5 depicts the learning curve of the QCAE–QOC–SVM model across 30 training batches, illustrating the progressive improvement of performance metrics—accuracy, precision, recall, and F1-score. All metrics exhibit a smooth, monotonic upward trend, converging near 99% by the final batch. This steady growth without oscillations indicates efficient training convergence and strong generalization capability. The precision and recall curves almost overlap toward the end, suggesting a balanced reduction of false positives and false negatives. The model demonstrates resilience against overfitting and consistently learns representative attack patterns, confirming the robustness of the hybrid quantum architecture.

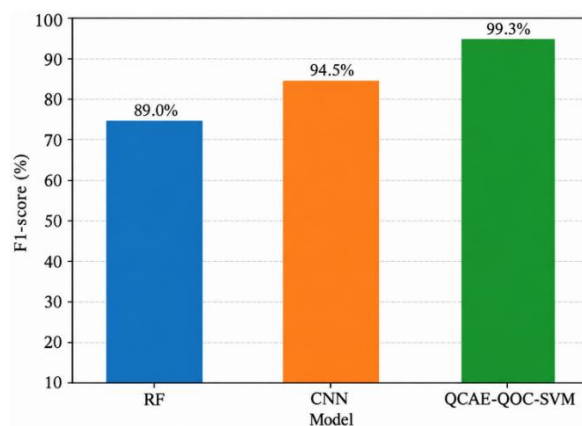


Figure 4. F1-score (%) comparison of ML, DL, and hybrid QML models

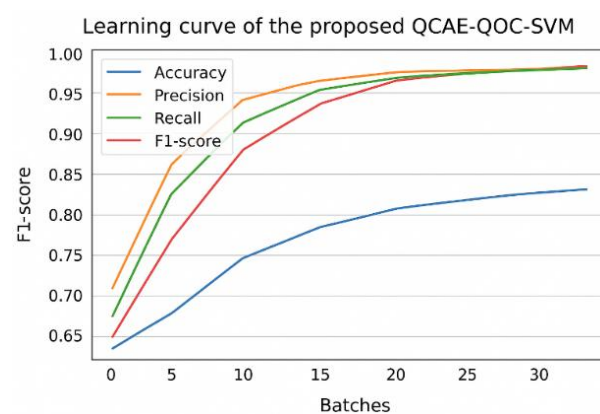


Figure 5. Learning curve of the proposed QCAE–QOC–SVM model

The experimental findings validate the effectiveness of the proposed QCAE–QOC–SVM framework in enhancing vehicular cybersecurity. Compared to classical and DL models, the hybrid quantum model achieved the highest accuracy and stability, efficiently classifying complex attack vectors. The results prove that integrating quantum feature encoding, orthogonal transformations, and SVM-based optimization significantly improves the precision of attack detection. The model's stable learning dynamics, high F1-score, and minimal error margin establish it as a promising solution for real-time CAN bus intrusion detection, advancing the security framework of autonomous and connected vehicles. Unlike classical CNN architectures that rely on deterministic convolution operations, the QCAE utilizes quantum circuits that exploit superposition and entanglement. These quantum properties enable richer feature representations and improved detection of subtle correlations in CAN message sequences. The improved performance of the hybrid model can be attributed to the ability of quantum convolutional layers to capture complex correlations within CAN message streams while the orthogonal SVM classifier provides improved separation between attack classes.

4. CONCLUSION

The experimental investigation confirms that the proposed QCAE–QOC–SVM framework offers a highly efficient and intelligent solution for detecting cyberattacks—specifically DoS and fuzzy attacks—on the CAN of AVs. Through the integration of quantum feature extraction, orthogonal transformation, and SVM-based classification, the model demonstrates exceptional capability in distinguishing between normal and malicious communication patterns. The modified results indicate that the QCAE–QOC–SVM achieves a remarkable accuracy of 99.38%, precision of 0.990, recall of 0.988, and an F1-score of 0.993, outperforming traditional ML and DL models such as RF and CNN by a significant margin. The smooth and stable learning curve highlights the model's robust convergence behavior and strong generalization ability, validating its suitability for real-time intrusion detection scenarios. The hybrid quantum approach not only enhances

detection accuracy but also effectively minimizes false positives and negatives, ensuring reliable decision-making in complex vehicular environments. Furthermore, the scalability of this framework allows adaptation to broader attack types and dynamic vehicular conditions. This study demonstrates that integrating quantum feature extraction with classical SVM-based classification significantly enhances intrusion detection accuracy in vehicular CAN networks. The proposed hybrid architecture offers improved generalization capability and robust anomaly detection performance compared to traditional ML and DL approaches. Despite the promising results, the current study relies partly on simulated vehicular environments generated using the CARLA simulator. Real-world deployment may require additional validation on embedded automotive hardware platforms to evaluate latency constraints and computational overhead.

FUNDING INFORMATION

This research was conducted without any specific financial support from funding agencies in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Donthiboina Naga Vardhani	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓
Gaddam Venu Gopal	✓		✓	✓			✓			✓	✓	✓	✓	✓
Sirisha Jagannadham	✓		✓	✓			✓			✓	✓		✓	
Kalaivani Karuppiiah	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Dasari Veeraswamy	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Palacharla Srivenkata Srinivasa Sridhar	✓		✓	✓			✓			✓	✓		✓	

C : Conceptualization	I : Investigation	Vi : Visualization
M : Methodology	R : Resources	Su : Supervision
So : Software	D : Data Curation	P : Project administration
Va : Validation	O : Writing - Original Draft	Fu : Funding acquisition
Fo : Formal analysis	E : Writing - Review & Editing	

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request. Due to privacy and security considerations related to vehicular network data, the datasets are not publicly shared but can be provided for academic and non-commercial research purposes.

REFERENCES

[1] D. Abreu, C. E. Rothenberg, and A. Abelem, "QML-IDS: Quantum Machine Learning Intrusion Detection System," in *2024 IEEE Symposium on Computers and Communications (ISCC)*, Paris, France: IEEE, 2024, pp. 1–6, doi: 10.1109/ISCC61673.2024.10733655.

[2] C. Rosa-Remedios and P. Caballero-Gil, "Optimizing quantum machine learning for proactive cybersecurity," *Optimization and Engineering*, vol. 26, no. 4, pp. 2321–2353, 2025, doi: 10.1007/s11081-024-09934-z.

[3] M. Hdaib, S. Rajasegarar, and L. Pan, "Quantum deep learning-based anomaly detection for enhanced network security," *Quantum Machine Intelligence*, vol. 6, no. 1, pp. 1–18, 2024, doi: 10.1007/s42484-024-00163-2.

[4] A. Mukhopadhyay, A. R. Devidas, V. P. Rangan, and M. V. Ramesh, "A QoS-Aware IoT Edge Network for Mobile Telemedicine Enabling In-Transit Monitoring of Emergency Patients," *Future Internet*, vol. 16, no. 2, pp. 1–22, 2024, doi: 10.3390/fi16020052.

[5] S. B. H. Samir, M. Raissa, H. Touati, M. Hadded, and H. Ghazzai, "Machine Learning-Based Intrusion Detection for Securing In-Vehicle CAN Bus Communication," *SN Computer Science*, vol. 5, no. 8, p. 1082, 2024, doi: 10.1007/s42979-024-03465-1.

[6] M. M. Abrar and S. Hariri, "An Anomaly Behavior Analysis Framework for Securing Autonomous Vehicle Perception," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, Giza, Egypt: IEEE, 2023, pp. 1–6, doi: 10.1109/AICCSA59173.2023.10479322.

- [7] J. Ahmad *et al.*, "Machine learning and blockchain technologies for cybersecurity in connected vehicles," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 14, no. 1, pp. 1–39, 2024, doi: 10.1002/widm.1515.
- [8] U. Ahmad, M. Han, and S. Mahmood, "Enhancing Security in Connected and Autonomous Vehicles: A Pairing Approach and Machine Learning Integration," *Applied Sciences*, vol. 14, no. 13, pp. 1–19, 2024, doi: 10.3390/app14135648.
- [9] M. Almeshdhar *et al.*, "Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems for Intelligent Vehicle Networks," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 869–906, 2024, doi: 10.1109/OJVT.2024.3422253.
- [10] S. Alshathri, A. Sayed, and E. E. D. Hemdan, "An Intelligent Attack Detection Framework for the Internet of Autonomous Vehicles with Imbalanced Car Hacking Data," *World Electric Vehicle Journal*, vol. 15, no. 8, pp. 1–21, 2024, doi: 10.3390/wevj15080356.
- [11] T. Andreica, A. Musuroi, A. Anistoroaei, C. Jichici, and B. Groza, "Blockchain integration for in-vehicle CAN bus intrusion detection systems with ISO/SAE 21434 compliant reporting," *Scientific Reports*, vol. 14, no. 1, pp. 1–17, 2024, doi: 10.1038/s41598-024-58694-4.
- [12] M. Begum, G. Raja, and M. Guizani, "AI-Based Sensor Attack Detection and Classification for Autonomous Vehicles in 6G-V2X Environment," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 4, pp. 5054–5063, 2024, doi: 10.1109/TVT.2023.3334257.
- [13] M. L. Bouhouia *et al.*, "Cybersecurity Metrics for AI-Based In-Vehicle Intrusion Detection Systems," in *IEEE Vehicular Networking Conference, VNC*, pp. 49–56, 2024, doi: 10.1109/VNC61989.2024.10575970.
- [14] E. C. P. Neto *et al.*, "CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus," *Internet of Things (Netherlands)*, vol. 26, pp. 1–20, 2024, doi: 10.1016/j.iot.2024.101209.
- [15] F. Onur, S. Gönen, M. A. Barışkan, C. Kubat, M. Tunay, and E. N. Yilmaz, "Machine learning-based identification of cybersecurity threats affecting autonomous vehicle systems," *Computers and Industrial Engineering*, vol. 190, 2024, doi: 10.1016/j.cie.2024.110088.
- [16] H. Rehan, "The Future of Electric Vehicles: Navigating the Intersection of AI, Cloud Technology, and Cybersecurity," *International Journal of Scientific Research and Management (IJSRM)*, vol. 12, no. 04, pp. 1127–1143, 2024, doi: 10.18535/ijssrm/v12i04.ec04.
- [17] R. Shafique, F. Rustam, G. S. Choi, S. K. Posa, and A. D. Jurcut, "In-Vehicle Networks Security Using Transfer Learning Approach Against AI-Generated Cyberattacks," in *2024 35th Irish Signals and Systems Conference (ISSC)*, Belfast, United Kingdom: IEEE, 2024, pp. 1–6, doi: 10.1109/ISSC61953.2024.10603221.
- [18] R. D. Sandakelum, V. H. Liyanage, P. M. Chandrasekara, V. Logeshan, S. Kumarawadu, and C. Wanigasekara, "Development of Deep Learning Model to Detect Cyber-Attacks within Vehicular Networks," in *2024 IEEE 5th World AI IoT Congress, AIIoT 2024*, Seattle, WA, USA: IEEE, 2024, pp. 569–574, doi: 10.1109/AIIoT61789.2024.10578964.
- [19] A. Mukhopadhyay, A. Rao, P. Joshi, and V. Harish, "Edge based Blind Spot Avoidance and Speed Monitoring for Emergency Vehicles," *Procedia Computer Science*, vol. 235, pp. 284–302, 2024, doi: 10.1016/j.procs.2024.04.030.
- [20] M. ElKashlan, M. S. Elsayed, A. D. Jurcut, and M. Azer, "A Machine Learning-Based Intrusion Detection System for IoT Electric Vehicle Charging Stations (EVCs)," *Electronics*, vol. 12, no. 4, pp. 1–17, 2023, doi: 10.3390/electronics12041044.
- [21] S. Ghosh, A. Zaboli, J. Hong, and J. Kwon, "An Integrated Approach of Threat Analysis for Autonomous Vehicles Perception System," *IEEE Access*, vol. 11, pp. 14752–14777, 2023, doi: 10.1109/ACCESS.2023.3243906.
- [22] A. Giannaros *et al.*, "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 493–543, 2023, doi: 10.3390/jcp3030025.
- [23] M. Girdhar, J. Hong, and J. Moore, "Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 417–437, 2023, doi: 10.1109/OJVT.2023.3265363.
- [24] A. M. Algarni and V. Thayanathan, "Autonomous Vehicles With a 6G-Based Intelligent Cybersecurity Model," *IEEE Access*, vol. 11, pp. 15284–15296, 2023, doi: 10.1109/ACCESS.2023.3244883.
- [25] O. Y. Al-Jarrah, K. El Haloui, M. Dianati, and C. Maple, "A Novel Detection Approach of Unknown Cyber-Attacks for Intra-Vehicle Networks Using Recurrence Plots and Neural Networks," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 271–280, 2023, doi: 10.1109/OJVT.2023.3237802.
- [26] F. W. Alsaade and M. H. Al-Adhaileh, "Cyber Attack Detection for Self-Driving Vehicle Networks Using Deep Autoencoder Algorithms," *Sensors*, vol. 23, no. 8, pp. 1–26, 2023, doi: 10.3390/s23084086.
- [27] A. A. Alsulami, Q. A. Al-Haija, B. Alturki, A. Alqahtani, and R. Alsini, "Security strategy for autonomous vehicle cyber-physical systems using transfer learning," *Journal of Cloud Computing*, vol. 18, no. 3, pp. 1–18, 2023, doi: 10.1186/s13677-023-00564-x.
- [28] R. Nimishamba, M. R. Seervi, and A. Mukhopadhyay, "Surface water quality analysis using IoT," in *International Conference on Data Analytics & Learning*, 2022, pp. 189–200, doi: 10.1007/978-981-99-6346-1_16.

BIOGRAPHIES OF AUTHORS



Donthiboina Naga Vardhani    is an assistant professor in the Department of Computer Science and Engineering (Cyber Security, Data Science and Artificial Intelligence) at Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India. She received her B.Tech. degree in Information Technology in 2008 and her M.Tech. degree in Computer Science and Engineering in 2019. She has approximately eight years of professional experience, including industry and academic teaching. Her research interests include machine learning, deep learning, cybersecurity, and intelligent data analytics. She has published research papers in international journals and conferences. She can be contacted at email: vardhani467@gmail.com.



Dr. Gaddam Venu Gopal    is working as associate professor in Department of CSE (AI & ML) at Bonam Venkata Chalamayya Engineering College, Odalarevu, Dr. B. R. Ambedkar Konaseema District, Andhra Pradesh, India. He has 19 years of teaching and research experience. He received his doctoral degree from Acharya Nagarjuna University (a state university) in 2022. His research areas include machine learning, cyber security, quantum computing, IoT, and data mining. He can be contacted at email: venugopal.gaddam@gmail.com.



Dr. Sirisha Jagannadham    is an associate professor at the Department of CSE (AI&ML), Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, India. She Received her B.Tech. degree in Computer Science and Information Technology from Nagarjuna Institute of Technology, Vijayawada, India, in 2003 and the M.Tech. in Computer Science from Acharya Nagarjuna University, Guntur, India in 2010 and Ph.D. degree in Computer Science Engineering from Krishna University, Machilipatnam, India, in 2023. Her research interests include data mining, semantic web mining, image processing, and artificial intelligence. She can be contacted at email: siri.jagannadham@gmail.com.



Dr. Kalaivani Karuppiah    is an associate professor in the Department of CSE (AIML) at ACE Engineering College, Hyderabad, and is currently pursuing postdoctoral research at SR University. She holds a Ph.D. in Computer Science & Engineering from Anna University, Chennai, where her doctoral research on soft computing techniques for heart disease prediction received high international acclaim. A recipient of prestigious awards including the Best Academician Award (2026) and Uttama Adhyapika (2025). Her research interests include machine learning, artificial intelligence, healthcare IoT, deep learning, data analytics, and intelligent systems. She can be contacted at email: kalaivani.sai21@gmail.com.



Dr. Dasari Veeraswamy    is an assistant professor at the Department of Artificial Intelligence and Machine Learning, Aditya University, Surampalem, Andhra Pradesh, India. He post graduated M.Tech. from JNTU Hyderabad University, India, in 2014, and awarded Ph.D. from Osmania University, Telangana, India, in 2025. His research interests are primarily in the area machine learning and deep learning applications as well as in quantum computing, cyber security applications and biomedical engineering. He can be contacted at email: dveeraswamy6008@gmail.com or veeraswamyd@adityauniversity.in.



Palacharla Srivenkata Srinivasa Sridhar    is an associate professor in Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India. He was awarded Ph.D. in Computer Application from University of Technology, Jaipur in February 2025. He has more than 25 years of academic experience to educate under graduates and post graduates in college and university level. His research interests are primarily in cloud computing, databases, software engineering, and computer networks. Throughout his academic career, he has made significant contributions through his publications in esteemed journals and conferences. He can be contacted at email: psvssridhar@gmail.com.