JOURNAL OF ADVANCED ELECTRICAL AND ELECTRONIC ENGINEERING

Vol 2 Issue 1 (2026)

http://jaeee.org/

Behavioral Pattern Mining for Securing Blockchain-Integrated IoT Gateways

James Walker[1], Sophie Harris[2], Benjamin Clarke[3]*

School of Computing and Information Systems, The University of Melbourne, Melbourne, VIC 3010, Australia

***Corresponding author:** b.clarke@x.edu.au

Abstract

Vehicle-to-everything networks rely on continuous communication among vehicles, roadside units, and cloud-based traffic services. However, abnormal network traffic caused by spoofing, denial-of-service, and message injection attacks can affect both communication reliability and driving safety. This study proposes an explainable ensemble-based intrusion detection framework for V2X network traffic using flow-level behavioral features. The proposed method combines CatBoost, Random Forest, and Histogram Gradient Boosting through a weighted voting strategy to improve detection stability under mixed attack scenarios. SHAP analysis is introduced to explain the contribution of packet-level and session-level features to each detection decision. Experiments are conducted on the VeReMi Extension dataset and a V2X traffic subset generated from CICIDS2017, containing 1.76 million labeled communication records in total. After preprocessing, 38 traffic features are selected, including packet rate, flow duration, message frequency, source-destination byte ratio, and TCP flag distribution. The proposed model achieves 98.16% accuracy, 97.42% F1-score, and 98.89% AUC, outperforming standalone CatBoost and Random Forest models by 1.31% and 2.08% in F1-score, respectively. The false alarm rate is reduced from 3.84% to 2.17% compared with the best single-model baseline. SHAP results show that abnormal packet burst frequency, short flow duration, high destination port concentration, and asymmetric byte transfer are the most important indicators of malicious V2X traffic. The results demonstrate that explainable ensemble learning can improve both detection accuracy and decision transparency in vehicular communication security.

Keywords

V2X security; vehicular networks; network traffic anomaly detection; explainable AI; ensemble learning; SHAP; intrusion detection..

INTRODUCTION

Vehicle-to-everything (V2X) communication has become a key component of connected and automated transportation systems. It enables continuous data exchange among vehicles, roadside units, pedestrians, and cloud-based traffic services, thereby supporting cooperative perception, traffic coordination, hazard warning, and near-real-time safety message dissemination [1,2]. With the increasing deployment of intelligent vehicles and roadside communication infrastructure, V2X networks are expected to improve road safety, traffic efficiency, and driving automation. However, the open, distributed, and highly dynamic nature of V2X communication also exposes vehicular networks to multiple cyber threats. Spoofing, denial-of-service, message injection, replay, and false data attacks may disrupt normal message exchange, mislead vehicle decision-making, and create safety risks in real traffic scenarios. Therefore, intrusion detection in V2X networks is not only a conventional cybersecurity problem but also a safety-critical requirement for intelligent transportation systems. Machine learning and deep learning methods have been widely investigated for vehicular network anomaly detection. Existing studies have used message behavior, packet statistics, timing patterns, and flow-level features to identify abnormal V2X communication activities [3,4]. Recent explainable anomaly detection research has also shown that ensemble learning combined with SHAP-based interpretation can provide useful evidence for understanding traffic anomalies in embedded security environments [5]. This direction is important because V2X intrusion detection models are expected not only to produce high detection accuracy but also to provide interpretable evidence that can support security analysis, incident response, and safety validation. In practical vehicular networks, however, anomaly detection remains challenging due to high vehicle mobility, short connection duration, frequent message exchange, unstable communication links, and rapidly changing network topology [6]. These characteristics make V2X traffic more dynamic than traffic in fixed enterprise or industrial networks. Traditional rule-based intrusion detection methods can identify some known attacks through predefined signatures, protocol rules, or fixed thresholds [7,8]. However, their effectiveness often decreases when attack patterns change, when traffic conditions vary across scenarios, or when abnormal behaviors appear in mixed or low-frequency forms. Deep learning models can capture complex nonlinear traffic patterns, but they usually require large training datasets, high computational resources, careful hyperparameter tuning, and stable deployment conditions [9,10]. Their decision-making process is also difficult to explain, which limits their practical use in safety-critical vehicular systems. For V2X security applications, a detection model should achieve strong classification performance, maintain a low false alarm rate, and provide interpretable outputs that can be understood by traffic security operators and system engineers. Ensemble learning offers a practical solution for V2X intrusion detection because it can integrate the advantages of multiple classifiers and reduce the instability of a single model [11,12]. CatBoost is effective in modeling complex feature interactions and handling structured tabular data. Random Forest can reduce variance through multiple decision trees and improve robustness against noisy features. Histogram Gradient Boosting provides efficient tree-based learning and can strengthen class separation in large-scale flow-level datasets [13,14]. A weighted voting strategy can further combine these models according to their detection strengths, allowing the final classifier to balance accuracy, robustness, and false alarm control. Recent intrusion detection studies have reported that ensemble models can perform well on structured network traffic data and can reduce false alarms compared with individual classifiers [15,16]. These advantages are particularly relevant to mixed V2X attack scenarios, such as spoofing with abnormal message frequency, denial-of-service with sudden packet bursts, injection attacks with unusual source-destination behavior, and replay attacks with inconsistent timing patterns [17,18]. Despite these advances, several limitations

remain in current V2X intrusion detection research. Many studies still emphasize overall accuracy while providing insufficient analysis of F1-score, AUC, false alarm rate, and attack-wise detection performance [19,20]. This may lead to an incomplete evaluation, especially when the dataset contains imbalanced classes or when some attacks are more difficult to distinguish from normal traffic [21,22]. In addition, model interpretability is often limited. For safety-related vehicular systems, a black-box detection result is not enough, because security analysts need to understand which packet-level, flow-level, or session-level features contribute to an alarm. Dataset limitations also affect the reliability of existing results. Public datasets such as VeReMi Extension and CICIDS2017 provide useful benchmarks, but they may not fully represent real road, vehicle-to-roadside, and roadside-to-cloud communication conditions [23,24]. Some studies also rely on small subsets or limited attack types, which may weaken the generalizability of the reported results. To address these gaps, this study proposes an explainable ensemble-based intrusion detection framework for V2X network traffic using flow-level behavioral features. The framework integrates CatBoost, Random Forest, and Histogram Gradient Boosting through a weighted voting mechanism to improve detection accuracy, reduce false alarms, and enhance robustness across different attack patterns. SHAP analysis is introduced to explain the contribution of packet-level and session-level features, making the detection results more transparent and suitable for safety-critical vehicular communication environments. The proposed framework is evaluated on VeReMi Extension and a V2X traffic subset generated from CICIDS2017, covering 1.76 million labeled communication records. The purpose of this study is to develop a detection approach that is not only accurate but also interpretable and operationally meaningful for V2X security. By combining ensemble classification with explainable AI, this research provides clearer evidence for identifying abnormal vehicular communication behavior and supports the development of more reliable intrusion detection mechanisms for connected and automated transportation systems.

2.Materials and Methods

2.1 Sample and Study Object Description

This study used two V2X network traffic datasets: the VeReMi Extension dataset and a V2X traffic subset generated from CICIDS2017. The combined dataset contained 1.76 million labeled communication records. Each record represented one traffic flow among vehicles, roadside units, or cloud-based services. The datasets included normal traffic and several attack types, such as spoofing, denial-of-service, and message injection. To reflect practical V2X traffic conditions, the datasets were processed to retain flows with different sources, destinations, and protocol types. The study focused on abnormal V2X traffic detection based on flow-level behavior. The main aim was to test whether an ensemble model could detect malicious vehicular traffic and provide clear feature-level explanations.

2.2 Experimental Design and Control Setting

The experiment compared the proposed ensemble model with single-classifier baselines. The experimental group was the proposed weighted voting ensemble, which combined CatBoost, Random Forest, and Histogram Gradient Boosting. These classifiers were selected because they work well with structured flow features, reduce model variance, and improve class separation. The control group included standalone CatBoost, standalone Random Forest, and standalone Histogram Gradient Boosting models. All models used the same training data, testing data, and selected feature set. This setting ensured a fair comparison. The weighted voting method combined the predicted probabilities of the base models to produce the final result. This design improved detection stability under mixed V2X attack scenarios.

2.3 Measurement Methods and Quality Control

Traffic records were checked before model training. Missing values, duplicate records, abnormal feature ranges, and inconsistent labels were identified. Invalid records were removed before feature extraction. Feature names were standardized to avoid preprocessing errors. Text labels were converted into numerical labels. Normal traffic was coded as 0, and attack traffic was coded according to the attack type. Feature distributions were checked to ensure data quality. Only flows that passed the initial filtering were used for model training and testing. Model performance was measured by accuracy, F1-score, macro-F1, AUC, and false positive rate. Macro-F1 was used to assess class-level balance. False positive rate was used to measure the proportion of normal flows incorrectly marked as attacks. All evaluations were performed on separate test data that were not used during model training.

2.4 Data Processing and Model Formulas

The raw traffic records were processed before model training. Invalid flows were removed first. Labels were then encoded into numerical form. After cleaning and feature selection, 38 features were retained, including packet rate, flow duration, message frequency, source-destination byte ratio, and TCP flag distribution. The proposed model used weighted voting to combine CatBoost, Random Forest, and Histogram Gradient Boosting. For a traffic flow x_i, the final probability of class ccc was calculated as follows:

$$P(c|x_i)=\frac{\sum_{k=1}^{K} w_k P_k(c|x_i)}{\sum_{k=1}^{K} w_k}$$

where K is the number of base classifiers, w_k is the weight of the k-th classifier, and $P_k(c|x_i)$ is the probability given by the k-th classifier. The final label was assigned to the class with the highest weighted probability. Macro-F1 was calculated as follows:

$$\text{Macro-F1}=\frac{1}{C}\sum_{c=1}^{C}\frac{2\times\text{Precision}_c\times\text{Recall}_c}{\text{Precision}_c+\text{Recall}_c}$$

where C is the number of classes, Precision_c is the precision of class c, and Recall_c is the recall of class c. This metric was used to avoid overly high results caused by dominant normal traffic or frequent attack types.

2.5 Explanation and Feature Contribution Analysis

SHAP analysis was used to explain the trained ensemble model. Local SHAP values showed the effect of each feature on a single traffic-flow prediction. Global SHAP analysis ranked the overall importance of the selected features across the dataset. Packet burst frequency, flow duration, destination port concentration, and byte asymmetry were examined as key features because they are closely related to abnormal V2X traffic behavior. This step helped determine whether the model decisions were based on meaningful flow-level features. The explanation results also provided clearer support for vehicular network security analysis. Model performance, feature importance, and explanation consistency were assessed across all test flows to check stability and practical value.

3.Results and Discussion

3.1 Detection Performance Under Mixed V2X Attacks

The proposed ensemble model demonstrated strong detection performance on the V2X traffic datasets. It achieved 98.16% accuracy, 97.42% F1-score, and 98.89% AUC. These results indicate that the model reliably distinguished normal communication from abnormal traffic across different attack types. Compared with standalone CatBoost and Random Forest models, F1-score improved by 1.31% and 2.08%, respectively. The false positive rate decreased from 3.84% to 2.17% relative to the best single-model baseline. Lower false alarms are important in V2X systems, as frequent

incorrect alerts can interfere with traffic monitoring and safety operations. The improvement is attributed to the weighted voting strategy, where CatBoost captured complex feature relations, Random Forest reduced variance, and Histogram Gradient Boosting improved class separation. Recent MDPI studies on VANET-based vehicle security also support the effectiveness of hybrid ensemble intrusion detection in improving both accuracy and false positive control [25,26]. The model comparison is shown in Fig. 1.

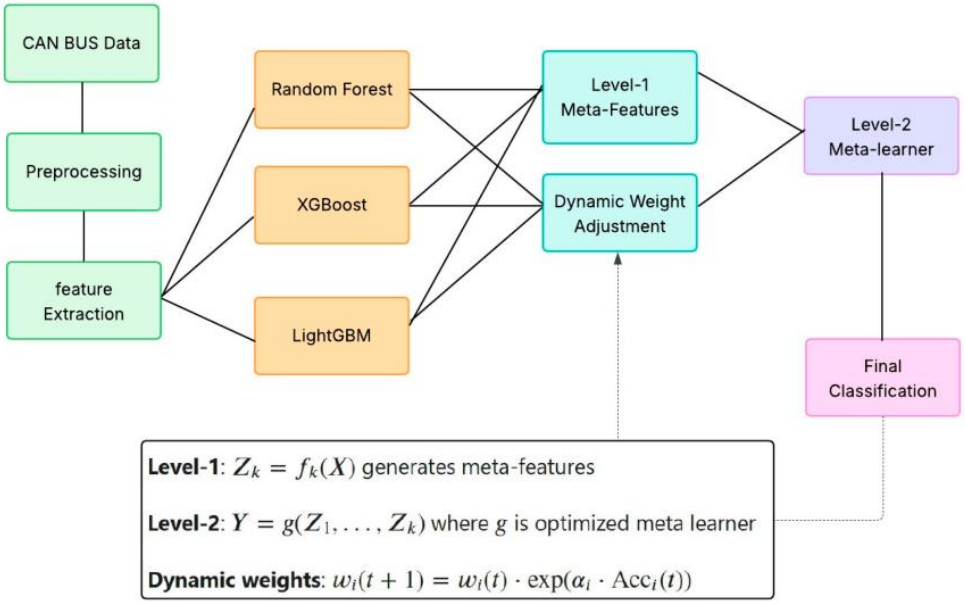


Fig.1. Comparison of detection results between the proposed ensemble model and baseline models for V2X traffic.

3.2 Comparison with Existing Vehicular Network Security Methods

Compared with existing vehicular intrusion detection methods, the proposed framework offered a better balance between detection accuracy, false alarm rate, and interpretability. Many prior studies focused on message-level misbehavior detection, such as false position or CAN bus anomalies. These methods are effective for specific attack types but may miss broader traffic-level anomalies. V2X attacks can influence packet rate, flow duration, byte transfer, message frequency, and TCP flag usage. The proposed model used 38 flow-level features to capture these variations, allowing detection of mixed attack patterns in a unified framework. This approach is consistent with recent findings showing that ensemble learning improves detection stability when traffic patterns vary across sources and attack types [27,28]. Compared with deep learning-based approaches, the model requires fewer training steps and provides clearer feature-level explanations, which is critical for practical V2X security systems.

3.3 SHAP-Based Feature Interpretation

SHAP analysis identified abnormal packet burst frequency, short flow duration, high destination port concentration, and asymmetric byte transfer as the most important indicators of malicious V2X traffic. Packet burst frequency reflects rapid injection or flooding, short flow duration indicates repeated probing or short malicious sessions, high destination port concentration suggests targeting of specific services, and asymmetric byte transfer shows one-sided communication. These findings indicate that the model decisions were based on meaningful traffic behavior rather than statistical artifacts. Local and global SHAP analyses allowed feature importance comparison across flows and ensured that explanation did not require access to raw traffic. Recent studies have confirmed that SHAP can provide effective feature-level interpretation for vehicular intrusion detection [29,30]. The global feature ranking is shown in Fig. 2.

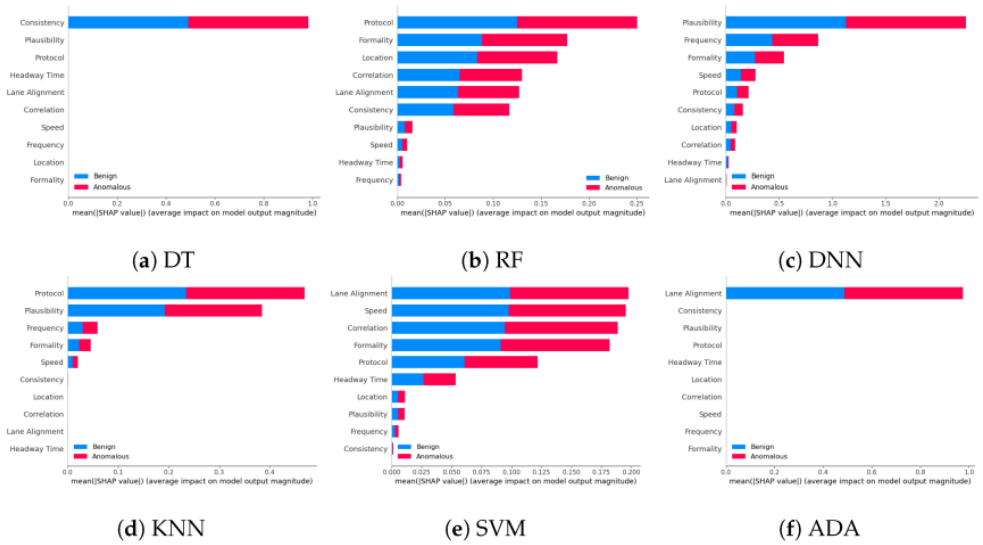


Fig.2.SHAP ranking of important flow-level features for explaining V2X attack detection.

3.4 Practical Implications and Limitations

The results demonstrate that the proposed framework is practical for V2X network security. It combines high detection accuracy, reduced false alarms, and interpretable feature-level explanations. This is critical because intrusion alerts in V2X systems may influence road safety warnings, roadside monitoring, and traffic management decisions. SHAP analysis provides analysts with clear insight into which traffic features contributed to each alarm. However, the study has limitations. Experiments were based on public datasets and a simulated V2X subset, which may not fully reflect real traffic conditions, including vehicle density, wireless channel variability, and roadside infrastructure [31]. The model focuses on flow-level behavior and does not incorporate message semantics or vehicle mobility. Evaluations were conducted offline. Future work should validate the framework on live V2X traffic, include more attack types, and test model stability under changing traffic and network conditions.

4.Conclusion

This study proposed an explainable ensemble model for V2X network intrusion detection using flow-level behavior features. The model combined CatBoost, Random Forest, and Histogram Gradient Boosting through weighted voting. This design improved detection stability under mixed attack conditions. The model achieved 98.16% accuracy, 97.42% F1-score, and 98.89% AUC. It also reduced the false alarm rate to 2.17%, showing better performance than single classifiers. SHAP analysis showed that packet burst frequency, short flow duration, high destination port concentration, and asymmetric byte transfer were the main indicators of malicious traffic. These results provide clear evidence for security monitoring. The main value of this study is that it combines accurate detection, low false alarms, and clear feature-level explanation in one framework. The proposed method can be used in connected vehicles, roadside units, and traffic management systems where both detection performance and interpretability are important. However, this study was limited to offline tests on public datasets. These datasets may not fully represent real V2X traffic conditions. Future work should test the model on real-time vehicular networks, include more attack types, and examine its stability under changing traffic and communication conditions.

References

Wang, Y., Chen, J., Arias, R., Wang, Y., & Yin, X. (2026). Development and Validation of a Patient-Friendly Digital Assessment Platform for Precision Screening of Oral Anti-Obesity Medications (AOMs).

Kandali, K., Nouh, S., Bennis, L., & Bennis, H. (2026). A Comprehensive Survey on VANET–IoT Integration Toward the Internet of Vehicles: Architectures, Communications, and System Challenges. Future Transportation, 6(1), 32.

Zhu, W., Yang, J., & Yao, Y. (2025). How Cross-Departmental Collaboration Structures Mitigate Cross-Border Compliance Risks: Network Causal Inference Based on ManpowerGroup's Staffing Projects.

Noor, K., Imoize, A. L., Li, C. T., & Weng, C. Y. (2025). A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond. Mathematics, 13(7), 1088.

Shao, W. (2026, March). Interpretable Ensemble Learning for Network Traffic Anomaly Detection: A SHAP-based Explainable AI Framework for Embedded Systems Security. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-4). IEEE.

Ahmad, T., Hadi, M. U., Vassiliou, V., Dimitriou, L., Anwar, A., & Tran, T. A. (2025). Real-time anomaly detection in smart vehicle-to-UAV networks for disaster management. Transactions on Emerging Telecommunications Technologies, 36(5), e70162.

Su, D., & Zhang, H. Developing a Data-Driven Computational Framework for Scalable Special Education Practices for Autism and Intellectual Disabilities in the US Public School System.

Sridevi, K., Masood, W., Tanveer, S., Mirza, O. M., Sivakumar, N. R., & Selvarajan, S. (2026). ZuraNet: a hybrid rule-based intrusion detection system with deep learning for securing SCADA-driven cyber-physical systems. Scientific Reports.

Xu, S., Ma, Q., Liu, H., & Yue, L. (2026). Continuous Reorganization and Performance Preservation of Agent Memory Structure Under Distributed Change Environments.

Elmorsy, S. M. A., Osman, S. M., & Gamel, S. A. (2025). Enhanced spectrum sensing for 5G and LTE signals using advanced deep learning models and hyperparameter tuning. Scientific Reports, 15(1), 24825.

Ma, Y. (2026). Industrial Financial Risk Prediction Model Based on Graph Neural Network and Knowledge Graph Inference. Journal of Circuits, Systems and Computers, 35(16), 2650103.

Alalwany, E., Mahgoub, I., Alsharif, B., & Alfahaid, A. (2025). An Intelligent Ensemble-Based Detection of In-Vehicle Network Intrusion. Applied Sciences, 15(12), 6869.

Gao, G., Gao, R., Lu, C., Gao, R., & Kuang, Y. (2026, March). Security Governance Methods and Quantitative Evaluation for Enterprise SMS and Verification Code Systems. In 2026 International Conference on Generative Artificial Intelligence and Information Security (GAIIS) (pp. 455-458). IEEE.

Drăguşin, S. A., Boştinaru, R. N., Bizon, N., & Iana, G. V. (2026). AI-Based Embedded Framework for Cyber-Attack Detection Through Signal Processing and Anomaly Analysis. Applied Sciences, 16(3), 1416.

Chen, F., Liang, H., Yue, L., Xu, P., & Li, S. (2025). Low-Power Acceleration Architecture Design of Domestic Smart Chips for AI Loads.

Sheelavant, K. K., Yamini, C., Bhushan, P., & Kumar, C. (2025). Ensemble Learning-Based Intrusion Detection and Classification for Securing IoT Networks: An Optimized Strategy

for Threat Detection and Prevention. Journal of Intelligent Systems and Internet of Things, 101-118.
Liang, R., Fan, F., Liang, Y., & Li, S. (2025). Constructing an Adaptive Optimization Model for Ribbon Recommendation and Interface for User Habits.
Zou, Y., Qi, N., Deng, Y., Xue, Z., Gong, M., & Zhang, W. (2025, July). Autonomous resource management in microservice systems via reinforcement learning. In 2025 8th International Conference on Computer Information Science and Application Technology (CISAT) (pp. 991-995). IEEE.
Sankar, S. R., & Jothi, B. (2026). EGOA-DL-IDS: explainable intrusion detection in SDN-based industrial cyber physical system with optimized deep learning techniques. Cluster Computing, 29(4), 242.
Yin, J., Huang, Y., & Rao, H. (2026). A Study on the Dynamic Evolution of Learning Behavior and Outcome Prediction in Digital Educational Environments. Available at SSRN 6607139.
Edo, G., Ahmad, T., & Putra, M. A. R. (2025). Hybrid GAN-LSTM for Enhancing DDoS Detection on Imbalance Dataset. International Journal of Safety & Security Engineering, 15(1).
Deng, X., & Yang, J. (2026). Design of a Quantitative Futures Trading Model Incorporating Multimodal Feature Fusion and Tail Risk Control. Available at SSRN 6702398.
Baharlouei, H., Makanju, A., & Zincir-Heywood, N. (2026). Comprehensive host-based malicious behaviour detection in vanets. Journal of Network and Systems Management, 34(4), 100.
Zhang, Z. (2026). A Study on the Identification of Manipulative Design in Subscription and Payment Interfaces of Digital Consumer Platforms and Its Behavioral Effects. Available at SSRN 6734760.
Aloqaily, A., Abdallah, E. E., Baarah, A., Alnabhan, M., Alshdaifat, E. A., & Milhem, H. (2025). Optimized Hybrid Ensemble Intrusion Detection for VANET-Based Autonomous Vehicle Security. Network, 5(4), 43.
Zhang, Z., Tong, Y., & Gao, Y. (2026). Retrieval-Augmented Generation with Low-Latency Deployment for Vertical Domains Question Answering: A Case Study on Economic Resource Platforms.
Ibrahim, N., Rajalakshmi, N. R., Sivakumar, V., & Sharmila, L. (2025). An optimized hybrid ensemble machine learning model combining multiple classifiers for detecting advanced persistent threats in networks. Journal of Big Data, 12(1), 212.
Qi, C., & Qiao, X. (2026). Efficient Data Sampling and Feature Selection Algorithms for Scalable Machine Learning Pipelines.
Taheri, R., Gegov, A., Arabikhan, F., Ichtev, A., & Georgieva, P. (2025, November). Explainable Artificial Intelligence for Intrusion Detection in Connected Vehicles. In Principle and Practice of Data and Knowledge Acquisition Workshop (pp. 162-176). Singapore: Springer Nature Singapore.
Huang, R. (2026). ConfSched: Confidence-Threshold Routing for Efficient Edge-Cloud Activity Recognition. World Journal of Engineering and Technology, 14(2), 471-486.
Bari, B. S., Puthal, D., & Yelamarthi, K. (2025). Datasets in vehicular communication systems: A review of current trends and future prospects. SN Computer Science, 6(3), 210.