International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/43 Volume 12, Issue 5, September – October (2025)

SURVEY ARTICLE

Machine and Deep Learning for VANET Security: A Survey of Intrusion Detection Models and Deployment Realities

Prachi Kapoor
School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India.
prachi.110779@stu.upes.ac.in

Ajay Prasad
School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India.
✉ aprasad@ddn.upes.ac.in

Received: 10 June 2025 / Revised: 13 September 2025 / Accepted: 30 September 2025 / Published: 30 October 2025

Abstract – Vehicular Ad Hoc Networks (VANETs) facilitate critical, real-time communication within intelligent transportation systems. However, they are vulnerable to various cyberattacks due to their decentralized and dynamic characteristics. Artificial Intelligence (AI)-based Intrusion Detection Systems (IDS) demonstrate strong capabilities in identifying threats within these vehicular environments. Despite the rapid advancements in research, many existing AI-based IDS solutions primarily emphasize enhancing detection accuracy in controlled or simulated settings, often neglecting essential practical considerations. This paper aims to address this gap by first discussing the primary security threats within VANETs and identifying a range of AI techniques employed to detect these attacks. Additionally, a comprehensive survey of existing literature from 2018 to 2024 has been conducted, evaluating contributions based on several key parameters, including computational and memory overhead, real-time latency considerations, and future challenges. The findings indicate that few studies adequately address these parameters in general terms. Furthermore, the paper surveys current state-of-the-art AI-based IDS for VANETs, revealing a significant lack of evaluations focused on practical deployment aspects. Building on these findings, this paper provides a comprehensive discussion of the challenges associated with the implementation and deployment of these systems. Ultimately, this study emphasizes the necessity for adaptive, lightweight, and robust AI-based IDS solutions to ensure effective real-time operation in vehicular networks.

Index Terms – VANETs, Intrusion Detection System, Machine Learning, Deep Learning, Computational Efficiency, Real-Time Latency, Resource-Constrained Systems.

1. INTRODUCTION

In today's world, maintaining road safety is crucial. According to a report by the World Health Organization (WHO)[1], approximately 1.19 million individuals lose their lives every year due to road traffic accidents. Several factors contribute to road accidents like driver drowsiness and lack of pre-warning for dangerous situations[2], [3]. Therefore, initiative must be taken to handle all these issues. VANETs emerge as a solution to this, as it is a network of vehicles[4] that exchange messages are known as Basic Safety Messages (BSM), which comprise position, speed, heading and acceleration[5].

Vehicles in vehicular environment are embedded with array of sensors and cameras to exchange vital information within the network[6]. This technology alerts the driver, enhancing road safety and efficiency. BSMs use the communication protocol defined by IEEE 802.11p and WAVE standards[7]. VANET scenario is presented in Figure 1.

It is essential to ensure security in VANETs, as they enable important real-time communication between vehicles and RSU. These networks' dynamic and decentralized behavior makes them vulnerable to different security attacks. While they offer many services to enhance road safety, the prevalence of cyberattacks has increased. As a result, strong security mechanisms are vital for identifying vulnerabilities. Solutions based on ML and DL have demonstrated promising outcomes in predicting intrusions and misbehavior. Given their exceptional accuracy in recognizing complex patterns within extensive datasets, AI/ML-based IDS[8] and MDS[9], [10] have garnered significant attention in academic circles over the past decade.

However, a considerable gap exists between theoretical research and practical deployment. Despite high accuracy scores, many proposed solutions have not considered computational and memory overhead, real-world feasibility and real-world prediction time[11], [12], [13], [14], [15]. These gaps raise a question.

SURVEY ARTICLE

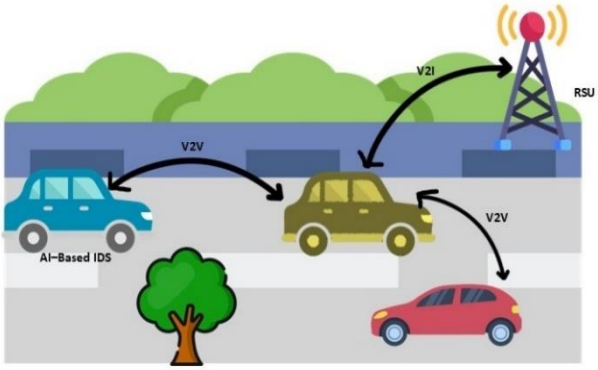

Figure 1 VANET Scenario

Have existing survey papers provided the necessary framework to guide the community toward more practical and deployable solutions?

To address this matter, we undertook a thorough review of survey papers published between 2018 and 2024. Our findings indicate that the existing surveys tend to exhibit a similar oversight. They primarily concentrate on taxonomies of attacks, learning models, and detection strategies. Few of them address these real-world constraints in the future scope or in general terms. Therefore, the objective of this survey is

- To develop a comprehensive taxonomy of VANET attacks.
- To conduct a systematic review and analysis of existing survey papers published between 2018 and 2024.
- To critically survey state-of-the-art AI-based IDS solutions for VANETs, evaluating their detection methods, computational requirements, real-time performance, and suitability for practical deployment in resource-constrained VANET scenarios.

To achieve the above objectives, following research questions are framed as

RQ 1: How do ML and DL techniques compare in terms of architecture, detection performance, and applicability for IDS in VANETs?

RQ2: What particular difficulties arise when implementing these AI-based IDS models in actual VANET environments?

RQ3: To what extent do existing AI-based IDS approaches meet the real-time latency, computational efficiency, and edge deployment feasibility required by practical VANET environments?

To answer the RQs and achieve the stated objectives, this work provides the following contributions that bridge the gap between theoretical analysis and practical deployment considerations.

- We systematically analyze the survey from 2018 to 2014 and revealed that most of them focus on AI techniques and very few pointed real-world challenges
- We surveyed state-of-the-art AI-based IDS for VANETs and evaluated them based on real-world parameters.
- Based on our analysis, we identify key research challenges and propose concrete future directions aimed at bridging the gap between theoretical research and practical implementation.
- Further, we give the future direction and design consideration for developing robust AI-based IDS for real-world operations.

To comprehensively evaluate AI-based IDS for VANETs, it is essential first to understand the diverse and evolving nature of security threats these networks face. VANETs are used in unpredictable and distributed settings, which leaves them vulnerable to cyberattacks that may harm the security of vehicles, their messages and users' privacy. So, the following section breaks down the main attack types affecting VANETs, organizing them using their characteristics and the possible damage they may cause. This attack classification serves as a foundation to analyse how existing AI-based IDS models address these threats effectively. The layout of the survey paper is illustrated in Figure 2.

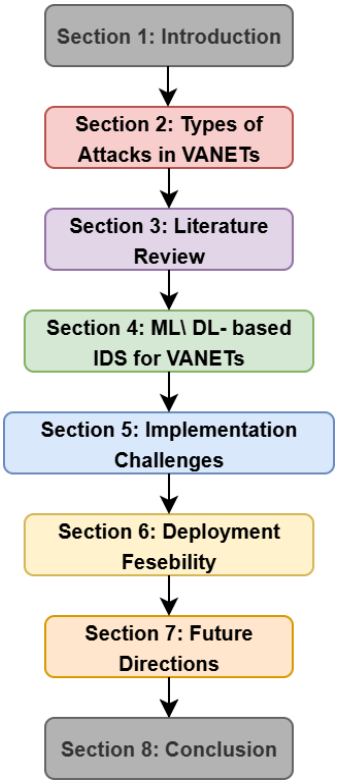

Figure 2 Roadmap of the Survey Paper

SURVEY ARTICLE

For complete comprehension, the study is structured as follows: Section 2 presents the types of attacks in VANET. Section 3 provides an elaborate literature review highlighting pertinent research that has shaped the current inquiry. Section 4 reviews the state-of-the-art AI-enabled IDS. Section 5 presents the implementation challenges of AI-based IDS. Section 6 provides the details of the deployment feasibility of IDS, and the following section gives the future direction.

2. TYPES OF ATTACKS IN VANET

VANETs face several security vulnerabilities due to their fundamental features, including dynamic topology, decentralized structure, and the use of wireless communication channels[4]. Understanding the nature and categories of these attacks is crucial for developing effective IDS[16], [17]. This section provides a detailed taxonomy of the principal attack types that target VANETs. This categorization is essential for comprehending the necessity and justification for IDS in safeguarding these networks. The classification provides a foundation for analyzing how AI-based IDS solutions detect and mitigate these threats. Attacks that are prevalent in VANET are picturized in Figure 3 and the impacts of these attacks and corresponding AI-based IDS are tabulated in Table 1.

Sybil Attack: This type of threat is considered one of the most hazardous attacks in VANET. In this scenario, a malicious node adopts several identities, which complicates the process of identifying whether the information comes from a reliable source or a harmful one. These numerous identities pose a considerable security threat to the network. An attacker can mislead other vehicles by fabricating the presence of different cars on the road or by transmitting false messages, such as alerts about traffic jams, incorrect route guidance, or misleading location data. This type of deception can severely disrupt the network and jeopardise the safety of passengers[18]. To address this challenge, several researchers have applied AI-based IDS approaches for VANETs. For example, the author in [19] utilised ML technique for sybil attack detection in VANET, whereas [20] used DL technique for detection. However, drawback with DL technique is that it has high computational overhead.

DoS Attack: This threat represents a significant risk to accessibility. Its main objective is to stop actual cars from utilizing the network's resources and services, rendering them inaccessible[21], [22]. It disrupts inter-communication channels, blocking interactions among legitimate vehicles, which is particularly problematic. Effective communication is crucial, especially in the life-critical safety services of VANET, where on-time prediction is vital to avert potential accidents[23]. Research has been conducted on AI-based IDS that utilize machine learning algorithms to detect Denial of Service (DoS) attacks [24] [25], [26]. However drawback with ML is that it struggles with huge real-world data[27].

Black Hole Attack: This threat occurs when vehicles drop packets or refuse to engage in communication, effectively creating a 'black hole' in the network[28]. This black hole is a destination for traffic rerouted to an unknown node. The perpetrator of such an attack presents itself as a node with the quickest path to the target by manipulating the routing protocol.

Rather than following the standard route discovery process, other nodes start to trust this fraudulent route, causing data packets to be intercepted by the malicious entity instead of reaching their intended destination. This packet loss can be leveraged to execute denial-of-service attacks or set the stage for subsequent man-in-the-middle attacks[17]. Authors in [29] various ML techniques to design IDS for preventing and detecting Blackhole attack in VANET.

Replay Attack: In this type of attack, an adversary sends out primarily transmitted messages to deceive other vehicular nodes in the network, effectively pushing legitimate priority messages out of the queue. This constant replaying not only diminishes the system's overall efficiency but also escalates bandwidth expenses[18], [30].

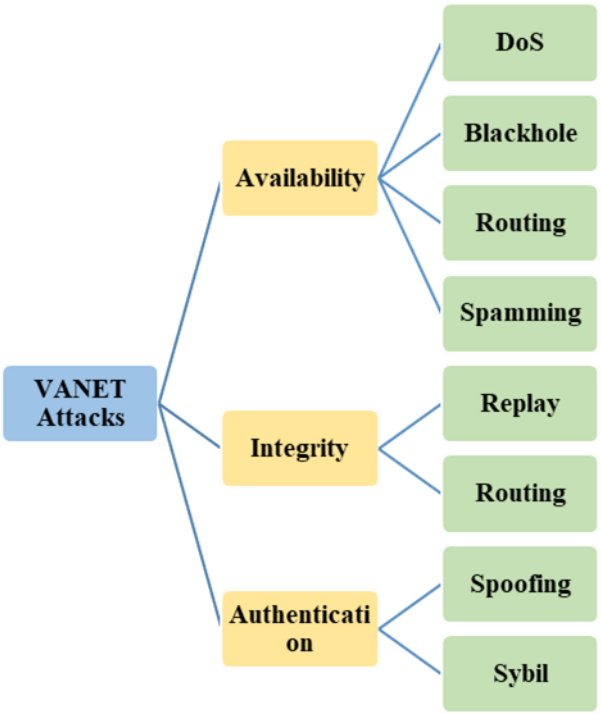

Figure 3 Security Attacks in VANETs

Spamming Attack: Spamming attacks occur when a hacker sends unwanted communications, such as ads, to users in an attempt to use bandwidth and cause deliberate collisions. The primary focus is to induce network congestion and delays, ultimately diminishing network performance. Managing this type of attack can be particularly challenging due to

SURVEY ARTICLE

centralized administration and insufficient foundational infrastructure[31].

Spoofing Attack: This is a passive attack where the perpetrator initially observes the communication patterns between the interacting nodes. Once they have gathered sufficient information, they interfere with the communication and access the data, using it to fulfil their objectives as necessary[32], [33].

Sinkhole Attack: The aim of this attack is to redirect the traffic of neighboring vehicles through malicious vehicles, allowing them to manipulate the information before sending it on. This technique can facilitate further attacks, including Grey Hole and Black Hole attacks[31].Authors in[34], [35] utilized ML techniques to detect Sinkhole attack.

Table 1 Impacts of VANET Attacks and Corresponding AI-Based Intrusion Detection Systems

Attack Type	Description	Impact	AI-based Detection Method	Pros of AI-based Detection Method	Cons of AI-based Detection Method
Sybil Attack	Fake identities injected[18]	False traffic data, congestion[18]	ML, DL[19], [20]	High detection accuracy, capable of capturing hidden patterns[19].	Requires large labelled datasets, high computational cost.
DoS Attack	Overload network and RSUs[23]	Service unavailability[21]	ML[24], [25]	ML are suitable for attack prevention and detection[26]	ML struggles with a massive amount of real-world data[27]
Spoofing Attack	Falsifying location and id[32]	Misdirects vehicles[33]	×	----	----
Replay Attack	Reusing valid messages[18]	System efficiency is affected, and bandwidth is increased[30]	×	----	----
Blackhole Attack	Malicious node drops packets[17]	Packet loss, communication disruption[28]	ML[29]	ML-based classification can identify malicious nodes that drop packets[29]	Requires labelled attack data for training, which may be hard to obtain.
Spamming Attack	Send excessive fake messages[31]	Congestion, delay[18]	×	----	----
Routing Attack	Alter routing information to mislead nodes[36]	Increases latency	×	----	----
Sinkhole Attack	Malicious node lures traffic by claiming best route[31]	Packet loss, false data, high delay, network disruption.	ML[34], [35]	High detection accuracy[34]	Need for a labelled dataset for training.

SURVEY ARTICLE

Routing Attack: This attack exploit vulnerabilities in VANET routing protocols to disrupt or manipulate message routing. This can result in packet loss, route diversions, or vehicle isolation from the network, compromising communication reliability and network connectivity[36]

The implications of these attacks are severe in vehicular environments, leading to the adoption of AI-based IDS for the detection of attacks within VANETs. Nonetheless, the implementation of AI-based IDS faces several challenges that must be addressed[27]. Therefore, it highlights the urgent need for effective Intrusion and Misbehaviour Detection Systems (IDS/MDS). This issue has led to many research studies, which are summarized in different survey papers. The following section will review these surveys to determine if they offer sufficient guidance for creating IDS/MDS that are both accurate and practical for addressing the real-world attacks mentioned earlier.

3. RELATED WORK

Several surveys have been conducted in recent years on AI-based IDS in VANETs. ML techniques have been studied by the researchers, which have shown significant results in identifying threats. Lately, the research paradigm has shifted from ML to DL based IDS, as it is good at learning complex patterns from vast volumes of data, while ML requires manual feature selection and often struggles with complex data. This section presents the survey of research papers that have been conducted in the past few years. Table 2 presents the study of the survey from 2018 to 2024.

Alia Mohammed Alrehan et al. concentrated their survey exclusively on the various types of DDoS attacks. However, their analysis did not address DL-based detection techniques, considerations regarding computational efficiency, or the challenges associated with real-time deployment [37].

The article by Mohammed Ali Al-Garadi et al. offers a detailed classification of ML and DL techniques relevant to IoT security, systematically reviewing their advantages, limitations, and applications across various IoT layers. While the authors identify key theoretical challenges and future research directions, including the integration of ML with edge computing and blockchain, the article falls short in evaluating the computational and memory overhead critical for resource-constrained IoT devices. Moreover, the discussion on real-world feasibility lacks concrete case studies and performance benchmarks to illustrate practical deployments [38].

Achref Haddaji et al. provides a thorough survey of AI techniques applied to the security of vehicular networks, categorizing approaches into ML, DL, reinforcement learning, and federated learning. The work offers a detailed taxonomy based on various dimensions, including technology, application level, usability, and temporal aspects. However, the discussion on computational and memory overhead considerations remains general, lacking specific performance evaluations. Additionally, while real-time prediction latency is acknowledged, it is not substantiated by empirical analysis. The exploration of real-world feasibility is presented conceptually, without concrete deployment studies or practical benchmarks [39].

Naqvi et al. conducted a systematic review of IDS in VANETs systematically classifying IDS architectures, detection methods, and attack types while providing a comparative analysis of recent research. However, the study does not assess the computational and memory overhead associated with these techniques, nor does it offer insights into real-world prediction times. While the authors address real-world feasibility in a conceptual manner, they do not include empirical benchmarks or practical deployment analyses, leaving important aspects of the topic unexplored [40].

Sowmya et al. presents a comprehensive review of AI-based IDS systematically classifying and comparing ML, DL and ensemble techniques in terms of accuracy, attack types addressed, and feature reduction strategies. The study highlights improvements in accuracy through feature reduction. However, the paper lacks a detailed assessment of computational and memory overhead, providing only general complexity categorizations without specific quantitative measurements. While the feasibility of real-world applications is discussed conceptually, there are no empirical case studies or deployment scenarios to support the findings, nor is there an experimental analysis of prediction times in practical, time-sensitive conditions [41].

Banafshehvaragh et al. conducted a comprehensive survey on IDS, focusing on signature-based, anomaly-based, and machine learning methodologies, including K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Decision Trees (DT), Clustering, AdaBoost, and Random Forest (RF). The authors highlighted several key challenges associated with these techniques, such as high training costs and durations, computational complexity, limited capacity to detect novel attacks, scalability issues in environments with an increasing number of vehicles, resource constraints, and difficulties in processing large volumes of data in real-time settings[42].

T. Nandy et al. conducted a comprehensive review of various security attacks and IDS techniques within VANETs. The study is particularly commendable for its well-structured taxonomy, systematic review methodology, and extensive coverage of available tools and datasets. However, it could be enhanced by incorporating critical performance comparisons, insights into real-world deployment, and in-depth analyses of emerging technologies. Additionally, the inclusion of more quantitative assessments, practical validation examples, and a

SURVEY ARTICLE

greater emphasis on standardization and adversarial robustness would further strengthen the findings [43].

The paper authored by Boualouache et al. provides a comprehensive systematic survey of ML-based misbehavior detection systems tailored for 5G and future vehicular networks. It presents an insightful taxonomy and thorough analysis from both security and ML perspectives. The work offers valuable insights into advanced concepts such as federated learning, reinforcement learning, and online learning, accompanied by lessons learned and recommendations for future research directions. However, certain aspects, such as computational and memory overhead, are discussed generally without specific empirical evaluation. Additionally, the considerations regarding real world prediction times and practical deployment feasibility are described in broad terms, lacking concrete benchmarks or case studies to support real-time implementation in vehicular contexts [44].

D. Man et al. present a comprehensive overview of AI-based intrusion detection methodologies for the Internet of Vehicles. However, the discussion surrounding aspects such as computational and memory overhead tends to remain at a high level, lacking specific measurements or evaluations of resource consumption in practical scenarios. Additionally, while real-world prediction time is recognized as a crucial performance metric, the absence of experimental benchmarks or latency analyses limits the substantiation of claims regarding low latency. The exploration of real-world feasibility is primarily positioned as an ongoing research challenge, with minimal investigation into actual deployment experiences or case studies that would demonstrate practical effectiveness under genuine IoV conditions[45].

Y.Zhong et al. provides valuable introductory review that effectively surveys the landscape of Sybil attack detection in ICVs using ML/DL. However, it lacks depth in critical evaluation, empirical analysis, and practical deployment considerations[46].

An analysis of existing surveys has identified several significant research gaps in the field. Many reviews either focus exclusively on ML-based IDS or limit their scope to specific attack types, such as Denial of Service (DoS) or Sybil attacks rather than in the entire spectrum of VANET attacks[37], [46]. While some studies touch on computational efficiency and resource overhead, they often lack in-depth evaluation and concrete benchmark [29] [30], [31]. Similarly, the acknowledgement of real-time latency's impact on system performance is discussed in general[39], [40], [41], [44]. These gaps highlight the need for focused research that connects theoretical insights with practical deployment challenges, particularly in developing lightweight, low-latency, and resource-efficient intrusion detection models for real-world vehicular environments.

Table 2 Various Surveys on IDS in VANET

Related Surveys	ML Techniques discussed	DL Techniques discussed	Computational and Memory Overhead Analysis	Real-Time Latency Consideration	Practical Deployment Consideration	Future Direction and Open Issues
Tarak Nandy et al.[43], 2024	--	CNN, DBN, ANN, RL	Discussed in broader terms	--	Discussed in broader terms	Concluded that further advancements are needed in achieving real-time threat detection.
Sowmya et al.[41], 2023	LR, DT, SVM, K-Means	CNN, RNN, LSTM, Autoencoders	--	Feasibility of real-time discussed conceptually	--	Investigating the viability of AI-based IDS for a broader variety of new threats in current cloud and network architectures.
S.T Banafshehvaragh et al.[42], 2023	KNN, SVM, DT, Clustering, Adaboost, RF	--	The cost and duration of training continue to be significant obstacles in detection techniques.	--	--	Computational complexity, effective detection of new attacks, scalability with growing numbers of vehicles, resource limits, high-volume data processing.

SURVEY ARTICLE

Abdelwahab Boualouache et al.[44], 2023	NB, LR, SVM, KNN, RF, AdaBoost, DT, Ensemble learning	CNN, RNN, LSTM, GRU and Autoencoders	--	Discussed in broader terms	--	Highlights several areas that require further research, including the lack of datasets designed explicitly for vehicular networks, challenges in mitigating the adversarial attacks and the constraints posed by inference latency limitations.
Dapeng Man et al.[45], 2023	K-NN, SVM, RF, Decision Tree, XGBoost	ANN, DBN, CNN, RNN, LSTM, GAN	--	Discussed in broader terms	--	Concluded that there are challenges including balancing detection accuracy and latency, ensuring privacy protection, handling adversarial attacks, and managing resource constraints in real-time vehicular environments.
Yongchao Zhong et al.[46], 2023	NB, DT, SVM, LR	CNN, LSTM	Identifies real world constraints, observes that DL techniques may demand substantial computational resources for both training and inference.	--	--	Future directions include improving model flexibility and generalizability in dynamic vehicular situations by utilizing adaptive and transfer learning to overcome issues with data quality and diversity
Achref Haddaji et al.[39], 2022	LR, DT, SVM, K-Means, NB	RNN, CNN, LSTM	--	--	--	Highlights the challenges associated with AI-based techniques which includes real time processing constraints.
Ila Naqvi et al.[40], 2022	RF, XGBboost, and SVM algorithms	CNN, LSTM	--	Discussed in broader terms	--	--
Mohammed Ali Al-Garadi et al.[38], 2020	DT, SVM, NB, KNN, RF, K-means, PCA	CNN, RNN, AE, DBN, GAN	Highlights the fact that ML and DL model needs significant memory, but devices in IoT have limited resources.	Acknowledge the real-time latency in broader terms.	--	Points out the necessity to create ML and DL frameworks that effectively lower computational complexity.

SURVEY ARTICLE

Alia Mohammed Alrehan et al.[37], 2019	SVM, NB, Adaboost	--	--	--	--	Highlights the need to use simulation to create datasets unique to VANETs.
Our Survey	✓	✓	✓	✓	✓	✓

4. SURVEY OF ML AND DL BASED IDS APPROACHES

Building upon the insights gained from analyzing existing survey works, this section discusses the state-of-the-art AI-based IDS for VANET environments. It presents a detailed review of recent ML and DL approaches, highlighting their architectures, targeted attack types, and performance metrics.

This comprehensive analysis aims to answer the first research question RQ1:

How do ML and DL techniques compare in terms of architecture, detection performance, and applicability for IDS in VANETs?

4.1. ML-Based IDS for VANETs

ML techniques are often used as a base for creating IDS in VANETs because they don't need as much processing power or memory as other methods. This subsection surveyed recently developed IDS for VANETS focused on significant metrics. Table 3 presents the state-of-the-art ML-based IDS for VANETs.

Table 3 Survey on State-of-the-art ML-Based IDS for VANET

Ref No.	Year	Model	Accuracy (In Percentage)	Computational Efficiency
R. Dineshkumar et al.[47]	2024	GLM	99.82 %	×
U. Garg et al.[48]	2021	RF	84 Precision, 82 Recall, 82 F1-score,	×
M.Injadat et al.[49]	2021	RS-KNN	99.7	This paper has computed complexity using a priori analysis, still room for a posteriori analysis.
A.R. Gad et al.[50]	2021	XGBoost	98.20	--
Y.Gao et al.[51]	2019	RF	99.9	×
Y.Gu et al.[52]	2019	K-Means	99.59 Recall	✓

Dineshkumar et al. proposed a novel IDS architecture based on a stacking ensemble ML framework to detect position falsification attacks to VANETs. A stacking ensemble strategy is used where three base classifiers, Decision Tree (DT), Random Forest (RF) and XGBoost, are combined to provide their outputs to a Generalized Linear Model (GLM) meta classifier.

By extracting the positional features from the VeReMi dataset, especially the vehicle location broadcast anomalies, an approach is proposed. Decentralized inference is supported for the vehicle level, while the training is centralized at the higher layer of infrastructure nodes.

They obtain high classification performance (99.82% accuracy, 97.56% recall, 97.28% F1-score), and the model outperforms baseline models, including Logistic Regression and Naive Bayes[47].

U.Garg et al. offers a mixture of semi-supervised ML, allowing unsupervised and supervised learning to reduce false positives but still keep up detection of DDoS attacks. This approach involves first checking network entropy, then analyzing information gain, and finally using spectral co-clustering on network traffic to produce three clusters such as benign, anomalous, and unclassified. The unsupervised part of the system spots and eliminates unimportant regular traffic to decrease noise in the classification task. The supervised part relies on Random Forest (RF) to correctly classify DDoS traffic with the improved dataset. The entropy and DDoS attack detection in the NSL-KDD dataset are carried out by examining the source and destination byte amounts from the FSD features[48].

Mohammad Noor Injadat et al. proposed a multi-stage ML-NIDS architecture that incorporates data preprocessing,

SURVEY ARTICLE

selects the most relevant features, and optimises the hyperparameters to address complexity and enhance threat detection. During preprocessing, Z-score normalisation and SMOTE help even out the distribution of features and make each class have the same number of training samples. Therefore, Information Gain and Correlation-Based Feature Selection techniques are chosen to reduce the number of features while keeping the important ones. In the final step, Random Search, PSO, GA, and Bayesian Optimization are employed to fine-tune parameters of KNN and Random Forest, making sure the trade-off between accuracy and performance is proper[49].

A R Gad et al. discuss an IDS for VANETs designed with machine learning technique and the ToN-IoT dataset. The goal is to improve detection against current attacks that traditional datasets, such as NSL-KDD and KDD-CUP99 cannot cover. Before using the Chi-square (Chi2) technique for selecting features, the framework requires extensive preparation of the data, such as filling in missing data, encoding categorical values, and normalising the data. The SMOTE technique is mainly used to deal with the issue of imbalanced classes, reducing the influence of the majority classes. The study investigates the efficiency of Logistic Regression, Naive Bayes, Decision Tree, k-NN, SVM, Random Forest, AdaBoost, and XGBoost algorithms for both binary and multi-class classification. To judge the effectiveness of the model, it is assessed with measures like accuracy, precision, recall, F1-score, and FPR, mainly focusing on choosing the best features[50].

Ying Gao et al. presents a solution for detecting DDoS attacks in vehicle networks by using a big data approach consisting of Apache Spark and Random Forest (RF). There are two main components to the architecture: A Network Traffic Collection Module that uses micro-batch processing to save network packets into the Message Queue system, and a Network Traffic Detection Module that identifies anomalies using statistical and basic packet features collected from the files in the Message Queue. The Spark-ML RF algorithm handles detailed vehicle data sets by using parallel processing to ensure both speed and accuracy. The detection accuracy on NSL-KDD reached 99.95%, and on UNSW-NB15, it was 98.75%, with FAR (false matches) of 0.05% and 1.08%. [51].

Yonghao Gu et al. proposed a framework that introduces a way to set up a network that keeps an eye out for DDoS attacks on VANETs by combining Apache Spark's big-data features with a Random Forest (RF) classifier. Performance evaluation was done with the NSL-KDD and UNSW-NB15 data, getting 99.95% and 98.75% accuracy, respectively. Although the framework works well at picking up data accurately, it focuses more on handling large amounts of data than looking at how quickly the calculations work. Critical parameters like how long it takes to run tests, how many parameters there are, and how much memory is needed are not clearly shown, which shows there's still room for research on how much extra work RF adds when there are a lot of vehicles in a VANET[52].

From the above analysis of the state-of-the-art ML-based IDS for VANET, very few have discussed computational efficiency[49], [52]. At the same time, the rest have focused on the detection accuracy of the threat.

4.2. DL-Based IDS for VANETs

DL techniques are effective for handling complex and large volumes of real-time data. Thus, the paradigm has shifted from ML-based IDS to DL based IDS in recent years. Table 4 presents the survey of the state-of-the-art DL-based IDS for VANETs.

Preetam Suman et al. propose an I-LeeNet IDS framework for VANETs with enhanced DL that integrates convolutional neural networks (CNN) and Adaptive neuro-fuzzy inference systems (ANFIS) that effectively detect both known and unknown attacks. Finally, the proposed framework is assessed using three datasets from i-VANET, ToN-IoT and CIC 2017 IDS, with different attack scenarios. For this purpose, the UIDS module utilizes CNN layers for feature extraction and ANFIS for adaptive learning that can detect known and unknown attacks via multi-layer processing[11].

According to S. Bayan, a DL-based system was developed and trained utilizing messages and GPS readings obtained from the VeReMi dataset. The Position Falsification Detection System (PFDS) demonstrates reduced complexity while enhancing accuracy, establishing itself as superior to previously existing position falsification intrusion detection systems [53].

Table 4 Survey on State-of-the-Art DL-Based IDS for VANETs

Ref No.	Year	Model	Accuracy (In Percentage)	Computational Efficiency
Suman P et al.[11]	2024	I-LeeNet	96.66(CIC-IDS) 97.75(ToN-IoT)	×
S.Bayan et al.[53]	2024	MLP	90.74	✓

SURVEY ARTICLE

Tejasvi Alladi et al.[10]	2023	CNN, LSTM	99.3	×
Y.Otoum et al.[12]	2022	Transfer Learning, CNN and DNN	97.96	×
Tejasvi Alladi et al.[54]	2021	LSTM, CNN	98.6	✓
G.Andresen et al.[13]	2020	Autoencoder, CNN	97.90	×
A.Rosay et al.[14]	2020	FNN	99.46	×
A.S Almogren et al.[15]	2019	DBN	85	×
Y.Zhang et al.[55]	2019	DBN	99.45 (DoS Attack), 97.78(R2L), 99.37(Probe), 98.68(U2R)	×

Tejasvi Alladi et al. develop a DL based Misbehaviour Classification Scheme for Intrusion Detection in Cooperative ITS utilising CNN and LSTM. To evaluate detection accuracy and prediction latency, the models are assessed in both an edge computing platform, Nvidia Jetson Nano and Raspberry Pi 3B and different combinations of CNN-LSTM and LSTM architectures are tested to determine the best fit for real-time deployment in VANETs[10].

Yazan Otoum et al. show how knowledge transfer between two benchmark datasets, namely CICIDS2017 and CSE-CIC-IDS2018 can be leveraged to infer an Internet of Vehicles (IoV) intrusion detection framework based on an identified set of Transfer Learning (TL) techniques. A global model is then created by using Deep Neural Networks (DNN) and CNN on the source domain (CICIDS2017) and is adapted to the target domain (CSE-CIC-IDS2018) using transfer learning.

A layer freezing technique is introduced within the architecture, freezing the top layers that encode generic features to retain previously learned knowledge, while fine-tuning the deeper layers to learn specific patterns in the target dataset. This reduces training time and computational cost of transferring knowledge, while maintaining high detection accuracy [12].

Tejasvi Alladi et al. proposed a DL-based IDS for Internet of Vehicles (IoV) based on CNN and LSTM to classify traffic as either benign or malicious. To evaluate the feasibility of deploying IDS based on DL models in resource-constrained environments, DL models are deployed on edge computing devices such as Nvidia Jetson Nano and Raspberry Pi 3B [54].

Giuseppina Andresini et al. presents a new Multi-Channel Deep Feature Learning (MINDFUL) method for Intrusion Detection in Network systems that fuses information from autoencoders and convolutional neural networks (CNNs) with multi-channel features. The proposed MINDFUL framework is evaluated using three benchmark datasets: KDDCUP99, UNSW-NB15, and CICIDS2017, demonstrating improved detection accuracy when compared to baseline IDS architectures and other state-of-the-art approaches[13].

Arnaud Rosay et al. present an IDS based on Feed-Forward Neural Network (FFNN) for vehicular networks to detect network intrusions using the dataset of CICIDS2017. The work has demonstrated significant accuracy, whereas the recall of the majority class is biased, as the dataset is imbalanced[14].

A.S. Almogren et al. proposed, a Deep Belief Network (DBN) based IDS optimized for Edge-of-Things (EoT) . The system can perform processing and intrusion detection at the edge layer with an efficient architecture. The architecture consists of three stages as follows: data collection, feature extraction and classification.

A Restricted Boltzmann Machine (RBM) is stacked to construct the Deep Belief Network (DBN) and trained using

SURVEY ARTICLE

Contrastive Divergence (CD) to learn hierarchical representations of network traffic patterns. This work has achieved the accuracy of 85% [15].

Yan Zhang et al. propose an intrusion detection framework based on a DBN optimized using an Improved Genetic Algorithm (IGA) to dynamically adapt the IDS architecture for different attack types in IoT environments. The proposed system is evaluated using the NSL-KDD dataset, where each type of attack is trained with a different DBN configuration derived from the GA. This multi-model adaptive approach aims to improve classification performance per attack class, with a focus on model adaptability and classification strength across distinct intrusion behaviors[55]. From the reviewed literature, it is evident that various ML and DL models have demonstrated high accuracy in detecting VANET-specific attacks. However, despite impressive detection capabilities, many studies fall short of providing a holistic view of their computational demands or feasibility in real-world vehicular scenarios. It is typically challenging to deploy full AI models (such as DL models) on the Edge device due to hardware limitations; either the model's size is too big, or the computing demands are too severe[56]. Most existing intrusion detection approaches either omit computational complexity analysis or rely solely on theoretical estimations without empirical validation. Furthermore, there is a noticeable gap in evaluating the practical deployability of these models on resource-constrained edge devices such as OBUs and RSUs, which possess limited processing power, memory, and energy budgets[57].

This gap in practical applicability motivates a deeper exploration of real-world implementation and deployment challenges, which are addressed in the following sections and picturized in Figure 4.

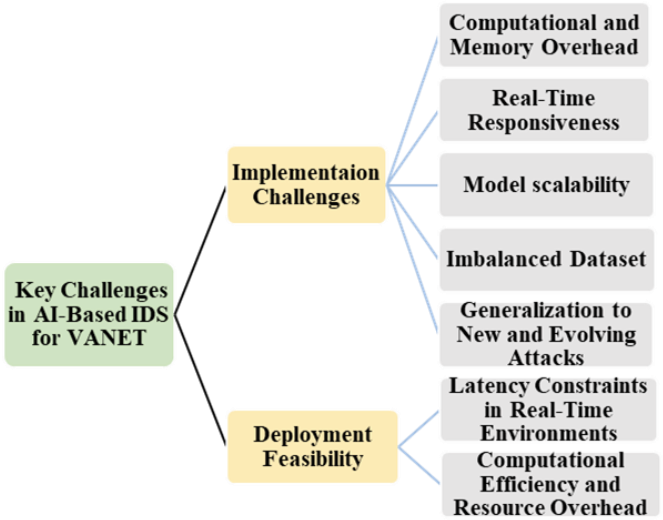

Figure 4 Key Challenges in AI-Based IDS for VANET

5. IMPLEMENTATION CHALLENGES IN AI-BASED IDS FOR VANET

A systematic and comprehensive review of recent survey papers on AI-based IDS for VANET has revealed a set of critical implementation challenges. These challenges represent fundamental barriers that hinder the transition of IDS models from theoretical research to practical deployment within real-world vehicular networks. The identification of these specific parameters is grounded in consistent observations across multiple surveys, where recurring limitations were either explicitly articulated or implicitly indicated as open research gaps. These challenges directly align with our second research question, RQ2:

What particular difficulties arise when implementing these IDS models in actual VANET environments?

5.1. Computational and Memory Overhead

The computational and memory complexity of AI models remains one of the foremost challenges in implementing IDS for VANET environments. Authors in[42] highlighted that most advanced AI algorithms, particularly deep learning require intensive computational resources for training and inference, making them impractical for resource-constrained devices such as On-Board Units (OBUs) and Road Side Units (RSUs). And the authors in [38]emphasized the need to create ML and DL frameworks that specifically optimize computational complexity to fit into vehicular hardware, which typically lacks powerful GPUs or large memory capacity. Hence, computational and memory overhead analysis is essential to evaluate whether the models can operate in constrained VANET environments without impacting vehicle performance or safety-critical tasks.

5.2. Real-Time Responsiveness

Real-time responsiveness encompasses the capability of the IDS to swiftly analyze incoming data from vehicular networks and identify potential intrusions within a stringent temporal framework, typically within milliseconds[58]. This prompt analysis is essential for facilitating timely threat mitigation efforts. Tarak Nandy et al.[43] emphasized the necessity for further advancements to achieve real-time threat detection in highly dynamic VANETs. Additionally, Authors in [39] highlighted that current AI-based IDS solutions predominantly concentrate on offline analysis or are evaluated in simulated, static environments, neglecting the analysis of actual prediction latency.

The challenge is heightened by the rapid pace of vehicular communication, wherein V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure) messages are transmitted at intervals of only a few milliseconds. Failure to meet real-time requirements can lead to system delays, undermining the effectiveness of IDS in critical applications such as collision

SURVEY ARTICLE

avoidance and autonomous driving. Notably, many of the reviewed studies do not provide empirical latency benchmarks such as average inference times and maximum allowable delays which underscores a significant gap in addressing real-time responsiveness effectively.

5.3. Model Scalability

Scalability becomes a significant challenge as VANET networks rapidly grow in size, involving hundreds or thousands of vehicles communicating simultaneously. Authors in [42] pointed out the difficulties in maintaining IDS performance as the number of vehicles increases. Specifically, high-volume data streams, along with dynamic topology and high node mobility, lead to substantial increases in data throughput and processing complexity.

Current models often operate on small-scale datasets or simulations representing a limited number of nodes, and their performance on large-scale vehicular networks remains untested. Scalability involves ensuring that the IDS model can sustain low false alarm rates, high detection accuracy, and efficient resource usage when handling massive concurrent vehicular communications, which is rarely evaluated in prior work.

In particular, the challenge lies in analyzing extensive data flows while mitigating latency to meet real-time requirements. Therefore, future research should focus on developing scalable IDS architectures that can adapt to the growing demands of VANETs, incorporating advanced algorithms and architectures that efficiently process large datasets while preserving critical performance metrics. Addressing these scalability issues is essential for the practical deployment of AI-based IDS solutions in real-world VANET scenarios.

5.4. Imbalanced Dataset

A common issue in anomaly-based IDS is the class imbalance problem, where instances of attacks represent a small fraction of the overall traffic compared to normal behaviour. Authors in [37] [59]highlighted the necessity of creating simulation-based datasets specifically for VANET, given that existing public datasets often lack diversity in attack types and do not accurately represent realistic traffic conditions in VANET environments.

Imbalanced datasets can lead to biased models that overfit on majority classes, significantly impairing the model's ability to detect rare yet critical attacks[60]. Although techniques like the Synthetic Minority Over-sampling Technique (SMOTE)[61] are occasionally employed to address this issue, there remains a notable absence of standardized or realistic dataset generation frameworks that encapsulate the true distribution of vehicular network behavior. This gap hinders the development of robust intrusion detection mechanisms capable of accurately identifying sophisticated attack vectors that threaten the integrity and safety of VANETs.

5.5. Generalization to New and Evolving Attacks

Generalization is a critical attribute of IDS, signifying their capability to identify new or previously unseen attack patterns. Most of IDS employ supervised learning on datasets that identify the types of attacks[62], [63] . Because of this, they have difficulty noticing both unknown and evolving threats. Since most frameworks overlook transfer learning, few-shot learning, and unsupervised anomaly detection, applying them in real-world settings is beneficial for zero-day attack[64]. Authors in [45] highlighted that numerous AI-based IDS models are often developed using static datasets, which limits their effectiveness in dynamically evolving vehicular environments. Whereas authors in[46] proposed the use of transfer learning and adaptive learning techniques as promising solutions to enhance model generalizability.

In summary, while AI-based IDS have demonstrated encouraging detection capabilities in experimental settings, there exist some challenges with the implementation of these models as discussed. Therefore, there is a need to bridge the gap between theoretical research and practical implementation challenges.

6. DEPLOYMENT FEASIBILITY OF AI-BASED IDS FOR VANET

As vehicular networks evolve towards real-time, safety-critical environments, the deployment of AI-based IDS must go beyond theoretical performance to address stringent operational constraints. While previous sections have examined architectural advancements and implementation barriers, this section focuses on the practical feasibility of deploying these models within the computationally constrained and latency-sensitive context of VANETs. This section examines core deployment challenges related to inference latency, computational efficiency, and edge-device compatibility, particularly in OBUs and RSUs. The analysis aligns with (RQ3):

To what extent do existing AI-based IDS approaches meet the real-time latency, computational efficiency, and edge deployment feasibility required by practical VANET environments?

6.1. Latency Constraints in Real-Time Environments

Because of the critical importance in safety, real-time vehicle networks (VANETs) require systems to be react fast, typically within a few milliseconds[65]. A failure to notice or decide on a problem quickly may result in major catastrophes. In the example of Uber’s 2018 AV crash illustrated by A.F Cooper et al.[66], the vehicle stopped at the first sign of danger but did not know what to do afterward for over six seconds, leading to an accident that caused someone’s death. The

SURVEY ARTICLE

reason for failure was not only the constraint of the sensors, but that the system could not handle uncertainty and act within the proper time[67]. This case highlights the need to strike a balance between accuracy and efficiency in areas where time is critical and mistakes can be hazardous. So, these systems for detecting threats in VANETs ought to support both fast inference and exact detection results, mainly when they run on edge devices with limited computing capabilities.

The Table 5 below presents a comparative overview of recent AI-based IDS approaches in VANET research with consideration of important parameters like latency and memory overhead. While most studies report high detection accuracy, very few provide latency measurements or memory overhead details both of which are essential for assessing real-time deployment feasibility on OBUs or edge devices. For example, work done in [8] achieves a latency of just 14.29 ms, making it relatively more viable for real-time applications. In contrast, [68] reports 1.34 seconds, which is far too high for safety-critical vehicular scenarios. Several works [69], [70], [71] have not talked about computational efficiency parameters.

This gap in the literature suggests that, while many IDS models demonstrate strong classification performance in experimental settings, their practical applicability to VANET environments may be limited due to insufficient consideration of end-to-end latency and resource constraints.

Table 5 Ccomparative Overview of Recent AI-Based IDS in VANET

Ref.	Accuracy	Latency	Memory Overhead	Dataset
[10]	99.63%	288.07 ms	------	Veremi Extension
[68]	98.5%	1.34 sec	16295 MB	i-VANET
[8]	99.65%	14.29 ms	------	Veremi Extension
[69]	97.76%	------	------	NSL-KDD
[70]	99.5%	------	------	Veremi
[71]	90.02%	------	------	NSL-KDD

6.2. Computational Efficiency and Resource Overhead

Edge devices primarily handle communication and processing tasks in VANETs. Usually, they do not have much RAM, not many CPU/GPU cycles, and must work under strict energy rules. Considering that huge data streams from VANETs must be handled by real-time intrusion detection for safe and joint driving, the IDS put on these nodes must work efficiently and be able to predict problems instantly.

Besides OBUs and RSUs, a wide range of edge devices, like Raspberry Pi[72], NVIDIA Jetson Nano[73], and MediaTek Helio G8[74] are also typically used for real-time processing of data and detecting possible attacks in VANET systems. Comparative overview of standard edge devices for DL-Based IDS deployment is presented in Table 6. While these devices are both cheaper and more accessible, they lack powerful computing and have less memory, a slower processing speed, and must consume less energy. Thus, they do not handle well the big numbers of parameters and FLOPs needed by orderly DL models.

Abir Mchergui et al.[75] illustrated that CNNs have high computational overheads. Therefore, deploying them in resource-constrained environments is challenging. To deal with these issues, one should use techniques such as model pruning, quantization, and knowledge distillation as well as design architectures that are efficient and accurate. Such methods allow intelligent IDS to be built for OBUs, RSUs, and edge devices that perform reliably and respond quickly.

Table 6 Comparative Overview of Standard Edge Devices for DL-Based IDS Deployment

Edge Device	CPU	RAM	Form
Jetson Nano (4GB)[73]	Quad-core ARM Cortex-A57	4GB	System on Module
Raspberry Pi 4 (8GB)[72]	Quad-core Cortex-A72 @ 1.5GHz	8GB	Single Board Computer
Hailo-8 Evaluation Board[74]	Host-dependent CPU (External)	Depends on Host	System on Module

7. DISCUSSIONS AND FUTURE RESEARCH DIRECTIONS

The development of AI-based IDS for VANETs has proved to be promising because of better results and flexibility. Nonetheless, there are major issues that need to be addressed to put machine learning into real-life use. According to our survey findings and noticing existing model limitations, we believe this future research subjects should be considered:

7.1. Lightweight and Resource-Efficient Architectures

Current IDS models, particularly DL-based, are computationally intensive and exceed the processing capabilities of OBUs and RSUs. Future research should focus

SURVEY ARTICLE

on designing quantized[76] or efficient neural architectures that maintain detection accuracy while ensuring real-time execution on constrained edge devices. Techniques such as knowledge distillation[77], neural architecture search (NAS), and model splitting across edge–cloud hierarchies offer promising pathways to achieving lightweight and deployable IDS solutions for VANET environments.

7.2. Standardized Benchmarks and Realistic Datasets

Many studies rely on non-representative datasets, which limits reproducibility and generalization. The development of standardized, large-scale, labeled datasets that reflect real-world VANET conditions, including attack scenarios, mobility patterns, and environmental noise is essential. Simulators like Veins, SUMO[78], and NS-3[79], integrated with GAN[80], [81] aid in constructing such datasets.

7.3. Explainability and Trustworthiness

AI models working in important transport domains like VANETs should be transparent and dependable. Using XAI methods in IDS can assist in seeing what factors cause the system to decide, detect false positives and make users trust the system. Very few efforts have been made to make explainable AI work in real-time systems[82].

8. CONCLUSION

This paper provides a detailed survey of AI-based IDS specifically designed for VANET, focusing on the application of ML and DL techniques for detecting threats. The study evaluates existing surveys based on key technical aspects, including computational and memory requirements, real-time performance, practical deployment challenges, and future research directions. The analysis reveals that most current surveys and solutions tend to prioritize improving detection accuracy in simulated settings. However, they often overlook practical considerations such as computational efficiency, responsiveness in real-time situations, and the feasibility of deployment in real-world scenarios. Based on the insights gained from the literature review, this paper highlights several significant challenges in implementing these systems. These include issues with scalability, dealing with imbalanced datasets, adapting to new types of attacks, meeting real-time inference demands, and ensuring model robustness against adversarial threats. The paper also examines deployment issues, such as hardware limitations, a lack of realistic datasets, delays in inference, and the need for system interoperability. In conclusion, the study emphasizes the need for ongoing research to develop adaptive, lightweight, and robust AI frameworks that can effectively operate in the fast-paced and resource-limited environment of VANETs. Future efforts should focus on testing real-time performance, creating standardized and realistic datasets, improving the generalization of models, and incorporating privacy-preserving techniques to enable the practical and secure use of AI-based IDS in real vehicular networks.

REFERENCES

[1] “Road traffic injuries.” <Accessed: Feb. 17, 2025>. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries.

[2] Md. Ebrahim Shaik, “A systematic review on detection and prediction of driver drowsiness,” Transp. Res. Interdiscip. Perspect., vol. 21, p. 100864, Sep. 2023, doi: 10.1016/j.trip.2023.100864.

[3] T. Bliss and J. Breen, “Meeting the management challenges of the Decade of Action for Road Safety,” IATSS Res., vol. 35, no. 2, pp. 48–55, 2012, doi: https://doi.org/10.1016/j.iatssr.2011.12.001.

[4] Y. Toor, P. Muhlethaler, A. Laouiti, and A. La Fortelle, “Vehicle Ad Hoc networks: applications and related technical issues,” IEEE Commun. Surv. Tutor., vol. 10, no. 3, pp. 74–88, 2008, doi: 10.1109/COMST.2008.4625806.

[5] G. Francia, D. Snider, and B. Cyphers, “Basic Safety Message (BSM) Test Data Generation for Vehicle Security Machine Learning Systems,” in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Las Vegas, NV, USA: IEEE, Jul. 2023, pp. 2515–2520. doi: 10.1109/CSCE60160.2023.00404.

[6] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. In Kim, “Mobility and handoff management in vehicular networks: a survey,” Wirel. Commun. Mob. Comput., vol. 11, no. 4, pp. 459–476, Apr. 2011, doi: 10.1002/wcm.853.

[7] S. S. Manvi and S. Tangade, “A survey on authentication schemes in VANETs for secured communication,” Veh. Commun., vol. 9, pp. 19–30, Jul. 2017, doi: 10.1016/j.vehcom.2017.02.001.

[8] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, “Artificial Intelligence (AI)-Empowered Intrusion Detection Architecture for the Internet of Vehicles,” IEEE Wirel. Commun., vol. 28, no. 3, pp. 144–149, Jun. 2021, doi: 10.1109/MWC.001.2000428.

[9] R. Sultana, J. Grover, J. Meghwal, and M. Tripathi, “Exploiting machine learning and deep learning models for misbehavior detection in VANET,” Int. J. Comput. Appl., vol. 44, no. 11, pp. 1024–1038, Nov. 2022, doi: 10.1080/1206212X.2022.2099122.

[10] T. Alladi, V. Kohli, V. Chamola, and F. R. Yu, “A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems,” Digit. Commun. Netw., p. S2352864822001407, Jul. 2022, doi: 10.1016/j.dcan.2022.06.018.

[11] P. Suman et al., “An Improved Deep Learning-Based Intrusion Detection for Reliable Communication in VANET,” IEEE Trans. Consum. Electron., pp. 1–1, 2024, doi: 10.1109/TCE.2024.3475823.

[12] Y. Otoum, Y. Wan, and A. Nayak, “Transfer Learning-Driven Intrusion Detection for Internet of Vehicles (IoV),” in 2022 International Wireless Communications and Mobile Computing (IWCMC), May 2022, pp. 342–347. doi: 10.1109/IWCMC55113.2022.9825115.

[13] G. Andresini, A. Appice, N. D. Mauro, C. Loglisci, and D. Malerba, “Multi-Channel Deep Feature Learning for Intrusion Detection,” IEEE Access, vol. 8, pp. 53346–53359, 2020, doi: 10.1109/ACCESS.2020.2980937.

[14] A. Rosay, F. Carlier, and P. Leroux, “Feed-forward neural network for Network Intrusion Detection,” in 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, May 2020. doi: 10.1109/VTC2020-Spring48590.2020.9129472.

[15] A. S. Almogren, “Intrusion detection in Edge-of-Things computing,” J. Parallel Distrib. Comput., vol. 137, pp. 259–265, Mar. 2020, doi: 10.1016/j.jpdc.2019.12.008.

[16] M. Aloqaily, S. Otoum, I. A. Ridhawi, and Y. Jararweh, “An intrusion detection system for connected vehicles in smart cities,” Ad Hoc Netw., vol. 90, p. 101842, Jul. 2019, doi: 10.1016/j.adhoc.2019.02.001.

[17] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges,”

SURVEY ARTICLE

Telecommun. Syst., vol. 50, no. 4, pp. 217–241, Aug. 2012, doi: 10.1007/s11235-010-9400-5.

[18] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent Advances in VANET Security: A Survey," in 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Sep. 2015, pp. 1–7. doi: 10.1109/VTCFall.2015.7391111.

[19] A. Balaram, S. A. Nabi, K. S. Rao, and N. Koppula, "Highly accurate sybil attack detection in vanet using extreme learning machine with preserved location," Wirel. Netw., vol. 29, no. 8, pp. 3435–3443, Nov. 2023, doi: 10.1007/s11276-023-03399-1.

[20] R. Sultana, J. Grover, M. Tripathi, M. S. Sachdev, and S. Taneja, "Detecting Sybil Attacks in VANET: Exploring Feature Diversity and Deep Learning Algorithms with Insights into Sybil Node Associations," J. Netw. Syst. Manag., vol. 32, no. 3, p. 51, May 2024, doi: 10.1007/s10922-024-09827-7.

[21] A. Rawat, S. Sharma, and R. Sushil, "VANET: Security Attacks and its Possible Solutions," vol. 3, no. 1, 2012.

[22] A. M. Malla and R. K. Sahu, "Security Attacks with an Effective Solution for DOS Attacks in VANET," Int. J. Comput. Appl., vol. 66(22), 2013.

[23] Z. A. Abdulkader, A. Abdullah, M. Taufik Abdullah, and Z. Ahmad Zukarnain, "Vehicular Ad Hoc Networks and Security Issues: Survey," Mod. Appl. Sci., vol. 11, no. 5, p. 30, Apr. 2017, doi: 10.5539/mas.v11n5p30.

[24] N. Kadam and R. S. Krovi, "Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET," Int. J. Adv. Comput. Sci. Appl., vol. 12, Jan. 2021, doi: 10.14569/IJACSA.2021.0120782.

[25] N. Ahmed, F. Hassan, K. Aurangzeb, A. H. Magsi, and M. Alhussein, "Advanced machine learning approach for DoS attack resilience in internet of vehicles security," Heliyon, vol. 10, no. 8, Apr. 2024, doi: 10.1016/j.heliyon.2024.e28844.

[26] X. Luo, D. Li, Y. Yang, and S. Zhang, "Spatiotemporal Traffic Flow Prediction with KNN and LSTM," J. Adv. Transp., vol. 2019, no. 1, p. 4145353, 2019, doi: 10.1155/2019/4145353.

[27] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," SN Comput. Sci., vol. 2, no. 3, p. 160, Mar. 2021, doi: 10.1007/s42979-021-00592-x.

[28] V. H. La and A. R. Cavalli, "Security attacks and solutions in Vehicular Ad Hoc Networks: a survey," Int. J. AdHoc Netw. Syst. IJANS, vol. 4, no. 2, pp. 1–20, Apr. 2014, doi: 10.5121/ijans.2014.4201.

[29] B. Shabbar, "Detection of blackhole and DDoS attack in 5g VANET using multiple machine learning algorithms," masters, Dublin, National College of Ireland, 2024. Accessed: Sep. 08, 2025. [Online]. Available: https://norma.ncirl.ie/8370/.

[30] Y. Sun et al., "Attacks and countermeasures in the internet of vehicles," Ann. Telecommun., vol. 72, no. 5, pp. 283–295, Jun. 2017, doi: 10.1007/s12243-016-0551-6.

[31] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," Veh. Commun., vol. 20, p. 100182, Dec. 2019, doi: 10.1016/j.vehcom.2019.100182.

[32] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Veh. Commun., vol. 1, no. 2, pp. 53–66, Apr. 2014, doi: 10.1016/j.vehcom.2014.05.001.

[33] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," Veh. Commun., vol. 7, pp. 7–20, Jan. 2017, doi: 10.1016/j.vehcom.2017.01.002.

[34] S. N and K. S. Archana, "Performance Analysis of Machine Learning-based Detection of Sinkhole Network Layer Attack in MANET," Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 12, 2022, doi: 10.14569/IJACSA.2022.0131262.

[35] D. Parida, U. Bhanja, and M. Okade, "Sink-Hole Attack Detection in VANET using Machine Learning Techniques," in 2024 6th International Conference on Computational Intelligence and Networks (CINE), Dec. 2024, pp. 1–6. doi: 10.1109/CINE63708.2024.10880882.

[36] P. Sirola, A. Joshi, and K. C. Purohit, "An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs)," vol. 3, 2014.

[37] A. M. Alrehan and F. A. Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey," in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), May 2019, pp. 1–6. doi: 10.1109/CAIS.2019.8769454.

[38] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," IEEE Commun. Surv. Tutor., vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.

[39] A. Haddaji, S. Ayed, and L. C. Fourati, "Artificial Intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey," Comput. Electr. Eng., vol. 104, p. 108460, Dec. 2022, doi: 10.1016/j.compeleceng.2022.108460.

[40] I. Naqvi, A. Chaudhary, and A. Kumar, "A Systematic Review of the Intrusion Detection Techniques in VANETS," TEM J., pp. 900–907, May 2022, doi: 10.18421/TEM112-51.

[41] T. Sowmya and E. A. Mary Anita, "A comprehensive review of AI based intrusion detection system," Meas. Sens., vol. 28, p. 100827, Aug. 2023, doi: 10.1016/j.measen.2023.100827.

[42] S. T. Banafshehvaragh and A. M. Rahmani, "Intrusion, anomaly, and attack detection in smart vehicles," Microprocess. Microsyst., vol. 96, p. 104726, Feb. 2023, doi: 10.1016/j.micpro.2022.104726.

[43] T. Nandy, R. Md Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," J. King Saud Univ. - Comput. Inf. Sci., vol. 36, no. 2, p. 101945, Feb. 2024, doi: 10.1016/j.jksuci.2024.101945.

[44] A. Boualouache and T. Engel, "A Survey on Machine Learning-Based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks," IEEE Commun. Surv. Tutor., vol. 25, no. 2, pp. 1128–1172, 2023, doi: 10.1109/COMST.2023.3236448.

[45] D. Man, F. Zeng, J. Lv, S. Xuan, W. Yang, and M. Guizani, "AI-based Intrusion Detection for Intelligence Internet of Vehicles," IEEE Consum. Electron. Mag., vol. 12, no. 1, pp. 109–116, Jan. 2023, doi: 10.1109/MCE.2021.3137790.

[46] Y. Zhong, B. Yang, Y. Li, H. Yang, X. Li, and Y. Zhang, "Tackling Sybil Attacks in Intelligent connected vehicles: A Review of Machine Learning and Deep Learning Techniques," presented at the 2023 8th International Conference on Computational Intelligence and Applications (ICCIA), IEEE Computer Society, Jun. 2023, pp. 8–12. doi: 10.1109/ICCIA59741.2023.00010.

[47] R. Dineshkumar, P. Siddhanti, S. Kodati, A. H. Shnain, and V. Malathy, "Misbehavior Detection for Position Falsification Attacks in VANETs Using Ensemble Machine Learning," in 2024 Second International Conference on Data Science and Information System (ICDSIS), Hassan, India: IEEE, May 2024, pp. 1–5. doi: 10.1109/ICDSIS61070.2024.10594423.

[48] U. Garg, M. Kaur, M. Kaushik, and N. Gupta, "Detection of DDoS Attacks using Semi-Supervised based Machine Learning Approaches," in 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST), Dec. 2021, pp. 112–117. doi: 10.1109/ICCMST54943.2021.00033.

[49] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection," IEEE Trans. Netw. Serv. Manag., vol. 18, no. 2, pp. 1803–1816, Jun. 2021, doi: 10.1109/TNSM.2020.3014929.

[50] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset," IEEE Access, vol. 9, pp. 142206–142217, 2021, doi: 10.1109/ACCESS.2021.3120626.

[51] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo, and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network," IEEE Access, vol. 7, pp. 154560–154571, 2019, doi: 10.1109/ACCESS.2019.2948382.

[52] Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm,"

SURVEY ARTICLE

IEEE Access, vol. 7, pp. 64351–64365, 2019, doi: 10.1109/ACCESS.2019.2917532.
[53] S. Bayan, U. Mohammad, and A. A. Mohammad, "Position Falsification Attack Detection in Inter-Vehicle Networks Using Deep Learning," in 2024 IEEE International Conference on Electro Information Technology (eIT), May 2024, pp. 621–626. doi: 10.1109/eIT60633.2024.10609919.
[54] T. Alladi, V. Kohli, V. Chamola, and F. R. Yu, "Securing the Internet of Vehicles: A Deep Learning-Based Classification Framework," IEEE Netw. Lett., vol. 3, no. 2, pp. 94–97, Jun. 2021, doi: 10.1109/LNET.2021.3058292.
[55] Y. Zhang, P. Li, and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," IEEE Access, vol. 7, pp. 31711–31722, 2019, doi: 10.1109/ACCESS.2019.2903723.
[56] Y. Shi, K. Yang, T. Jiang, J. Zhang, and K. B. Letaief, "Communication-Efficient Edge AI: Algorithms and Systems," IEEE Commun. Surv. Tutor., vol. 22, no. 4, pp. 2167–2191, 2020, doi: 10.1109/COMST.2020.3007787.
[57] K. Bhardwaj, N. Suda, and R. Marculescu, "EdgeAI: A Vision for Deep Learning in IoT Era," Oct. 23, 2019, arXiv: arXiv:1910.10356. doi: 10.48550/arXiv.1910.10356.
[58] A. Moubayed, A. Shami, P. Heidari, A. Larabi, and R. Brunner, "Edge-Enabled V2X Service Placement for Intelligent Transportation Systems," IEEE Trans. Mob. Comput., vol. 20, no. 4, pp. 1380–1392, Apr. 2021, doi: 10.1109/TMC.2020.2965929.
[59] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection," IEEE Access, vol. 8, pp. 132911–132921, 2020, doi: 10.1109/ACCESS.2020.3009843.
[60] J. M. Johnson and T. M. Khoshgoftaar, "Survey on deep learning with class imbalance," J. Big Data, vol. 6, no. 1, p. 27, Dec. 2019, doi: 10.1186/s40537-019-0192-5.
[61] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," J. Artif. Intell. Res., vol. 16, pp. 321–357, Jun. 2002, doi: 10.1613/jair.953.
[62] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs)," Sensors, vol. 23, no. 5, p. 2594, Feb. 2023, doi: 10.3390/s23052594.
[63] L. Wei, J. Yang, H. Jin, J. Cui, J. Li, and D. He, "Sustainable Learning-Based Intrusion Detection System for VANETs," IEEE Trans. Intell. Transp. Syst., pp. 1–12, 2025, doi: 10.1109/TITS.2025.3562226.
[64] A. Sarıkaya, B. G. Kılıç, and M. Demirci, "RAIDS: Robust autoencoder-based intrusion detection system model against adversarial attacks," Comput. Secur., vol. 135, p. 103483, Dec. 2023, doi: 10.1016/j.cose.2023.103483.
[65] J. Bian et al., "Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey," IEEE Internet Things J., vol. 9, no. 11, pp. 8364–8386, Jun. 2022, doi: 10.1109/JIOT.2022.3161050.
[66] A. F. Cooper, K. Levy, and C. De Sa, "Accuracy-Efficiency Trade-Offs and Accountability in Distributed ML Systems," in Equity and Access in Algorithms, Mechanisms, and Optimization, -- NY USA: ACM, Oct. 2021, pp. 1–11. doi: 10.1145/3465416.3483289.
[67] L. Plaza, "Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona, March 18, 2018".
[68] B. Karthiga, D. Durairaj, N. Nawaz, T. K. Venkatasamy, G. Ramasamy, and A. Hariharasudan, "Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches," Wirel. Commun. Mob. Comput., vol. 2022, pp. 1–13, Oct. 2022, doi: 10.1155/2022/5069104.
[69] J. Shu, L. Zhou, W. Zhang, X. Du, and M. Guizani, "Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 4519–4530, Jul. 2021, doi: 10.1109/TITS.2020.3027390.
[70] C. Fan, J. Cui, H. Jin, H. Zhong, I. Bolodurina, and D. He, "Auto-Updating Intrusion Detection System for Vehicular Network: A Deep Learning Approach Based on Cloud-Edge-Vehicle Collaboration," IEEE Trans. Veh. Technol., vol. 73, no. 10, pp. 15372–15384, Oct. 2024, doi: 10.1109/TVT.2024.3399219.
[71] N. Nissar, N. Naja, and A. Jamali, "Securing VANETs: Multi-Objective Intrusion Detection with Variational Autoencoders," IEEE Trans. Consum. Electron., vol. 70, no. 1, pp. 3867–3874, Feb. 2024, doi: 10.1109/TCE.2024.3372691.
[72] R. P. Ltd, "Buy a Raspberry Pi 4 Model B," Raspberry Pi. <Accessed: Jun. 09, 2025>. [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/.
[73] Jetson Nano, "NVIDIA Developer", <Accessed: Jun. 09, 2025>. [Online]. Available: https://developer.nvidia.com/embedded/jetson-nano.
[74] "The World's Top Performing Edge AI Processor for Edge Devices," Hailo. <Accessed: Jun. 09, 2025>. [Online]. Available: https://hailo.ai/
[75] A. Mchergui, T. Moulahi, and S. Zeadally, "Survey on Artificial Intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs)," Veh. Commun., vol. 34, p. 100403, Apr. 2022, doi: 10.1016/j.vehcom.2021.100403.
[76] T. Liang, J. Glossner, L. Wang, S. Shi, and X. Zhang, "Pruning and Quantization for Deep Neural Network Acceleration: A Survey," Jun. 15, 2021, arXiv: arXiv:2101.09671. doi: 10.48550/arXiv.2101.09671.
[77] G. Hinton, O. Vinyals, and J. Dean, "Distilling the Knowledge in a Neural Network," Mar. 09, 2015, arXiv: arXiv:1503.02531. doi: 10.48550/arXiv.1503.02531.
[78] "SUMO Documentation." <Accessed: Jun. 09, 2025>. [Online]. Available: https://sumo.dlr.de/docs/index.html.
[79] nsnam, "ns-3," ns-3. <Accessed: Jun. 09, 2025>. [Online]. Available: https://www.nsnam.org/.
[80] I. J. Goodfellow et al., "Generative Adversarial Networks," Jun. 10, 2014, arXiv: arXiv:1406.2661. doi: 10.48550/arXiv.1406.2661.
[81] T. Rosenstatter and K. Melnyk, "Towards Synthetic Data Generation of VANET Attacks for Efficient Testing," in 2023 IEEE Intelligent Vehicles Symposium (IV), Jun. 2023, pp. 1–7. doi: 10.1109/IV55152.2023.10186685.
[82] S. Nazat, L. Li, and M. Abdallah, "XAI-ADS: An Explainable Artificial Intelligence Framework for Enhancing Anomaly Detection in Autonomous Driving Systems," IEEE Access, vol. 12, pp. 48583–48607, 2024, doi: 10.1109/ACCESS.2024.3383431.

Authors

Prachi Kapoor is the Ph.D. scholar in Computer Science at the University of Petroleum and Energy Studies (UPES), Dehradun. She holds a B.E. (Hons.) in Computer Science and Engineering from the University of Rajasthan and M.Tech in Computer Science from Mody Institute of Engineering and Technology, Rajasthan. With over 7 years of teaching experience, her areas of expertise include Deep Learning, Machine Learning, Edge AI, Cybersecurity and Computer Networks. Her current research focuses on the development of efficient AI-based IDS for VANETs.

Dr. Ajay Prasad bears diversified personal attributes in Academics over the past 25 years and has been contributing significantly as a multi-faceted personality with his vivid active roles as a Researcher, an Academician demonstrating his abilities to deliver for the Undergraduates, Postgraduates, and Doctorate students, in a much organized and focused manner by sincerely following the practices of Outcome-Based Modern Teaching Methodologies. He specializes in Computer Architecture, Simulation and Modelling, Network/Data Security Principles, System Programming, Cloud Systems, Compilers, Digital Forensics. In his academic

SURVEY ARTICLE

career he has been in various leadership roles, including HoD for more than 10 years at various places. He has contributed to several different MOOC courses at the state/national level. He is a panellist in Cyber Cell Uttarakhand India. He is a regular contributor to the society through conduct of Cyber-Awareness Seminars and Key-note Speaker for government agencies like STF (Cyber Police), DITAC for the Uttarakhand Govt, and as a Member, Uttarakhand Police Digital Volunteers.

How to cite this article:

Prachi Kapoor, Ajay Prasad, "Machine and Deep Learning for VANET Security: A Survey of Intrusion Detection Models and Deployment Realities", International Journal of Computer Networks and Applications (IJCNA), 12(5), PP: 720-736, 2025, DOI: 10.22247/ijcna/2025/43.