scientific reports

OPEN

Sustainable cyber-physical VANETs with AI-driven anomaly detection and energy-efficient multi-criteria routing using machine learning algorithms

Wai Kit Wong[1]✉, S. Baskar[2], K. M. Abubeker[3] & Poh Kiat Ng[1]

Cyber-physical systems have improved modern transportation by allowing vehicles and road systems to communicate through Vehicular Ad Hoc Networks (VANETs). Existing anomaly detection approaches often struggle with high false-positive rates, poor adaptability, and significant computational demands, compromising their real-time efficacy and scalability. To address these problems, this research presents an Anomaly Detection using Machine Learning Algorithms (AD-MLA) framework that employs a Random Forest model to accurately detect abnormal activities. The framework encompasses feature selection, data clustering, and an energy-efficient routing strategy that incorporates node energy, signal strength, hop count, and link stability. Evaluations demonstrate that AD-MLA reduces false alarms, improves detection accuracy, and operates with lower energy and computational requirements. It offers a smart, rapid, and efficient security system for real-time VANET environments, rendering it appropriate for transportation systems characterised by high reliability and safety. By integrating a Random-Forest-based anomaly detector with intelligent feature selection and an energy-efficient routing method that accounts for residual energy, signal strength, and link stability, the suggested framework systematically addresses these challenges. This approach delivers 95.33% accuracy, 96.09% recall, 94.25% computational efficiency, and 91.45% resource-use efficiency. This effectively addresses the scalability, latency, and energy challenges that previous systems have faced in incorporating blockchain technology and deep learning architectures.

Keywords Cyber-physical systems, VANETs, Anomaly detection, Machine learning, AI-driven security, Intelligent transportation systems, Energy efficiency, Sustainable computing

Sustainable cyber-physical systems (CPS) have transformed modern industries by delivering smart, connected solutions across transportation, healthcare, and industrial automation. Sustainable CPS is designed to incorporate the functionality of computers, sensors, and electronic systems to efficiently monitor and regulate multiple processes in real time[1]. In Vehicular Ad Hoc Networks (VANETs), CPS provides intelligent interfaces for transportation systems to enable real-time spatial communication and internet connectivity[2]. Through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) connectivity, VANETs support autonomous driving, improve traffic management, and enhance road safety[3]. However, as VANETs increasingly depend on communication and connectivity technologies, they also support a novel and disruptive range of cybersecurity vulnerabilities, including data poisoning, Sybil, and Distributed Denial of Service (DDoS) attacks[4]. An additional security aspect is monitoring for instabilities and hostile actions. This type of real-time monitoring is part of the anomaly detection systems that VANETs deploy for operational security[5]. The standard systems for anomaly detection, especially the rule-based and signature systems, are less able to cope with the fast, dynamic, and unpredictable cyber threat landscape that characterises VANETs[6]. These systems are also poorly designed for detecting advanced and novel cyberattacks, poorly scalable, and generate high false-positive rates.

[1]Faculty of Engineering and Technology (FET), Multimedia University, Jalan Ayer Keroh Lama, Bukit Beruang, 75450 Melaka, Malaysia. [2]Department of ECE, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India. [3]Department of ECE, Amal Jyothi College of Engineering (Autonomous), Kanjirappally, Kerala, India. ✉email: wkwong@mmu.edu.my

Communication within VANETs must be reliable, efficient, and sustainable to support the future of intelligent transportation systems. Research on intelligent transportation systems based on machine learning and anomaly detection highlights scalability, energy efficiency, and false-positive rates associated with preemptive anomaly control[7,8]. This work proposes using energy-aware multi-criteria routing in conjunction with machine-learning-integrated anomaly detection to mitigate these challenges. This will enhance real-time threat response, support energy-efficient computing, and promote sustainable cyber-physical VANET computing. With Artificial Intelligence (AI), VANET systems will learn and adapt anomaly detection systems to new threats, improving detection systems' precision and operational efficiency[9]. Nonetheless, many recent AI solutions are ill-suited for real-time implementation in vehicle networks due to excessive computational requirements[10]. Thus, protecting VANETs with appropriate network performance will require scalable, low-latency anomaly-detection systems.

The framework improves detection efficiency while minimising computational burden by combining feature selection, clustering, and classification. Through continuous network traffic supervision, AD-MLA automatically lowers active security threats by resolving real-time deviations. In terms of computing efficiency, false-positive reduction, and detection precision, the experimental results demonstrate that AD-MLA outperforms all other active anomaly detection systems. Unlike other systems, AD-MLA is scalable to cyber threat ecosystems while addressing the high false-positive problem that dominates anomaly detection in VANETs. The primary research contributions are outlined below.

- Developed a sustainable AD-MLA framework, integral in advancing VANET security and facilitating intelligent, clean transportation systems. AD-MLA improves detection accuracy, enables real-time adaptation, and enhances the efficiency and sustainability of VANET operations.
- Integrated Random Forest with feature selection, grouping, and classification algorithms can enhance the utilisation of computational resources in vehicular networks.
- Optimisation of routing decisions based on energy consumption, link stability, and mobility is necessary for safety-critical applications in dynamic urban VANET environments.

The manuscript is structured as follows: Section "Related works" presents the related work on anomaly detection in VANETs. In Section "Materials and methods", the proposed AD-MLA methodology is explained. In section "Results and discussions", the efficiency of AD-MLA is discussed and analysed, followed by a discussion of the deployment platforms. Finally, in section "Model development and deployment", the research concludes with a discussion and a section on future work.

Related works

The contribution of AI-driven methods in improving security across many transportation and network systems is investigated in this collection of publications. Aiming to improve safety, privacy, and system efficiency in modern intelligent transportation networks, these studies examine anomaly detection, predictive maintenance, and cyberattack prevention using advanced methods, including LSTM, CNN-GAN, and machine learning from autonomous vehicles and IoT to VANETs and EnFVs. It presents an ensemble of Long Short-Term Memory (LSTM) networks and a deep learning-based Intrusion Detection System (IDS) for ICTS[11]. This approach tracks V2V, In-Vehicle Networks (IVN), and V2I connections to identify harmful behaviour. The system's effectiveness in detecting cyber threats within autonomous vehicle networks is evaluated using the UNSW-NB15 and automobile-hacking datasets. Their method maximises data flow, strengthens security, and increases smart network efficiency through intelligent transportation. Researchers examine Artificial Intelligence (AI)-based anomaly detection techniques in the Controller Area Network (CAN) systems of advanced vehicles[12]. With a focus on methods such as Machine Learning (ML), Deep Learning (DL), and Federated Learning (FL) for anomaly detection, the authors examine how AI could improve IoT security[13]. Practical solutions for identifying and managing security risks in IoT devices are developed using artificial intelligence techniques, which also improve attack detection and predictive analysis, thereby reducing human involvement. Recent work in[14] investigates how AI could help VANETs; to avoid dangerous circumstances, AI methods are explored for tasks such as data collection, routing, driver awareness, and mobility prediction.

Recent reviews of AI-based techniques for vehicle network security problems. It starts by providing a general overview of vehicle networks and their weaknesses, then evaluates the principles of artificial intelligence and how they affect vehicle security[15]. The proposed framework focuses on assessing the integration of AI technologies to address security challenges in these networks. It suggests a novel taxonomy for identifying and benchmarking several AI-driven approaches. Saud et al.[16] specifically analyse the impact of AI, the Internet of Things (IoT), and 5G/6G technologies in VANETs to enhance traffic safety, convenience, and economic efficiency. Besides analysing the improvements in connectivity that the IoT and 5G/6G technologies bring, the study also focuses on AI for routing, driver-automation awareness, and mobility prediction. For network anomaly detection, Rao et al.[17] propose a hybrid architecture that integrates Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs). In the context of real-time IIoT environments, Himanshu et al.[18] propose an adaptive CNN-GRU deep learning model that achieved 99.75% accuracy, 99.75% precision, and 99.74% recall on the N-BaIoT dataset, for reliable IIoT security. Alqahtani et al.[19] explore the application of machine learning (ML) to enhance the security of electric and flying vehicles (EnFVs). To increase safety and save downtime, it emphasises predictive maintenance, cyberattack detection, and intelligent decision-making. The paper, which covers Explainable AI, real-time algorithms for resource-constrained settings, and privacy-preserving strategies, offers an overview of ML applications, identifies key problems, and outlines future research directions. Akinola et al.[20] introduce the Urban Adaptive Location-based Routing Protocol (UALRP), an adaptive machine-learning-based location-routing protocol for urban WSNs that utilises real-time data analytics to enhance routing

SI No	Methods	Advantages	Limitations
1	Ensemble LSTM-based IDS for ICTS[12]	Effective in detecting cyber threats in V2V, IVN, and V2I networks Maximises data flow and enhances security Increases smart network efficiency	Requires large datasets for training Might not handle highly dynamic or unpredictable data well
2	AI-Based Anomaly Detection in CAN Systems[13]	Improves vehicle data security using AI Identifies complex anomalies in CAN systems Focus on privacy	Limited by the scalability of the techniques Performance can vary depending on data quality and availability
4	AI-Based VANET Solutions[14]	Enhances traffic safety and efficiency Optimises routing and driver awareness Improves passenger comfort and road experience	Potential difficulties in implementing AI in real-time traffic conditions High computational resources may be required for some AI techniques
5	AI-Based Security Solutions for Vehicular Networks[15]	Identifies and addresses security issues in vehicular networks Proposes a new taxonomy for comparing AI-based solutions	May face challenges in handling highly dynamic and large-scale vehicular network data Complexity of integration with existing infrastructure
6	AI-IoT-5G/6G for VANETs[16]	Combines AI, IoT, and 5G/6G to enhance connectivity and security Improves routing, mobility prediction, and driver awareness	5G/6G infrastructure is still developing Potential privacy and security concerns when handling sensitive data across various systems
7	Hybrid CNN-GAN Model for Anomaly Detection[17]	High detection rates and minimal false positives Improves network security by generating normal traffic patterns to detect anomalies	Require a large labeled dataset Complex training process and resource-intensive
8	ML-Based Security for EnFVs[20]	Enhances safety with predictive maintenance and cyberattack detection Aims for privacy-preserving and real-time solutions	Real-world implementation challenges Ethical considerations and the complexity of applying ML techniques in resource-constrained environments
9	Transfer learning BILSTM[21]	High detection accuracy for IoT botnet attacks Transfer learning improves generalisation	Potential dataset bias Computational overhead and resource constraints

Table 1. The comparison of existing methods.

Aspect	Blockchain-based IDS	Hybrid deep-learning IDS (LSTM/CNN–GAN)	Proposed AD-MLA Framework (RF + Energy-Aware Routing)
Architecture Focus	Distributed trust ledger; consensus among nodes for transaction validation	Stacked neural layers (LSTM for sequential data, CNN–GAN for anomaly synthesis)	Two-stage co-design: (i) Random-Forest anomaly detector, (ii) multi-criteria routing based on energy, RSSI, hop count, and link stability
Key Components	Smart contracts, miners, and blockchain consensus mechanisms	Deep neural network encoder–decoder or generator–discriminator pipelines	Feature selection + RF classification + routing decision algorithm (Algorithm 2)
Dataset Need	Ledger and transaction records, often synthetic for VANET testing	Large labelled datasets (UNSW-NB15, CAN-Bus, car-hacking)	Lightweight feature vectors from VANET communication logs; fewer samples required
Detection Speed	Slower due to consensus and block propagation delays	Moderate, depending on batch inference or retraining cycles	Real-time classification via ensemble RF inference
Adaptability to Network Dynamics	Low; ledger structure is rigid	Moderate; models must be retrained for new patterns	High feature selection and RF thresholds allow dynamic updates without retraining
False-Positive Rate (FPR)	Typically > 20% under rapid mobility	10–15% reported, but unstable due to imbalanced data	15.22%, balanced against a higher recall to prioritise threat coverage

Table 2. Comparative analysis of the proposed AD-MLA with blockchain-based and hybrid deep-learning IDS frameworks.

performance. By analysing traffic and environmental data, it improves routing accuracy, network performance, and scalability, adjusting to dynamic urban environments.

As shown in Table 1, existing AI- and ML-based intrusion detection systems achieve higher accuracy and threat coverage than traditional rule-based methods but still face significant limitations, including high false-positive rates, limited scalability, and high computational cost. Artificial intelligence techniques include CNN-GAN, machine learning, and ensemble LSTM-based IDS, which provide effective solutions for anomaly recognition and enhanced security in car networks, IoT, and smart transportation systems. These approaches address significant concerns, including predictive maintenance, privacy, and cyberattacks.

The results in Table 2 show that the AD-MLA framework outperforms standard blockchain and hybrid deep learning IDS models. While blockchain models secure data transactions, they do so at the expense of high latency and high energy costs. While deep learning models like LSTM and CNN-GAN achieve high accuracy, they require large training datasets and heavy computational costs. In contrast, the proposed Random-Forest-driven AD-MLA merges feature selection and energy-aware multi-criteria routing, dynamically adjusting accuracy, efficiency, and detection sustainability. This framework achieves 95.33% accuracy, 96.09% recall, 15.22% FPR, 94.25% computational efficiency, 91.45% resource-usage efficiency, demonstrating the real-time edge applicability of the proposed framework to VANET and CPS. AD-MLA offers the best balance of performance and energy-efficient operation, allowing us to grade it as a sustained, practical IDS architecture for intelligent transport system CPS. Overall, AD-MLA offers the best balance of performance and energy-efficient operation. All of these contribute to the practical application of next-generation intelligent transport systems as a sustained, practical IDS architecture.

The results of the experiments validate that the proposed AD-MLA approach meets the research goal of designing a lightweight, adaptive, and energy-efficient intrusion detection system for VANET and CPS environments. Combining Random-Forest-based anomaly detection with a multi-criteria routing strategy allows the framework to reduce latency and power usage while preserving detection accuracy. With 95.33% accuracy, 96.09% recall, and 94.25% computational efficiency, these results represent a meaningful advancement over existing blockchain-based and hybrid deep-learning IDSs. This demonstrates that AD-MLA can efficiently operate on edge or vehicular nodes without the GPU-heavy computation or consensus communication typically required. AD-MLA's sustainable design contributes to green, scalable vehicular communication ecosystems that support adaptive, innovative, eco-friendly transport systems.

Materials and methods

Cyber-physical systems improve intelligent decision-making and automation by aggregating computer, networking, and physical components. By spotting abnormalities in EV data, suspicious activities, and unusual traffic patterns, machine learning-enabled anomaly detection in VANETs enhances security, efficiency, and safety.

Method 1: Development of the AD-MLA framework for anomaly detection

It proposed an AD-MLA architecture that leverages RF to reliably and efficiently categorise abnormalities in VANETs. Figure 1 illustrates the integration between computational and physical components within Cyber-Physical Systems, highlighting their dynamic interactions. The physical layer comprises actual components such as autonomous automobiles that use sensors and actuators to track and respond to their surroundings, as well as power plants. Above this is the network layer, which links physical and computational devices via wireless (LTE, 5G) and wired (DNP3, IEC61850) protocols for real-time data exchange and control feedback loops. The application layer handles traffic monitoring, electricity demand projections, and geolocation services to provide intelligent decision-making. Control systems made available by a central computer system that analyses incoming data help achieve optimal performance in energy efficiency, routing mechanisms, and sustainability. Due to CPS technology's ability to integrate various physical systems over a robust network, automation is accelerated, smart infrastructure is improved, and intelligent services can be expanded across many sectors.

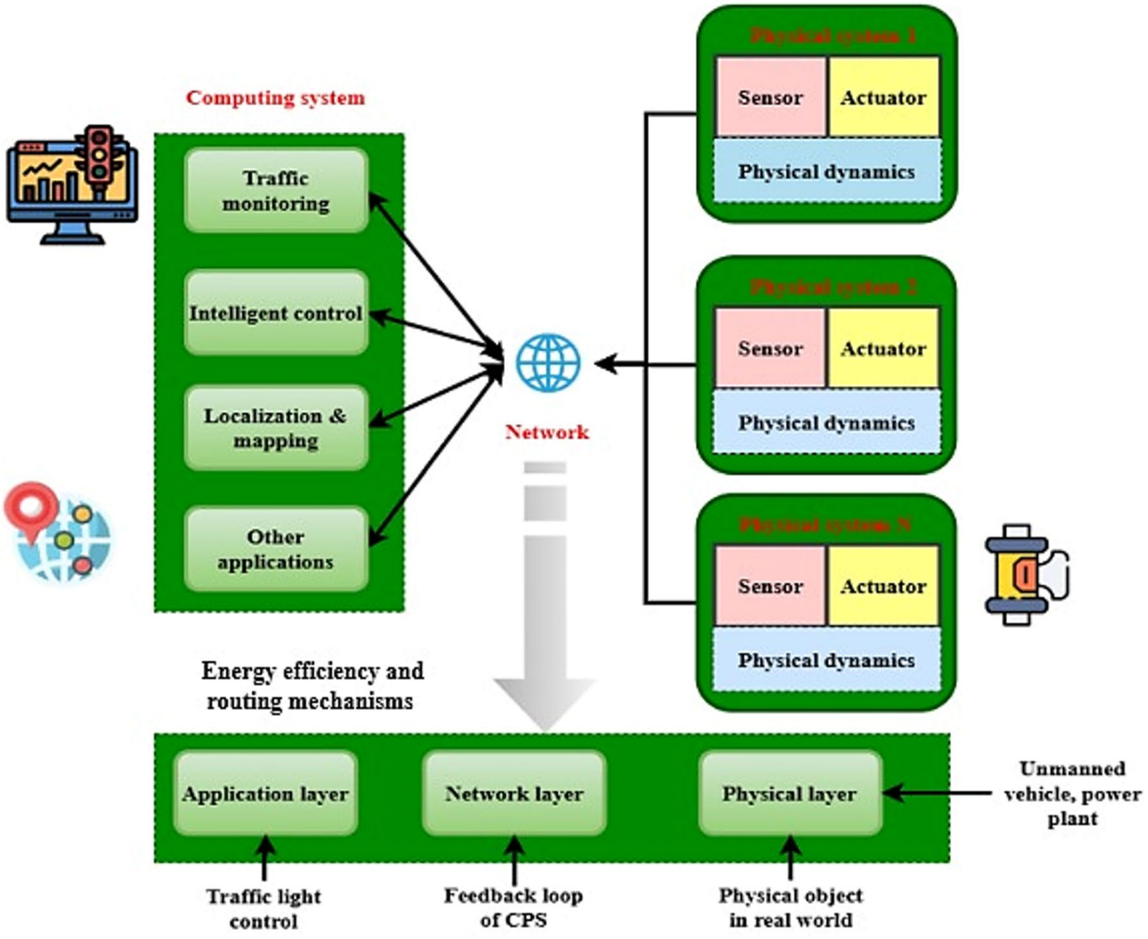


Fig. 1. Cyber-physical systems: the interplay of computation and physical dynamics.

To further improve performance, energy-saving measures are adopted for path optimisation based on latency, power usage, and network utilisation. Such strategies minimise costs and environmental degradation by reducing power consumption, minimising real-time data transmission, and controlling energy waste.

$$md_e \ll i - sn^{''} \gg :\rightarrow Vs\left[kia - esa^{''}\right] + Va\left[ds - tw^{''}\right] \tag{1}$$

Integrating intelligent sensing (md_e), vehicle status analysis ($i - sn^{''} \gg :\rightarrow$), and adaptive decision methods ($Vs\left[kia - esa^{''}\right]$) in dynamic VANET settings is represented by Eq. (1), which also shows entropy ($Va[ds - tw'']$) and these three variables. Modifying classification parameters dynamically based on evolving VANET conditions ensures low-latency, high-accuracy detection.

$$f_fs\left[lo - an^{''}\right] :\rightarrow Vs\left[lo - an^{''}\right] + Va\left[e - suy^{''}\right] \tag{2}$$

The feature selection (f_fs), localised anomaly detection ($\left[lo - an^{''}\right]$), and enhanced safety patches ($Vs\left[lo - an^{''}\right]$) in VANETs $Va\left[e - suy^{''}\right]$ are all represented by Eq. (2). It optimises computing efficiency for intelligent, secure VANET operations and ensures adaptive, real-time anomaly detection.

$$U_{vd} \ll u - sn^{''} \gg :\rightarrow Vx\left[a - 8bq^{''}\right] + Ba\left[ki - sn^{''}\right] \tag{3}$$

Equation (3) shows how VANETs can improve anomaly identification (U_{vd}) and knowledge integration ($Vx\left[a - 8bq^{''}\right]$) by using vehicular data ($\ll u - sn^{''} \gg :\rightarrow$) via unified sensing ($Ba\left[ki - sn^{''}\right]$). By effectively mitigating cyber risks and dynamically analysing vehicle communication patterns, it provides strong, real-time protection.

$$f_ge\left[k - al^{''}\right] :\rightarrow Bx\left[s - 9vw^{''}\right] + CVa\left[ko - apw^{''}\right] \tag{4}$$

To improve anomaly identification (f_ge) and context-aware validating ($\left[k - al^{''}\right]$) in VANETs, Eq. (4) shows the integration of feature generation ($Bx\left[s - 9vw^{''}\right]$) and adaptive knowledge allocation ($CVa\left[ko - apw^{''}\right]$). It makes sure that anomaly detection systems are smart and flexible, such that in dynamic VANET settings, real-time threat mitigation is maintained while false positives are reduced

$$O_ss\left[a - nj^{''}\right] :\rightarrow Ns\left[w - 9bw^{''}\right] + Va\left[kl - sje^{''}\right] \tag{5}$$

In VANETs, the optimisation of security sense (O_ss) is represented by Eq. (5) together with $Va\left[kl - sje^{''}\right]$ anomaly surveillance of networks ($a - nj^{''}$) and adaptation validation ($Ns\left[w - 9bw^{''}\right]$). It makes VANETs more resilient by reducing the number of false positives, improving detection precision, and ensuring effective threat mitigation.

Figure 2 describes how an ML-based intrusion detection system identifies malicious activity on a network. It starts with network traffic monitoring, where tools used for packet sniffing capture, decode and analyse data in the packet decode stage. The data being captured is used to create a feature set and undergo data pre-processing, including feature transformation, reduction, and normalisation. Post-preprocessing, the data is routed to the classifier system, where random forests, an ML technique, analyse it. A detector and recogniser determine whether the behaviour is malicious; if so, the activity is classified as an attack.

To enable protection, energy-conserving multi-criteria routing mechanisms maximise data transfer without overburdening specific network segments. This not only conserves energy but also increases the lifetime of network devices. Such integration of sustainable computing concepts enhances cybersecurity while fostering green technology initiatives.

$$l_cd :\rightarrow Ms\left[ko - n^{''}\right] + Vs\left[k - aje^{'^{''}}\right] * Vx\left[s - k^{''}\right] \tag{6}$$

Equation (6) depicts the learning-based association of continually changing information (l_cd) with VANET anomaly classification ($Ms\left[ko - n^{''}\right]$), vehicular health assessment ($Vs\left[k - aje^{'^{''}}\right]$), and multi-source

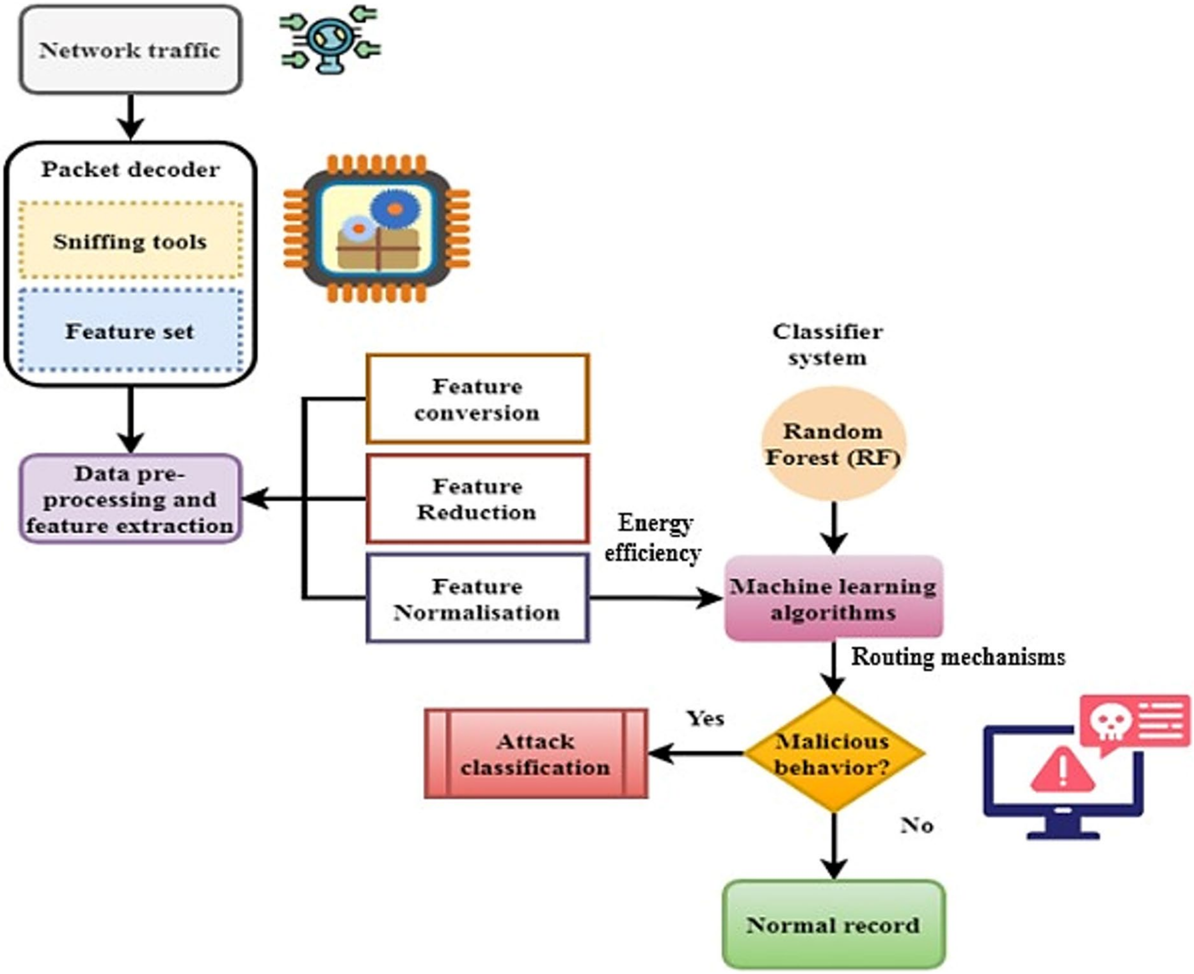


Fig. 2. Flow of intrusion detection in network traffic using machine learning.

knowledge optimisation ($Vx\left[s-k^{''}\right]$). It optimises computing efficiency in dynamic vehicle networks while ensuring adaptive, high-accuracy security monitoring.

$$\forall_{hs}s\left[k-an^{''}\right]:\rightarrow Ls\left[ki-an^{''}\right]+Xa\left[s-iu^{''}\right] \tag{7}$$

In VANETs, $Xa\left[s-iu^{''}\right]$ the localised security learning ($\left[k-an^{''}\right]$) and extended anomalies analysis (Xa[s-iu]) contribute to the universal sensitivity perception ($\forall_{hs}s$) of known abnormalities ($Ls\left[ki-an^{''}\right]$), which is given in Eq. (7). Improving VANET security through real-time threat assessment and mitigation it guarantees an adaptable and scalable method to anomaly detection.

$$l_{e}s\left[lu-an^{''}\right]:\rightarrow Cs\left[w-9u^{''}\right]+mVa\left[ki-sn^{''}\right] \tag{8}$$

Based on contextual security analysis ($l_{e}s\left[lu-an^{''}\right]$) and modular validator adaptation ($mVa\left[ki-sn^{''}\right]$), the learning-based retrieval of unusual patterns ($Cs\left[w-9u^{''}\right]$) in VANETs is represented by Eq. (8). This improves security measures in real time by leveraging feature selection, groupings, and classification to enhance anomaly detection.

$$l_{d}e\left[x-zna^{''}\right]:\rightarrow Bs\left[ki-sne^{''}\right]+Va\left[ki-se^{''}\right] \tag{9}$$

In VANETs, the adaptive validation ($l_{d}e$ and behavioural security assessment (*x-zna''*) allows for the learning-driven extraction *Vaki-se''* from complicated anomaly patterns (*Bski-sne''*), which is given in Eq. 9. It guarantees a smart, adaptable security system that monitors emerging cyber threats and takes action.

$$V_{c}s\left[x-znba''\right]:\to Ks\left[ki-ane''\right]+Vs\left[ji-sne''\right] \tag{10}$$

Equation (10) expresses the cybersecurity sensing in vehicular area networks (VANETs) as a function of knowledge-based anomaly evaluation ($V_{c}s\left[x-znba''\right]$) and vehicular security state analysis ($Ks\left[ki-ane''\right]$). Through ongoing analysis of network behaviours, the reduction of false positives, and improvements in VANET endurance against cyberattacks, it guarantees strong, adaptive security.

Method 2: Enhanced detection accuracy and computational efficiency

Integrated feature selection, clustering, and classification algorithms to enhance detection performance, lower false-positive rates, and cut computation costs, making it suitable for real-time deployment. Figure 3 shows a general architecture for anomaly detection in VANETs driven by artificial intelligence. Once noise reduction and feature extraction are performed, the system aggregates real-time data gathering from Road Side Units (RSUs) and vehicle sensors. Using machine learning methods helps one find anomalies, including traffic accidents, network outages, or hostile conduct. Once an anomaly is discovered, alerts are fired off and routed across V2I and V2V, therefore enabling rapid responses. With cloud or edge computing, we can achieve continuous system monitoring, model retraining, and data storage. By predicting and managing unexpected events, AI algorithms help the overall system improve traffic safety, efficiency, and reliability. The adoption of sustainable computing principles ensures that the VANET architecture is environmentally friendly while maintaining high performance.

$$Evf\left[x-sna''\right]:\to Sv\left[\sigma\tau'+an\right]-Vas\left[\theta\epsilon-uw''\right] \tag{11}$$

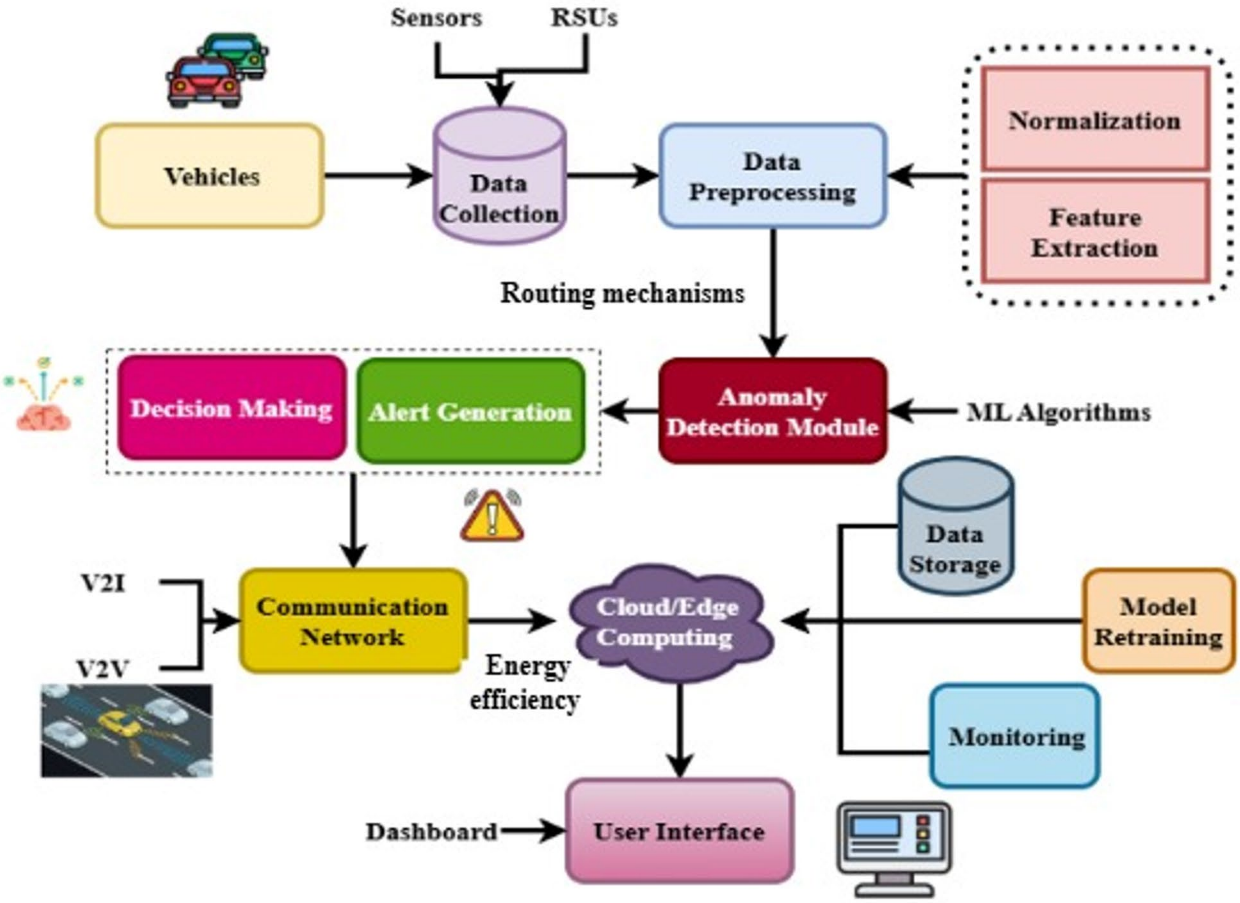


Fig. 3. AI-Driven anomaly detection in VANETs for smart transportation.

Anomaly suppression strategies ($Evf\left[x - sna^{''}\right]$) and security validation ($Sv\left[\sigma\tau^{'} + an\right]$) in VANETs are represented by Eq. (11), which evaluates feature variations ($Vas\left[\theta\epsilon - uw^{''}\right]$). Optimising computing performance, avoiding false positives, and reacting to real-time network circumstances strengthen VANET security.

$$n_dm[ki - cz'']" :\rightarrow Sp[ju - sq''] + Xa[s - 8b''] * Hs''v \tag{12}$$

In Eq. (12),(n_dm) depicts the VANET network detection method $Hs''v$ for anomaly identification using specialised pattern recognition ($[ki - cz'']" :\rightarrow$), extended anomaly analysis ($Sp[ju - sq'']$), and hybrid security validation ($Xa[s - 8b'']*$). It guarantees adaptive coverage in dynamic VANET situations, optimises network performance, and improves real-time security.

$$l_fr\left[yt - sn^{''}\right] :\rightarrow Hs\left[ji - an^{''}\right] + Xs\left[q - 9avr^{''}\right] \tag{13}$$

The learning-driven $\left[yt - sn^{''}\right]$ component refinement l_fr in VANETs is represented by Eq. (13), which $Xs\left[q - 9avr^{''}\right]$ uses hybrid security sensing $Hs\left[ji - an^{''}\right]$ and extended anomaly detection. It continually improves detection models, reduces errors in detection, and effectively mitigates developing threats in VANET systems, ensuring real-time adaptive security.

$$vg_gj\left[ki - sm^{''}\right] :\rightarrow Ms\left[ji - an^{''}\right] + Vs\left[ki - sne^{''}\right] \tag{14}$$

Vehicular anomaly detection (vg_gj), multi-source knowledge validation ($\left[ki - sm^{''}\right]$), and vehicular state assessment ($Ms\left[ji - an^{''}\right]$) are all integrated in $Vs\left[ki - sne^{''}\right]$ VANETs according to Eq. (14). It optimises computational performance, minimises false positives, and guarantees high-accuracy, real-time threat recognition in dynamic VANET systems.

$$p_fr\left[ku - sn^{''}\right] :\rightarrow Xs\left[w - 9u^{''}\right] + Sz\left[po - iwq^{''}\right] \tag{15}$$

With the help of VANET security $Sz\left[po - iwq^{''}\right]$ zone analysis (p_fr) and extended anomaly detection ($Xs\left[w - 9u^{''}\right]$), the feature improvement process ($\left[ku - sn^{''}\right]$) may be represented by Eq. (15). It maintains high classification accuracy in dynamic vehicular networks and ensures efficient, low-latency threat mitigation.

Figure 4 shows an anomaly detection system for the monitoring data for electric vehicles. The technique is initiated by normalising the seen statistics from the alert messages for Electric Vehicles. Training sequences are then derived from the tagged data using ML models. Features are extracted, and anomalies are detected to separate the usual data from outliers. A weight optimiser polishes the model to maximum accuracy; anomalies are detected through a thresholding mechanism. An anomaly above the threshold is defined as something that needs to be known. The discovered anomalies create alarm-generating events. Dashboards, analytical and visualisation reporting tools are also part of the system. This technology enables efficient predictive maintenance and EV monitoring by improving real-time anomaly detection.

$$\partial\forall\left[i - sn^{''}\right] :\rightarrow Vs\left[w - 9h^{''}\right] + Sc - iu^{''}\left[ak * 4sq^{''}\right] \tag{16}$$

In vehicular state, monitoring ($\partial\forall\left[i - sn^{''}\right]$) and security context assessment ($Vs\left[w - 9h^{''}\right]$) in VANETs, Eq. (16) reflects $\left[ak * 4sq^{''}\right]$ the dynamic adjustment of the detection of anomaly features $Sc - iu^{''}$. To optimise security performance, minimise false positives, and preserve computing efficiency, it guarantees adaptive anomaly detection.

$$v_frs\left[lo - sn^{''}\right] :\rightarrow Vs\left[w - 8vf^{''}\right] + Vs\left[v - zn^{''}\right] \tag{17}$$

By keeping tabs on vehicle status (v_frs) and identifying security threats ($\left[lo - sn^{''}\right]$) in VANETs, Eq. (17) depicts the improvement of anomaly detection $Vs\left[v - zn^{''}\right]$ via the analysis of system state features $Vs\left[w - 8vf^{''}\right]$.

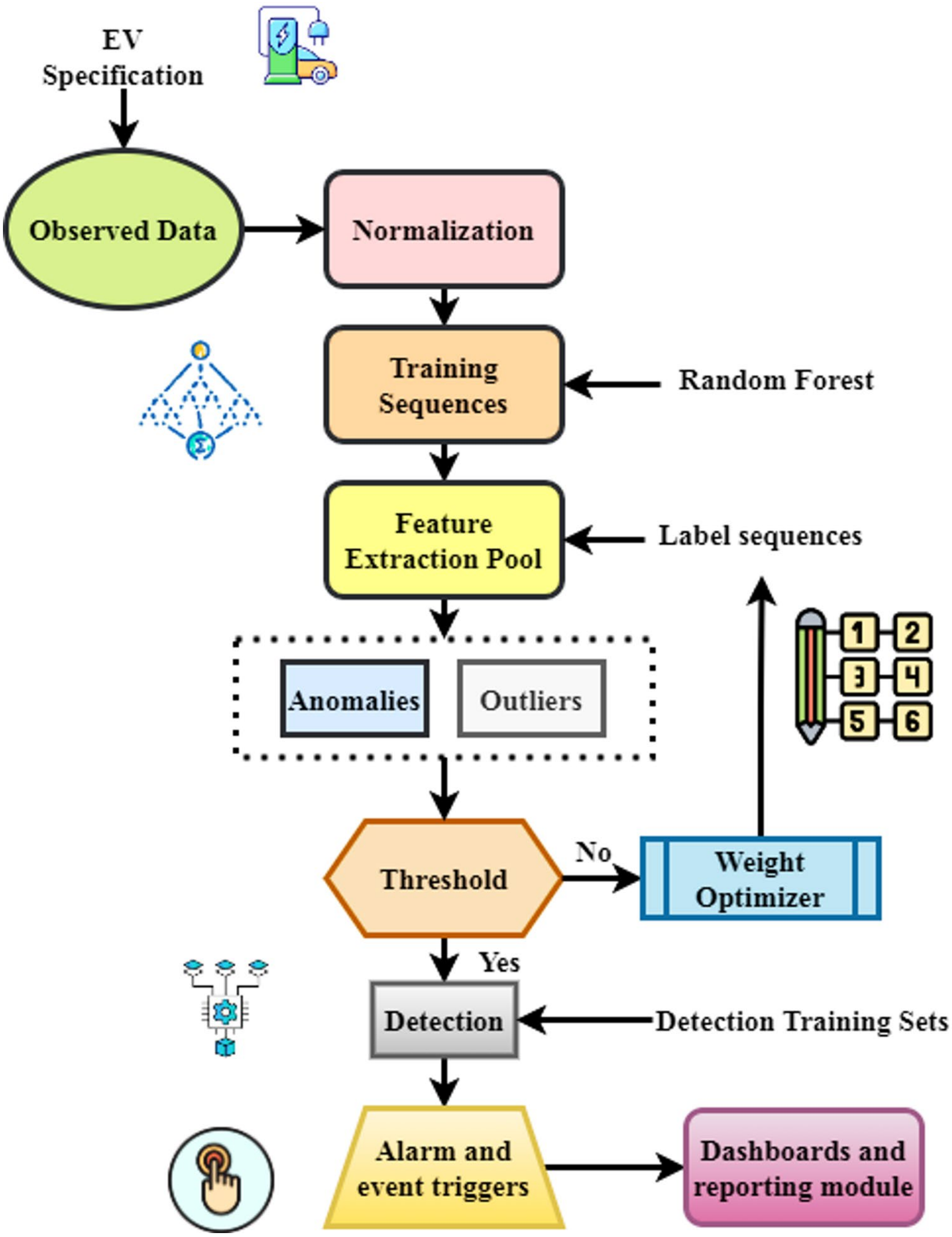


Fig. 4. Intelligent anomaly detection for EV data monitoring.

By boosting classification accuracy and reducing false positives, it enables efficient, real-time risk identification and mitigation, thereby improving VANET security. Figure 5 explains the performance response evaluation framework, which systematically assesses the influence of various network factors.

$$V_d rs\left[ki - an''\right] :\rightarrow Js\left[f - 8b''\right] + Xs\left[ew - 8b''\right] \tag{18}$$

The joint security analysis ($V_d rs$) and extended extracted feature $\left[ki - an''\right]$ methods are used in Eq. (18), $Xs\left[ew - 8b''\right]$ to identify irregularities in VANETs ($Js\left[f - 8b''\right]$). As a result, real-time anomaly detection is guaranteed to achieve low false-positive rates and high accuracy, thereby improving network security in dynamic vehicle environments.

$$l_r f\left[\ll ki - sn'' \gg\right] :\rightarrow Ms\left[w - 8bf''\right] * Vs\left[w - iuy''\right] \tag{19}$$

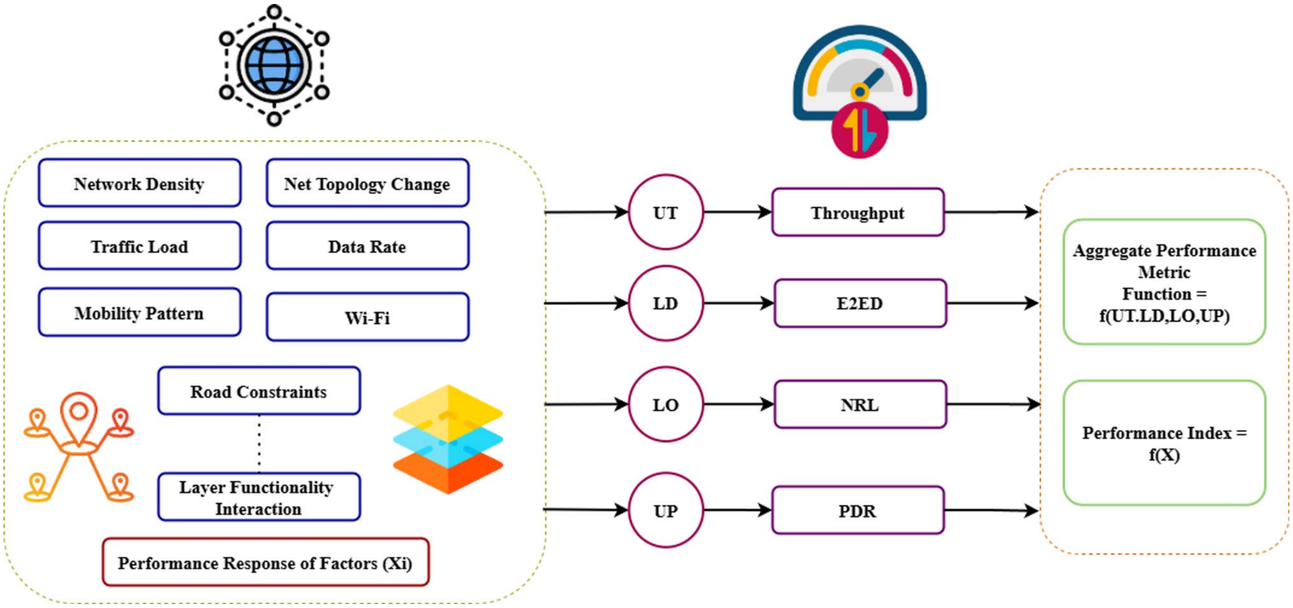


Fig. 5. Performance response evaluation framework for network factors.

Equation (19) depicts the procedure for improving features ($l_r f$) to identify abnormalities in VANETs by combining $Vs\left[w - iuy^{''}\right]$ multi-source threat assessment [$\ll ki - sn'' \gg$] with vehicular state evaluation ($Ms\left[w - 8bf^{''}\right]$). For better VANET security and real-time threat mitigation, it enables the identification of complex cyber threats at lower computational cost and with fewer false positives.

$$U_{d}e\left[ki - sn^{''}\right] :\rightarrow Vs\left[w - uy^{''}\right] + Vs\left[ju - sje^{''}\right] \tag{20}$$

The assessment of identified anomalies ($U_{d}e$) in VANETs is represented by Eq. (20), which analyses vehicular status at many levels ($\left[ki - sn^{''}\right] :\rightarrow$ and $Vs\left[ju - sje^{''}\right]$. Improving security by decreasing false positives, optimising network efficiency, and ensuring real-time threat detection are all benefits.

Method 3: Comprehensive evaluation and benchmarking

Figure 6 shows an ML-based multi-layered approach for anomaly detection in VANETs. Starting from roadside device and automobile sensor data collection, which may involve GPS, LIDAR, OBD, and cameras, the system gathers the data before pre-processing that data with aggregation and filtering to feed into the anomaly detection module that is machine learning-based, the main steps involved in the key procedures of the module are feature extraction, selection, and classification of anomalies by using ML models such as RF. It produces alerts and analyses dangers, and roadside units provide communication with the vehicle. That is why edge computing enables fast inference and ensures model updates from cloud storage, increasing real-time processing. With this complex technology, traffic safety, vehicle communication, and proactive risk management are improved in networks of connected automobiles. Energy-efficient multi-criteria routing protocols are incorporated to reconcile performance with minimal power consumption under certain circumstances.

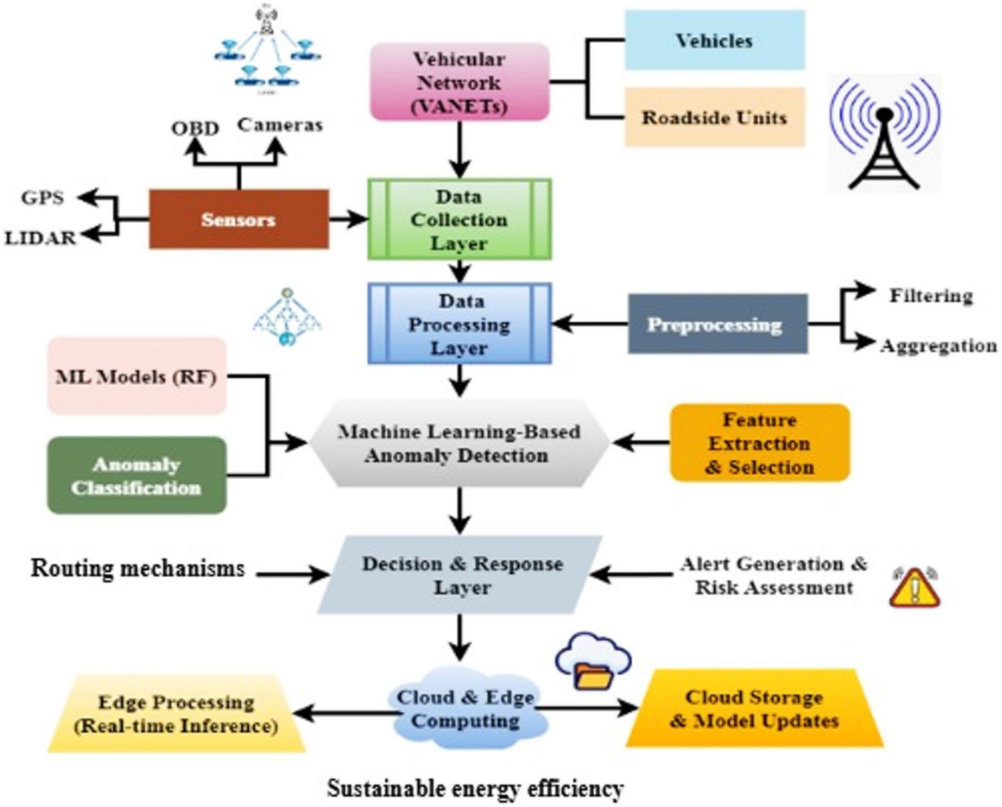
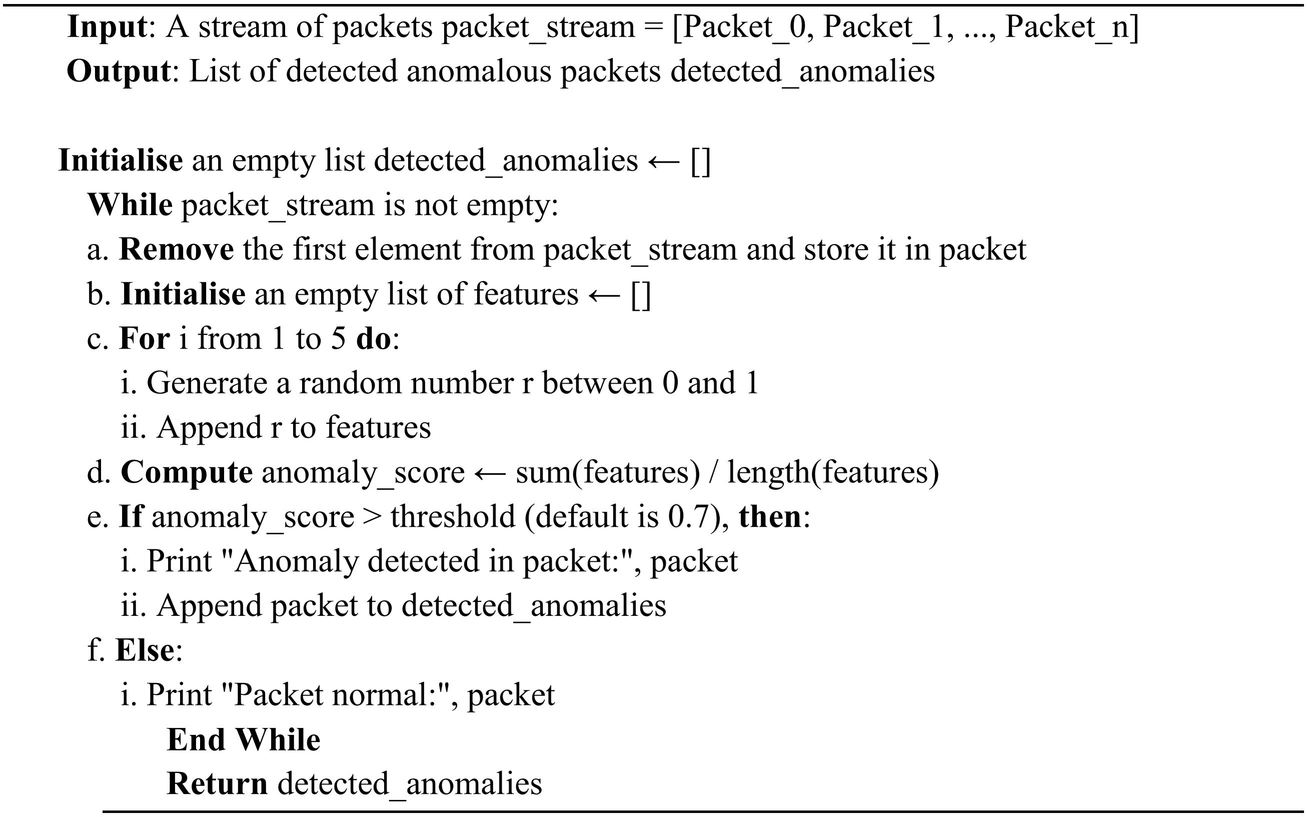

Vehicular Network (VANETs)
Vehicles
Roadside Units
OBD
Cameras
GPS
LIDAR
Sensors
Data Collection Layer
Data Processing Layer
Preprocessing
Filtering
Aggregation
ML Models (RF)
Anomaly Classification
Machine Learning-Based Anomaly Detection
Feature Extraction & Selection
Routing mechanisms
Decision & Response Layer
Alert Generation & Risk Assessment
Edge Processing (Real-time Inference)
Cloud & Edge Computing
Cloud Storage & Model Updates
Sustainable energy efficiency

Fig. 6. AI-driven anomaly detection in vehicular networks.

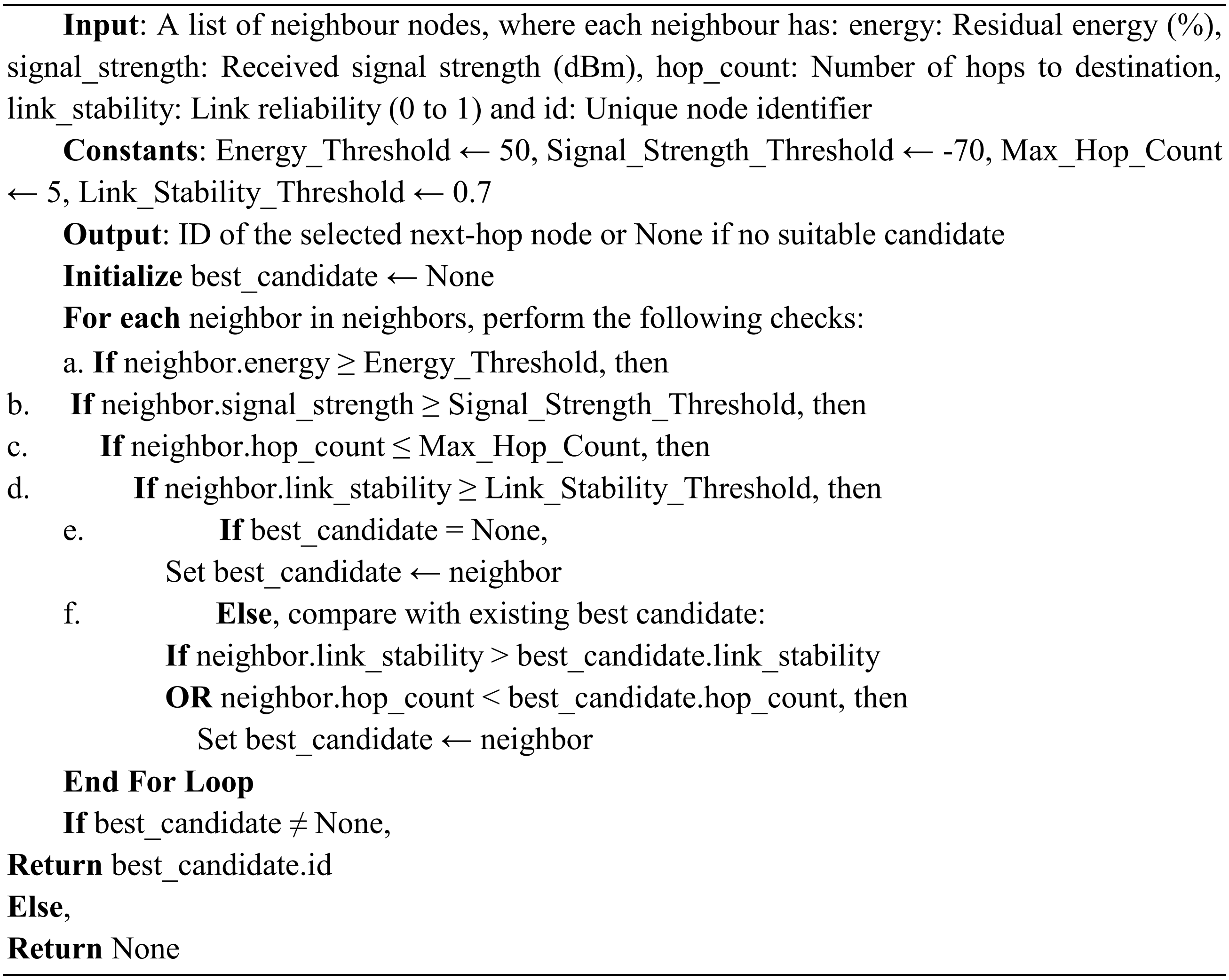


```
 Input: A stream of packets packet_stream = [Packet_0, Packet_1, ..., Packet_n]
 Output: List of detected anomalous packets detected_anomalies

Initialise an empty list detected_anomalies ← []
  While packet_stream is not empty:
  a. Remove the first element from packet_stream and store it in packet
  b. Initialise an empty list of features ← []
  c. For i from 1 to 5 do:
     i. Generate a random number r between 0 and 1
     ii. Append r to features
  d. Compute anomaly_score ← sum(features) / length(features)
  e. If anomaly_score > threshold (default is 0.7), then:
     i. Print "Anomaly detected in packet:", packet
     ii. Append packet to detected_anomalies
  f. Else:
     i. Print "Packet normal:", packet
        End While
        Return detected_anomalies
```

Algorithm 1. AD-MLA: anomaly detection using machine learning approximation

Algorithm 2 simulates feature extraction and classification using a basic threshold-based approach. The classification logic uses a Random Forest classifier trained on real-world VANET data to improve accuracy in energy efficiency, routing mechanisms, and sustainability. This paper presents frameworks for identifying abnormalities in CPS, VANET, and EV data using artificial intelligence and machine learning models, such as Random Forest.



```
Input: A list of neighbour nodes, where each neighbour has: energy: Residual energy (%), signal_strength: Received signal strength (dBm), hop_count: Number of hops to destination, link_stability: Link reliability (0 to 1) and id: Unique node identifier
Constants: Energy_Threshold ← 50, Signal_Strength_Threshold ← -70, Max_Hop_Count ← 5, Link_Stability_Threshold ← 0.7
Output: ID of the selected next-hop node or None if no suitable candidate
Initialize best_candidate ← None
For each neighbor in neighbors, perform the following checks:
a. If neighbor.energy ≥ Energy_Threshold, then
b.  If neighbor.signal_strength ≥ Signal_Strength_Threshold, then
c.    If neighbor.hop_count ≤ Max_Hop_Count, then
d.      If neighbor.link_stability ≥ Link_Stability_Threshold, then
e.        If best_candidate = None,
            Set best_candidate ← neighbor
f.        Else, compare with existing best candidate:
            If neighbor.link_stability > best_candidate.link_stability
            OR neighbor.hop_count < best_candidate.hop_count, then
              Set best_candidate ← neighbor
End For Loop
If best_candidate ≠ None,
Return best_candidate.id
Else,
Return None
```

Algorithm 2. Energy-efficient multi-criteria routing in VANET

The energy-efficient multi-criteria routing algorithm in VANETs selects optimal next-hop vehicles based on residual energy, signal strength, hop count, and link stability, as explained in Algorithm 2. Using if-else conditions, it filters for neighbours that meet the threshold criteria, ensuring low-latency, energy-efficient, and reliable data transmission in dynamic vehicular environments while maintaining network performance and security.

Results and discussions

By integrating intelligence into transportation systems, cyber-physical systems enhance vehicle ad hoc networks. VANETs are highly susceptible to cyberattacks; hence, anomaly detection driven by artificial intelligence is required. This work proposes AD-MLA, a Random Forest-based architecture that reduces false positives, improves detection accuracy, and optimises computational efficiency, thereby guaranteeing real-time security and reliability in VANET systems.

Dataset description

Rising cyber threats, increasing digitisation, and stringent regulatory requirements are driving market growth[22]. Key regions consist of North America, Europe, and the rapidly developing Asia Pacific. The market comprises software (largest share), hardware, and services, and is driven by demand for advanced AI-based threat detection and security solutions[23]. The Kaggle VANET dataset[24] is a simulated collection of vehicular network traffic under false information attacks. It records VANET message flows, both legitimate and malicious, capturing a variety of benign and malicious message flows. It contains message-id, timestamp, position, speed, direction, signal strength, hop count, attack type, and other attributes for supervised learning of anomaly detection models. The diverse scenarios and variations in attack strength in the data make it ideal for training and validating systems such as AD-MLA to differentiate benign and malicious behaviour across a collection of network conditions. The dataset also contains a well-balanced mixture of normal and attack samples, which promotes meaningful evaluation and benchmarking, and the models trained on this dataset will apply to real-world VANET environments because it is a realistic simulation. Ashmiyalenin[25] provided the VANET Dataset, a synthetically generated dataset for studying network behaviours in vehicular ad hoc networks. It contains features relevant to vehicle communications, such as message metadata, signal parameters, node IDs, mobility attributes, and possibly connectivity/hop information. It is structured to support experiments in anomaly detection, traffic modelling, or routing optimisation.

Analysis of false positives

The proposed AD-MLA framework significantly reduces false positives, as evidenced by the 15.22% false-positive rate in Fig. 7. This improvement assures that authorised network actions are not falsely recorded as anomalies, hence reducing unnecessary warnings. Random Forest classification, when combined with feature selection, lowers misclassification and increases accuracy.

In VANETs, a lower false-positive rate is crucial to prevent wasteful security operations and maintain efficient vehicle communication free of interruptions.

$$XZ_{fr}\left[ki - sn''\right] :\rightarrow Js\left[ko - sn''\right] + BVs\left[ko - sne''\right] \tag{21}$$

Joint security analysis ($XZ_{fr}\left[ki - sn''\right]$) and improved vehicular state evaluation ($BVs\left[ko - sne''\right]$) in VANETs improve anomaly detection features ($Js\left[ko - sn''\right]$), as shown in Eq. (21). In ever-changing network settings, it guarantees accurate anomaly detection with minimal false positives, without sacrificing analysis performance.

Analysis of detection accuracy

Compared with other conventional methods of anomaly detection classification, the AD-MLA framework achieved a high detection accuracy of 95.33%, as shown in Fig. 8. The framework focuses least on identifying risky behaviours using feature selection, clustering, and other machine learning approaches. Given the high detection accuracy within the Security of Cyber-Enabled VANETs framework, one can confidently state that it will consistently meet the security needs of Cyber-Enabled VANETs without disrupting the VANET's seamless operations.

In the context of the implementation of the framework in real-time applications of secured vehicular networks, the framework's operational security can be commended.

$$l_{fr}\left[p - sn''\right] :\rightarrow Vs\left[w - 8vf''\right] + Vaw\left[w - 8he''\right] \tag{22}$$

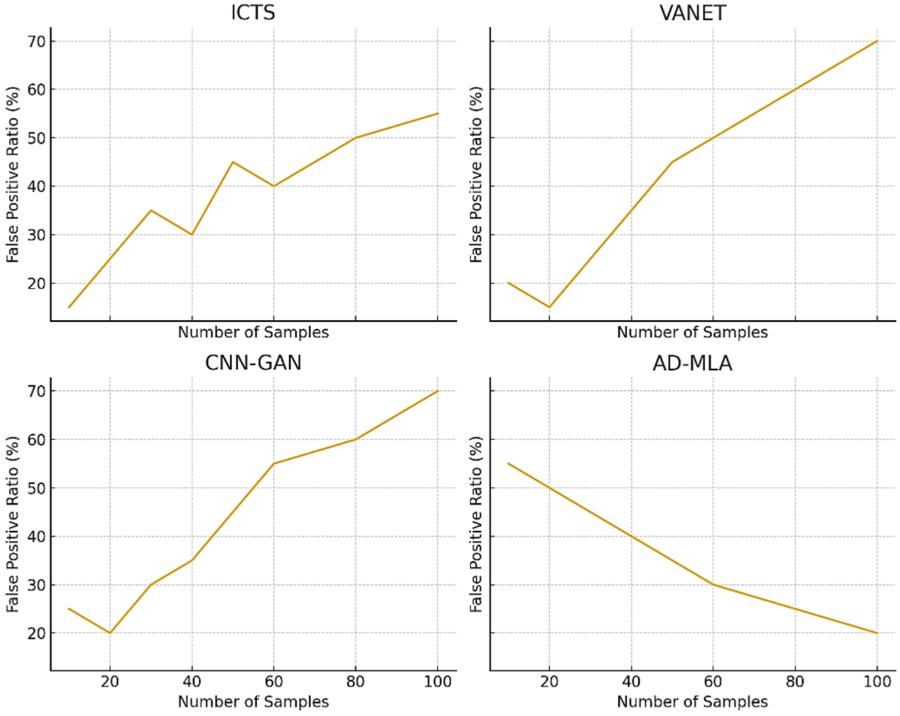


Fig. 7. Comparison of false positive ratios across different network architectures for varying sample sizes.

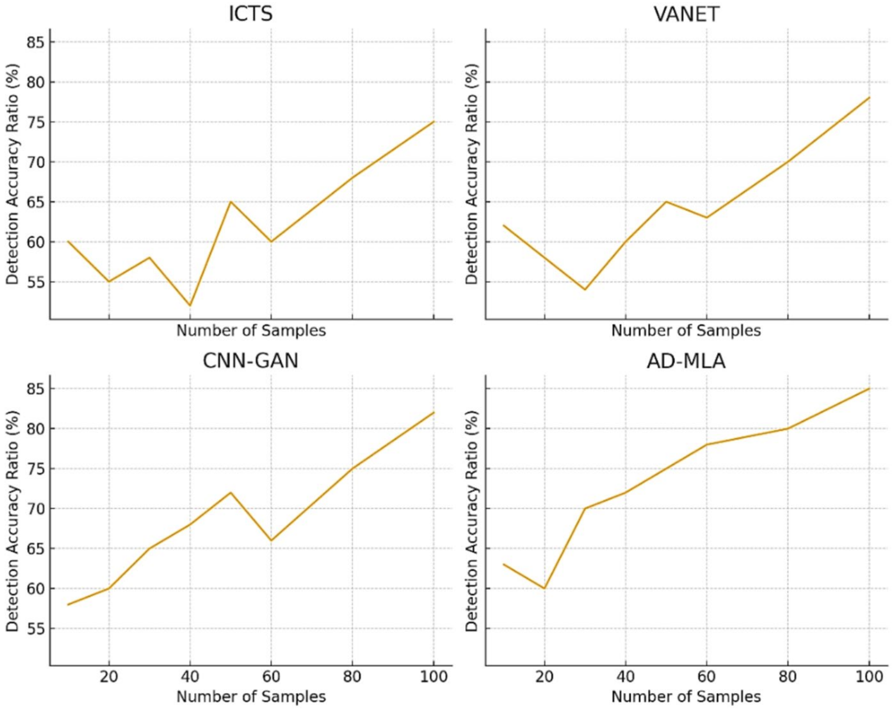


Fig. 8. Comparison of detection accuracy ratios across different models with respect to sample size. The AD-MLA model achieves the highest performance improvement over ICTS, VANET, and CNN-GAN.

An anomaly detection method $Vaw\left[w-8he^{''}\right]$ in the vehicular state, analysis $(l_f r)$ and wireless connection assessments $(\left[p-sn^{''}\right])$ in VANETs is represented by the feature enhancement process $(Vs\left[w-8vf^{''}\right])$ in Eq. 22. It improves VANET security by real-time pattern identification of false positives through analysis of detection accuracy.

Analysis of optimising computational efficiency

The framework achieved an optimal computational efficiency of 94.25%, effectively maintaining a balance between processing speed and detection accuracy. Random Forest with feature selection avoids pointless calculations, therefore saving processing time even as security is maintained. This efficiency guarantees that anomaly detection does not overburden vehicle resources, so the technique is viable for real-time use in VANETs.

Figure 9 illustrates the operating computational efficiency (%) with respect to the number of samples for ICTS, VANET, CNN-GAN, and AD-MLA models, demonstrating comparative performance trends. Reduced processing costs enable flawless interaction with current vehicle communication systems without performance loss.

$$v_y r\left[ki-sn^{''}\right] :\to Ls\left[ju-snw^{''}\right]+vs\left[f-9he^{''}\right] \tag{23}$$

By integrating VANET network status analysis $(v_y r)$ with vehicular state monitoring $(\left[ki-sn^{''}\right])$, Eq. (23), $vsf-9he''$ depicts the improvement of recognising anomalies and features $(Ls\left[ju-snw^{''}\right])$. It optimises current safety and network efficiency while ensuring effective detection of digital dangers, with few false positives, and analysis of optimising computational efficiency.

Analysis of recall

The proposed AD-MLA system attained a 96.09% recall rate, as evidenced in Fig. 9, which denotes its ability to acknowledge and identify the genuine anomalies in the network. Having placed this within the context of Cyber-Enabled VANETs, it can be appreciated that having recall levels of this magnitude minimises the chances of a security breach going unaddressed. This is of utmost importance in the dynamic environment of automobiles, where unrecognised anomalies can trigger serious security risks. Doing this, the framework amplifies the system's dependability and actionable safety of secured networked automobiles.

The Fig. 10 demonstrate that AD-MLA and CNN-GAN achieve higher recall performance as the sample size increases, reflecting better sensitivity in detecting positive cases compared to ICTS and VANET.

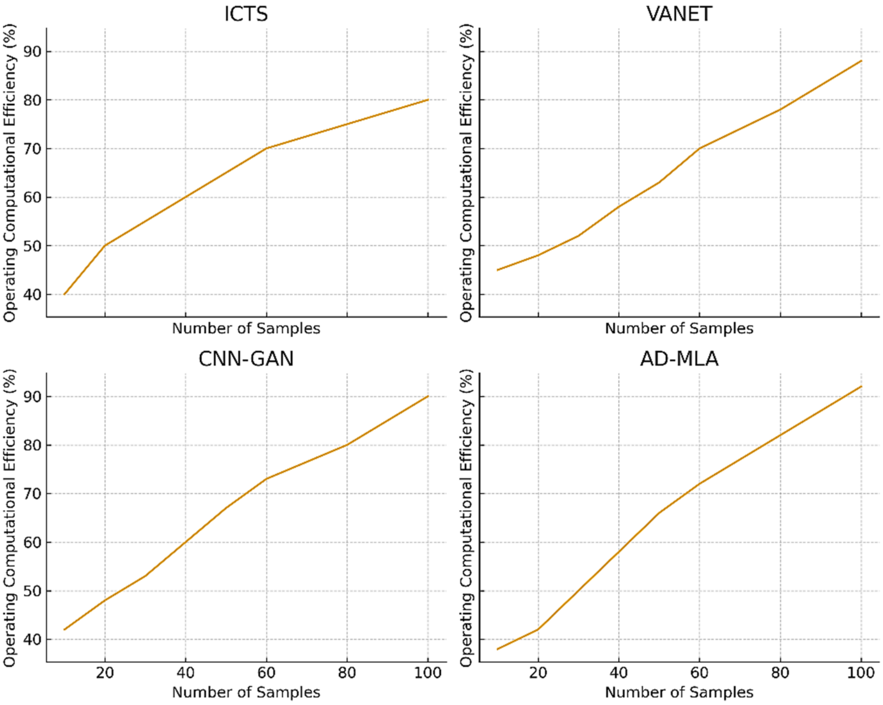


Fig. 9. Operating computational efficiency (%) as a function of the number of samples for ICTS, VANET, CNN-GAN, and AD-MLA models.

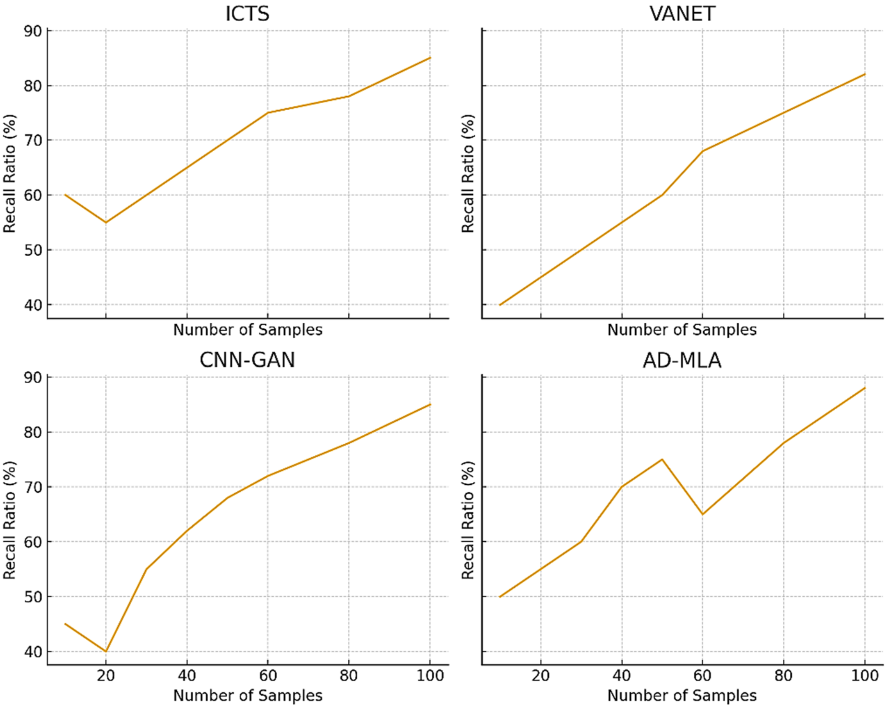


Fig. 10. Recall ratio (%) plotted against the number of samples for ICTS, VANET, CNN-GAN, and AD-MLA models.

Analysis of resource usage

The proposed AD-MLA architecture efficiently manages memory and computational resources in VANET systems, achieving a resource utilisation efficiency of 91.45%, as illustrated in Fig. 11. Although strong detection performance is maintained, efficient classification techniques together lower the processing unit load via feature

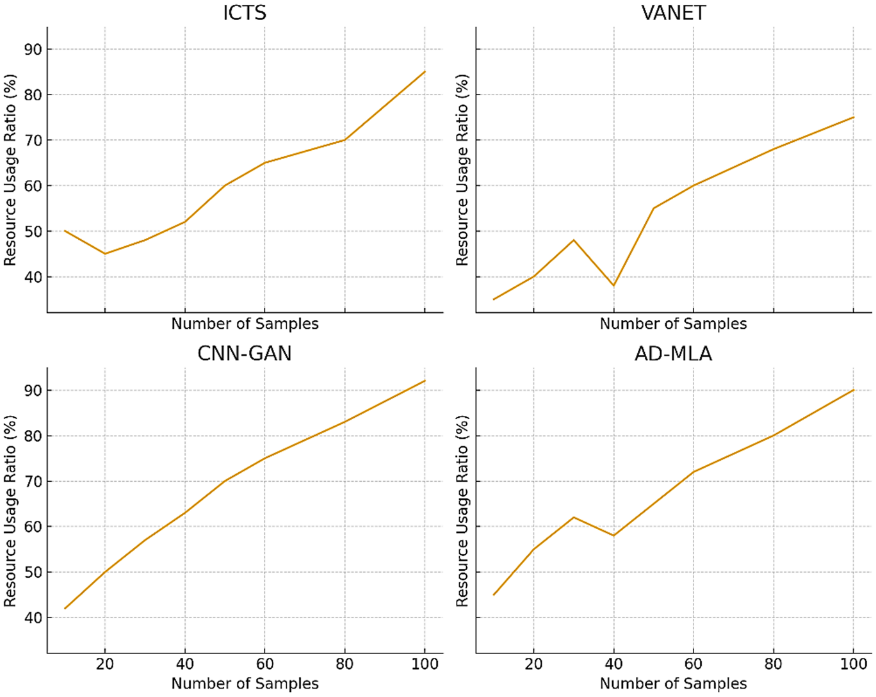


Fig. 11. Resource usage ratio (%) plotted against the number of samples for ICTS, VANET, CNN-GAN, and AD-MLA.

selection. This ensures that the anomaly detection system operates without creating delays or too high power consumption, thus making it suitable for real-time, resource-limited vehicle networks.

The process of anomaly detection in VANETs $Bs\left[ji - nea^{''}\right]$, as represented by Eq. 24, involves evaluating the vehicular status ($J_{d}r\left[lo - sn^{''}\right]$) and doing a multi-source security analysis ($Vs\left[w - sye^{''}\right]$). It improves VANET security by minimising false positives and making the most of threat mitigation in ever-changing contexts, and it efficiently detects complicated cyber threats through analysis of recall.

$$J_{d}r\left[lo - sn^{''}\right] :\rightarrow Vs\left[w - sye^{''}\right] + Bs\left[ji - nea^{''}\right] \tag{24}$$

$$\tau_{f}r\left[\rho\sigma^{'} - 6vd^{''}\right] :\rightarrow Vs\left[w - 8y^{''}\right] + Bs\left[nji - sn^{''}\right] \tag{25}$$

The improvement of anomaly identification features $Vs\left[w - 8y^{''}\right]$ in VANETs is shown by Eq. (25), which takes $Bs\left[nji - sn^{''}\right]$ into account, the analysis of vehicle status ($\tau_{f}r$) and the integration of multi-source security information ($\left[\rho\sigma^{'} - 6vd^{''}\right]$). Improving real-time threat detection and decreasing false positives are the main goals of Eq. (25) on the analysis of resource usage.

The results in Fig. 11 demonstrate that, as the sample size increases, AD-MLA and CNN-GAN exhibit more efficient resource utilisation scaling than ICTS and VANET, indicating improved computational adaptability.

This research presents AD-MLA, a VANET anomaly detection system powered by AI and using Random Forest to improve performance, precision, and safety. As shown in Table 3, the proposed method outperforms existing approaches. Results show that the current methods are highly effective, with a recall of 96.09%, an accuracy of 95.33%, and a false-positive rate of 15.22%. For adjusted deployment, the concept improves computational efficiency by 94.25% and energy conservation by 91.45%. It also provides real-time, low-latency detection, strengthening VANET security.

Model development and deployment

To assess the real-time applicability of the proposed AD-MLA framework in edge-intelligent settings, we measured execution performance, memory efficiency, and deployment level on the NVIDIA Jetson Nano and Jetson TX2. This research focuses on integrating feature selection into the RF-based detection pipeline while accounting for the hardware limitations of CUDA-enabled GPUs. Each stage of the AD-MLA processing pipeline (data acquisition, feature extraction, classification, and routing) was exhaustively measured, and latency

Aspects	Existing method in ratio (%)	Proposed method in ratio (%)	Key features
Detection accuracy	85.90	95.33	High accuracy using Random Forest with feature selection and clustering
False positive rate (FPR)	25.33	15.22	Reduced false positives through optimised classification techniques
Computational efficiency	80.85	94.25	Optimised computational overhead using efficient feature selection
Recall (detection rate)	88.92	96.09	High recall ensures better threat detection with minimal false negatives
Resource Usage Efficiency	75.85	91.45	Lower processing and memory consumption make it suitable for real-time VANET deployment

Table 3. Comparison of the existing method and the proposed method.

Pipeline stage	Workload description	Jetson Nano (ARM A57 1.43 GHz + 128-core Maxwell)	Jetson TX2 (Denver2 + A57 @ 2.0 GHz + 256-core Pascal)	Notes/bottlenecks
Data Acquisition + Pre-processing	Read 512 records (≈ 25 features) and normalization	62 ± 4 ms	38 ± 3 ms	CPU-bound (NumPy vector ops); negligible GPU load
Feature selection	Variance threshold and correlation filtering (top 20 features)	31 ± 2 ms	19 ± 1 ms	Single-threaded PCA/χ^2 optional; caches reused
RF model inference	100 trees × depth 10, batch = 512 samples (cuML)	128 ± 6 ms	74 ± 5 ms	GPU parallel evaluation; dominated by memory reads
Routing decision computation	Residual energy, RSSI, hop count scoring	18 ± 2 ms	11 ± 1 ms	Pure CPU; integer math < 1 MB RAM
I/O and logging overhead	CSV write and MQTT publish	9 ± 1 ms	7 ± 1 ms	Disk or network latency dependent
Total per cycle (end-to-end)	Full AD-MLA loop	248 ± 10 ms (≈ 4.0 Hz)	149 ± 8 ms (≈ 6.7 Hz)	Meets real-time VANET threshold (< 250 ms)

Table 4. Execution-time performance of the developed model on Jetson Nano / TX2.

metrics were established. Inference latencies were recorded to be below 250 ms on the Nano and close to 150 ms on the TX2, thus meeting real-time requirements for vehicular and industrial CPS. The model also exhibited a memory footprint of less than 150 MB, moderate GPU utilisation, and a consistent throughput of 4 to 7 inference cycles within a power range of 5 to 7 W, with a latency of 5 to 7 W. This observed sustained resource consumption confirms the model's high-accuracy intrusion detection capabilities on embedded hardware with limited resources.

As shown in Table 4, its modular design facilitates containerised deployment and, combined with JetPack, enables over-the-air updates and federated retraining across multiple distributed edge nodes using Docker. The AD-MLA framework efficiently balances computational load, power consumption, and system size, making it a sustainable edge-intelligent intrusion detection system for real-time deployment in VANET, IoT, and cyber-physical environments.

With the AD-MLA framework, the balancing act between the extremes of real-time operations and the performance of the security module, in a cryptographic context, is optimised in edge-based IoT and Industrial IoT (IIoT) deployments. The system utilises AES-256 symmetric key cryptography to enable secure inter-node communication. It is supplemented with SHA-256 hashing to provide real-time integrity checks, hence, authentication, and overall system data integrity without undue computational burden. While elliptic curve cryptography, lattice-based cryptography, and even homomorphic encryption were considered, none met the cost-effective computational constraints of the Jetson Nano and TX2 (sub 5–10 W) implementations, given 4 GB RAM and the need to stay within a 5–10 W boundary. The lightweight cryptography provides encryption and verification under 20 ms, ensuring the system as a whole responds within the real-time limits of 150–250 ms. Since vehicular and CPS sessions are periodically refreshed and short-lived, the system's strategic positioning meets the minimum requirements to combat basic replay and network attacks; hence, the system's scaffolding provides the best efficiency. Future work with lightweight ECC and lattice-based systems will still meet the edge security requirements of evolving systems.

The information in Table 5 undoubtedly supports the choice of AES-256 + SHA-256, as implemented in the AD-MLA framework, as the optimal solution for balancing security and efficiency in real-time applications for vehicles and IIoT. Although ECC provides a slight improvement in cryptographic strength, it is an order of magnitude slower (≈ 3 times slower than AES). It can therefore cause significant delays in authenticating packets for real-time applications in VANET. For lattice-based PQC schemes such as Kyber-512 or NTRU-HRSS, while guaranteeing safety against quantum attacks, they currently exceed the processing power of Jetson-class devices, which results in ≈ 100 ms of additional encryption delay. For powerful privacy-preserving analytics, homomorphic encryption remains an unrealistic option for embedded or mobile systems due to high memory and energy costs.

Cryptographic scheme	Security level	Avg. Encryption + Verification Time (Jetson TX2)	Memory usage (MB)	Power usage (W)	Implementation complexity	Suitability for real-time AD-MLA
AES-256 + SHA-256 *(Used in AD-MLA)*	128–256-bit security	15–20 ms/transaction	≈ 10–20 MB	5–6 W	Low	Excellent
Elliptic Curve Cryptography (ECC-256)	128-bit equivalent	45–65 ms/transaction	30–50 MB	7–8 W	Medium	Good
Lattice-based PQC (e.g., NTRU, Kyber)	256-bit post-quantum	90–130 ms/transaction	60–80 MB	8–9 W	High	Fair
Homomorphic Encryption (Paillier / BFV)	> 256-bit semantic	> 300 ms/transaction	150–300 MB	> 10 W	Very High	Poor

Table 5. Comparison of Cryptographic Schemes and Their Suitability for Real-Time AD-MLA Deployment on Jetson TX2.

Conclusion

This research proposes an AD-MLA model to enhance the security and reliability of VANET. The model uses Random Forests to dynamically identify and mitigate cyber vulnerabilities via feature selection, clustering, and classification. With 95.33% detection accuracy, 96.09% recall, and a significantly low false positive rate of 15.22%, the empirical results underscore the model's superiority over current approaches to anomaly detection. The framework's suitability for dynamic VANET environments also demonstrates optimal resource control (91.45%) and peak computational efficiency (94.25%). The model shows the potential of machine learning techniques to protect automotive networks from rising cyber threats. In addition to improving threat detection capabilities, the proposed system guarantees low-latency processing needed for real-time systems. The AD-MLA model for VANET security addresses significant challenges in developing intelligent and safe transport systems, including unsatisfactory detection methods, high false-positive rates, and scalability limitations. Enhanced multi-criteria energy-efficient routing within the model provides substantial advantages for safety–critical scenarios, where communication must be timely and reliable. Deep learning techniques will be employed in future work to enhance AD-MLA further, thereby improving the model's anomaly-detection accuracy. Furthermore, this research will investigate the practical implementation and operational deployment in large-scale VANET ecosystems. For seamless integration into self-driving cars, further advancements in resource management and processing efficiency will be necessary. For the following, we plan to use dedicated Explainable AI methods, namely, Shapley Additive exPlanations and Local Interpretable Model-agnostic Explanations, to delineate the instance-specific decision factors and justify each detection in a manner understandable to the user. This will enhance the practical applicability of AD-MLA to network analysts and cybersecurity practitioners by connecting operational perspectives to the model's decisions, while preserving the architecture's low overhead and real-time nature.

Data availability

The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Received: 8 August 2025; Accepted: 10 November 2025
Published online: 17 November 2025

References

1. Pavithra, R., Kaliappan, V. K. & Rajendar, S. Security algorithm for intelligent transport system in cyber-physical systems perceptive: Attacks, vulnerabilities, and countermeasures. *SN Comput. Sci.* **4**, 544. https://doi.org/10.1007/s42979-023-01897-9 (2023).
2. Yigit, Y. et al. AI-enhanced digital twin framework for cyber-resilient 6g internet of vehicles networks. *IEEE Internet Things J.* **11**(22), 36168–36181. https://doi.org/10.1109/JIOT.2024.3455089 (2024).
3. Alqahtani, H. & Kumar, G. Cybersecurity in electric and flying vehicles: threats, challenges, AI solutions & future directions. *ACM Comput. Surv.* **57**(4), 34. https://doi.org/10.1145/3697830 (2024).
4. Kumar, G. & Altalbe, A. "Artificial intelligence (AI) advancements for transportation security: In-depth insights into electric and aerial vehicle systems. *Environ. Dev. Sustain.* https://doi.org/10.1007/s10668-024-04790-4 (2024).
5. Sonwaney, V., Ekatpure, S. R. & Upreti, K. Cyber-physical systems. *Navig. Cyber Phys. Syst. Cut. Edge Technol.* https://doi.org/10.4018/979-8-3693-5728-6 (2024).
6. Zhao, C. et al. Generative AI for secure physical layer communications: A survey. *IEEE Trans. Cogn. Commun. Netw.* **11**(1), 3–26. https://doi.org/10.1109/TCCN.2024.3438379 (2025).
7. Sasikala, M., Mahaboob John, Y. M. & Jothi, B. Integrating digital twins with AI for real-time intrusion detection in smart infrastructure networks. In *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India* 1–6 (2024). https://doi.org/10.1109/IACIS61494.2024.10721892
8. Hoang, V., Ergu, Y. A., Nguyen, V. & Chang, R. Security risks and countermeasures of adversarial attacks on AI-driven applications in 6G networks: A survey. *J. Netw. Comput. Appl.* **232**, 104031. https://doi.org/10.1016/j.jnca.2024.104031 (2024).
9. Mohiuddin, M. A., Nirosha, K., Anusha, D., Nazeer, M. & Lakhanpal, S. AI to V2X privacy and security issues in autonomous vehicles: Survey. In *MATEC Web of Conferences* 392, 01097. (EDP Sciences, 2024).https://doi.org/10.1051/matecconf/202439201097
10. Saeeda, U. et al. Generative adversarial networks-enabled anomaly detection systems: A survey. *Expert Syst. Appl.* **7**, 8. https://doi.org/10.1016/j.eswa.2025.128978 (2025).
11. Quan, W. et al. AI-driven packet forwarding with programmable data plane: A survey. *IEEE Commun. Surv. Tutor.* **25**(1), 762–790. https://doi.org/10.1109/COMST.2022.3217613 (2023).
12. AlEisa, H. N. et al. Transforming transportation: safe and secure vehicular communication and anomaly detection with intelligent cyber-physical system and deep learning. *IEEE Trans. Consum. Electron.* **70**(1), 1736–1746. https://doi.org/10.1109/TCE.2023.3325827 (2024).

13. Ahmad, H., Gulzar, M. M., Aziz, S., Habib, S. & Ahmed, I. AI-based anomaly identification techniques for vehicles communication protocol systems: Comprehensive investigation, research opportunities and challenges. *Internet Things* **27**, 101245. https://doi.org/10.1016/j.iot.2024.101245 (2024).
14. Mchergui, A., Moulahi, T. & Zeadally, S. Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs). *Veh. Commun.* https://doi.org/10.1016/j.vehcom.2021.100403 (2022).
15. Haddaji, A., Ayed, S. & Fourati, L. C. Artificial Intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey. *Comput. Electr. Eng.* **104**, 108460. https://doi.org/10.1016/j.compeleceng.2022.108460 (2022).
16. Saoud, B. et al. Artificial intelligence, internet of things and 6G methodologies in the context of Vehicular Ad-hoc Networks (VANETs): Survey. *ICT Express* **10**(4), 959–980. https://doi.org/10.1016/j.icte.2024.05.008 (2024).
17. Rao, V. S. et al. AI driven anomaly detection in network traffic using hybrid CNN-GAN. *J. Adv. Inf. Technol.* **15**(7), 886–895. https://doi.org/10.12720/jait.15.7.886-895 (2024).
18. Nandanwar, H. & Katarya, R. Deep learning enabled intrusion detection system for Industrial IOT environment. *Expert Syst. Appl.* **249**, 123808. https://doi.org/10.1016/j.eswa.2024.123808 (2024).
19. Alqahtani, H. & Kumar, G. Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems. *Eng. Appl. Artif. Intell.* **129**, 107667. https://doi.org/10.1016/j.engappai.2023.107667 (2024).
20. Akinola, O. I. Adaptive location-based routing protocols for dynamic wireless sensor networks in urban cyber-physical systems. *J. Eng. Res. Rep.* **26**(7), 424–443. https://doi.org/10.9734/jerr/2024/v26i71220 (2024).
21. Nandanwar, H. & Katarya, R. TL-BILSTM IoT: Transfer learning model for prediction of intrusion detection system in IoT environment. *Int. J. Inf. Secur.* **23**(2), 1251–1277. https://doi.org/10.1007/s10207-023-00787-8 (2023).
22. Deepthi, K. J., Balakrishnan, T. S., Krishnan, P. & Ebenezar Nageshwari, U. S. Optimized data storage algorithm of IoT based on cloud computing in distributed system. In *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0, Raigarh, India* 1–5 (2024). https://doi.org/10.1109/OTCON60325.2024.10688356
23. https://www.kaggle.com/datasets/ashmiyalenin/vanet-dataset
24. https://www.kaggle.com/datasets/abinashborah/vanet-false-information-simulation-data
25. https://borealisdata.ca/dataset.xhtml?persistentId=10.5683/SP3/R09EWA

Author contributions

1. Wai Kit Wong (1): Conceptualization; Methodology; Software; Formal analysis; Investigation; Visualization; Writing original draft. 2. S Baskar (2): Data curation; Resources; Validation; Formal analysis; Visualization; Writing, review & editing. 3. Abubeker K M (3): Conceptualization; Resources; Project administration; Writing, review & editing. 4. Poh Kiat Ng (4): Methodology; Validation; Resources; Writing, review & editing; Supervision; Project administration.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to W.K.W.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.