AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

Neuro Fusion-CART: A Hybrid Intelligence Framework for Anomaly Detection in VANETs

S. Sundeep Kumar[1], Penti Bhavani[1], Mohammed Mudassir[1], Goshika Navya[1], Kurmeti Prem Kumar[1]

[1]Department of Computer Science and Engineering, [1]Sree Dattha Institute of Engineering and Science, Nagarjuna Sagar Road, Sheriguda, Ibrahimpatnam, Rangareddy Dist, 501510, Telangana, India.

ABSTRACT

Vehicular Ad Hoc Network (VANET) generate large volumes of real-time data such as packet size, latency, vehicle speed, and signal strength, which can be vulnerable to malicious attacks. Ensuring secure and reliable communication is therefore a critical challenge. Traditionally, anomaly detection in such networks relied on rule-based systems and statistical threshold techniques. These methods depended heavily on predefined rules and manual monitoring, making them less effective in handling complex, dynamic traffic patterns. They often failed to detect unknown or evolving attack behaviors and lacked adaptability to real-time scenarios. In the proposed system, a Machine Learning (ML) and Deep Learning (DL) – Classification and Regression Trees (CART) based hybrid approach is implemented to improve detection accuracy and adaptability. The system utilizes multiple algorithms including Linear Regression (LR), Decision Tree (DT), Passive Aggressive (PA) algorithms, and a novel proposed model called K-NeuroFusion CART. This hybrid model integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) for feature extraction, combined with K-Nearest Neighbors (KNN) for final classification and regression. The models are trained on VANET dataset features such as packet rate, vehicle speed, and anomaly score, achieving high accuracy in detecting normal and attack patterns. The research is developed using Flask for web deployment, SQLite for database management, and libraries like Scikit-learn, TensorFlow, Pandas, and Matplotlib. The system provides both single and batch prediction capabilities, along with visualization and analysis tools.

Key words: Intrusion Detection System, Network Anomaly Detection, Secure Vehicular Communication, Intelligent Network Security

1. INTRODUCTION

With the rapid advancement of intelligent transportation systems, Vehicular Ad Hoc Networks (VANETs) have emerged as a key technology enabling communication between vehicles (V2V) and between vehicles and infrastructure (V2I). VANETs facilitate real-time data exchange such as vehicle speed, location, traffic conditions, and safety alerts, thereby improving road safety, traffic efficiency, and driving experience. However, due to their open wireless communication environment, VANETs are highly vulnerable to various cyber-attacks such as message tampering, denial-of-service attacks, and false data injection.

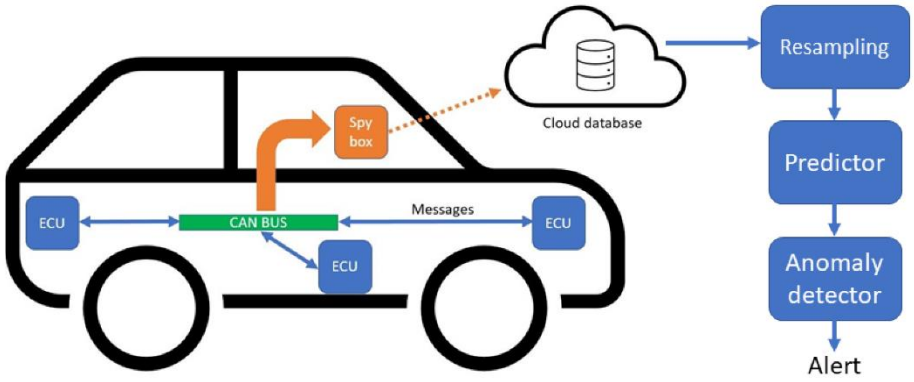

Fig. 1. Anomaly Detection in VANETs

During research, it was found that vehicular networks are highly vulnerable to real-time cyber threats due to their open and dynamic nature. Traditional security approaches are often not sufficient to handle continuously changing network conditions. It was also observed that real-time parameters such as packet transmission, latency, and signal strength vary significantly with traffic conditions, making anomaly detection a challenging task. This created an interest in developing a more intelligent and adaptive system that can monitor and analyze such data effectively. In real-time Vehicular Ad Hoc Networks (VANETs), ensuring secure and reliable communication between vehicles is a major challenge due to the highly dynamic and decentralized nature of the network. Vehicles continuously exchange critical information such as speed, location, and traffic alerts, which, if compromised, can lead to serious safety risks. One of the major problems is the presence of cyber-attacks such as false message injection, data manipulation, and denial-of-service attacks, which can disrupt communication and mislead drivers. Another significant issue is the inability of traditional systems to detect anomalies in real-time. Since vehicular data is generated at high speed and in large volumes, manual monitoring or rule-based systems fail to identify abnormal patterns effectively. This can result in delayed detection of malicious activities, increasing the chances of accidents and traffic congestion.

2. LITERATURE SURVEY

2.1 Graph-Based and Data-Driven Anomaly Detection

Meng et al. [1] introduced a graph-based anomaly detection framework for vehicular networks, where communication interactions among vehicles were modeled as graph structures. This approach enabled effective identification of complex attack patterns and improved detection of network-level anomalies. Alkhatib et al. [9] proposed a sequence-based anomaly detection method using recurrent neural networks, focusing on analyzing temporal communication sequences. Their model effectively captured sequential dependencies and enhanced detection of time-series anomalies in vehicular data.

2.2 Machine Learning and Hybrid Intrusion Detection Systems

Taslimasa et al. [2] developed a hybrid intrusion detection system integrating machine learning and deep learning techniques to improve detection accuracy in dynamic vehicular environments. Their model demonstrated strong adaptability to varying data patterns. Amutha et al. [3] proposed a multi-layer intrusion detection framework based on ensemble learning, combining multiple classifiers to enhance prediction performance and reduce false positives, thereby improving robustness in complex network scenarios.

2.3 Deep Learning-Based Temporal and Sequential Models

Yang et al. [4] introduced a deep learning-based anomaly detection system utilizing recurrent neural networks to capture temporal dependencies in vehicular communication data. Their approach improved the identification of sequential anomalies. Luo et al. [5] combined rule-based analysis with neural network models to detect both known and unknown attacks by examining protocol behavior and payload characteristics, achieving enhanced detection performance.

2.4 Rule-Based and Signature-Based Detection Approaches

Herold et al. [6] proposed a rule-based intrusion detection approach using event processing techniques to analyze communication patterns across multiple layers, enabling effective identification of protocol violations. Koyama et al. [8] developed a whitelist-based detection system that defines normal communication behavior and flags deviations as anomalies, ensuring high precision in detecting unauthorized activities.

2.5 Host-Based and Communication-Level Security Mechanisms

Casparsen et al. [7] designed a host-based intrusion detection system that analyzes packet timing and payload inconsistencies to identify abnormal communication behavior, improving device-level security. Lee et al. [10] proposed a secure communication framework incorporating authentication mechanisms to prevent attacks such as replay and man-in-the-middle, thereby enhancing data integrity. Zuo et al. [11] introduced a secure gateway architecture integrating multiple layers of protection to ensure safe communication between vehicular network components, improving overall system reliability.

3. PROPOSED SYSTEM

The proposed system is developed to provide an intelligent and automated solution for anomaly detection in VANET communication. In this project, real-time vehicular network data is collected and processed to identify whether the communication behavior is normal or malicious. The system is designed to improve security, reliability, and accuracy compared to traditional manual and rule-based methods. It uses a combination of data preprocessing, feature analysis, classification, and anomaly score prediction to monitor vehicular communication effectively as demonstrate in Fig. 2. In addition, the project is implemented as a web-based application so that users can easily perform prediction, analysis, and result visualization.

The first step in the proposed system is collecting the VANET dataset containing important vehicular communication parameters. The dataset includes features such as timestamp, vehicle ID, packet size, packet rate, vehicle speed, message type, signal strength, latency, anomaly score, and target label. These parameters represent the communication behavior of vehicles in the network. The collected data acts as the foundation for training and testing the system. After data collection, the raw dataset is preprocessed to make it suitable for analysis and model implementation.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

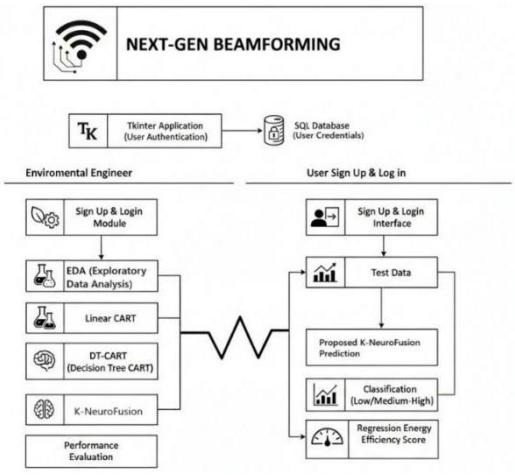

Fig. 2. Proposed system architecture.

In this stage, categorical values such as vehicle ID and message type are converted into numerical form. Unnecessary inconsistencies are removed, and the data is organized in a structured format for training and prediction. This step is important because proper preprocessing improves the efficiency and performance of the overall system. In this step, the system applies different algorithms for both classification and regression tasks. Classification is used to identify whether the network data belongs to the Normal or Attack category, while regression is used to predict the anomaly score. Multiple techniques are implemented and compared to analyze their performance. This step forms the core part of the project, where intelligent analysis is performed on vehicular communication data.

Once the models are implemented, the dataset is divided into training and testing sets. The training data is used to teach the system how to recognize patterns, while the testing data is used to evaluate its performance. During this process, the system learns the difference between normal and abnormal communication behavior. This step ensures that the project can provide reliable predictions on unseen data. After successful training, the proposed system is used for prediction. It accepts input data either as a single record or as a batch file and processes it through the trained system. Based on the input features, the system predicts the communication status as Normal or Attack and also provides the anomaly score. This step enables real-time and practical anomaly detection in vehicular network environments. In the final step, the complete project is deployed as a web-based application using Flask. The system provides interfaces for admin and vehicle users to access dataset details, perform predictions, and view analysis results. It also includes graphical visualizations such as EDA plots, confusion matrices, ROC curves, and comparison results. This step makes the project user-friendly, interactive, and suitable for practical usage.

K-Neuro Fusion CART Model

The K-Neuro Fusion CART Model is a hybrid approach proposed in this project that combines Deep Learning and Machine Learning techniques for improved anomaly detection. It integrates neural network-based feature extraction with a K-Nearest Neighbors (KNN) algorithm for final prediction. The term “NeuroFusion” represents the fusion of neural networks with traditional models, while CART indicates its use in both classification and regression tasks. This model is designed to handle complex and dynamic patterns in VANET data more effectively than individual models.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

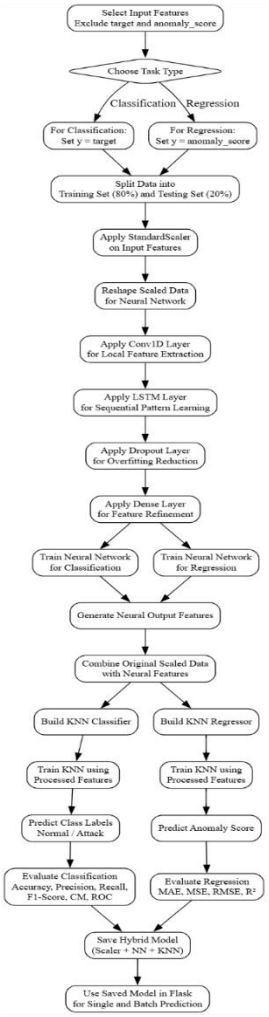

Fig. 3. proposed K-Neuro Fusion CART model internal working process.

The K-NeuroFusion CART model works in two main stages. In the first stage, deep learning techniques such as CNN and LSTM are used to extract meaningful patterns and features from the input data. CNN helps in capturing spatial relationships between features, while LSTM helps in understanding sequential or temporal dependencies in the data as demonstrate above Fig 3.

In the second stage, the extracted features are combined with the original input data and passed to a KNN model. KNN then performs classification or regression by comparing the input with its nearest neighbors in the dataset. This combination improves prediction accuracy by leveraging both deep feature learning and similarity-based decision-making.

The proposed K-NeuroFusion CART framework begins with loading the VANET dataset and performing preprocessing steps, including conversion of categorical attributes such as vehicle ID and message type into numerical representations. The processed data is then divided into input features and output variables, where all relevant attributes are used as inputs, while classification and regression targets are defined separately. The dataset is split into training and testing subsets in an 80:20 ratio to ensure proper model validation. Feature scaling is applied using StandardScaler to normalize the data, followed by reshaping the inputs into a sequence format suitable for deep learning layers. A hybrid deep learning pipeline is then employed, where a Conv1D layer extracts local feature patterns and an LSTM layer captures sequential dependencies

within vehicular communication data. To improve generalization and reduce overfitting, dropout is applied, and dense layers further refine the learned representations. The neural network is trained using appropriate loss functions—categorical cross-entropy for classification and mean squared error for regression—allowing the model to learn complex data patterns effectively.

After training, the neural network generates high-level feature representations that are used as input for the KNN-based learning stage. In this phase, KNeighborsClassifier and KNeighborsRegressor are employed to perform final predictions based on similarity in the learned feature space. During inference, new input data undergoes the same preprocessing and neural feature extraction before being passed to the KNN model for classification (Normal or Attack) and regression (anomaly score). The system performance is evaluated using multiple metrics, including accuracy, precision, recall, F1-score, confusion matrix, ROC curve for classification, and MAE, MSE, RMSE, and R^2 for regression, along with visualization techniques such as scatter plots. Finally, the complete hybrid model including the neural network, KNN model, scaler, and configuration is saved and integrated into a Flask-based web application, enabling real-time prediction for both individual inputs and batch data, thereby ensuring efficient and practical deployment of the proposed system

4. RESULT DESCRIPTION

The results of the proposed system demonstrate the successful implementation of a web-based VANET anomaly detection platform with secure user access and intelligent prediction capabilities. The system integrates data preprocessing, EDA, ML/DL model execution, and result visualization into a unified interface. The application ensures efficient interaction between users and backend models such as LR CART, DT CART, PA CART, and K-NeuroFusion CART.

Dataset Preview (First 10 Records)

	TIMESTAMP	VEHICLE_ID	PACKET_SIZE	PACKET_RATE	VEHICLE_SPEED	MSG_TYPE	SIGNAL_STRENGTH	LATENCY	ANOMALY_SCORE	TARGET
1		VEH_103	919	175	89.983192	DENM	-36.119738	79.135135	0.634030	0
2		VEH_271	519	33	109.564976	DENM	-40.494302	36.492255	0.843652	1
3		VEH_107	223	190	68.654756	BSM	-64.379558	12.716188	0.261127	0
4		VEH_72	521	19	21.694218	CAM	-68.275319	99.648600	0.097703	0
5		VEH_189	1354	195	32.255714	CAM	-79.623085	78.937780	0.615932	1
6		VEH_21	1186	74	23.837349	BSM	-47.550440	41.465363	0.434690	1
7		VEH_103	867	168	29.622843	CAM	-86.436653	82.511400	0.426441	0
8		VEH_122	582	175	36.769854	BSM	-50.784546	68.379783	0.526748	0
9		VEH_215	618	193	66.616054	DENM	-40.240296	79.207501	0.361383	1
10		VEH_88	254	157	70.558996	BSM	-80.149348	81.705431	0.626060	1

Fig. 4. Sample Dataset Preview

Fig. 4 presents a preview of the VANET dataset used in the project, displaying the initial rows of the data in tabular format. It includes key attributes such as timestamp, vehicle_id, packet_size, packet_rate, vehicle_speed, msg_type, signal_strength, latency, anomaly_score, and target. The preview provides a clear view of how each communication record is structured, combining both numerical and categorical features. It highlights the presence of real-time vehicular communication parameters along with the corresponding anomaly score and classification label.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

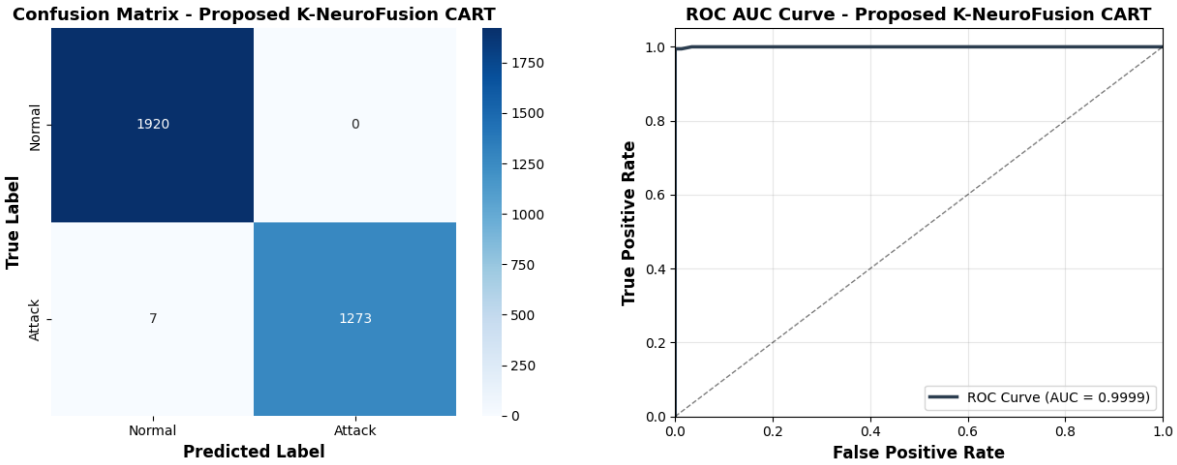

Fig. 5. Obtained Confusion Matrix and ROC Curve of K-NeuroFusion CART Model

Fig. 5. presents the performance of the proposed K-NeuroFusion CART model using confusion matrix and ROC curve. The confusion matrix shows a high number of correctly classified normal and attack instances, indicating strong prediction capability. The hybrid model combines CNN and LSTM for feature extraction with KNN for final prediction, enabling it to capture both spatial and sequential patterns in VANET data. The ROC curve demonstrates superior classification performance with better class separation compared to other models. This figure confirms the effectiveness of the hybrid approach in improving anomaly detection accuracy and reliability in the proposed system.

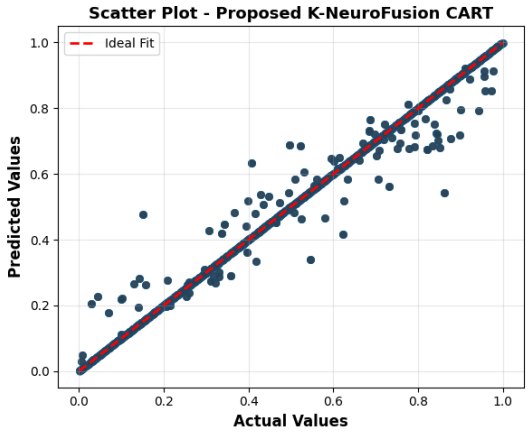

Fig 6. Illustration of Scatter plot using K-NeuroFusion CART Model

Fig. 6. presents the scatter plot that compare actual anomaly scores with predicted values for K-NeuroFusion CART, the scatter points are densely aligned along the ideal diagonal line, showing strong agreement between actual and predicted anomaly scores. This reflects the effectiveness of the hybrid approach, where CNN and LSTM extract meaningful features and KNN performs accurate prediction. The overall comparison highlights that the proposed K-NeuroFusion CART model achieves superior regression performance, providing more precise anomaly score estimation in VANET communication analysis.

Received: 07-05-2026 | Accepted: 15-06-2026 | Published: 22-06-2026 | www.ajaccm.com

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

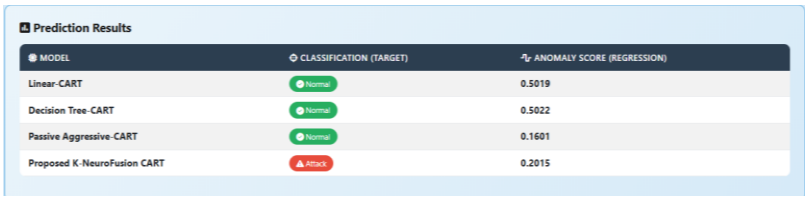

Fig. 7. Predictions on Sample Test Data using K-Neuro fusion model

Fig. 7 shows the prediction results generated by the system using sample test data. The interface displays outputs from all implemented models, including LR CART, DT CART, PA CART, and K-NeuroFusion CART. For each input record, the system provides classification results as *Normal* or *Attack* along with the corresponding anomaly score. The results demonstrate how different models analyze the same input features and produce predictions based on learned patterns. This output confirms the successful integration of preprocessing, model loading, and prediction modules within the Flask application, enabling real-time analysis of vehicular communication data.

Table 1. Classification Performance Comparison

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
LR CART	60.00	36.00	60.00	45.00
DT CART	60.00	36.00	60.00	45.00
PA CART	55.97	51.91	55.97	51.72
Proposed K-NeuroFusion CART	99.78	99.78	99.78	99.78

Table 1. classification performance comparison demonstrates the effectiveness of different CART-based models. The traditional models such as LR CART and DT CART show moderate accuracy but relatively low precision and F1-scores, indicating weaker prediction consistency. PA-CART improves precision and F1-score slightly but still lacks overall balance. In contrast, the Proposed K-NeuroFusion CART model significantly outperforms all other models across all metrics. With nearly perfect accuracy, precision, recall, and F1-score, it highlights the robustness and reliability of the proposed hybrid approach. This indicates that the model effectively captures complex patterns in the dataset.

Table 2. Regression Performance Comparison

Model	**MAE**	**MSE**	**RMSE**	**R^2-Score**
LR CART	0.245	0.0801	0.2831	-0.0024
DT CART	0.2452	0.0801	0.2831	-0.0025
PA CART	0.2953	0.1288	0.3589	-0.6115
Proposed K-NeuroFusion CART	0.0114	0.0016	0.0394	0.9806

Table 2. shows regression performance comparison highlights the predictive accuracy of various models using error metrics. LR CART and DT CART exhibit similar performance with moderate error values and near-zero R^2-scores, indicating poor model fitting. PA CART performs worse, with higher error rates and a negative R^2-score, showing weak predictive capability. In contrast,

Received: 07-05-2026 | Accepted: 15-06-2026 | Published: 22-06-2026 | www.ajaccm.com

the Proposed K-NeuroFusion CART model achieves exceptionally low MAE, MSE, and RMSE values, indicating minimal prediction error. Additionally, its R^2-score is close to 1, confirming a strong fit to the data. This demonstrates the superior regression capability of the proposed model compared to traditional approaches.

5. CONCLUSION

The proposed system successfully implements an intelligent VANET anomaly detection framework using a combination of ML and DL techniques. The project integrates data preprocessing, EDA, model training, evaluation, and real-time prediction within a Flask-based web application. Multiple models including LR CART, DT CART, PA CART, and the proposed K-NeuroFusion CART are applied for both classification and regression tasks. The system effectively analyzes vehicular communication data using features such as packet size, packet rate, vehicle speed, signal strength, and latency. The experimental results demonstrate that the K-NeuroFusion CART model achieves better performance compared to other models by combining CNN and LSTM feature extraction with KNN-based prediction. The system accurately classifies communication as Normal or Attack and also predicts anomaly scores, enabling severity analysis. The integration of visualization techniques such as confusion matrix, ROC curve, scatter plots, and EDA graphs provides deeper insights into data behavior and model performance. The developed application ensures secure user authentication, efficient model handling, and real-time prediction capability, making it suitable for intelligent transportation systems.

REFERENCES

[1] Seo, E.; Kim, J.; Lee, W.; Seok, J. Adversarial attack of ML-based intrusion detection system on in-vehicle system using GAN. In Proceedings of the 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France, 4–7 July 2023; pp. 700–703.

[2] Jeong, S.; Kim, H.K.; Han, M.L.; Kwak, B.I. AERO: Automotive Ethernet real-time observer for anomaly detection in in-vehicle networks. IEEE Trans. Ind. Inform. 2023, 20, 4651–4662.

[3] Peng, R.; Li, W.; Yang, T.; Huafeng, K. An internet of vehicles intrusion detection system based on a convolutional neural network. In Proceedings of the 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Xiamen, China, 16–18 December 2019; pp. 1595–1599.

[4] Shahriar, M.H.; Xiao, Y.; Moriano, P.; Lou, W.; Hou, Y.T. CANShield: Deep learning-based intrusion detection framework for controller area networks at the signal level. IEEE Internet Things J. 2023, 10, 22111–22127.

[5] Anand, M.; Kumar, S.P.; Selvi, M.; SVN, S.K.; Ram, G.D.; Kannan, A. Deep learning model based IDS for detecting cyber attacks in IoT based smart vehicle network. In Proceedings of the 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 23–25 March 2023; pp. 281–286.

[6] Meng, Y.; Li, J.; Liu, F.; Li, S.; Hu, H.; Zhu, H. GB-IDS: An intrusion detection system for CAN bus based on graph analysis. In Proceedings of the 2023 IEEE/CIC International Conference on Communications in China (ICCC), Dalian, China, 10–12 August 2023; pp. 1–6.

Received: 07-05-2026 | Accepted: 15-06-2026 | Published: 22-06-2026 | www.ajaccm.com

[7] Taslimasa, H.; Dadkhah, S.; Neto, E.C.P.; Xiong, P.; Iqbal, S.; Ray, S.; Ghorbani, A.A. ImageFed: Practical privacy preserving intrusion detection system for in-vehicle CAN bus protocol. In Proceedings of the 2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), High Performance and Smart Computing (HPSC) and Intelligent Data and Security (IDS), Xi'an, China, 6–8 May 2023; pp. 122–129.

[8] Amutha, S.; Ramathilagam, A. Improved IDS for Vehicular Ad-Hoc Network using Deep Learning Approaches. In Proceedings of the 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Tiruchengode, India, 20–22 April 2023; pp. 341–346.

[9] Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles. IEEE Internet Things J. 2021, 9, 616–632.

[10] Wu, W.; Li, R.; Xie, G.; An, J.; Bai, Y.; Zhou, J.; Li, K. A survey of intrusion detection for in-vehicle networks. IEEE Trans. Intell. Transp. Syst. 2020, 21, 919–933.

[11] Rajapaksha, S.; Kalutarage, H.; Al-Kadri, M.O.; Petrovski, A.; Madzudzo, G.; Cheah, M. AI-based intrusion detection systems for in-vehicle networks: A survey. ACM Comput. Surv. 2023, 55, 237.

Received: 07-05-2026 | Accepted: 15-06-2026 | Published: 22-06-2026 | www.ajaccm.com